Cisco SD-WAN モニタリングおよびメンテナンス コンフィギュレーション ガイド

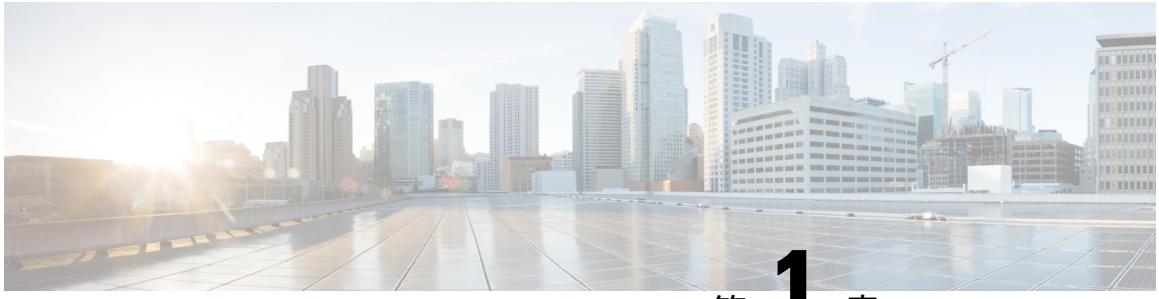
初版：2019 年 7 月 19 日

最終更新：2022 年 8 月 26 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

最初にお読みください

参考資料

- 『Release Notes』[英語]
- 『Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations』[英語]

ユーザマニュアル

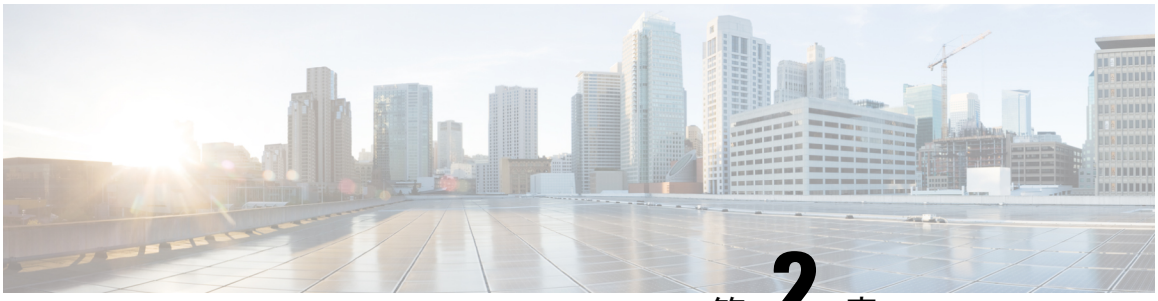
- Cisco IOS XE (Cisco IOS XE SD-WAN Devices)[英語]
- Cisco SD-WAN (Cisco vEdge Devices)[英語]
- Cisco IOS XE (SD-WAN) Qualified Command Reference[英語]
- Cisco IOS XE（SD-WAN）リリース 17 のユーザーマニュアル
- Cisco vEdge デバイスのユーザーマニュアル

通信、サービス、およびその他の情報

- Cisco Profile Manager で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、シスコサービスにアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリ、製品、ソリューション、サービスをお求めの場合は、CiscoDevnet にアクセスしてください。
- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、Cisco Bug Search Toolにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 2 章

Cisco IOS XE（SD-WAN）および Cisco SD-WAN リリースにおける新機能

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

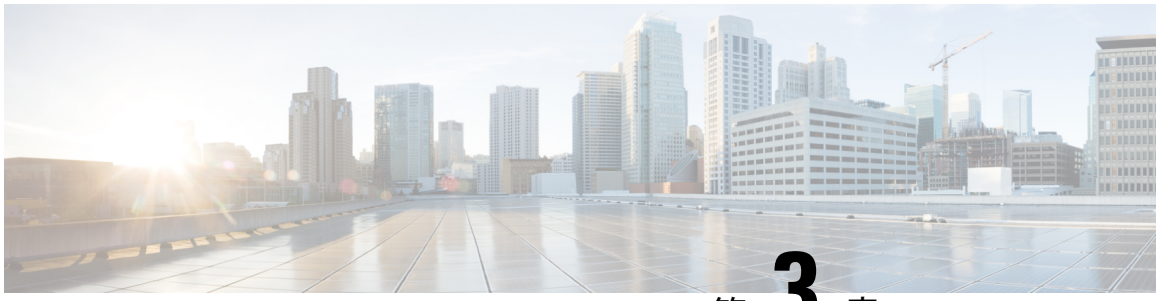
シスコでは、リリースごとに SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次のリンクには、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されているリリースごとの新機能と変更された機能が含まれています。Cisco SD-WAN ソリューションに関係する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

『What's New in Cisco IOS XE (SD-WAN) Release 17.x』[英語]

『What's New in Cisco IOS XE SD-WAN Release 16.x』[英語]

『What's New in Cisco SD-WAN (vEdge) Release 20.x』[英語]

『What's New in Cisco SD-WAN (vEdge) Release 19.x』[英語]



第 3 章

Cisco vManage モニターの概要

表 *1* : 機能の履歴

機能名	リリース情報	説明
統合型のモニタリングビュー向けに強化された Cisco vManage のユーザーインターフェイス	Cisco vManage リリース 20.7.1	Cisco vManage の強化されたユーザーインターフェイスがこの機能に導入されました。[Monitor] ウィンドウは、Cisco SD-WAN オーバーレイネットワークのすべてのモニタリングコンポーネントとサービスの統合ビューに対応した単一ページのリアルタイムのユーザーインターフェイスを提供します。[Main Dashboard]、[VPN Dashboard]、[Security]、[Multicloud] を含む Cisco vManage ダッシュボードすべてのエントリポイントになります。これらのダッシュボードは、以前は [Dashboard] メニューからアクセスできました。さらに、すべてのモニタリングコンポーネントがユーザーインターフェイス内でボタンとして表示されるため、別のページにすばやく移動できます。 このリリースでは、Cisco vManage の [Tools] メニューも拡充されています。以前は [Monitor] メニューからアクセスできた [Network Wide Path Insight] と [On Demand Troubleshooting] オプションが [Tools] メニューに移動し、これらの機能を簡単に見つけられるようになりました。
Cisco vManage のカスタマイズ可能な [Monitor Overview] ダッシュボード	Cisco vManage リリース 20.9.1	この機能により、[Monitor Overview] ダッシュボードがカスタマイズ可能になりました。好みに合わせて、表示するダッシュボードを自由に指定したり、並べ替えたりできます。

Cisco vManage の**[Monitor]** > **[Overview]**ダッシュボードには、次のダッシュレットがあります。Cisco vManage リリース 20.6.x 以前では、これらのダッシュレットは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。

- WAN Edge Health
- Site BFD Connectivity
- Transport Interface Distribution
- WAN Edge Inventory
- Transport Health
- **Top Applications**
- **Application-Aware Routing**

[Monitor Overview] ダッシュボードのカスタマイズについて

最小リリース：Cisco vManage リリース 20.9.1

デフォルトでは、[Monitor Overview] ダッシュボードには、Cisco SD-WAN オーバーレイネットワークのさまざまなコンポーネントとサービスをモニタリングする際に役立つすべてのダッシュレットが表示されます。カスタマイズ可能なダッシュボード機能を使用すると、次のことができます。

- ダッシュレットの追加

- ダッシュレットの削除
- ダッシュレットの再配置
- デフォルト設定の復元

カスタマイズされたダッシュボード設定はデータベースに保存されます。Cisco vManage にログインするとき、または別のウィンドウから [Monitor Overview] ダッシュボードに移動するときに、これらの設定が取得されます。

この機能は、シングルテナント展開とマルチテナント展開の両方で使用できます。ただし、マルチテナント展開の場合、この機能はテナントダッシュボードでのみ使用できます。

（注） 標準およびカスタムユーザーグループに属するすべてのユーザーは、読み取り権限や書き込み権限に関係なく、[Monitor Overview] ダッシュボードをカスタマイズできます。

[Monitor Overview] ダッシュボードのカスタマイズのメリット

- 柔軟性：ダッシュボードをカスタマイズすることで、最も重要なダッシュレットを表示できます。目的に合わないダッシュレットを削除して煩雑さを軽減できます。
- 効率性：すべての主要メトリックを一目で確認し、迅速に評価および分析できます。
- 簡単な編成：ダッシュレットをドラッグアンドドロップして、要件に応じてダッシュボードを編成できます。たとえば、特に重要なダッシュレットを上部に簡単にドラッグできます。

[Monitor Overview] ダッシュボードのカスタマイズに関する制限事項

最小リリース：Cisco vManage リリース 20.9.1

- マルチテナント展開の場合、この機能はテナントダッシュボードでのみ使用できます。
- この機能は、[Monitor Overview] ダッシュボードでのみ使用できます。
- [Monitor Overview] ダッシュボードの上部にあるメニューバーはカスタマイズできません。
- ダッシュボードが編集モードの場合、データを表示する期間の選択、リアルタイムデータの表示などの他のアクションは無効になります。

[Monitor Overview] ダッシュボードのカスタマイズ

最小リリース：Cisco vManage リリース 20.9.1

ダッシュレットの追加

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Edit Dashboard] を選択します。
3. [Add Dashlet] をクリックします。

（注） [Add Dashlet] オプションは、追加できるダッシュレットがある場合にのみ使用できます。デフォルトのダッシュボードでは使用できません。

4. 追加するダッシュレットを選択します。
5. [Add] をクリックします。
6. [Save] をクリックします。

ダッシュレットの削除

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Edit Dashboard] を選択します。
3. 対応するダッシュレット名の横にある [Delete] アイコンをクリックします。
4. ダッシュレットの削除を確定するには、[Yes] をクリックします。
5. [Save] をクリックします。

ダッシュレットの再配置

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Edit Dashboard] を選択します。
3. 要件に応じてダッシュレットをドラッグアンドドロップします。
4. [Save] をクリックします。

デフォルト設定の復元

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Reset to Default View] を選択します。
3. [Apply] をクリックします。

コントローラとデバイス情報の表示

[Monitor] > **[Overview]**ページの上部にあるメニューバーの [Controllers] および [WAN Edges] 領域には、オーバーレイ ネットワーク内の Cisco vSmart コントローラ、Cisco vBond オーケストレーション、Cisco vManage インスタンスの総数が表示されます。また、ネットワーク内のデバイスのステータスも表示されます。

デバイス番号をクリックすると、**[Monitor]** > **[Devices]**ページに各デバイスの詳細情報が表示されます。対応するデバイスの隣にある [...] をクリックして、デバイスダッシュボードまたはリアルタイムビューにアクセスするか、**[Tools]** > **[SSH Terminal]**にアクセスします。

Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Controllers] 領域と [WAN Edges] 領域は、[Summary] 領域にまとめられています（[Summary] 領域は**[Dashboard]** > **[Main Dashboard]** ページ内にあります）。
- デバイス番号をクリックすると、各デバイスの詳細情報が表示されたポップアップウィンドウが開きます。
- デバイスダッシュボードやリアルタイムビューは、**[Monitor]** > **[Network]**ページ内にあります。

Cisco vManage ステータスの表示

デバイスやコントローラの状態、およびCPUとメモリの使用状況に関する詳細をCisco vManageで表示できます。

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

   表の [Health] 列には、デバイスやコントローラの正常性が表示されます。列のアイコンにカーソルを合わせると、[Good]、[Fair]、[Poor] のいずれの状態であるかが表示されます。

   Cisco vManage コントローラの場合、正常性ステータスは次の状態を示します。

   - [Good]：使用可能なメモリの 75% 未満、および CPU リソースの 75% 未満が Cisco vManage で使用されています。
   - [Fair]：合計メモリまたは CPU の 75% ～ 90% が Cisco vManage で使用されています。
   - [Poor]：合計メモリまたは CPU の 90% 超が Cisco vManage で使用されています。

2. 表から Cisco vManage コントローラをクリックします。
3. [ECURITY MONITORING] で [System Status] をクリックします。

   [Device 360] ページには、CPU とメモリの使用率が表示されます。

（注） Cisco vManage コントローラで合計メモリまたは CPU の 90% 超が使用されている場合、パフォーマンスが低下する可能性があります。Cisco vManage にログインできない場合は、Cisco TAC までご連絡ください。

[Certificate Status] ペインの表示

[Certificate Status] ペインには、すべてのコントローラデバイス上にあるすべての証明書の状態が表示されます。また、期限切れや無効になった証明書の総数が表示されます。[Certificate Status] ペインをクリックして**[Monitor]** > **[Devices]** > **[Certificate]** ページを開きます。このページには、証明書がインストールされているデバイスのホスト名とシステム IP、証明書のシリアル番号、および有効期限の日付とステータスが表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Certificate Status] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Certificate Status] ペインをクリックすると、**[Monitor]** > **[Devices]** > **[Certificate]** ページの代わりにポップアップウィンドウが開きます。

[Licensing] ペインの表示

[Licensing] ペインには、設定されたデバイスの総数とライセンス付与されたデバイスの数が表示されます。[Licensing] ペインをクリックして**[Monitor]** > **[Devices]** > **[Licensing]**ページを開きます。このページには、デバイスに関する次の情報が表示されます。

- ホスト名
- シャーシ番号とデバイスモデル
- IP アドレス
- テンプレート名
- デバイスのスマートアカウントとバーチャルアカウント
- マスターソフトウェアライセンス契約（MSLA）

- デバイスのライセンスステータス
- ライセンスタイプとライセンス名
- サブスクリプション ID

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Licensing] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Licensing] ペインをクリックすると、**[Monitor]** > **[Devices]** > **[Licensing]**ページの代わりにポップアップウィンドウが開きます。ポップアップウィンドウには、デバイス名、ライセンスが付与されたデバイス数、ライセンスの総数、および最後に割り当てられたステータスが表示されます。

[Reboot] ペインの表示

[Reboot] ペインには、ネットワーク内にあるすべてのデバイスについて、過去 24 時間の再起動の合計数が表示されます。これには、ソフト再起動とコールド再起動、およびデバイスの電源再投入の結果として発生した再起動が含まれます。[Reboot] をクリックすると、[Reboot] サイドバーが表示され、再起動のたびに再起動したデバイスのシステム IP とホスト名、再起動が発生した時刻、および再起動の理由が一覧で表示されます。同じデバイスが 2 回以上再起動すると、各再起動オプションが個別に報告されます。

[Reboot] サイドバーで [Crashes] をクリックすると、すべてのデバイスクラッシュについて、クラッシュが発生したデバイスのシステム IP とホスト名、クラッシュインデックス、コア時刻とファイル名が一覧で表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Reboot] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Reboot] をクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。

[Control Status] ペインの表示

[Control Status] ペインは、Cisco vManage リリース 20.7.x 以前にのみ実装されています。

[Control Status] ペインには、Cisco vSmart および WAN エッジデバイスが必要な数の Cisco vSmart コントローラ に接続されているかどうかが表示されます。それぞれの Cisco vSmart コントローラ が、ネットワーク内の他のすべての Cisco vSmart コントローラ に接続されている必要があ

ります。各 WAN エッジルータは、設定された最大数の Cisco vSmart コントローラ に接続する必要があります。

[Control Status] ペインには、次の 3 つのカウントが表示されます。

- [Up]：必要な数の動作可能なコントロールプレーンが Cisco vSmart コントローラ に接続されているデバイスの総数。
- [Partial]：動作可能なコントロールプレーンの一部（すべてではない）が Cisco vSmart コントローラ に接続されているデバイスの総数。
- [Down]：Cisco vSmart コントローラ にコントロールプレーンが接続されていないデバイスの総数。

（注） [Control Status] ペインは、Cisco vManage コントロール接続と vSmart コントロール接続の両方の状態に依存します。

[UP]/[Down]/[Partial] データをクリックすると、**[Monitor]** > **[Devices]**ページが表示されます。目的のデバイスで [...] をクリックして、デバイスダッシュボードまたはリアルタイムビューにアクセスするか、**[Tools]** > **[SSH Terminal]**にアクセスします。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Control Status] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Up]、[Partial]、[Down] の各ステータスには、それぞれ [Control Up]、[Partial]、[Control Down] というタイトルが付けられています。
- ドーナツグラフの代わりにステータスバーにデータが表示されます。
- データをクリックすると、**[Monitor]** > **[Devices]**ページの代わりにポップアップウィンドウが開きます。

[BFD Connectivity] ペインの表示

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。

[Site BFD Connectivity] ペインには、サイトのデータ接続の状態が表示されます。サイトに複数の WAN エッジルータがある場合、このペインには、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] ペインには、次の 3 つの状態が表示されます。

- [Full]：すべての WAN Edge ルータのすべての BFD セッションが稼働状態にあるサイトの総数。

- [Partial]：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。
- [Unavailable]：すべての WAN エッジルータのすべての 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。

（注） サイト数には、稼働中のデバイスが設置されているサイトのみが含まれます。サイトに設置されているデバイスのいずれかがダウンしている場合、または TLOC やトンネルがダウンしている場合（2 つのデバイスがあるサイト）、一部のサイトはサイト数から除外されます。

[Full]、[Partial]、または [Unavailable] ステータスをクリックすると、サイドバーが表示され、各サイト、ノード、トンネルの詳細情報が表示されます。**[Monitor]** > **[Devices]**ページで目的のデバイスの [...] をクリックして、デバイスダッシュボードまたはリアルタイムビューにアクセスするか、**[Tools]** > **[SSH Terminal]**にアクセスします。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Site BFD Connectivity] ペインのタイトルは [Site Health] になります。[Site Health] ペインは **[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Full]、[Partial]、[Unavailable] のステータスのタイトルは、それぞれ [Full WAN Connectivity]、[Partial WAN Connectivity]、[No WAN Connectivity] になります。
- データをクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。
- デバイスダッシュボードやリアルタイムビューは、**[Monitor]** > **[Network]**ページ内にあります。

[Transport Interface Distribution] ペインの表示

[Transport Interface Distribution] ペインには、VPN 0 のすべての WAN エッジインターフェイスにおける過去 24 時間のインターフェイスの使用状況が表示されます。これには、すべての TLOC インターフェイスが含まれます。使用統計情報をクリックすると、サイドバーが現れ、システム IP、インターフェイス、およびインターフェイス使用状況の平均的な詳細が表示されます。

[View Percent Utilization] をクリックすると、すべての WAN エッジインターフェイスの過去 24 時間の使用状況がグラフィック形式で表示されます。このグラフでは、インターフェイス数に対する TLOC 使用率の分散 （%） について示されています。表形式の統計には、ホスト名、インターフェイス、平均/低/高アップストリーム（%）、平均/低/高ダウンストリーム（%）、および帯域幅使用率の情報が表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Transport Interface Distribution] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- 使用統計情報をクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。

[WAN Edge Inventory] ペインの表示

[WAN Edge Inventory] ペインには、次の 4 つのカウントが表示されます。

- [Total]：認可されたシリアル番号が vManage サーバーにアップロードされている WAN エッジルータの総数。シリアル番号は**[Configuration]** > **[Devices]**ページでアップロードします。
- [Authorized]：オーバーレイネットワーク内で認可されている WAN エッジルータの総数。**[Configuration]** > **[Certificates]** > **[WAN Edge List]**ページで [Valid] と表示されているルータを指します。
- [Deployed]：導入されている WAN エッジルータの総数。ネットワークで現在稼働中で、[Valid] と表示されているルータを指します。
- [Staging]：ステージング状態の WAN エッジルータの総数。実際のブランチに出荷してオーバーレイネットワークの構成要素にする前に、ステージングサイトで構成するルータです。これらのルータは、ルーティングの決定には関与せず、 Cisco vManage によるネットワークモニタリングに影響を与えることもありません。

統計情報のいずれかをクリックするとサイドバーが現れ、ホスト名、システム IP、サイト ID などの各ルータの詳細が記載されたテーブルが表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [WAN Edge Inventory] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- データをクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。

[WAN Edge Health] ペインの表示

[WAN Edge Health] ペインには、各ルータの状態に関する集約されたビューと、その状態にある WAN エッジルータの数が表示され、ハードウェアノードの正常性が示されます。次の 3 つの状態があります。

- [Good]：メモリ、ハードウェア、CPUが良好な状態にあるルータの数。合計メモリまたは合計 CPU の使用率が 75% 未満の場合は、良好な状態に分類されます。
- [Fair]：メモリ、ハードウェア、CPU が普通の状態にあるルータの数。合計メモリまたは合計 CPU の使用率が 75% ～ 90% の場合は、普通の状態に分類されます。
- [Fair]：メモリ、ハードウェア、CPU が不良な状態にあるルータの数。合計メモリまたは合計 CPU の使用率が 90% を超える場合は、不良な状態に分類されます。

統計をクリックすると、サイドバーが表示され、過去 1 時間のメモリ使用量や CPU 使用率に加えて、温度、電源、PIMモジュールなどのハードウェア関連のアラームが記載されたテーブルが表示されます。**[Monitor]** > **[Devices]**ページで目的のホスト名の [...] をクリックして、デバイスダッシュボードまたはデバイス詳細ビューにアクセスするか、**[Tools]** > **[SSH Terminal]** ページにアクセスします。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [WAN Edge Health] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Good]、[Fair]、および [Poor] ステータスには、それぞれ、[Normal]、[Warning]、および [Error] というタイトルが付けられています。
- ハードウェアノードは、合計メモリまたは合計 CPU の 75% ではなく 70% を使用している場合、正常状態に分類されます。同様に、合計メモリまたは合計 CPU の 70% ～ 90% の範囲ではなく、75% ～ 90% を使用している場合、警告状態に分類されます。
- データをクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。
- デバイスダッシュボードやデバイス詳細ビューは、**[Monitor]** > **[Network]**ページ内にあります。

[Transport Health] ペインの表示

[Transport Health] ペインには、すべてのリンクとすべてのカラーの組み合わせ（すべての LTE-to-LTE リンク、すべての LTE-to-3G リンクなど）の集約された平均損失、遅延、およびジッターが表示されます。

- [Type] ドロップダウンリストから、損失、遅延、またはジッターを選択します。

- [Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。
- [View Details] をクリックすると、サイドバーに表形式で情報が表示されます。前述したように、表示するデータの種類と期間を変更できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Transport Health] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Transport Health] ポップアップウィンドウを開きます。

[Top Applications] ペインの表示

Cisco vManage の**[Monitor]** > **[Overview]**ページの [Top Applications] ペインには、オーバーレイネットワーク内の WAN エッジルータを通過するトラフィックの SD-WAN アプリケーションインテリジェンス エンジン（SAIE）フロー情報が表示されます。

（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。

VPN 別に上位のアプリケーションを一覧表示するには、ドロップダウンリストから VPN を選択します。データを表示する期間を選択するには、[Time] ドロップダウンリストをクリックします。

サイドバーに上位のアプリケーションを一覧表示するには、次の手順を実行します。

1. [View Details] をクリックして、[Top Applications] サイドバーを開くと、同じ情報がより詳細なビューで表示されます。
2. **SAIE アプリケーション**で [VPN] ドロップダウンリストから目的の VPN を選択し、[Search] をクリックします。

（注） 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。

- [Chart] をクリックすると、アプリケーションの一覧が表示されます。
- [Details] をクリックすると、アプリケーションに関する詳細情報が表示されます。

3. [SSL Proxy] をクリックし、[View by Policy Actions] ドロップダウンリストからポリシーアクションを選択します。すべてのポリシーアクション（暗号化、非暗号化、復号）のビューがサポートされています。[VPN] ドロップダウンリストから目的の VPN を選択し、[Search] をクリックします。[Hour] オプションには、選択した時間の統計情報が表示されます。
   - [Chart] をクリックすると、SSL アプリケーションの一覧が表示されます。
   - [Details] をクリックすると、SSL アプリケーションに関する詳細情報が表示されます。
4. [X] をクリックしてウィンドウを閉じて、**[Monitor]** > **[Overview]**ページに戻ります。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Top Applications] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、VPN オプションの一覧を表示し、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Top Applications] ポップアップウィンドウを開きます。

（注） フロー DPI データは、スケジュールに従って Cisco vManage によって収集されますが、ユーザーの要求に応じて処理されます。Flow DPI ベースのレポートは、データが処理された後に利用できます。

[Application-Aware Routing] ペインの表示

[Application-Aware Routing] ペインには、[Type] ドロップダウンリストで指定した基準（損失、遅延、ジッターなど）に基づいて、状態の最も悪い 10 のトンネルが表示されます。したがって、損失を選択した場合、このペインには、過去 24 時間の平均損失が最も大きい 10 のトンネルが表示されます。

任意の行をクリックすると、データがグラフィック形式で表示されます。データを表示する期間を選択するか、[Custom] をクリックして、カスタム期間を指定するためのドロップダウンを表示します。

[View Details] をクリックして、[Application-Aware Routing] サイドバーを開きます。[Type] ドロップダウンリストで指定した基準（損失、遅延、ジッターなど）に基づいて、状態の最も悪い 25 のトンネルが表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Application-Aware Routing] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Application-Aware Routing] ポップアップウィンドウを開きます。

Web サーバーの証明書期限日通知の表示

認証証明書を使用して Web ブラウザと Cisco vManage サーバーの間のセキュアな接続を確立する際、**[Administration]** > **[Settings]**画面で証明書の有効期間を設定します。この期間が終了すると、証明書が期限切れになります。[Web Server Certificate] バーに、有効期限の日時が表示されます。

証明書の有効期限が切れる 60 日前から、Cisco vManage の**[Monitor]** > **[Overview]**ページには証明書の有効期限が近づいていることを示す通知が表示されます。この通知は、有効期限の 30 日前、15 日前、および 7 日前に再表示され、その後は毎日表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、証明書の有効期限の通知は**[Dashboard]** > **[Main Dashboard]**ページに表示されます。

メンテナンス時間帯のアラート通知の表示

Cisco vManage サーバーで**[Administration]** > **[Settings]**に次のメンテナンス時間帯が設定されている場合、Cisco vManage の**[Monitor]** > **[Overview]** ページには、メンテナンス時間帯が開始する 2 日前にアラート通知が表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、メンテナンス時間帯のアラート通知は **[Dashboard]** > **[Main Dashboard]**ページに表示されます。

セキュリティ

Cisco vManage では、**[Monitor]** > **[Security]**ページに次のペインがあります。

（注） Cisco vManage リリース 20.6.x 以前では、これらのペインは**[Dashboard]** > **[Security]**ページ内にあります。

- Firewall Enforcement
- Top Signature Hits
- URL Filtering
- Advanced Malware Protection

[Firewall Enforcement] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。[Firewall Enforcement] ペインには、指定された期間に検査またはドロップされたセッションの数が表示されます。

アプリケーション認識機能を備えたシスコのエンタープライズファイアウォールは、柔軟で理解しやすいゾーンベースのモデルを使用してデータトラフィックを検査します。ゾーンベースのファイアウォールにより、TCP、UDP、および ICMP データトラフィックの検査が可能になります。ゾーンには、1 つ以上の VPN グループを含めることができます。VPN をゾーンにグループ化すると、ユーザーはオーバーレイネットワークにセキュリティ境界を確立できるため、ゾーン間を通過するすべてのデータトラフィックを制御できます。

ファイアウォールポリシーにより、送信元ゾーンから宛先ゾーンへのデータトラフィックフローを許可するために必要な一致条件が定義されます。ファイアウォールポリシーでは、IP プレフィックス、IP ポート、プロトコル TCP、UDP、ICMP、およびアプリケーションを一致条件にできます。プレフィックス、ポート、およびプロトコルが一致するフローを許可またはドロップし、パケットヘッダーをログに記録できます。

[Inspected] をクリックすると、検査されたデータセッション数が表示されます。

[Dropped] をクリックすると、ドロップされたパケット数が表示されます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックすると、[Firewall Enforcement] サイドバーが開き、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の詳細情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [FireWall Enforcement] ペインは、**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。

- [View Details] ボタンの代わりに展開アイコンを使用して、[FireWall Enforcement] ポップアップウィンドウを開きます。

[Top Signature Hits] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。[Top Signature Hits] ペインには、指定された期間のシビラリティ（重大度）別またはカウント別に、侵入防御システム（IPS）のシグネチャ違反が表示されます。IPS では、Cisco Talos のシグネチャを使用してネットワークトラフィックがモニタリングされます。

[By Severity] をクリックして、シビラリティ（重大度）別にシグネチャ違反をフィルタリングできます。

[By Count] をクリックして、カウント別にシグネチャ違反をフィルタリングできます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックして、[Top Signature Hits] サイドバーを開くと、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Top Signature Hits] ペインは、**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Top Signature Hits] ポップアップウィンドウを開きます。

[URL Filtering] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。[URL Filtering] ウィンドウには、指定した期間にブロックまたは許可された URL の数と種類が表示されます。

[Blocked] をクリックすると、ブロックされた Web サイトのリストが表示されます。

[Allowed] をクリックすると、許可された Web サイトのリストが表示されます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックすると、[URL Filtering] サイドバーが開き、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [URL Filtering] ペインは、**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[URL Filtering] ポップアップウィンドウを開きます。

[Advanced Malware Protection] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。Cisco Advanced Malware Protection（AMP）は、ファイルレピュテーションに基づいてマルウェアをブロックし、不明なファイルを Cisco AMP Threat Grid にアップロードして詳細な分析を行います。このペインには、指定した期間のファイルレピュテーションおよびファイル分析イベントの数が表示されます。

[File Reputation] をクリックすると、選択した時間内に AMP によって検出された悪意のあるファイルの数が表示されます。

[File Analysis] をクリックすると、選択した時間間隔で Cisco AMP Threat Grid にアップロードされた不明ファイルの数が表示されます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックすると、[Advanced Malware Protection] サイドバーが開き、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Advanced Malware Protection] ペインは**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Advanced Malware Protection] ポップアップウィンドウを開きます。

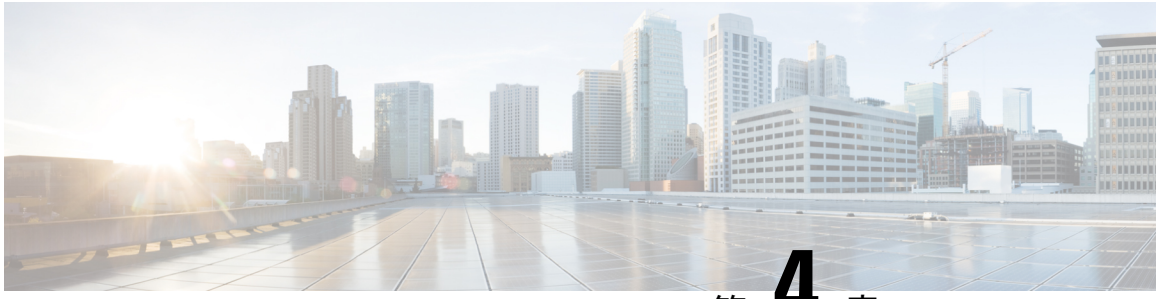
マルチクラウド

Cisco vManage では、**[Monitor]** > **[Multicloud]**ページに次のペインがあります。

（注） Cisco vManage リリース 20.6.x 以前では、これらのペインは**[Dashboard]** > **[Multicloud]**ページ内にあります。

- Amazon Web Service
- Google Cloud Platform
- Microsoft Azure
- Megaport

これらのペインの詳細については、『Cisco SD-WAN Cloud OnRamp Configuration Guide』[英語]を参照してください。



第 4 章

デバイスとコントローラ

このセクションでは、Cisco SD-WAN デバイスとコントローラに関する情報を記載します。

• Cisco SD-WAN コントローラと Cisco vEdge デバイスのリソースのモニタリング （50 ページ）

デバイスの地理的な位置の表示

Cisco vManage の [Geography] ウィンドウでは、オーバーレイネットワーク内の Cisco SD-WAN デバイスとリンクに関する情報を表示できます。[Geography] ウィンドウには、オーバーレイネットワーク内のデバイスの地理的位置を示すマップが表示されます。

（注） Cisco vManage を実行しているブラウザは、インターネットにアクセスできる必要があります。インターネットにアクセスできない場合は、ブラウザが「*.openstreetmaps.org」にアクセスできることを確認してください。

オーバーレイネットワーク内のデバイスの地理的位置を表示するには、次の手順を実行します。

1. [VPN Group] リストから、VPN グループを選択します。
2. [VPN Segment] リストから、VPN セグメントを選択します。
3. フィルタを設定します。

マップフィルタの設定

マップに表示するデバイスとリンクを選択するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Geography]**の順に選択します。
2. [Filter] をクリックします。
3. 表示されるオプションから、デバイスグループを選択します。デフォルトでは、[All] のグループが選択されており、オーバーレイネットワーク内のすべてのデバイスが表示されます。[No Groups] のグループを選択すると、デバイスグループに属していないデバイスが表示されます。すべてのデバイスがグループに属している場合、[No Groups] オプションは表示されません。
4. 表示するデバイスを選択します。デフォルトでは、マップにはエッジデバイス、Cisco vBond、Cisco vSmart、Cisco vManage を含むすべてのデバイスタイプが表示されます。
5. 制御リンクとデータリンクの状態を選択します。デフォルトでは、マップにはすべての制御接続とデータ接続が表示されます。
6. カーソルをボックスの外に移動して、[Filter] ボックスを閉じます。

マップは動的に更新され、選択内容が表示されます。

デバイス情報の表示

デバイスの基本情報を表示するには、デバイスアイコンにカーソルを合わせます。ポップアップボックスに、システム IP、ホスト名、サイト ID、デバイスタイプ、およびデバイスステータスが表示されます。

デバイスの詳細情報を表示するには、デバイスアイコンをダブルクリックします。[Device Dashboard]、[Device Details]、[SSH Terminal]、[Site Topology]、[Links] のいずれかをクリックして、デバイスの詳細を表示します。

リンクについての説明は以下のとおりです。

- 細い青色の線は、2 つのデバイス間のアクティブな制御接続を示します。
- 太い青色の線は、デバイス間の複数のアクティブな接続を示します。
- 赤色の点線は、停止している制御接続を示します。
- 太い赤色の点線は、停止している複数の制御接続を示します。
- 細い緑色の線は、2 つのデバイス間のアクティブなデータ接続を示します。
- 太い緑色の線は、複数のアクティブなデータ接続を示します。
- 赤色の点線は、停止しているデータ接続を示します。
- 太い赤色の点線は、停止している複数のデータ接続を示します。
- 太い灰色の線は、2 つのデバイス間のアクティブな統合型の制御接続とデータ接続を示しています。

  線にカーソルを合わせると、接続が稼働中か停止中かを示すホバーボックスが表示されます。

デバイスの地理座標の設定と表示

デバイスの地理座標を設定するには、**[Configuration]** > **[Templates]**にある [System Feature] テンプレートを使用します。

Cisco SD-WAN デバイスが設定テンプレートに関連付けられていない場合は、次の手順でデバイスで緯度と経度を直接設定できます。

1. Cisco vManage のメニューから、**[Tools]** > **[SSH Terminal]**を選択します。
2. 左ペインでデバイスを選択します。右ペインに [SSH Terminal] ウィンドウが開きます。
3. ユーザー名とパスワードを入力して、デバイスにログインします。
4. デバイスが設定テンプレートと関連付けられているかどうかを確認するには、`show system status` コマンドを使用します。

```
Device# show system status...
    Personality:           vedge
    Model name:            vedge-cloud
    Services:              None
    vManaged:              false
```

```
Commit pending:         false
Configuration template: None
```

出力結果で、[vManaged] および [Configuration template] 出力フィールドの値を確認します。[vManaged] フィールドの値が false の場合、デバイスは設定テンプレートと関連付けられておらず、[Configuration template] フィールドの値は `None` になります。このようなデバイスの場合、CLI から直接 GPS 座標を設定できます。[vManaged] フィールドの値が `true` の場合、Cisco vManage サーバーはデバイス設定をダウンロードしており、[Configuration template] フィールドには設定テンプレートの名前が表示されます。このようなデバイスの場合、CLI から直接 GPS 座標を設定することはできません。GPS 座標を設定しようとすると、`validate` または `commit` コマンドでエラーが発生し、次のメッセージが表示されます。

```
Aborted: 'system is-vmanaged': This device is being managed by the vManage.
Configuration through the CLI is not allowed.
```

5. コンフィギュレーション モードに入ります。

   Cisco vEdge デバイスの場合：

   ```
   デバイス# config
       デバイス(config)#
   ```

   Cisco IOS XE SD-WAN デバイスの場合：

   ```
   Device# configure-transaction
       デバイス(config)#
   ```

6. デバイスの緯度と経度を設定します。

   ```
   デバイス(config)# system gps-location latitude
                               degrees.minutes.seconds
       デバイス(config-system)# gps-location longitude
                               degrees.minutes.seconds
   ```

7. 設定を保存します。

   ```
   デバイス(config-system)# commit
       デバイス(config-system)#
   ```

システムステータスの表示

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. デバイスを選択します。Cisco vEdge デバイスを選択すると、ウィンドウにはデフォルトで [System Status] が表示されます。

   Cisco IOS XE SD-WAN デバイスまたは任意のコントローラを選択した場合は、左ペインで [System Status] をクリックします。右ペインにデバイスに関する情報が表示されます。

システムステータスのパラメータについて

[System Status] ウィンドウには次の情報が表示されます。

- [Reboot]：デバイスが再起動した回数。それぞれの再起動について詳細を確認するには、[Reboot] をクリックします。[Reboot] ウィンドウが開き、次の情報が表示されます。
- [Crash]：デバイスがクラッシュした回数。それぞれのクラッシュの詳細を確認するには、[Crash] をクリックします。[Crash] ウィンドウが開き、次の情報が表示されます。
- ハードウェアコンポーネントのステータス。選択したデバイスがハードウェアの場合にのみ該当します。
  - モジュール
  - 温度センサー
  - USB
  - 電源モジュール
  - ファン

ハードウェアコンポーネントのステータスは、次のいずれかの方法で表されます。

- 緑色のチェックマーク：コンポーネントは動作しています。
- X の付いた赤い円：コンポーネントは停止しています。
- 感嘆符の付いたオレンジ色の三角形：コンポーネントにエラーがあります。
- N/A：選択したデバイスはハードウェアの Cisco vEdge デバイス ではないため、該当しません。
- CPU とメモリ：右側に期間が示されます。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。
  - CPU 使用率：CPU 使用率は、選択した時間範囲で使用可能な CPU の割合で表示されます。
  - メモリ使用率：メモリ使用率は、選択した時間範囲で使用可能なメモリの割合で表示されます。

TAC ケースのオープンと表示

表 *2:* 機能の履歴

機能名	リリース情報	説明
Cisco vManage からの TAC ケースへのアクセス	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1 Cisco SD-WAN リリース 20.9.1	この機能では、Cisco vManage を使用してサポートケースマネージャ（SCM）ウィザードにアクセスできます。別のケースマネージャポータルに移動することなく、Cisco vManage から直接サポートケースを作成、表示、編集できます。

サポートされるデバイス数

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

概要

Cisco vManage のトラブルシューティングの問題については、SCM ポータルでサポートケースを作成します。Cisco vManage では、SR 番号とトークンの詳細を入力して、SCM サーバー上の特定のサービスリクエスト（SR）に admin-tech ファイルをアップロードするという準備があります。

Cisco vManage リリース 20.9.1 以降では、Cisco vManage から SCM ポータルにアクセスできます。SCM ポータルでは、admin-tech ファイルを作成、表示、アップロードできます。admin-tech ファイルの詳細については、「admin-tech ファイル」を参照してください。

TAC ケースにアクセスするための前提条件

- アクティブな Cisco シングルサインオン（SSO）ログインで、SCM ウィザードとクラウドサーバーにアクセスする必要があります。

TAC ケースの表示

Cisco vManage から TAC ケースを表示するには、次の手順を実行します。

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

   TAC サポートケースポータルには、ケースの一覧が表示されます。

2. Cisco SSO ログインを使用して SCM ポータルにログインします。

TAC ケースのオープン

Cisco vManage から TAC ケースを開くには、次の手順を実行します。

1. Cisco vManage のメニューから**[Tools]** > **[TAC Cases]**の順に選択します。
2. TAC ケースのウィザードで、[Open a Case] をクリックします。
3. 関連する詳細をすべて入力します。
4. [Create] をクリックします。

   TAC サポートケースポータルには、ケースの一覧が表示されます。

SCM ポータルの使用方法の詳細については、『Cisco TAC Connect』[英語] を参照してください。

Cisco vBond オーケストレーション のステータスの表示

Cisco vBond オーケストレーション のステータスは、次の方法で表示できます。

ダッシュボード画面を使用する

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. Cisco vManage リリース 20.6.1 より前の場合は、[Cisco vBond] の横にある上向きまたは下向きの矢印をクリックします。

   Cisco vManage リリース 20.6.1 以降の場合は、オーバーレイネットワーク内の Cisco vBond オーケストレータ番号を示す数字をクリックします。
3. Cisco vBond オーケストレーション のステータスは、開いたダイアログボックスの [Reachability] 列で確認できます。

[Geography] 画面を使用する

1. Cisco vManage のメニューから**[Monitor]** > **[Geography]**の順に選択します。
2. [Filter] をクリックし、[Types] で [vBond] を選択します。
3. Cisco vBond アイコンをクリックして、ステータスを確認します。

[Network] 画面を使用する

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

   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. ステータスを確認する Cisco vBond オーケストレーション を見つけます。デバイステーブルでデバイスのリストをスクロールするか、検索バーに**vBond**をキーワードとして入力します。
3. [Hostname] 列で該当する Cisco vBond オーケストレーション をクリックします。[Control Connections] 画面がデフォルトで開き、そのデバイスとネットワーク内の他のコントローラデバイスとの間で確立されているすべての制御接続に関する情報が表示されます。

Cisco vSmart コントローラ のステータスの表示

Cisco vSmart コントローラ のステータスは、次の方法で表示できます。

[Dashboard] 画面を使用する

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. Cisco vManage リリース 20.6.1 より前の場合は、[Cisco vSmart] の横にある上向きまたは下向きの矢印をクリックします。

   Cisco vManage リリース 20.6.1 以降の場合は、オーバーレイネットワーク内の Cisco vSmart コントローラ番号を示す数字をクリックします。
3. Cisco vSmart コントローラ のステータスは、開いたダイアログボックスの [Reachability] 列で確認できます。

[Geography] 画面を使用する

1. Cisco vManage のメニューから**[Monitor]** > **[Geography]**の順に選択します。
2. [Filter] をクリックし、[Types] で [vSmartv] を選択します。
3. Cisco vSmart アイコンをクリックして、ステータスを確認します。

[Network] 画面を使用する

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

   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. ステータスを確認する Cisco vSmart コントローラ を見つけます。デバイステーブルでデバイスのリストをスクロールするか、検索バーに vBond をキーワードとして入力します。
3. [Hostname] 列で該当する Cisco vSmart コントローラ インスタンスをクリックします。[Control Connections] 画面がデフォルトで開き、そのデバイスとネットワーク内の他のコントローラデバイスとの間で確立されているすべての制御接続に関する情報が表示されます。

制御接続の表示

デバイスのすべての制御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]** > **[Geography]**の順に選択します。
2. 制御接続を表示するデバイスを選択します。

   コントローラデバイス（Cisco vBond オーケストレーション、Cisco vManage、Cisco vSmart コントローラ）を選択すると、 [Control Connections] 画面がデフォルトで表示されます。
3. エッジデバイスを選択すると、[System Status] 画面がデフォルトで表示されます。デバイスの制御接続を表示するには、左ペインで [Control Connections] をクリックします。右ペインには、デバイスとネットワーク内の他のコントローラデバイスとの間で確立されているすべての制御接続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。

- 予想される接続数と実際の接続数。
- グラフィック形式の制御接続データデバイスに複数のインターフェイスがある場合は、Cisco vManage ではすべての制御接続のグラフィカルトポロジが色ごとに表示されます。

右ペインの下部は、次の要素から構成されています。

- 検索バー：部分一致または完全一致を選択できる [Search Options] ドロップダウンが組み込まれています。
- 表形式の制御接続データデフォルトでは、最初の 6 つの制御接続が選択されています。右ペインの上部には、選択された制御接続の情報がグラフで表示されます。

Cisco vManage に接続されているデバイスの表示

1. Cisco vManage のメニューから**[Administration]** > **[Cluster Management]**の順に選択します。
2. [Service Configuration] で、目的の Cisco vManage サーバーのホスト名をクリックします。[vManage Details] 画面が表示されます。
3. 別の方法：

   [Service Configuration] で目的の Cisco vManage インスタンスの [...] をクリックし、[Device Connected] を選択します。

Cisco vManage で実行中のサービスの表示

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

2. [Service Configuration] で、目的の Cisco vManage サーバーのホスト名をクリックします。画面には、Cisco vManage で有効になっているすべての Cisco vManage サービスのプロセス ID が表示されます。

オーバーレイネットワークでのデバイスステータスの表示

オーバーレイネットワーク内にあるデバイスのステータスの表示方法には、次のオプションがあります。

[Dashboard] 画面を使用する

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. Cisco vManage リリース 20.6.1 より前の場合は、[WAN Edge] の横にある上向きまたは下向きの矢印をクリックします。

   Cisco vManage リリース 20.6.1 以降の場合は、[WAN Edge] デバイスの番号を表す数字をクリックします。

3. WAN エッジデバイスのステータスは、開いたダイアログボックスの [Reachability] 列で確認できます。

[Geography] 画面を使用する

1. Cisco vManage のメニューから**[Monitor]** > **[Geography]**の順に選択します。
2. [Filter] をクリックし、[Types] で [WAN Edge] を選択します。
3. ルータアイコンをクリックしてステータスを確認します。

[Network] 画面を使用する

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

   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. ステータスを表示する WAN エッジルータを見つけます。デバイステーブルでデバイスのリストをスクロールするか、検索バーにキーワードを入力します。
3. [Hostname] 列で該当する WAN エッジルータをクリックします。[System Status] 画面がデフォルトで開きます。

デバイス情報の表示

オーバーレイネットワーク内のデバイスの基本情報や詳細情報を表示できます。

基本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]** > **[Geography]**の順に選択します。
2. デバイスアイコンにカーソルを合わせます。

   ポップアップボックスに、システムの IP アドレス、ホスト名、サイト ID、デバイスタイプ、およびデバイスのステータスが表示されます。デバイスの詳細情報を表示するには、デバイスアイコンをダブルクリックして、[View More Details] ポップアップボックスを開きます。[Device Dashboard]、[Device Details]、[SSH Terminal]、[Links] のいずれかをクリックして、デバイスの詳細を取得します。

詳細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. ステータスを表示する WAN エッジルータを見つけます。デバイステーブルでデバイスのリストをスクロールするか、検索バーにキーワードを入力します。
3. [Hostname] 列で該当するデバイスをクリックします。右ペインには、デフォルトでシステムのステータスが表示されます。デバイスの詳細情報を表示するには、左ペインでカテゴリの 1 つを選択します。

デバイス設定の表示

1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
2. [WAN Edge List] または [Controllers] をクリックします。
3. 実行コンフィギュレーションを表示するには、目的のデバイスで[...]をクリックし、[Running Configuration] を選択します。

   ローカル コンフィギュレーションを表示するには、目的のデバイスで [...] をクリックし、[Local Configuration] を選択します。

デバイスに搭載されたソフトウェアバージョンの表示

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. [Hostname] 列でデバイス名をクリックして、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、[Software Versions] を選択します。

デバイスインターフェイスの表示

デバイスのインターフェイス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. [Hostname] 列でデバイス名をクリックして、デバイスを選択します。
3. 左ペインで [Interface] をクリックします。右ペインには、デバイスのインターフェイス情報が表示されます。

右ペイン上部は、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ります。このバーには以下が組み込まれています。
  - [Chart Options] ドロップダウン：[Chart Options] をクリックして、データの表示方法を選択します。
  - [IPv4 & IPv6] ドロップダウン：[IPv4 & IPv6] をクリックして、表示するインターフェイスのタイプを選択します。情報はグラフィック形式で表示されます。デフォルトではグラフは結合されており、IPv4 アドレスと IPv6 アドレスの両方が設定されているインターフェイスを示します。IPv4インターフェイスとIPv6インターフェイスを別々のグラフで表示するには、分離トグルボタンを選択します。
  - 期間：[Real Time]、事前定義した期間、カスタム期間のいずれかをクリックして、データの表示対象期間を選択します。
- グラフィック形式のインターフェイス情報。
- インターフェイスグラフの凡例：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。

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。

- すべてのインターフェイスに関する情報を一覧表示するインターフェイステーブル。デフォルトでは、最初の6つのインターフェイスが表示されます。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。
  - インターフェイス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のインターフェイスを選択して情報を表示できます。
  - 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。
  - セルラーインターフェイスの場合、インターフェイス名をクリックすると、セルラーインターフェイスに関する詳細情報が表示されます。

インターフェイスのステータスと統計を表示するには、show interfaceと show interface statistics のコマンドページを参照してください。

WAN インターフェイスの表示

VPN 0 のトランスポート インターフェイスは、インターネット、メトロ イーサネット ネットワーク、MPLS ネットワークなどの WAN ネットワークに接続します。

次のいずれかのオプションを使用して、デバイスの WAN インターフェイスに関する情報を表示できます。

[Real Time] ペイン

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. ステータスを表示するデバイスを見つけます。デバイステーブルでデバイスのリストをスクロールするか、検索バーにキーワードを入力します。
3. [Hostname] 列でデバイス名をクリックして、デバイスを選択します。
4. 開いたウィンドウの左ペインで [Real Time] を選択します。
5. 右ペインの [Device Options] ドロップダウンから、[Control WAN Interface Information] を選択します。

[Interface] ペイン

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. [Device Groups] ドロップダウンリストから、デバイスが属するデバイスグループを選択します。

3. [Hostname] 列でデバイス名をクリックして、デバイスを選択します。
4. 左ペインで [Interface] を選択します。

管理 VPN または VPN 512 のインターフェイスの表示

VPN 512 は、アウトオブバンド管理トラフィックで一般的に使用されます。ルータ上の VPN 512 のインターフェイス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. ステータスを表示するデバイスを見つけます。デバイステーブルでデバイスのリストをスクロールするか、検索バーにキーワードを入力します。
3. [Hostname] 列でデバイス名をクリックして、デバイスを選択します。
4. 左ペインで [Real Time] をクリックします。
5. 右ペインの [Device Options] ドロップダウンリストから、[Interface Detail] を選択します。
6. フィルタを使用する場合は、[Select Filter] ダイアログボックスで [Show Filters] をクリックします。そうでない場合は、[Do Not Filter] をクリックします。
7. **検索バー**に、管理 VPN である **512** を入力します。

CLI での同等コマンド：show interface vpn 512。

DHCP サーバーとインターフェイス情報の表示

デバイスでトンネルインターフェイスを設定すると、そのインターフェイスではDHCPを含むいくつかのサービスがデフォルトで有効になります。デバイスは接続されているサービス側ネットワークの DHCP サーバーとして機能し、サービス側ネットワークのホストに IP アドレスを割り当てます。また、DHCPヘルパーとしても機能し、サービス側ネットワーク内のデバイスから、サービス側のデバイスの異なるサブネットにある DHCP サーバーに IP アドレスの要求を転送することもできます。

DHCP サーバーとインターフェイスの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. [Hostname] 列でデバイス名をクリックして、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次のいずれかを選択して、特定の DHCP サーバーとインターフェイスの情報を表示します。

デバイスオプション	コマンド	説明
DHCP サーバー	show dhcp server	デバイスで有効になっている DHCP サーバー機能に関する情報を表示します
DHCP インターフェイス	show dhcp interface	エッジデバイスまたは Cisco vSmart コントローラで DHCP が有効になっているインターフェイスに関する情報を表示します

インターフェイスの MTU 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. [Hostname] 列でデバイス名をクリックして、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、[Interface Detail] を選択します。

セルラーインターフェイスの表示とモニタリング

ここでは、Cisco SD-WAN デバイスのセルラーインターフェイスの状態をモニタリングする方法について説明します。

セルラーインターフェイスのモニタリング

Cisco vManage またはルータの LED を使用して、信号強度とサービスの提供状況を確認できます。セルラーインターフェイスで最後に表示されたエラーメッセージを Cisco vManage から確認できます。

信号強度の確認

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. [Device Groups] ドロップダウンリストから、デバイスが属するグループを選択します。
3. [Hostname] 列でデバイス名をクリックして、デバイスを選択します。
4. 左ペインで [Real Time] をクリックします。
5. 右ペインの [Device Options] ドロップダウンリストから、[Cellular Radio] を選択します。

   各種セルラー信号の値が表示されます。信号強度が弱い場合や信号がない場合は、「一般的なセルラーインターフェイスの問題のトラブルシューティング」を参照してください。

CLI の同等コマンド： **show cellular status**

ルータ LED を使用した無線信号強度の確認

ルータからセルラー接続の信号強度とサービスの提供状況を確認するには、WWAN 信号強度 LED を確認します。通常、この LED はルータの前面にあり、ワイヤレスアイコンのラベルが付いています。

次の表で、LED の色と関連するステータスについて説明します。

表 3:

色	信号強度	状態	説明
オフ	—	—	LTE インターフェイスが無効（管理ステータスがダウン）または設定されていない
緑	優良	点灯	LTE インターフェイスが有効で休止モード（データが送受信されていない）
		点滅	LTE インターフェイスが有効でアクティブモード（データが送受信されている）
黄	良	点灯	LTE インターフェイスが有効で休止モード（データが送受信されていない）
		点滅	LTE インターフェイスが有効でアクティブモード（データが送受信されている）
オレンジ	不良	点灯	LTE インターフェイスが有効で休止モード（データが送受信されていない）
		点滅	LTE インターフェイスは有効でアクティブモード（データが送受信されている）
赤	重大な問題	点灯	LTE インターフェイスは有効だが、ベース トランシーバー ステーション（BTS）との接続が確立されていない、信号がないなどの問題がある

セルラーインターフェイスのエラーメッセージの表示

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. [Hostname] 列でデバイス名をクリックして、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、[Cellular Status] を選択します。

   表示される出力結果に [Last Seen Error] の列があります。

CLI の同等コマンド： **show cellular status**

コロケーションクラスタ情報の表示

ここでは、クラスタ情報とクラスタの正常性ステータスを表示する方法について説明します。この情報を確認すると、サービスチェーン内の各 VNF をホストする CSP デバイスを判断できます。

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. [Colocation Cluster] をクリックします。

   関連する情報を保有するすべてのクラスタが表形式で表示されます。クラスタ名をクリックします。

   左ペインの主要部分では、クラスタトポロジを確認できます。右ペインでは、Cloud OnRamp for Colocation のサイズに基づいて、使用可能な CPU リソースと合計 CPU リソース、使用可能なメモリと割り当て済みのメモリといったクラスタ情報を確認できます。

   左ペインの詳細部分は、次の要素から構成されます。

   - フィルタ条件：検索オプションのドロップダウンから表示するフィールドを選択します。
   - クラスタ内のすべてのデバイス（CSP デバイスおよびスイッチ）に関する情報が一覧表示された表。

     CSP クラスタをクリックすると、VNF 情報が表形式で表示されます。この表には、VNF 名、サービスチェーン、CPU 使用率、メモリ消費量、ディスク、管理 IP などの情報の他に、ネットワークサービスのパフォーマンスを決定づけるその他の主要パラメータが記載されています。

3. [Services] をクリックします。

この領域では、次の情報を確認できます。

- クラスタに割り当てられているすべてのサービスグループが表形式で示されます。最初の 2 列には、サービスグループ内のサービスチェーン名と説明が表示されます。
- [Diagram] をクリックすると、サービスグループとそのすべてのサービスチェーンと VNF がデザインビューウィンドウに表示されます。
- VNF をクリックすると、VNF に割り当てられた CPU、メモリ、およびディスクがダイアログボックスに表示されます。
- [Service Group] ドロップダウンリストからサービスグループを選択すると、選択したサービスグループと一緒に、そのすべてのサービスチェーンと VNF がデザインビューに表示されます。

Cisco Colo Manager の正常性の表示

デバイス、CCM ホストシステム IP、CCM IP、および CCM 状態に関する Cisco Colo Manager（CCM）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。

   右ペインに VNF 情報が表形式で表示されます。この表には、CPU 使用率、メモリ消費量、ディスク、およびネットワークサービスのパフォーマンスを決定するその他の主要パラメータなどの情報が表示されます。

2. 表から CSP デバイスをクリックします。
3. 左ペインで、[Colo Manager] をクリックします。

   右ペインには、Colo マネージャのメモリ使用率、CPU 使用率、稼働時間などに関する情報が表示されます。

CLI を使用した Cisco vManage クラスタ情報の表示

表 *4:* 機能の履歴

機能名	リリース情報	説明
CLI を使用した Cisco vManage クラスタの正常性とクラスタサービスの分析	Cisco vManage リリース 20.9.1	この機能では、**request nms cluster diagnostics** CLI コマンドを使用して、Cisco vManage クラスタの正常性とクラスタサービスのステータスを分析できます。

request nms cluster diagnostics コマンドを使用すると、Cisco vManage クラスタの正常性と、クラスタで実行されているクラスタサービスのステータスを確認できます。Cisco vManage クラスタを実行している Cisco vManage デバイスで直接コマンドを実行します。

request nms cluster diagnostics コマンドは、Cisco vManage クラスタの診断情報と、次の Cisco vManage サービスのステータス情報を提供します。

- アプリケーションサーバー
- メッセージングサーバー
- コンフィギュレーション データベース
- 統計設定データベース
- 調整サーバー

request nms cluster diagnostics コマンドの詳細については、『*Cisco SD-WAN* Command Reference Guide』[英語] を参照してください。

admin-tech ファイルにシステム情報を収集する

表 *5 :* 機能の履歴

機能名	リリース情報	説明
admin-tech の拡張	Cisco IOS XE リリース 17.2.1r Cisco SD-WAN リリース 20.1.1	この機能により、admin-tech ファイルが拡張され、admin-tech ログに **show tech-support memory**、**show policy-firewall stats platform**、および **show sdwan confd-log netconf-trace** コマンドが含まれるようになります。admin-tech tar ファイルには、メモリ、プラットフォーム、およびオペレーションの詳細情報が格納されます
admin-tech を使用した Cisco vManage クラスタのシステムステータス情報の生成	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 クラスタの admin-tech ファイル生成に関するサポートが追加されます。admin-tech ファイルは一連のシステムステータス情報であり、Cisco SD-WAN のテクニカルサポートがトラブルシューティングのために使用することを目的としています。 この機能が導入される前は、Cisco SD-WAN では単一デバイスの admin-tech ファイルしか生成できませんでした。

機能名	リリース情報	説明
生成された admin-tech ファイルの随時表示	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	この機能を使用すると、admin-tech ファイルがデバイスで利用可能な場合、いつでも生成された admin-tech ファイルを表示できます。 生成された admin-tech ファイルのリストを表示し、デバイスから Cisco vManage にコピーするファイルを決定できます。その後、選択した admin-tech ファイルをローカルデバイスにダウンロードするか、ダウンロードした admin-tech ファイルを Cisco vManage、デバイス、またはその両方から削除できます。
admin-tech ファイルに追加された診断情報	Cisco IOS XE リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能により、アプリケーションサーバー、設定データベース、統計データベース、およびその他の内部サービスから収集された追加の診断情報で、admin-tech ファイルの出力情報が充実します。
TAC ケースへの admin-tech ファイルのアップロード	Cisco IOS XE リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能を使用すると、TAC ケースを開くときに、Cisco vManage から admin-tech ファイルを直接アップロードできます。 TAC ケースを作成すると、生成された admin-tech ファイルを Cisco vManage から TAC サービスリクエストにアップロードできます。これにより、TAC と協力して問題をトラブルシュートするために必要な手順が合理化されます。

システム情報を収集するための Admin Tech について

admin-tech ファイルは、特定の問題のトラブルシューティングに使用される一連のシステムステータス情報です。問題を解決するには、Cisco vManage admin-tech ファイルを Cisco SD-WAN テクニカルサポートに送信します。

Cisco vManage クラスタ内の単一デバイスまたはすべてのノードについて、admin-tech ファイルを生成できます。

システム情報を収集するための admin-tech ファイルの利点

- システムステータス情報を含む統合ファイルが提供されます。このファイルを Cisco SD-WAN テクニカルサポートに送信し、診断およびトラブルシューティングを受けることができます。

- admin-tec ファイルを Cisco SD-WAN テクニカルサポートに直接アップロードするためのサポートが提供されます。

admin-tech ファイルにシステム情報を収集するための前提条件

- クラスタ内にあるすべてのノードの admin-tech ファイルを生成するには、Cisco vManage クラスタ内のすべてのノードが正常な状態である必要があります。

admin-tech ファイルにシステム情報を収集する際の制限事項

- 処理中の admin-tech 要求はすべて 3 時間ごとに削除されます。
- 1 つの Cisco vManage クラスタに対して一度に保持できる未処理の admin-tech 要求は 1 つだけです。既存 の admin-tech 要求がある場合、2 番目の admin-tech 要求でエラーが発生します。
- Cisco vManage クラスタの admin-tech は、個々のデバイスに対して admin-tech が実行されていない場合にのみ正常に実行されます。

admin-tech ファイルの生成

admin-tech ファイルを生成するには、次の手順を実行します。

1. Cisco vManage のメニュー,から**[Tools]** > **[Operational Commands]**の順に選択します。
2. [Generate Admin Tech for vManage] をクリックして、Cisco vManage クラスタ内にあるすべてのノードの admin-tech ファイルを生成します。
3. 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックし、[Generate Admin Tech] を選択します。
4. 必要に応じて [Generate admin-tech File] ウィンドウで、admin-tech tar ファイルの内容を制限します。
   1. デフォルトでは、[Include Logs] チェックボックスがオンになっています。圧縮された tar ファイルからログファイルを除外するには、このチェックボックスをオフにします。

（注） ログファイルは、ローカルデバイスの /var/log ディレクトリに保存されます。

   2. コアファイルを含めるには、[Include Cores] チェックボックスをオンにします。

（注） コアファイルは、ローカルデバイスの /var/crash ディレクトリに保存されます。

3. デバイスプロセス（デーモン）、メモリの詳細、およびオペレーションに関連するファイルを含めるには、[Include Tech] チェックボックスをオンにします。

5. [Generate] をクリックします。

   Cisco vManage で admin-tech ファイルが作成されます。

   ファイル名は、*date-time*-admin-tech.tar.gz という形式になります。

（注） Cisco vManage リリース 20.7.1 以降では、admin-tech ファイルにはアプリケーションサーバー、設定データベース、統計データベース、およびその他の内部サービスから収集された追加の診断情報が格納されます。

admin tech コマンドおよび technical support コマンドの詳細については、request admin-tech および show tech-support のコマンドページを参照してください。

admin-tech ファイルの表示

admin-tech ファイルが生成された後、次の操作を実行できます。

- 生成された admin-tech ファイルのリストを表示する。
- 選択した admin-tech ファイルをデバイスから Cisco vManage にコピーする。
- 選択した admin-tech ファイルをローカルデバイスにダウンロードする。
- 選択した admin-tech ファイルを Cisco vManage、デバイス、またはその両方から削除する。

1. Cisco vManage のメニュー,から**[Tools]** > **[Operational Commands]**の順に選択します。
2. 目的のデバイスで **[. . .]** をクリックし、[View Admin Tech List] を選択します。

   前に選択したデバイスの admin-tech コンテンツが格納された tar ファイルが表示されます。このファイル名は `ip-address-hostname-20210602-032523-admin-tech.tar.gz` のようになります。数値フィールドは日付と時刻です。

   生成された admin-tech ファイルのリストを表示し、Cisco vManage にコピーするファイルを決定できます。
3. [Copy] アイコンをクリックして、admin-tech ファイルをデバイスから Cisco vManage にコピーします。

   ファイルがデバイスから Cisco vManage にコピーされていることを知らせるヒントが表示されます。
4. ファイルがデバイスから Cisco vManage にコピーされたら、[Download] アイコンをクリックして、ファイルをローカルデバイスにダウンロードできます。

   ファイルが Cisco vManage にコピーされた後、admin-tech ファイルのサイズを確認できます。

5. admin-tech ファイルが Cisco vManage に正常にコピーされたら、[Delete] アイコンをクリックして、Cisco vManage から削除するファイル、デバイス、またはその両方を選択できます。

admin tech コマンドおよび technical support コマンドの詳細については、request admin-tech および show tech-support のコマンドページを参照してください。

TAC ケースへの admin-tech ファイルのアップロード

Cisco vManage リリース 20.7.1、Cisco IOS XE リリース 17.7.1a、および Cisco SD-WAN リリース 20.7.1 以降では、TAC ケースを開く際に、Cisco vManage から直接 admin-tech ファイルをアップロードできます。

はじめる前に

Cisco vManage で admin-tech ファイルを生成したことを確認します。

TAC ケースへの admin-tech ファイルのアップロード

TAC ケースに admin-tech ファイルをアップロードするには、次の手順を実行します。

1. Cisco vManage のメニュー,から**[Tools]** > **[Operational Commands]**の順に選択します。
2. **admin-tech** ファイルを生成したら、[Show Admin Tech List] をクリックします。

   [List of Admin-techs] ウィンドウが表示されます。
3. admin-tech ファイルのリストから該当する admin-tech ファイルを選択し、[Upload] をクリックします。
4. [SR Number] および [Token] フィールドに、詳細を入力します。
5. VPN オプションから該当する **VPN** を選択します。オプションは [VPN 0] と [VPN 512] です。
6. [Upload] をクリックします。

   選択した admin-tech ファイルが、関連するサービスリクエストにアップロードされます。

デバイスの再起動

[Device Reboot] 画面では、1 つ以上の Cisco SD-WAN デバイスを再起動できます。

デバイスの再起動

1. Cisco vManage のメニューから、**[Maintenance]** > **[Device Reboot]**を選択します。
2. 再起動するデバイスタイプに応じて、[WAN Edge]、[Controller]、または [vManage] をクリックします。

3. 再起動するデバイスの横にあるチェックボックスをオンにします。
4. [Reboot] をクリックします。

アクティブデバイスの表示

再起動操作が実行されたデバイスのリストを表示するには、次の手順を実行します。

1. Cisco vManage ツールバーから、[Tasks] アイコンをクリックします。Cisco vManage には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。
2. 行をクリックして、タスクの詳細を表示します。Cisco vManage ではペインが開き、タスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

セキュリティ アプリケーションのリロード

[Maintenance] > **[Device Reboot]** ウィンドウの [Reload Services] オプションを使用すると、セキュリティアプリケーションを動作不能状態から回復できます。このサービスを初期リカバリオプションとして使用してください。動作不能状態のセキュリティ アプリケーションの特定（47 ページ）を参照してください。

サービスをリロードするデバイスにセキュリティアプリケーションがすでにインストールされていることを確認します。1 つ以上のセキュリティアプリケーションをリロードするには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Maintenance]** > **[Device Reboot]**を選択します。
2. [WAN] エッジで、選択する Cisco SD-WAN デバイスのチェックボックスをオンにします。
3. [Reload Services] をクリックします。

   [Reload Container] ダイアログボックスが表示されます。
4. セキュリティアプリケーションのバージョンが正しければ、セキュリティアプリケーションのバージョンのチェックボックスをオンにします。
5. [Reload] をクリックします。

   セキュリティアプリケーションが停止し、アンインストールされた後に、再インストールおよび再起動されます。

セキュリティ アプリケーションのリセット

[Maintenance] > **[Device Reboot]** ウィンドウの [Reset Services] オプションを使用すると、セキュリティアプリケーションを動作不能状態から回復できます。

デバイスの仮想ポートグループ設定など、セキュリティアプリケーションの仮想ネットワーク設定が変更された場合は、[Reset Services] オプションを使用します。

- サービスをリセットするデバイスにセキュリティアプリケーションがすでにインストールされていることを確認します。

• 選択したセキュリティ アプリケーションが実行状態であることを確認します。

1 つ以上のセキュリティ アプリケーションをリセットするには、次の手順を実行します。

1. [WAN Edge] をクリックし、セキュリティ アプリケーションをリロードする Cisco SD-WAN デバイスのチェックボックスをオンにします。
2. [Reset Services] をクリックします。

   [Reset Container] ダイアログボックスが開きます。
3. セキュリティ アプリケーションのバージョンが正しければ、デバイスのチェックボックスをオンにします。
4. [Reset] をクリックします。

   セキュリティ アプリケーションが停止し、再起動されます。

動作不能状態のセキュリティ アプリケーションの特定

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. [Hostname] 列でデバイス名をクリックして、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。

   右ペインにリアルタイムでデバイス情報が表示されます。
4. [Device Options] ドロップダウンリストから、[App Hosting Details] を選択します。

   デバイス固有のアプリケーション ホスティング情報が記載された表が表示されます。この表で、デバイスの状態が「ACTIVATED」、「DEPLOYED」、または「STOPPED」の場合は、セキュリティ アプリケーションでリロードまたはリセット操作を実行します。

   デバイスの状態が「RUNNING」の場合、セキュリティ アプリケーションは動作状態にあります。
5. [Device Options] ドロップダウンリストから、[Security App Dataplane Global] を選択します。

   デバイス固有のアプリケーション データ プレーン情報が記載された表が表示されます。この表で、デバイスの [SN Health] が 黄色または赤色の場合は、セキュリティ アプリケーションでリロードまたはリセット操作を実行します。

   デバイスの [SN Health] が緑色の場合、セキュリティ アプリケーションは動作状態にあります。

インターフェイスのリセット

Interface Reset コマンドを使用すると、デバイスの設定を変更することなく、1 回の操作でデバイスのインターフェイスをシャットダウンして、次に再起動できます。

1. Cisco vManage のメニュー,から**[Tools]** > **[Operational Commands]**の順に選択します。
2. 目的のテンプレートで […] をクリックし、[Reset Interface] を選択します。
3. [Interface Reset] ダイアログボックスで、目的のインターフェイスを選択します。
4. [Reset] をクリックします。

デバイスの無効化

デバイスが対象ロケーションを超えた場合、デバイスを無効にできます。

1. Cisco SD-WAN のメニュー,から**[Tools]** > **[Operational Commands]**の順に選択します。
2. 目的のデバイスで […] をクリックし、[Make Device Invalid] を選択します。
3. デバイスを無効にすることを確認し、[OK] をクリックします。

デバイスの復旧

1. Cisco SD-WAN のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
2. 無効なデバイスを選択し、[Validate] 列を探します。
3. [Validate] をクリックします。
4. [Send to Controllers] をクリックして、アクションを完了します。

データトラフィックの停止

デバイスが対象ロケーションを超えた場合は、デバイスへのデータトラフィックを停止できます。

1. Cisco SD-WAN のメニュー,から**[Tools]** > **[Operational Commands]**の順に選択します。
2. 目的のデバイスで […] をクリックし、[Stop Traffic] を選択します。
3. デバイスへのデータトラフィックを停止することを確認し、[OK] をクリックします。

工場出荷時の状態へのリセット

デバイスが対象の境界外にある場合は、デバイスを工場出荷時の状態にリセットする必要性が生じる場合があります。

（注） [Factory Reset] 操作オプションは、Cisco ISR 1000 シリーズおよび Catalyst 8K デバイスでのみサポートされています。

ジオフェンシングの詳細については、『*Cisco IOS XE SD-WAN Systems and Interfaces Configuration Guide*』[英語] を参照してください。

1. Cisco SD-WAN のメニュー,から**[Tools]** > **[Operational Commands]**の順に選択します。
2. 目的のデバイスで […] をクリックし、[Factory Reset] を選択します。
3. 次のいずれかのオプションを選択します。
   - [Retain License]：ライセンスを除くすべてのデバイス設定とパーティションを消去します。[Retain License] は、factory-reset オプションのサブオプションです。
   - [Full Wipe factory-reset]：すべてのデバイス設定とパーティションを消去します。

（注） 完全消去操作の後、デバイスは USB または TFTP を使用してのみ起動できます。

4. [Reset] をクリックします。

Cisco SD-WAN コントローラと Cisco vEdge デバイスのリソースのモニタリング

表 *6 :* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN コントローラと Cisco vEdge デバイスのリソースのモニタリング	Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能を使用すると、Cisco SD-WAN コントローラおよび Cisco vEdge デバイスの CPU、メモリ、ディスクなどのリソース使用率のウォーターマークを設定できます。さらに、Cisco vManage サーバーでは、ウォーターマークを設定してディスクの読み取りおよび書き込み速度を監視できます。デバイスはリソースの使用状況をポーリングし、イベントを Cisco vManage に通知します。必要な修正アクションを実行できるように、Cisco vManage はリソース使用率の変化やディスクの読み取りまたは書き込み速度に関するアラームを生成します。

Cisco SD-WAN コントローラと Cisco vEdge デバイスのリソースのモニタリングについて

Cisco SD-WAN リリース 20.7.1 および Cisco vManage リリース 20.7.1 では、Cisco SD-WAN コントローラと Cisco vEdge デバイスの CPU、メモリ、およびディスクの使用状況をモニタリングするための Monit ユーティリティベースのワークフローが導入されています。Cisco SD-WAN リリース 20.6.x 以前、および Cisco vManage リリース 20.6.x 以前においても、リソースの使用状況をモニタリングできましたが、モニタリングとレポートは事前定義されたウォーターマークとデフォルトのポーリング間隔に基づいていました。Cisco SD-WAN リリース 20.7.1 および Cisco vManage リリース 20.7.1 以降では、環境内のリソースに応じてウォーターマークやポーリング間隔をカスタマイズできます。

CPU、メモリ、ディスクの使用状況をモニタリングするには、高、中、低使用率のウォーターマーク、およびデバイスがリソースの使用状況をチェックして Cisco vManage に報告する頻度を設定できます。さらに、適切な読み取りと書き込みウォーターマークやポーリング間隔を設

定することで、Cisco vManage サーバーでディスクの読み取りと書き込みの速度を監視できます。必要に応じて、CLI テンプレートを使用するか、デバイスの CLI にログインして、各種デバイスおよびコントローラのカスタムウォーターマークとポーリング間隔を設定できます。

デフォルト設定

CPU、メモリ、ディスクの使用状況を監視するために、デバイスとコントローラには次の使用率ウォーターマークとポーリング間隔がデフォルトで設定されています。

- 高い使用率のウォーターマーク：90%
- 中程度の使用率のウォーターマーク：75%
- 低い使用率のウォーターマーク：60%
- ポーリング間隔：5 秒

Cisco vManage のディスクの読み取りおよび書き込み速度にはデフォルト設定がなく、必要なウォーターマークとポーリング間隔を設定した後にのみ監視されます。

ポーリング、イベント、およびアラーム

デバイスやコントローラは、設定に基づいてリソースの使用状況を monit を介してポーリングし、ポーリングされた使用状況の情報に基づいて Cisco vManage にイベントを通知します。Cisco vManage は、そのイベント情報を前のポーリング間隔で受信したイベント情報と比較します。Cisco vManage がリソース使用状況の変化を検出すると、適切なアラームを生成します。

デバイスとコントローラは、次のイベントを Cisco vManage に通知します。

- CPU 使用率
- ディスク使用率
- メモリ使用率
- ディスク読み取り速度（Cisco vManage のみ）
- ディスク書き込み速度（Cisco vManage のみ）

イベント通知は、ポーリング使用率の値が設定されたウォーターマークとどのように比較されるかに基づいて、次のシビラリティ（重大度）とステータスに分類されます。

比較	シビラティ（重大度）	ステータス
ウォーターマークより上	Critical	usage-critical
中程度のウォーターマークと高いウォーターマークの間	Major	usage-warning
低いウォーターマークと中程度ウォーターマークの間	Minor	usage-notice
低ウォーターマーク未満	Minor	usage-healthy

イベントの表示と管理の詳細については、「イベント」を参照してください。

Cisco vManage はイベントに基づいて、次のタイプのアラームを生成できます。

- CPU 使用率
- ディスク使用率
- メモリ使用率
- ディスク読み取り速度（Cisco vManage のみ）
- ディスク書き込み速度（Cisco vManage のみ）

アラームにより、イベントステータスとシビラリティ（重大度）が次のようにマッピングされます。

アラーム	シビラティ（重大度）	ステータス
Critical（赤色）	Critical	usage-critical
Major（オレンジ色）	Major	usage-warning
Minor（黄色）	Minor	usage-notice
Minor（緑色）	Minor	usage-healthy

- 最初に、Cisco vManage はイベントステータスが「usage-health」以外の場合にアラームを生成し、過度のリソース使用を示します。
- 後続のイベントのステータスが、Cisco vManage が以前に受信したイベントと同じ場合、アラームは変更されません。
- 後続のイベントの重大度が低く、より健全な使用状況を示している場合、Cisco vManage は適切なアラームを生成します。新しいアラームにより、以前の重大度の高いアラームはクリアされます。
- Cisco vManage は、リソースの使用状況が深刻な状態から正常な状態に戻った場合にのみ、Minor（緑色）アラームを生成します。Minor（緑色）アラームは、リソースの使用状況が以前の過剰なレベルから通常のレベルに戻ったことを示します。

アラームの表示と管理の詳細については、「アラーム」を参照してください。

Cisco SD-WAN コントローラと Cisco vEdge デバイスのリソースモニタリングでサポートされるデバイス

- Cisco vManage リリース 20.7.1 以降を実行する Cisco vManage サーバー
- Cisco SD-WAN リリース 20.7.1 以降を実行する Cisco vSmart コントローラ

- Cisco SD-WAN リリース 20.7.1 以降を実行する Cisco vBond Orchestrator
- Cisco SD-WAN リリース 20.7.1 以降を実行する Cisco vEdge デバイス

CLI を使用した Cisco SD-WAN コントローラと Cisco vEdge デバイスのリソースモニタリングの設定

CLI テンプレートで CLI コマンドを使用して、リソースモニタリングのウォーターマークとポーリング間隔を設定できます。

このセクションでは、リソースモニタリングのウォーターマークとポーリング間隔を設定するための CLI 設定例を紹介します。

CPU 使用率のウォーターマークとポーリング間隔の設定

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# cpu-usage
Device(config-cpu-usage)# high-watermark-percentage percentage
Device(config-cpu-usage)# medium-watermark-percentage percentage
Device(config-cpu-usage)# low-watermark-percentage percentage
Device(config-cpu-usage)# interval seconds
```

例：

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# cpu-usage
Device(config-cpu-usage)# high-watermark-percentage 80
Device(config-cpu-usage)# medium-watermark-percentage 70
Device(config-cpu-usage)# low-watermark-percentage 50
Device(config-cpu-usage)# interval 10
```

メモリ使用率のウォーターマークとポーリング間隔の設定

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# memory-usage
Device(config-memory-usage)# high-watermark-percentage percentage
Device(config-memory-usage)# medium-watermark-percentage percentage
Device(config-memory-usage)# low-watermark-percentage percentage
Device(config-memory-usage)# interval seconds
```

例：

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# memory-usage
Device(config-memory-usage)# high-watermark-percentage 80
Device(config-memory-usage)# medium-watermark-percentage 70
Device(config-memory-usage)# low-watermark-percentage 50
Device(config-memory-usage)# interval 10
```

ディスク使用率のウォーターマークとポーリング間隔の設定

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# disk-usage file-system-path
Device(config-disk-usage-/opt/data)# high-watermark-percentage percentage
Device(config-disk-usage-/opt/data)# medium-watermark-percentage percentage
Device(config-disk-usage-/opt/data)# low-watermark-percentage percentage
Device(config-disk-usage-/opt/data)# interval seconds
```

例：

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# disk-usage /opt/data
Device(config-disk-usage-/opt/data)# high-watermark-percentage 80
Device(config-disk-usage-/opt/data)# medium-watermark-percentage 70
Device(config-disk-usage-/opt/data)# low-watermark-percentage 50
Device(config-disk-usage-/opt/data)# interval 10
```

Cisco vManage でのディスク IO 速度のウォーターマークとポーリング間隔の設定

```
vManage# config
vManage(config)# system
vManage(config-system)# alarms
vManage(config-alarms)# disk-speed disk-partition
vManage(config-disk-speed-/dev/nvme1n1)# read-high-watermark-kBps speed
vManage(config-disk-speed-/dev/nvme1n1)# read-medium-watermark-kBps speed
vManage(config-disk-speed-/dev/nvme1n1)# read-low-watermark-kBps speed
vManage(config-disk-speed-/dev/nvme1n1)# write-high-watermark-kBps speed
vManage(config-disk-speed-/dev/nvme1n1)# write-medium-watermark-kBps speed
vManage(config-disk-speed-/dev/nvme1n1)# write-low-watermark-kBps speed
vManage(config-disk-speed-/dev/nvme1n1)# interval seconds
```

例：

```
vManage# config
vManage(config)# system
vManage(config-system)# alarms
vManage(config-alarms)# disk-speed /dev/nvme1n1
vManage(config-disk-speed-/dev/nvme1n1)# read-high-watermark-kBps 1000
vManage(config-disk-speed-/dev/nvme1n1)# read-medium-watermark-kBps 500
vManage(config-disk-speed-/dev/nvme1n1)# read-low-watermark-kBps 100
vManage(config-disk-speed-/dev/nvme1n1)# write-high-watermark-kBps 1000
vManage(config-disk-speed-/dev/nvme1n1)# write-medium-watermark-kBps 500
vManage(config-disk-speed-/dev/nvme1n1)# write-low-watermark-kBps 100
vManage(config-disk-speed-/dev/nvme1n1)# interval 100
```

CLI を使用した Cisco SD-WAN コントローラと Cisco vEdge デバイスのリソースモニタリング設定の確認

CPU 使用率のウォーターマークとポーリング間隔の設定を確認する

show alarms cpu-usage コマンドの出力例を以下に示します。設定されている CPU 使用率のウォーターマークとポーリング間隔が表示されます。

```
Device# show alarms cpu-usage

            HIGH        MEDIUM      LOW
            WATERMARK   WATERMARK   WATERMARK
CPU USAGE   PERCENTAGE  PERCENTAGE  PERCENTAGE  INTERVAL
-----------------------------------------------------------------
cpu-usage   80          70          50          10
```

メモリ使用率のウォーターマークとポーリング間隔の設定を確認する

show alarms memory-usage コマンドの出力例を以下に示します。設定されているメモリ使用率のウォーターマークとポーリング間隔が表示されます。

```
Device# show alarms memory-usage

              HIGH        MEDIUM      LOW
              WATERMARK   WATERMARK   WATERMARK
MEMORY USAGE  PERCENTAGE  PERCENTAGE  PERCENTAGE  INTERVAL
-----------------------------------------------------------------
memory-usage  80          70          50          10
```

ディスク使用率のウォーターマークとポーリング間隔の設定を確認する

show alarms disk-usage コマンドの出力例を以下に示します。設定されているディスク使用率のウォーターマークとポーリング間隔が表示されます。

```
Device# show alarms disk-usage

             HIGH          MEDIUM        LOW
FILESYSTEM   WATERMARK     WATERMARK     WATERMARK
PATH         PERCENTAGE    PERCENTAGE    PERCENTAGE  INTERVAL
-----------------------------------------------------------------
/rootfs.rw    90            75            60          5
/tmp          90            75            60          5
/opt/data     80            70            50          10
```

ディスク I/O 速度のウォーターマークとポーリング間隔の設定を確認する

show alarms disk-speed コマンドの出力例を以下に示します。設定されている I/O 速度のウォーターマークとポーリング間隔が表示されます。

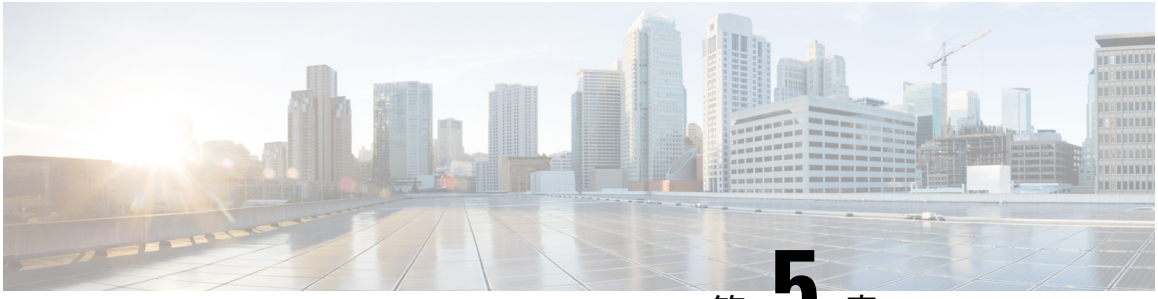
```
vManage# show alarms disk-speed

                      READ                    WRITE       WRITE
            READ HIGH MEDIUM     READ LOW     HIGH        MEDIUM     WRITE LOW
            WATERMARK WATERMARK  WATERMARK    WATERMARK   WATERMARK  WATERMARK
DISK PATH   K BPS      K BPS      K BPS       K BPS       K BPS      K BPS      INTERVAL
-----------------------------------------------------------------------------------------
/dev/sda2   1000       500        100         1000        500        100        100
```

デバイスのイベント通知を表示する

show notification stream viptela コマンドの出力例を以下に示します。CPU 使用率イベントが表示されます。

```
vManage# show notification stream viptela
notification
 eventTime 2021-09-08T02:57:14.91578+00:00
 cpu-usage
  severity-level minor
```

```
  host-name vm12
  system-ip 172.16.255.22
  cpu-status usage-notice
  warning System CPU usage is above 50%
  cpu-user-percentage 40.9
  cpu-system-percentage 10.6
  cpu-idle-percentage 48.50
 !
!
```



第 5 章

ネットワーク

表 7: 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 *8 :* 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 *9*: 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 *10* : 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 （81 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 （81 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 （81 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 *11 : 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 *12 : [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 *13 : [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 *14*：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 *15 :* 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 *16* : 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 *17 :* 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 *18* : 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。

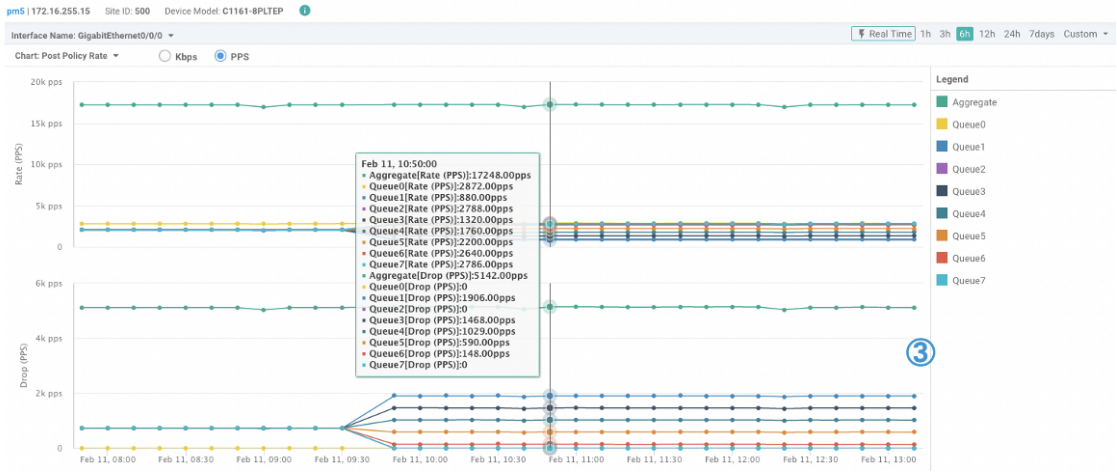
5. [Chart] ドロップダウンリストから、次のいずれかを選択します。
   - [Post Policy Rate]：1 秒あたりのデータ転送速度を kbps（デフォルト）または 1 秒あたりのパケット数（PPS）で表示します。この値の計算では、ポストポリシーカウンタ/10 の式を使用して 1 秒あたりの速度が求められます。

   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 *19 :* 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 *20 :* 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 *21* : 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

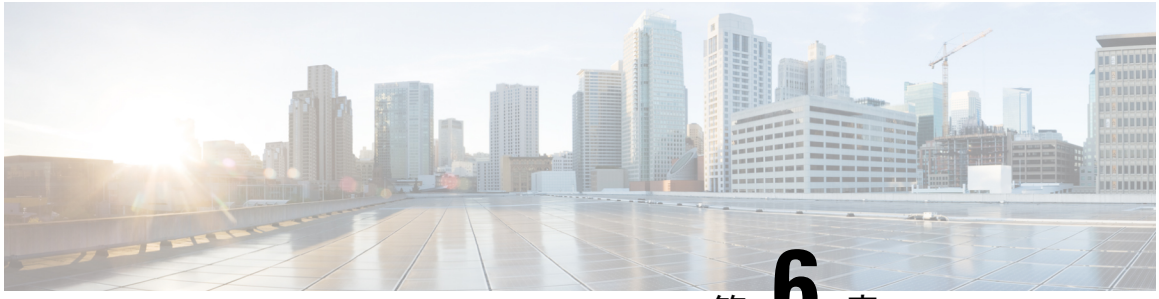
システムクロックを表示するには、次の手順を実行します。

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。



第 6 章

アラーム、イベント、ログ

アラーム

オーバーレイネットワークの個々のデバイスでイベントが発生すると、デバイスは通知をCisco vManage に送信して報告します。次に、Cisco vManage はイベント通知をフィルタリングしてから関連するイベントを相互に関連付けし、やや重大なイベントと重大なイベントをアラームに統合します。

Cisco vManage で生成されるアラームのリストについては、「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。

[Alarms] 画面では、オーバーレイネットワーク内のコントローラとルータによって生成されたアラームに関する詳細情報を表示できます。

アラームの状態

Cisco vManage アラームには、シビラリティ（重大度）に基づいてステータスが割り当てられます。

- Critical（赤）：オーバーレイネットワーク機能の動作を損なう、またはシャットダウンを引き起こす重大なイベント。
- Major（黄）：ネットワーク機能の動作に影響を与えるが、シャットダウンを引き起こすことのない重大なイベント。

- Medium（青）：ネットワーク機能のパフォーマンスを損なう可能性のあるイベント。
- Minor（緑）：ネットワーク機能のパフォーマンスを低下させる可能性のあるイベント。

通常、シビラリティ（重大度）が Critical または Major のアラームがアクティブとして一覧表示されます。

Cisco vManage が受信した通知イベントがアラーム条件が経過したことを示すと、ほとんどのアラームは自動的にクリアされます。その後、Cisco vManage はアラームをクリア済みとしてリストし、アラームの状態は通常、Medium または Minor に変わります。

Cisco vManage リリース 20.5.1 でのアラームの変更

表 *22*：機能の履歴

機能	リリース情報	説明
アラームの最適化	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、重複したアラームを自動的に抑制することで、Cisco vManage のアラームを最適化します。これにより、問題の原因となっているコンポーネントを簡単に特定できます。 これらのアラームを表示するには、Cisco vManage のメニューから**[Monitor]** > **[Logs]** > **[Alarms]**の順に選択します。

サイトがダウンすると、Cisco vManage は次のアラームを報告します。

- サイトの停止
- ノードの停止
- TLOC の停止

Cisco vManage は、停止しているコンポーネントごとにアラームを表示します。サイトのサイズによっては、ノードアラームだけでなく、ノード内の各 TLOC のアラームなど、重複したアラームが何度も表示される場合があります。Cisco vManage リリース 20.5.1 では、Cisco vManage が重複したアラームをインテリジェントに抑制します。たとえば、ノード内のすべての TLOC が停止している場合、Cisco vManage は各 TLOC からのアラームを抑制し、ノードからのアラームだけを表示します。マルチテナント構成の場合、各テナントでは、そのテナント内のサイトに関するアラームが表示されます。

シナリオ	表示されるアラーム	
Cisco vManage リリース 20.5.1	以前のリリース	

シナリオ	表示されるアラーム	
リンク 1 が停止 リンク 2 が稼働	bfd-tloc-1_down	bfd-tloc-1_down
リンク 1 が停止 リンク 2 が停止	bfd-site-1_down bfd-node-1_down、bfd-tloc-1_down、および bfd-tloc-2_down は、サイトアラームによって抑制されます。	bfd-site-1_down bfd-tloc-1_down
リンク 1 が稼働 リンク 2 が停止	bfd-site-1_up bfd-node-1_up bfd-tloc-1_up bfd-tloc-2_up	bfd-site-1_up bfd-tloc-1_up

アラーム表示

上部のバーにあるアラームベルアイコンをクリックすると、Cisco vManage ダッシュボードからアラームを表示できます。アラームベルでは、アクティブアラームまたはクリア済みアラームにグループ化されています。

または、次の手順に従って、Cisco vManage の [Alarms] 画面からアラームを表示します。

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

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

   アラームはグラフィック形式と表形式で表示されます。

2. 特定のアラームの詳細を表示するには、目的のアラームで[…]をクリックしてから、[Alarm Details] をクリックします。

   [Alarm Details] ウィンドウが開き、アラームの考えられる原因、影響を受けるエンティティなどの詳細が表示されます。

アラームフィルタの設定

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

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

2. [Filter] をクリックします。

3. [Severity] フィールドで、ドロップダウンリストからアラームのシビラリティ（重大度）レベルを選択します。複数のシビラリティ（重大度）レベルを指定できます。

4. [Active] フィールドで、ドロップダウンリストからアクティブアラーム、クリア済みのアラーム、または両方のタイプのアラームを選択します。アクティブアラームは、現在デバイス上にあるが、まだ認識されていないアラームです。
5. [Alarm Name] フィールドで、ドロップダウンリストからアラーム名を選択します。アラーム名は複数指定できます。
6. [Search] をクリックして、フィルタ条件に一致するアラームを検索します。

Cisco vManage では、アラームが表形式とグラフィック形式の両方で表示されます。

アラームデータを CSV 形式でエクスポートする

すべてのアラームのデータを CSV 形式のファイルにエクスポートするには、[Download] アイコンをクリックします。

Cisco vManage では、すべてのデータが CSV 形式でアラームテーブルから Excel ファイルにダウンロードされます。ファイルはブラウザのデフォルトのダウンロード場所にダウンロードされ、Alarms.csv という名前が付けられます。

グラフに表示されるアラームデータは、Excel ファイルでも参照できます。

たとえば、2022 年 2 月 15 日午前 3:30 の日時でグラフにアラームデータ（Critical 2、Major 274、Medium 4、Minor 405）が表示される場合、2022 年 2 月 15 日午前 3:00 から 2022 年 2 月 15 日午前 3:29 までの日時の範囲で、同じアラームデータが Excel ファイルでも使用できます。

電子メール通知の有効化

オーバーレイネットワーク内のデバイスでアラームが発生したときに電子メール通知を送信するように Cisco vManage を設定できます。これには、最初に SMTP および電子メール受信者のパラメータを設定する必要があります。まず、次の画面で SMTP および電子メール受信者のパラメータを設定します。

1. Cisco vManage のメニューから **[Administration]** > **[Settings]** の順に選択します。
2. [Alarm Notifications] オプションの横にある [Edit] をクリックします。
3. [Enable Email Notifications] で [Enabled] を選択します。
4. [Email Settings] チェックボックスをオンにします。
5. 電子メール通知を送信する際のセキュリティレベルを選択します。セキュリティレベルには、[None]、[SSL]、または [TLS] を指定できます。
6. [SMTP Server] フィールドには、電子メール通知を受信する SMTP サーバーの名前または IP アドレスを入力します。
7. [SMTP Port] フィールドに、SMTP ポート番号を入力します。セキュリティなしの場合、デフォルトのポートは 25 です。 SSL の場合は 465、TLS の場合は 587 です。
8. [From Address] フィールドには、電子メール通知の送信者として表示する電子メールアドレスを入力します。

9. [Reply to address] フィールドには、電子メールの [Reply-To] フィールドに表示する電子メールアドレスを入力します。このアドレスには、noreply@cisco.com などの返信不可アドレスを指定できます。

10. [Use SMTP Authentication] チェックボックスをオンにして、SMTP サーバーへの SMTP 認証を有効にします。

    SMTP 認証で使用するユーザー名とパスワードを入力します。デフォルトユーザーの電子メールサフィックスが、ユーザー名に付加されます。入力したパスワードは非表示になります。

11. [Save] をクリックします。

（注） 電子メールは、送信元インターフェイスとして VPN0（トランスポート インターフェイス）の vManage パブリック IP から送信されます。

アラーム通知の送信

開始する前に、電子メール通知が**[Administration]** > **[Settings]**で有効になっていることを確認します。[Alarm Notifications] の横にある [Edit] をクリックして、[Alarm Notifications] が有効になっているかどうか、また [Email Settings] チェックボックスがオンになっているかどうかを確認します。

アラームの発生時に電子メール通知を送信するには、次の手順を実行します。

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

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

2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。

3. [Add Alarm Notification] をクリックします。

4. [Name] フィールドに、電子メール通知の名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。

5. [Severity] フィールドで、ドロップダウンリストからアラームのシビラリティ（重大度）レベルを 1 つ以上選択します。

6. [Alarm Name] フィールドで、1 つ以上のアラームを選択します。

7. [Account Details] では、次の情報を入力します。

   1. [Email] フィールドに、電子メールアドレスを 1 つ以上入力します。

   2. （任意）[Add New Email List] をクリックし、必要に応じて電子メールリストを入力します。

   3. [Email Threshold] フィールドでは、1 分あたりに送信する電子メールの最大数を設定します。1 から 30 までの値を指定できます。デフォルトは 5 です。

4. [WebHook] チェックボックスをオンにすると。アラーム通知イベントが発生したときに HTTP コールバックをトリガーされます。
   1. [WebHook URL] フィールドには、ウェブフックサーバーの URL を入力します。
   2. ウェブフックサーバーを認証するためのユーザー名とパスワードを [Username] と [Password] にそれぞれ入力します。
   3. [WebHook Threshold] フィールドに、しきい値を入力します。

（注） 入力した値は、そのウェブフック URL で 1 分あたりに発行される通知の数を示します。たとえば、[WebHook Threshold] が 2 の場合、そのウェブフック URL の通知を 1 分あたり 2 つ受け取ります。しきい値を超えて生成された通知はドロップされます。

8. [Selected Devices] では、[All Devices] または [Custom] を選択します。

   [Custom] を選択すると、デバイスリストが表示されます。
   1. 左側の [Available Devices] リストで、1 つ以上のデバイスを選択します。
   2. 右矢印をクリックして、デバイスを右側の [Selected Devices] リストに移動します。
   3. [Add] をクリックします。
9. [Add] をクリックします。

電子メール通知の表示および編集

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

   Cisco vManage のメニューから**[Monitor]** > **[Alarms]**の順に選択します。
2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。
3. 目的の通知で、行の右側にある [View] アイコンをクリックします。
4. 通知の表示が完了したら、[OK] をクリックします。

電子メール通知の編集

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

   Cisco vManage のメニューから**[Monitor]** > **[Alarms]**の順に選択します。
2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。
3. 目的の電子メール通知で、[Edit] アイコンをクリックします。
4. 通知の編集が完了したら、[Update] をクリックします。

電子メール通知の削除

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

   Cisco vManage のメニューから**[Monitor]** > **[Alarms]**の順に選択します。
2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。
3. 目的の電子メール通知で、[Trash Bin] アイコンをクリックします。
4. 確認ダイアログボックスで、[OK] をクリックします。

イベント

表 *23* : 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス のイベント通知サポート	Cisco IOS XE リリース 17.2.1r	Cisco IOS XE SD-WAN デバイス でイベント通知のサポートが追加されました。

[Events screen] 画面を使用して、Cisco SD-WAN デバイスで生成されたイベントに関する詳細情報を表示できます。

イベントフィルタの設定

1 つ以上の Cisco SD-WAN デバイスで生成されたイベントを検索するためのフィルタを設定するには、次の手順を実行します。

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

   Cisco vManage のメニューから**[Monitor]** > **[Events]**の順に選択します。
2. [Filter] をクリックします。
3. [Severity] フィールドをクリックし、ドロップダウンリストからシビラリティ（重大度）レベルを選択します。

   Cisco SD-WAN デバイスで生成されたイベントは Cisco vManage によって収集されて、次のように分類されます。

   - Critical：すぐにアクションを実行する必要があることを示します。
   - Major：問題を調査する必要があるが、ネットワークをダウンさせるほど重大ではないことを示します。
   - Minor：情報提供のみです。

   複数のシビラリティ（重大度）レベルを指定できます。

1. [Component] フィールドでは、ドロップダウンリストから、イベントの原因となった 1 つ以上の構成コンポーネントを選択します。
2. [System IP] フィールドでは、生成されたイベントを表示するデバイスのシステム IP をドロップダウンリストから選択します。
3. [Event Name] フィールドでは、生成されたイベントを表示するイベント名をドロップダウンリストから選択します。複数のイベント名を選択できます。
4. [Search] をクリックして、フィルタ条件に一致するイベントを検索します。

Cisco vManage では、イベントが表形式とグラフィック形式の両方で表示されます。

イベントデータを CSV 形式でエクスポートする

すべてのイベントのデータを CSV 形式のファイルにエクスポートするには、[Download] アイコンをクリックします。

Cisco vManage では、すべてのデータが CSV 形式でイベントテーブルから Excel ファイルにダウンロードされます。ファイルはブラウザのデフォルトのダウンロード場所にダウンロードされ、Events.csv という名前が付けられます。

デバイスの詳細の表示

イベントが生成されたデバイスに関する詳細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]** > **[Logs]** > **[Events]**の順に選択します。

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

   このウィンドウには、イベントがグラフィック形式と表形式の両方で表示されます。
2. デバイスで生成されたイベントに関する詳細情報を表示するには、表からイベントの行を選択します。
3. 目的のデバイスで […] をクリックし、[Device Details] を選択します。

   [Device Details] ダイアログボックスが開き、イベントを発生させたデバイスのホスト名などの詳細が表示されます。

CLI の使用

CLI を使用して、Cisco vEdge デバイス でイベントが生成されたデバイスに関する情報を表示する場合は、**show notification stream viptela** コマンドを使用できます。コマンドの出力例を以下に示します。出力の最初の行は、メッセージが生成された時刻（SNMP eventTime）を示しています。時刻はデバイスの現地時間ではなく、UTC 形式で表示されます。通知の 2 行目にはイベントの説明が表示され、3 行目ではシビラリティ（重大度）レベルが示されます。

```
vEdge# show notification stream viptela
notification
 eventTime 2015-04-17T14:39:41.687272+00:00
 bfd-state-change
  severity-level major
  host-name vEdge
```

```
  system-ip 1.1.4.2
  src-ip 192.168.1.4
  dst-ip 108.200.52.250
  proto ipsec
  src-port 12346
  dst-port 12406
  local-system-ip 1.1.4.2
  local-color default
  remote-system-ip 1.1.9.1
  remote-color default
  new-state down
 !
!
notification
 eventTime 2015-04-17T15:12:20.435831+00:00
 tunnel-ipsec-rekey
  severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
  color default
 !
!
notification
 eventTime 2015-04-17T16:56:50.314986+00:00
 system-login-change
  severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
  user-name admin
  user-id 9890
 !
```

CLI を使用して、Cisco IOS XE SD-WAN デバイス でイベントが生成されたデバイスに関する情報を表示する場合は、**show sdwan notification stream** コマンドを使用できます。コマンドの出力例を以下に示します。出力の最初の行は、メッセージが生成された時刻（SNMP eventTime）を示しています。時刻はデバイスの現地時間ではなく、UTC 形式で表示されます。通知の 2 行目にはイベントの説明が表示され、3 行目ではシビラリティ（重大度）レベルが示されます。

```
Device# show sdwan notification stream
notification
 eventTime 2020-03-03T02:50:04.211317+00:00
sla-change
  severity-level major
  host-name SanJose
  system-ip 4.4.4.103
  src-ip 10.124.19.15
  dst-ip 10.74.28.13
  proto ipsec
  src-port 12426
  dst-port 12346
  local-system-ip 4.4.4.103
  local-color default
  remote-system-ip 4.4.4.106
  remote-color biz-internet
  mean-loss 17
  mean-latency 13
  mean-jitter 19
  sla-classes None
  old-sla-classes Voice-And-Video
!
!
```

Cisco IOS XE リリース 17.6.3 以降では、**alarms alarm bfd-state-change syslog** コマンドを使用して、デバイスの BFD 状態変化イベントが発生した場合に BFD 状態変化の syslog メッセージを表示できます。詳細については、alarms alarm bfd-state-change syslog のコマンドページを参照してください。

```
Device(config-system)# alarms alarm bfd-state-change syslog
Device(config-alarm-bfd-state-change)# commit
```

BFD 状態変化の syslog メッセージの例を以下に示します。

```
Jul 10 07:09:07.583: %Cisco-SDWAN-vm5-FTMD-5-NTCE-1000009: BFD-session 10.1.15.15:12346
 -> 10.1.16.16:12366,
local-tloc-index: 32775 -> remote-tloc-index: 32777, TLOC- local sys-ip: 172.16.255.15,
 local color: lte -> remote
sys-ip: 172.16.255.16, remote color: lte, encap: IPSEC, new state->UP delete:false,
reason:REMOTE_FSM
```

BFD 状態変化を有効にした後の実行コンフィギュレーション：

```
 Device# show sdwan running-config
system
 gps-location latitude 35.0
 gps-location longitude -120.0
 system-ip             170.16.1.1
 simulated-devices     27 2
 simulated-color       red blue
 simulated-wan-ip      192.168.1.1
 domain-id             1
 site-id               10000
 admin-tech-on-failure
 organization-name     "vIPtela Inc Regression"
 vbond 10.0.12.26
 alarms alarm bfd-state-change
  syslog
 !
!
```

イベント通知のモニタリング

表 *24*：機能の履歴

機能名	リリース情報	説明
OMP エージェントおよび SD-WAN サブシステムのイベントトレースのモニタリング	Cisco IOS XE リリース 17.2.1r Cisco SD-WAN リリース 20.1.1	この機能により、指定した SD-WAN サブシステムのイベントトレース機能をモニタリングおよび制御できます。イベントトレースは、SD-WAN デーモンと SD-WAN サブシステム間の SD-WAN トレースをキャプチャする機能を提供します。

オーバーレイネットワーク内の個々のデバイスで問題が発生すると、デバイスは次の方法でイベントを報告します。

- Cisco vManage に通知を送信します。Cisco vManage はイベント通知をフィルタリングしてイベントを相互に関連付けて、やや重大なイベントと重要なイベントをアラームに統合します。
- 設定されたトラップターゲットに SNMP トラップを送信します。デバイスは SNMP トラップを生成するたびに、対応する通知メッセージも生成します。
- システムロギング（syslog）メッセージを生成し、ローカルデバイスの /var/log ディレクトリにある syslog ファイルに保存します。設定に応じて、リモートデバイスにも保存します。

通知はデバイスから Cisco vManage サーバーに送信されるメッセージです。

指定した SD-WAN サブシステムのイベントトレース機能をモニタリングおよび制御するには、特権 EXEC モードで **monitor event-trace** コマンドを実行します。イベントトレースは、SD-WAN デーモンと SD-WAN サブシステム間の SD-WAN トレースをキャプチャする機能を提供します。コマンドの詳細については、monitor event-trace sdwan および show monitor event-trace sdwan のコマンドページを参照してください。

ACL ログ

[ACL Log] 画面では、ルータに設定されているアクセスリスト（ACL）のログを表示できます。ルータは 10 分ごとに ACL ログを収集します。

ACL ログフィルタの設定

1. Cisco vManage のメニューから**[Monitor]** > **[Logs]** > **[ACL Log]**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]** > **[ACL Log]** の順に選択します。
2. [Filter] をクリックします。
3. [VPN] フィールドで、ドロップダウンリストから ACL ログを収集するエンティティを選択します。選択できる VPN は 1 つだけです。
4. [Search] をクリックして、フィルタ条件に一致するログを検索します。

Cisco vManage ではアクティビティのログが表形式で表示されます。

監査ログ情報の表示

監査ログフィルタの設定

表 *25 :* 機能の履歴

機能名	リリース情報	説明
監査ログを使用したテンプレート設定変更の比較	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能には、デバイステンプレートと機能テンプレートの監査ログ用の **Config Diff** オプションが導入されています。**Config Diff** オプションにより、現在の設定と以前の設定を比較してテンプレート設定の変更箇所が表示されます。 テンプレートがデバイスにアタッチされていない場合、**Config Diff** オプションを監査ログで使用して、設定の変更箇所を表示できます。

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

2. [Filter] をクリックします。
3. [Module] フィールドで、監査ログを収集するエンティティを選択します。複数のエンティティを選択できます。
4. [Search] をクリックして、フィルタ条件に一致するログを検索します。

Cisco vManage ではアクティビティのログが表形式とグラフィック形式の両方で表示されます。

監査ログデータを CSV 形式でエクスポートする

すべての監査ログのデータを CSV 形式のファイルにエクスポートするには、[Export] をクリックします。

Cisco vManage では、すべてのデータが CSV 形式で監査ログテーブルから Excel ファイルにダウンロードされます。ファイルはブラウザのデフォルトのダウンロード場所にダウンロードされ、Audit_Logs.csv という名前が付けられます。

監査ログの詳細を表示する

監査ログに関する詳細情報を表示するには、次の手順を実行します。

1. テーブルからの監査ログの行を選択します。
2. 目的の行で […] をクリックし、[Audit Log Details] を選択します。

[Audit Log Details] ダイアログボックスが開き、監査ログの詳細が表示されます。

設定テンプレートの変更箇所の表示

テンプレートの以前の設定と現在の設定を比較した変更箇所を表示できます。テンプレート設定の変更箇所を表示するには、次の手順を実行します。

1. テーブル内の監査ログの行をクリックします。テーブルではモジュールタイプがテンプレートになります。
2. テンプレートモジュールの隣にある [...] をクリックし、[Config Diff] をクリックします。

   [Config Difference] ペインには、テンプレートの元の設定と、設定に加えられた変更との相違点が並べて表示されます。変更をインラインで表示するには、[Inline Diff] をクリックします。

デバイスの更新後の設定を表示するには、[Configuration] をクリックします。

Cisco IOS XE リリース 17.6.1a および Cisco SD-WAN リリース 20.6.1 以降では、テンプレートとポリシー設定の変更については、[Audit Logs] オプションを使用すると、実行されたアクションが表示されます。アクション前の設定と現在の設定を表示するには、[Audit Log Details] をクリックします。デバイステンプレート、機能テンプレート、ローカライズされたポリシー、一元化されたポリシー、およびセキュリティポリシーを作成、更新、削除すると、監査ログが収集されます。監査ログには、テンプレートやポリシーがアタッチされている場合とアタッチされていない場合の API ペイロードの変更箇所が表示されます。

設定テンプレートアクティビティのログの表示

設定テンプレートの作成に関連するアクティビティのログ、デバイスと設定テンプレートの関連付けのステータスを表示するには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
2. [WAN Edge List] または [Controllers] を選択し、デバイスを選択します。
3. 目的のデバイスで […] をクリックし、[Template Log] を選択します。

syslog メッセージ

オーバーレイネットワーク内の個々のデバイスで問題が発生した場合、デバイスは報告方法の 1 つとして、システムログ （syslog） メッセージを生成し、ローカルデバイスの /var/log ディレクトリ内にある syslog ファイルに記録します。設定すれば、リモートデバイスに記録することも可能です。

Cisco SD-WAN デバイスでは、イベント通知システムログ（syslog）メッセージをローカルデバイスまたはリモートホスト、あるいはその両方のファイルに記録できます。ローカルデバイスでは、syslog ファイルは /var/log ディレクトリに配置されます。

システムロギングの設定

デフォルトでは、優先度レベルが「エラー」の syslog メッセージをローカルデバイスのハードディスクに記録するように設定されています。ログファイルは、ローカルの /var/log ディレクトリに配置されます。デフォルトでは、ログファイルのサイズは 10 MB で、最大 10 個のファイルが保存されます。10 個のファイルが作成されると、最も古いファイルが破棄され、新しい syslog メッセージ用のファイルが作成されます。

デフォルトの syslog パラメータを変更するには、Cisco vManage からロギング機能テンプレートを使用します。CLI から、デバイス設定で **logging disk** または **logging server** コマンドを含めます。

syslog ロギング情報の表示

1. Cisco vManage のメニューから**[Administration]** > **[Settings]**の順に選択し、[Data Stream] が有効になっていることを確認します。
2. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。

   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、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. [Logs] 領域で [Debug Log] をクリックします。
5. [Log Files] フィールドで、ログファイル名を選択します。画面の下部にログ情報が表示されます。

CLI から syslog ファイルの内容を表示するには、**show log** コマンドを使用します。次に例を示します。

```
Device# show log auth.log tail 10==> /var/log/auth.log <==auth.info: Nov 14 14:33:35
vedge sshd[2570]: Accepted publickey for admin from 10.0.1.1 port 39966 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 14 14:39:42 vedge
sshd[2578]: Received disconnect from 10.0.1.1 port 39966:11: disconnected by userauth.info:
 Nov 14 14:39:42 vedge sshd[2578]: Disconnected from 10.0.1.1 port 39966auth.info: Nov
16 10:51:45 vedge sshd[6106]: Accepted publickey for admin from 10.0.1.1 port 40012 ssh2:
 RSA SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 16 11:21:55 vedge
```

```
 sshd[6108]: Received disconnect from 10.0.1.1 port 40012:11: disconnected by
userauth.info: Nov 16 11:21:55 vedge sshd[6108]: Disconnected from 10.0.1.1 port
40012auth.info: Nov 17 12:59:52 vedge sshd[15889]: Accepted publickey for admin from
10.0.1.1 port 40038 ssh2: RSA SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info:
 Nov 17 13:45:13 vedge sshd[15894]: Received disconnect from 10.0.1.1 port 40038:11:
disconnected by userauth.info: Nov 17 13:45:13 vedge sshd[15894]: Disconnected from
10.0.1.1 port 40038auth.info: Nov 17 14:47:31 vedge sshd[30883]: Accepted publickey for
 admin from 10.0.1.1 port 40040 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1s
```

デバイスのシステムロギングの設定を表示するには、CLI から **show logging** コマンドを実行します。次に例を示します。

```
Device# show logging
System logging to host  in vpn 0 is disabled
Priority for host logging is set to: emerg

System logging to disk is disabled
Priority for disk logging is set to:  err
File name for disk logging is set to:  /var/log/vsyslog
File size for disk logging is set to:  10 MB
File recycle count for disk logging is set to:  10

Syslog facility is set to: all facilities
```

システムのログファイル

デフォルトまたは設定された優先度の値以上の syslog メッセージは、ローカルデバイスの /var/log ディレクトリ内にあるいくつかのファイルに記録されます。ファイルの種類は次のとおりです。

- auth.log：ログイン、ログアウト、スーパーユーザーのアクセスイベント、および認可システムの使用状況。
- kern.log：カーネルメッセージ
- messages：すべてのソースからの syslog メッセージが記録された統合ログファイル
- vconfd：設定に関するすべての syslog メッセージ
- vdebug：デバッグ機能が有効になっているモジュールのすべてのデバッグメッセージ、および設定された優先度の値を超えるすべての syslog メッセージ。デバッグロギングは、モジュールに基づいてさまざまなレベルのロギングをサポートします。実装されているロギングレベルは、モジュールごとに異なります。たとえば、システムマネージャ（sysmgr）には 2 つのロギングレベル（オンとオフ）があり、シャーシマネージャ（chmgr）には 4 つの異なるロギングレベル（オフ、低、標準、高）があります。デバッグメッセージをリモートホストに送信することはできません。デバッグを有効にするには、**debug** 操作コマンドを使用します。
- vsyslog：設定された優先度の値を超える Cisco SD-WAN プロセス（デーモン）からのすべての syslog メッセージ。デフォルトの優先度の値は「informational」（重大度レベル 6）であるため、デフォルトでは「notice」、「warning」、「error」、「critical」、「alert」、および「emergency」のすべての syslog メッセージ（重大度レベル 5 ～ 0）が保存されます

Cisco SD-WAN ソフトウェアは、/var/log にある標準の Linux ファイル（cron.log、debug、lpr.log、mail.log、syslog）をロギングに使用しません。

syslog ファイルへのメッセージの書き込みに、レート制限はありません。つまり、短時間に多くの syslog メッセージが生成された場合、オーバーフローメッセージはバッファに入れられ、syslog ファイルに書き込まれるまでキュー内に置かれます。オーバーフローメッセージはドロップされません。

syslog メッセージが繰り返された場合（連続して同一メッセージが複数回発生）、メッセージは 1 回だけ syslog ファイルに記録されます。メッセージの発生回数を示す注釈がメッセージに付けられています。

syslog メッセージの最大長は 1024 バイトです。それより長いメッセージは切り捨てられます。

AAA 認証および Netconf CLI のアクセス状況と使用状況に関連する syslog メッセージは、auth.log およびメッセージファイルに記録されます。Cisco vManage が Cisco vEdge デバイス にログインして統計情報とステータス情報を取得し、ファイルをルータにプッシュするたびに、ルータは AAA 認証と Netconf のログメッセージを生成します。したがって、時間の経過とともに、これらのメッセージでログファイルがいっぱいになる可能性があります。これらのメッセージでログファイルがいっぱいにならないようにするには、AAA 認証と Netconf の syslog メッセージのロギングを無効にします。

```
Device(config)# system aaa logsViptela(config-logs)# audit-disableViptela(config-logs)#
 netconf-disable
```

syslog メッセージ形式

Cisco SD-WAN ソフトウェアによって生成される syslog メッセージの形式は次のとおりです。

```
facility.source
date - source - module - level - MessageID: text-of-syslog-message
```

syslog メッセージの例を次に示します。このログのファシリティは local7、レベルは「notice」です。

syslog メッセージの頭字語

次の頭字語は、syslog メッセージやメッセージの説明で使用されます。

表 *26 :*

略語	意味
confd	CLI 設定プロセス
FIM	転送テーブルマネージャ
FP	転送プロセス
RIM	ルートテーブルマネージャ

略語	意味
TIM	トンネルテーブルマネージャ

生成された各種 syslog メッセージのリストを表示するには、付録の「syslog メッセージ」を参照してください。

認定アクティビティログの表示

証明書関連のアクティビティのステータスを表示するには、Cisco vManage の**[Configuration]** > **[Certificates]**ウィンドウを使用します。

1. Cisco vManage ツールバーから、タスクアイコンをクリックします。Cisco vManage には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。
2. 行をクリックして、タスクの詳細を表示します。Cisco vManage ではステータスウィンドウが開き、タスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

Cisco SD-WAN デーモンのバイナリトレース

表 *27 :* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN デーモンのバイナリトレース	Cisco IOS XE リリース 17.4.1a	バイナリトレースにより、Cisco SD-WAN デーモンのトラブルシューティングが強化されます。バイナリトレース機能は、デーモンからのメッセージをバイナリ形式で記録します。メッセージはバイナリ形式で高速に記録されるため、ロギングのパフォーマンスが向上し、記憶領域も ASCII 形式より少なくなります。バイナリトレースの CLI を使用すると、**debug** コマンドと比較して、追加のプロセスモジュールでデバッグレベルを設定できます。 Cisco IOS XE リリース 17.4.1a 以降では、バイナリトレースは次の Cisco SD-WAN デーモンでサポートされています。 • fpmd • ftm • ompd • vdaemon • cfgmgr

バイナリトレース機能は、プロセスモジュールからメッセージを収集し、その情報をバイナリ形式で記録します。バイナリトレースのログメッセージのレベルを設定し、記録されたメッセージを表示して、プロセス実行中のエラーのトレースとトラブルシューティングを行うことができます。

バイナリトレースは、ASCII 形式よりも高速なバイナリ形式でメッセージをで記録することで、ランタイムパフォーマンスを向上させます。また、バイナリ形式は ASCII 形式よりも効率的に格納できます。トレース結果を表示またはファイルに保存すると、メッセージはバイナリ形式から ASCII 形式に復号化されます。

サポートされる Cisco SD-WAN デーモン

バイナリトレースは、次の Cisco SD-WAN デーモンとそのモジュールでサポートされています。

Cisco SD-WAN デーモン	サポートされているリリース
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE リリース 17.4.1a

バイナリトレースレベルの設定

特定のハードウェアスロットで実行されている 1 つまたはすべての Cisco SD-WAN プロセスモジュールのバイナリトレースレベルを設定します。

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **set platform software trace** *process slot module level*

例：

```
Device# set platform software trace fpmd R0 config debug
```

特定のハードウェアスロットで実行されている 1 つまたはすべての Cisco SD-WAN プロセスモジュールのトレースレベルを設定します。

- *process*：fpmd、ftm、ompd、vdaemon、cfgmgr から Cisco SD-WAN プロセスを指定します。
- *slot*：プロセスメッセージを記録するハードウェアスロットを指定します。
- *module*：1 つまたはすべてのプロセスモジュールのトレースレベルを設定します。
- *level*：次のトレースレベルから 1 つ選択します。
  - debug：Debug（デバッグ）メッセージ
  - emergency：Emergency（致命的）エラーの可能性があるメッセージ
  - error：エラーメッセージ
  - info：Informational（情報提供）メッセージ

- noise：可能性のある最大メッセージ
- notice：通知メッセージ
- verbose：詳細デバッグメッセージ
- warning：警告メッセージ

バイナリトレースレベルの表示

特定のハードウェアスロットで実行されている Cisco SD-WAN プロセスモジュールのバイナリトレースレベルを表示します。

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **show platform software trace level** *process slot*

例：

```
Device# show platform software trace level fpmd R0
```

指定したハードウェアスロット上のすべてのプロセスモジュールについて、バイナリトレースレベルが表示されます。

- *process*：fpmd、ftm、ompd、vdaemon、cfgmgr から Cisco SD-WAN プロセスを指定します。
- *slot*：プロセスメッセージを記録するハードウェアスロットを指定します。

CiscoSD-WANプロセスのバイナリトレースで記録されたメッセージの表示

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **show logging process** *process-name* [*filtering-options*]

例：

```
Device# show logging process fpmd internal fru R0 reverse
```

指定したプロセスのログを表示します。

process-name には、fpmd、ftm、ompd、vdaemon、cfgmgr からプロセスを指定します。プロセスのカンマ区切りリストを指定することもできます（例：`fpmd, ftm`）。

filtering-options を指定しない場合、コマンドは過去 10 分間に収集されたバイナリトレースレベル情報とシビラリティ（重大度）レベルの高いログを表示します。

フィルタリングオプションの詳細については、**show logging process** のコマンドページを参照してください。

すべてのCiscoSD-WANプロセスのバイナリトレースで記録されたメッセージの表示

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **show logging profile sdwan** [*filtering-options*]

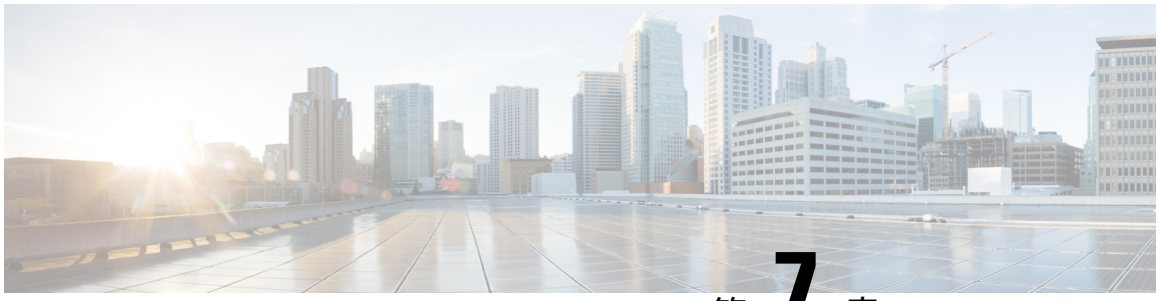
例：

```
Device# show logging profile sdwan start last boot
```

すべての Cisco SD-WAN プロセスとそのモジュールのログを時系列で表示します。

filtering-options を指定しない場合、コマンドは過去 10 分間に収集されたバイナリトレースレベル情報とシビラリティ（重大度）レベルの高いログを表示します。

フィルタリングオプションの詳細については、**show logging profile sdwan** のコマンドページを参照してください。



第 7 章

ソフトウェアのアップグレードとリポジトリの管理

表 *28* : 機能の履歴

機能名	リリース情報	説明
リモートサーバーを使用したソフトウェアのアップグレード	Cisco IOS XE リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能により、リモートサーバーに保存されているソフトウェアイメージを使用して、デバイスやコントローラのソフトウェアをアップグレードできます。リモートサーバーを Cisco vManage に登録し、リモートサーバー上のソフトウェアイメージの場所を Cisco vManage ソフトウェアリポジトリに追加できます。デバイスまたはコントローラのソフトウェアをアップグレードすると、デバイスまたはコントローラはリモートサーバーから新しいソフトウェアイメージをダウンロードできます。 また、リポジトリで使用可能なイメージのリストも更新されます。2つ以上のイメージのバージョンが同じでファイル名が異なる場合、各イメージは個別のエントリとして表示されます。

- ソフトウェアアップグレード （150 ページ）

• ソフトウェアのリポジトリの管理 （156 ページ）

ソフトウェアアップグレード

[Software Upgrade] ウィンドウを使用して、新しいソフトウェアイメージをダウンロードし、Cisco SD-WAN デバイスで実行されているソフトウェアイメージをアップグレードできます。

集中管理型の Cisco vManage からオーバーレイネットワーク内にある Cisco SD-WAN デバイスのソフトウェアをアップグレードし、新しいソフトウェアでデバイスを再起動できます。これは、1つのデバイスに対して行うことも、複数のデバイスに対して同時に行うこともできます。

スタンドアロン展開または Cisco vManage クラスタ展開の Cisco vBond オーケストレーション、Cisco vSmart コントローラ、Cisco IOS XE SD-WAN デバイス、Cisco vEdge デバイス のグループをアップグレードする場合、ソフトウェアのアップグレードと再起動は、最初に Cisco vBond オーケストレーション、次に Cisco vSmart コントローラ で実行され、最後に Cisco IOS XE SD-WAN デバイス または Cisco vEdge デバイス で実行されます。 CPU リソースに応じて、最大 40 の Cisco IOS XE SD-WAN デバイス または Cisco vEdge デバイス のアップグレードと再起動を並行して行うことができます。

Cisco vManage リリース 20.8.1 で導入されたソフトウェア アップグレード ワークフロー機能は、ガイド付きワークフローを通じて Cisco SD-WAN エッジデバイスのソフトウェア アップグレードプロセスを簡素化し、さまざまなデバイスやソフトウェアのアップグレードステータスを表示します。ソフトウェア アップグレード ワークフローの作成の詳細については、「ソフトウェア アップグレード ワークフロー」を参照してください。

（注）

- グループのソフトウェアアップグレード処理に Cisco vManage を含めることはできません。Cisco vManage サーバーを単体でアップグレードして再起動する必要があります。
- Cisco SD-WAN エッジデバイスのアップグレード専用のソフトウェア アップグレード ワークフローを作成できます。
- すべてのソフトウェアアップグレードは、CLI からではなく、Cisco vManage から実行することを推奨します。
- ソフトウェアの互換性については、『Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations』[英語] を参照してください。

デバイスの仮想イメージのアップグレード

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. デバイスを選択するには、目的のデバイスのチェックボックスをオンにします。
3. [Upgrade Virtual Image] をクリックします。

[Virtual Image Upgrade] ダイアログボックスが開きます。

4. 必要に応じて、[vManage] または [Remote Server - vManage] を選択します。
5. [Upgrade to Version] ドロップダウンリストから、デバイスのアップグレード先の仮想イメージバージョンを選択します。
6. [Upgrade] をクリックします。

デバイスのソフトウェアイメージのアップグレード

（注）
- ここで説明する手順では、旧ソフトウェアバージョンにダウングレードすることはできません。ダウングレードする必要がある場合は、『Cisco SD-WAN Getting Started Guide』の「Downgrade a Cisco vEdge Device to an Older Software Image」[英語] を参照してください。
- vManage クラスタのアップグレードを実行する場合は、「Upgrade Cisco vManage Cluster」[英語] を参照してください。
- Cisco vManage リリース 20.1.1 以降では、設定データベースをアップグレードする前に、データベースのサイズを確認してください。データベースのサイズは 5 GB 以下にすることを推奨します。データベースのサイズを確認するには、次の診断コマンドを使用します。

  request nms *configuration-db diagnostics*

デバイスでソフトウェアイメージをアップグレードするには、次の手順を実行します。

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. ソフトウェアをアップグレードするデバイスのタイプに基づいて、[WAN Edge]、[Controller]、[vManage] のいずれかをクリックします。
3. デバイステーブルで、アップグレードするデバイスの左端にあるチェックボックスをオンにして選択します。

（注）Cisco vManage クラスタのアップグレード時には、テーブル内に表示されるクラスタのすべてのノードを選択します。

4. [Upgrade] をクリックします。
5. [Software Upgrade] スライドイン ペインで、次の手順を実行します。
   1. どのサーバーからデバイスにイメージをダウンロードするかを選択します。[vManage]、[Remote Server]、[Remote Server – vManage] のいずれかです。

（注）
- リモートサーバーのオプションは、Cisco vManage リリース 20.7.1 で導入されました。[Remote Server] を選択する場合は、デバイスがリモートサーバーに到達可能になっていることを確認してください。
- Cisco vManage リリース 20.9.1 以降では、リモートサーバーからイメージを手動でダウンロードする際に、次の有効な文字のみが使用されていることを確認してください。
  - ユーザー ID：a ～ z、0 ～ 9、.、_、-
  - パスワード：a ～ z、A ～ Z、0 ～ 9、_、*、.、+、=、%、-
  - URL 名またはパス：a ～ z、A ～ Z、0 ～ 9、_、*、.、+、=、%、-、:、/、@、?、~

2. [vManage] の場合は、[Version] ドロップダウンリストからイメージのバージョンを選択します。
3. [Remote Server – vManage] の場合、ドロップダウンリストから [vManage OOB VPN] を選択し、[Version] ドロップダウンリストからイメージのバージョンを選択します。
4. [Remote Server] の場合は、次のフィールドを設定します。

[Remote Server Name]	イメージが存在するリモートサーバーを選択します。
[Image Filename]	ドロップダウンリストからイメージのファイル名を選択します。

5. [Activate and Reboot] チェックボックスをオンにします。

   このチェックボックスをオフにすると、ソフトウェアイメージはダウンロードされてデバイスにインストールされますが、イメージはアクティブ化されず、デバイスは再起動されません。アップグレードタスクが完了したら、イメージをアクティブ化する必要があります。
6. [Upgrade] をクリックします。

   現在のデバイス構成が保持したままで、新しいソフトウェアバージョンを使用してデバイスが再起動します。[Task View] ページが開き、デバイスのアップグレードの進行状況が表示されます。

6. アップグレードが完了するまで待ちます。完了までに数分かかります。[Status] 列に「Success」と表示されたら、アップグレードは完了です。
7. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択し、デバイスを表示します。
8. ソフトウェアをアップグレードするデバイスのタイプに基づいて、[WAN Edge]、[Controller]、[vManage] のいずれかをクリックします。

9. デバイステーブルで、アップグレードされたデバイスの [Current Version] 列に新しいバージョンが表示されていることを確認します。[Reachability] 列に「reachable」と表示されていることを確認します。

（注）
- Cisco vManage への制御接続が設定された時間制限内に確立されなかった場合、Cisco vManage はデバイスを以前に実行されていたソフトウェアイメージに自動的に戻します。ソフトウェアのアップグレード後にすべての Cisco SD-WAN デバイスが起動するまでの時間制限は 5 分に設定されていますが、Cisco vEdge デバイス については、デフォルトの時間は 12 分です。
- コントローラデバイスで実行されているバージョンよりも高いバージョンに Cisco vEdge デバイス ソフトウェアをアップグレードすると、ソフトウェアの非互換性が発生する可能性があることを伝える警告メッセージが表示されます。Cisco vEdge デバイス のソフトウェアをアップグレードする前に、コントローラのソフトウェアをアップグレードすることを推奨します。
- Cisco CSR1000V または Cisco ISRv デバイスを Cisco IOS XE リリース 17.4.1a 以降にアップグレードする場合、ソフトウェアのアップグレードによってデバイスも Cisco Catalyst 8000V にアップグレードされます。アップグレード後、[Devices] ページの [Chassis Number] および [Device Model] 列にはデバイスが Cisco CSR1000V または Cisco ISRv と表示されますが、実際にはデバイスは Cisco Catalyst 8000V にアップグレードされています。古い名前が保持される理由は、ライセンスの無効化などを避けるためです。デバイスが Cisco Catalyst 8000V にアップグレードされていることを確認するには、デバイスの [Current Version] 列に 17.4.1 以降が表示されているかに注目します。

新しいソフトウェアイメージのアクティブ化

現在デバイスにロードされているソフトウェアイメージをアクティブ化するには、下記の手順を使用します。ソフトウェアイメージは、現在アクティブなリリースより新しいリリースにすること（アップグレード）も以前のリリースにすること（ダウングレード）も可能です。

Cisco vManage を使用してデバイスのソフトウェアイメージをアップグレードする際の手順で、[Activate and Reboot] チェックボックスをオンにしなかった場合、デバイスでは既存の設定が引き続き使用されます。アップグレードしたソフトウェアバージョンをアクティブ化するには、以下に示す手順を実行します。

（注） カスタムユーザーグループの使用中に Cisco vManage のソフトウェアをアクティブ化するには、各ソフトウェア機能をアップグレードするための読み取り権限および読み取り/書き込み権限が必要です。

ソフトウェアイメージをアクティブ化するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. **[WAN Edge]**, **[Controller]**、**[Cisco vManage]** のいずれかを選択します。
3. 目的のデバイスのチェックボックスをオンにしてデバイスを選択します。
4. [Activate] をクリックします。[Activate Software] ダイアログボックスが開きます。
5. デバイスでアクティブ化するソフトウェアバージョンを選択します。
6. [Activate] をクリックします。Cisco vManage はデバイスを再起動し、新しいソフトウェアイメージをアクティブ化します。

Cisco vManage への制御接続が設定された時間制限内に確立されなかった場合、Cisco vManage はデバイスを以前に実行されていたソフトウェアイメージに自動的に戻します。ソフトウェアのアップグレード後にすべての Cisco SD-WAN デバイスが起動するまでの時間制限は 5 分に設定されていますが、Cisco vEdge デバイス については、デフォルトの時間は 12 分です。

Cisco NFVIS アップグレードイメージを使用した CSP デバイスのアップグレード

始める前に

Cisco NFVIS ソフトウェアバージョンが、`.nfvispkg` 拡張子を持つファイルであることを確認します。

ステップ 1 [Cisco vManage] メニューから、**[Maintenance]** > **[Software Upgrade]** > **[WAN Edge]**を選択します。

ステップ 2 選択するデバイスの 1 つ以上の CSP デバイスのチェックボックスをオンにします。

ステップ 3 **[Upgrade]** をクリックします。[Software Upgrade] ダイアログボックスが表示されます。

ステップ 4 CSP デバイスにインストールする Cisco NFVIS ソフトウェアバージョンを選択します。ソフトウェアがリモートサーバーにある場合は、適切なリモートバージョンを選択します。

ステップ 5 新しい Cisco NFVIS ソフトウェアバージョンで自動的にアップグレードしてアクティブ化し、CSP デバイスをリブートするには、[Activate and Reboot] チェックボックスをオンにします。

[Activate and Reboot] チェックボックスをオンにしない場合、CSP デバイスはソフトウェアイメージをダウンロードして検証します。ただし、CSP デバイスは引き続き古いバージョンまたは現在のバージョンのソフトウェアイメージを実行します。CSP デバイスが新しいソフトウェアイメージを実行できるようにするには、デバイスを再度選択し、[Software Upgrade] ウィンドウで [Activate] ボタンをクリックして、新しい Cisco NFVIS ソフトウェアバージョンを手動でアクティブ化する必要があります。

ステップ 6 **[Upgrade]** をクリックします。

[Task View] ウィンドウには、実行中のすべてのタスクのリストと、成功と失敗の合計数が表示されます。ウィンドウは定期的に更新され、アップグレードの進行状況またはステータスを示すメッセージが表示されます。Cisco vManage ツールバーにある [Task View] アイコンをクリックすると、ソフトウェア アップグレード ステータス ウィンドウに簡単にアクセスできます。

（注） 同じクラスタに属する 2 つ以上の CSP デバイスがアップグレードされる場合、CSP デバイスのソフトウェアアップグレードは順番に実行されます。

（注） [Set the Default Software Version] オプションは、Cisco NFVIS イメージでは使用できません。

CSP デバイスがリブートし、新しい NFVIS バージョンがデバイスでアクティブ化されます。このリブートは、[Activate] フェーズ中に発生します。[Activate and Reboot] チェックボックスをオンにした場合、または CSP デバイスを再度選択した後に手動で [Activate] をクリックすると、アクティブ化はアップグレードの直後に行われます。

CSP デバイスがリブートして実行されているかどうかを確認するには、タスクビューウィンドウを使用します。Cisco vManage は、ネットワーク全体を 90 秒ごとに最大 30 回ポーリングし、タスクビューウィンドウにステータスを表示します。

（注） イメージバージョンがデバイスで実行されているアクティブなバージョンでない場合は、CSP デバイスから Cisco NFVIS ソフトウェアイメージを削除できます。

ソフトウェアイメージの削除

Cisco SD-WAN デバイスからソフトウェアイメージを削除するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. [WAN Edge]、[Controller]、[vManage] のいずれかをクリックします。
3. ソフトウェアイメージを削除するデバイスを 1 つ以上選択します。
4. [Delete Available Software] をクリックします。

   [Delete Available Software] ダイアログボックスが開きます。
5. 削除するソフトウェアバージョンを選択します。
6. [Delete] をクリックします。

デフォルト ソフトウェア バージョンの設定

ソフトウェアイメージを Cisco SD-WAN デバイスのデフォルトイメージとして設定できます。この操作を実行すると、工場出荷時のデフォルトのソフトウェアイメージが上書きされ、選択したイメージに置き換えられます。ソフトウェアがデバイスやネットワーク上で想定どおりに動作していることを確認した後でのみ、ソフトウェアイメージをデフォルトに設定することを推奨します。

ソフトウェアイメージをデバイスのデフォルトイメージに設定するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. [WAN Edge]、[Controller]、[vManage] のいずれかをクリックします。
3. 目的のデバイスのチェックボックスをオンにして、1 つ以上のデバイスを選択します。
4. [Set Default Version] をクリックします。

   [Set Default Version] ダイアログボックスが開きます。
5. [Version] ドロップダウンリストから、選択したデバイスのデフォルトとして使用するソフトウェアイメージを選択します。
6. [Set Default] をクリックします。

CSV 形式でのデバイスデータのエクスポート

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. [WAN Edge]、[Controller]、[vManage] のいずれかをクリックします。
3. 目的のデバイスのチェックボックスをオンにして、1 つ以上のデバイスを選択します。
4. ダウンロードアイコンをクリックします。

Cisco vManage はデバイステーブルのすべてのデータを CSV 形式で Excel ファイルにダウンロードします。このファイルはブラウザのデフォルトのダウンロード場所にダウンロードされ、`Software_Upgrade.csv` という名前が付けられます。

ソフトウェア アップグレード アクティビティ ログの表示

1. Cisco vManage のツールバーから [Tasks] アイコンをクリックします。

   Cisco vManage には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。
2. 矢印をクリックして、タスクの詳細を表示します。Cisco vManage ではステータスウィンドウが開き、タスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

ソフトウェアのリポジトリの管理

リモートサーバーの登録

リモートサーバーを Cisco vManage に登録すると、リモートサーバー上のソフトウェアイメージの場所を Cisco vManage ソフトウェアリポジトリに追加し、追加したソフトウェアイメージを使用して、デバイスまたはコントローラのソフトウェアをアップグレードできます。Cisco

SD-WANのマルチテナント展開では、プロバイダーだけがリモートサーバーを登録し、リモートサーバー上のイメージを使用してソフトウェアのアップグレードを実行できます。

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Repository]**の順に選択します。
2. [Add Remote Server] をクリックします。
3. [Add Remote Server] スライドインページで、次のように設定します。

サーバー情報	• [Server Name]：サーバー名を入力します。 • [Server IP] または [DNS Name]：サーバーの IP アドレスまたはドメインネームシステム（DNS）名を入力します。 • [Protocol]：[HTTP] または [FTP] を選択します。 • [Port]：アクセスポート番号を入力します。
ログイン情報	• [User ID]：サーバーへのアクセスに必要なユーザー ID を入力します。ユーザー名に使用できるのは、a ～ z、0 ～ 9、.、_、- のみです。 • [Password]：サーバーのアクセスに必要なパスワードを入力します。パスワードに使用できる文字は、a ～ z、A ～ Z、0 ～ 9、_、*、.、+、=、%、 - のみです。 （注） /、?、:、@などの特殊文字やスペースは、URL で使用され、関連するプロトコルでファイルを適切に取得するためのフィールド解析で必要ですが、ユーザー名とパスワードでは使用できません。Cisco vManage リリース 20.9.1 以降では、有効な文字を使用できます。
イメージ情報	• [Image Location Prefix]：アップロードされたイメージを保存するフォルダーパスを入力します • [VPN]：トランスポート VPN、管理 VPN、サービス VPN のいずれかの VPN ID を入力します。

4. [Add] をクリックしてリモートサーバーを追加します。

リモートサーバーの管理

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Repository]**の順に選択します。
2. 目的のリモートサーバーで、[…] をクリックします。
3. リモートサーバーの設定を表示するには、[View Details] をクリックします。
4. リモートサーバーの設定を編集するには、[Edit] をクリックします。必要に応じて次の設定を編集し、[Save] をクリックします。

（注） リモートサーバー上のソフトウェアイメージの場所を Cisco vManage ソフトウェアリポジトリに追加している場合、リモートサーバーの設定を編集することはできません。リモートサーバーの設定を編集するには、ソフトウェアリポジトリからソフトウェアイメージのエントリを削除してから、設定を編集します。

サーバー情報	• [Server Name]：サーバー名を入力します。 • [Server IP] または [DNS Name]：サーバーの IP アドレスまたはドメインネームシステム（DNS）名を入力します。 • [Protocol]：[HTTP] または [FTP] を選択します。 • [Port]：アクセスポート番号を入力します。
クレデンシャル	• [User ID]：サーバーへのアクセスに必要なユーザー ID を入力します。ユーザー名に使用できるのは、a ～ z、0 ～ 9、.、_、- のみです。 • [Password]：サーバーのアクセスに必要なパスワードを入力します。パスワードに使用できる文字は、a ～ z、A ～ Z、0 ～ 9、_、*、.、+、=、%、 - のみです。 （注） /、?、:、@ などの特殊文字やスペースは、URL で使用され、関連するプロトコルでファイルを適切に取得するためのフィールド解析で必要ですが、ユーザー名とパスワードでは使用できません。Cisco vManage リリース 20.9.1 以降では、有効な文字を使用できます。
イメージ情報	• [Image Location Prefix]：アップロードされたイメージを保存するフォルダーパスを入力します • [VPN]：トランスポート VPN、管理 VPN、サービス VPN のいずれかの VPN ID を入力します。

5. リモートサーバーを削除するには、[Remove] をクリックします。ダイアログボックスで、リモートサーバーを削除することを確認します。

（注） リモートサーバーを削除する前に、Cisco vManage ソフトウェアリポジトリに追加したリモートサーバーのソフトウェアイメージのエントリがある場合は削除します。

リポジトリへのソフトウェアイメージの追加

エッジデバイス、Cisco vSmart コントローラ、または Cisco vManage のソフトウェアを新しいソフトウェアバージョンにアップグレードする前に、ソフトウェアイメージを Cisco vManage ソフトウェアリポジトリに追加する必要があります。リポジトリを使用して、ローカルの Cisco vManage サーバーにソフトウェアイメージを保存したり、リモートファイルサーバーに保存されているソフトウェアイメージの場所を追加したりできます。

Cisco vManage のソフトウェアリポジトリでは、次の 3 つの方法でイメージを保存できます。

- ローカルの Cisco vManage サーバーに保存後、コントロールプレーン接続経由でダウンロード：ソフトウェアイメージはローカルの Cisco vManage サーバーに保存されてから、コントロールプレーン接続経由で Cisco SD-WAN デバイスにダウンロードされます。通常、受信側デバイスはコントロールプレーン接続を介して受信できるデータトラフィックの量をスロットリングします。そのため、大容量ファイルの場合、Cisco vManage サーバーはデバイスへのソフトウェアインストールが正しく実行されていても、それを監視できない場合があります。
- ローカルの Cisco vManage サーバーに保存後、アウトオブバンド接続経由でダウンロード：ソフトウェアイメージはローカルの Cisco vManage サーバーに保存されてから、アウトオブバンド管理接続経由で Cisco SD-WAN デバイスにダウンロードされます。この方法を使用する場合、イメージをソフトウェアリポジトリにコピーするときに、アウトオブバンド管理インターフェイスの IP アドレスを指定します。この方法は、ソフトウェア イメージ ファイルが大きい場合に推奨されます。デバイスが実行するスロットリングをバイパスし、Cisco vManage サーバーがソフトウェアのインストールを監視できるためです。
- リモートサーバー上：Cisco vManage リリース 20.7.1 以降では、FTP または HTTP URL を介して到達可能なリモートファイルサーバーにソフトウェアイメージを保存できます。ソフトウェア アップグレード プロセスの一環として、Cisco vManage サーバーはこの URL を Cisco SD-WAN デバイスに送信します。これにより、ファイルサーバーへの接続が確立され、ソフトウェアイメージがダウンロードされます。Cisco SD-WAN のマルチテナント展開では、プロバイダーだけがリモートサーバーを Cisco vManage に登録し、リモートサーバー上のソフトウェアイメージの場所を Cisco vManage リポジトリに追加できます。

（注） Cisco vManage リリース 20.9.1 以降では、リモートサーバーからイメージを手動でダウンロードする際に、次の有効な文字のみが使用されていることを確認してください。

- ユーザー ID：a ～ z、0 ～ 9、.、_、-
- パスワード：a～z、A～Z、0～9、_、*、.、+、=、%、-
- URL 名またはパス：a ～ z、A ～ Z、0 ～ 9、_、*、.、+、=、%、-、:、/、@、?、~

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Repository]**の順に選択します。
2. [Add New Software] をクリックします。
3. ソフトウェアイメージの場所を選択します。

（注） ローカルの Cisco vManage サーバーに NFVIS アップグレードイメージを保存します。

1. ローカルの Cisco vManage サーバーにソフトウェアイメージを保存した後に、コントロールプレーン接続経由で Cisco SD-WAN デバイスにダウンロードするには、[vManage] を選択します。[Upload Software to vManage] ダイアログボックスが開きます。
   1. ソフトウェアイメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックして、ローカルの Cisco vManage サーバーのディレクトリからソフトウェアイメージを選択します。
   2. [Upload] をクリックして、イメージをソフトウェアリポジトリに追加します。
2. リモートの Cisco vManage サーバーにイメージを保存した後に、アウトオブバウンド管理接続経由で Cisco SD-WAN デバイスにダウンロードするには、[Remote Server - vManage] を選択します。[Upload Software to Remote Server - vManage] ダイアログボックスが開きます。
   1. [vManage Hostname/IP Address] フィールドに、管理 VPN（通常は VPN 512）にある Cisco vManage サーバー上のインターフェイスの IP アドレスを入力します。
   2. ソフトウェアイメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックして、ローカルの Cisco vManage サーバーのディレクトリからソフトウェアイメージを選択します。
   3. [Upload] をクリックします。
3. ソフトウェアイメージがリモートサーバーに保存されている場合は、[Remote Server（preferred）] を選択します。[Add New Software via Remote Server] スライドインペインが表示されます。このオプションを選択する前に、リモートサーバーが Cisco vManage に登録されていることを確認してください。
   1. [Image] をクリックして新しいソフトウェアイメージをアップロードするか、[SMU Image] をクリックして SMU イメージをアップロードします。デフォルトでは [Image] が選択されています。
   2. [Remote Server Name] ドロップダウンリストから目的のリモートサーバーを選択します。
   3. [Image Filename]：ファイル拡張子を含むイメージファイル名を入力します。SMU イメージの場合、ファイル拡張子は `.smu.bin` にする必要があります。

4. SMU イメージの場合は、[SMU Defect ID] に正確な SMU 障害 ID を入力し、[SMU Type] に正確な SMU タイプを選択します。間違った 障害 ID や SMU タイプを選択すると、ソフトウェアのアップグレードが失敗する可能性があります。
5. [Save] をクリックします。

ソフトウェアイメージの表示

Cisco vManage のメニューから、**[Maintenance]** > **[Software Repository]**を選択します。

[Software Repository] ウィンドウには、リポジトリ内にあるイメージが表示されます。

[Software Version] 列にはソフトウェアイメージのバージョンが表示され、[Controller Version] 列にはそのソフトウェアバージョンに相当するコントローラソフトウェアのバージョンが表示されます。コントローラバージョンは、サポートされているシスココントローラの最小バージョンです。ソフトウェアイメージは、リストに記載されているコントローラバージョン以上で動作できます。

[Software Location] 列はソフトウェアイメージの保存場所を示します。Cisco vManage サーバーのリポジトリまたはリモートロケーションのリポジトリになります。

[Available Files] 列には、ソフトウェアイメージのファイル名が表示されます。

[Updated On] 列は、ソフトウェアイメージがリポジトリに追加された場合に表示されます。

目的のソフトウェアバージョンの [...] オプションでは、リポジトリからソフトウェアイメージを削除するオプションを選択できます。

Cisco vManage リリース 20.6.x 以前では、2 つ以上の同じバージョンのソフトウェアイメージが、異なるファイル名でアップロードされている場合、イメージは1行で表示されます。[Available Files] 列には、複数のファイル名が表示されます。ソフトウェアイメージを削除する場合、このリストスキームにはデメリットがあります。削除操作を行うと、ソフトウェアバージョンに対応するすべてのソフトウェアイメージが削除されるためです。

Cisco vManage リリース 20.7.1 では、2 つ以上の同じバージョンのソフトウェアイメージが異なるファイル名でアップロードされている場合、各ソフトウェアイメージが個別の行に表示されます。これにより、特定のソフトウェアイメージを選択して削除できます。

VNF イメージのアップロード

VNF イメージは Cisco vManage ソフトウェアリポジトリに保存されます。これらの VNF イメージは、サービスチェーンの展開中に参照され、サービスチェーンの接続中に Cisco NFVIS にプッシュされます。

ステップ 1 [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。

ステップ 2 事前にパッケージ化された VNF イメージを追加するには、[Virtual Images] をクリックしてから、[Upload Virtual Image] をクリックします。

ステップ 3 仮想イメージを保存する場所を選択します。

- 仮想イメージをローカルの Cisco vManage サーバーに保存し、コントロールプレーン接続を介して CSP デバイスにダウンロードするには、[vManage] をクリックします。[Upload VNF's Package to vManage] ダイアログボックスが表示されます。

  1. 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco vManage サーバーから仮想イメージを選択します。例：CSR.tar.gz、ASAv.tar.gz、または ABC.qcow2

  2. ファイルをアップロードする場合は、アップロードするファイルのタイプ（**イメージパッケージ**または**スキャフォールド**）を指定します。必要に応じて、ファイルの説明を指定し、カスタムタグをファイルに追加します。タグは、サービスチェーンを作成するときに、イメージとスキャフォールドファイルをフィルタリングするために使用できます。

  3. qcow2 イメージファイルをアップロードする場合は、サービスまたは VNF タイプ（**FIREWALL** または **ROUTER**）を指定します。必要に応じて、以下を指定します。

     - イメージの説明
     - イメージのバージョン番号
     - Checksum
     - Hash algorithm

     また、サービスチェーンの作成時にイメージやスキャフォールドファイルをフィルタリングするために使用できるカスタムタグをファイルに追加することもできます。

     （注）
     - qcow2 イメージファイルを選択した場合は、スキャフォールドファイルをアップロードする必要があります。
     - qcow2 イメージファイルを選択するオプションは、Cisco vManage リリース 20.7.1 以降で利用できます。Cisco vManage リリース 20.6.1 以前のリリースでは、tar.gz ファイルのみを選択できます。

  4. [Upload] をクリックして、イメージを仮想イメージリポジトリに追加します。仮想イメージリポジトリテーブルには、追加された仮想イメージが表示され、CSP デバイスにインストールできるようになります。

- イメージをリモート Cisco vManage サーバーに保存してから CSP デバイスにダウンロードするには、[Remote Server - vManage] をクリックします。[Upload VNF's Package to Remote Server-vManage] ダイアログボックスが表示されます。

  1. [vManage Hostname/IP Address] フィールドに、管理 VPN（通常は VPN 512）にある Cisco vManage サーバー上のインターフェイスの IP アドレスを入力します。

  2. 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco vManage サーバーから仮想イメージを選択します。

3. ファイルをアップロードする場合は、アップロードするファイルのタイプ（**イメージパッケージ**または**スキャフォールド**）を指定します。必要に応じて、ファイルの説明を指定し、カスタムタグをファイルに追加します。タグは、サービスチェーンを作成するときに、イメージとスキャフォールドファイルをフィルタリングするために使用できます。
4. qcow2 イメージファイルをアップロードする場合は、サービスまたは VNF タイプ（**FIREWALL** または **ROUTER**）を指定します。必要に応じて、以下を指定します。
   - イメージの説明
   - イメージのバージョン番号
   - Checksum
   - Hash algorithm

   また、サービスチェーンの作成時にイメージやスキャフォールドファイルをフィルタリングするために使用できるカスタムタグをファイルに追加することもできます。

   （注）
   - qcow2 イメージファイルを選択した場合は、スキャフォールドファイルをアップロードする必要があります。
   - qcow2 イメージファイルを選択するオプションは、Cisco vManage リリース 20.7.1 以降で利用できます。Cisco vManage リリース 20.6.1 以前のリリースでは、tar.gz ファイルのみを選択できます。

5. [Upload] をクリックして、イメージを仮想イメージリポジトリに追加します。仮想イメージリポジトリテーブルには、追加された仮想イメージが表示され、CSP デバイスにインストールできるようになります。

同じベンダーまたは異なるベンダーのファイアウォールなど、複数の VNF エントリを持つことができます。また、同じ VNF のリリースに基づく異なるバージョンの VNF を追加することもできます。ただし、VNF 名が一意であることを確認してください。

カスタマイズされた VNF イメージの作成

始める前に

ルートディスクイメージに加えて、入力ファイルとして 1 つ以上の qcow2 イメージを VM 固有のプロパティ、ブートストラップ構成ファイル（存在する場合）とともにアップロードし、圧縮 TAR ファイルを生成できます。カスタムパッケージを使用すると、次のことができます。

- イメージプロパティとブートストラップファイル（必要な場合）とともにカスタム VM パッケージを TAR アーカイブファイルに作成します。
- カスタム変数をトークン化し、ブートストラップ構成ファイルで渡されるシステム変数を適用します。

次のカスタムパッケージの要件が満たされていることを確認します。

- VNF のルートディスクイメージ：qcow2
- Day-0 構成ファイル：システム変数とトークン化されたカスタム変数
- VM 構成：CPU、メモリ、ディスク、NIC
- HA モード：VNF が HA をサポートしている場合は、Day-0 のプライマリファイルとセカンダリファイル、HA リンクの NIC を指定します。
- 追加のストレージ：より多くのストレージが必要な場合は、事前定義されたディスク（qcow2）、ストレージボリューム（NFVIS レイヤ）を指定します。

ステップ 1 [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。

ステップ 2 **[Virtual Images]** > [Add Custom VNF Package] をクリックします。

ステップ 3 次の VNF パッケージプロパティを使用して VNF を構成し、[Save] をクリックします。

表 *29 : VNF* パッケージのプロパティ

フィールド	必須またはオプション	説明
Package Name	必須	ターゲット VNF パッケージのファイル名。これは、.tar または .gz 拡張子が付いた Cisco NFVIS イメージ名です。
App Vendor	必須	Cisco VNF またはサードパーティの VNF。
Name	必須	VNF イメージの名前。
Version	オプション	プログラムのバージョン番号。
Type	必須	選択する VNF のタイプ。 サポートされている VNF タイプは、ルータ、ファイアウォール、ロードバランサ、およびその他です。

ステップ 4 VM qcow2 イメージをパッケージ化するには、[File Upload] をクリックし、qcow2 イメージファイルを参照して選択します。

ステップ 5 VNF のブートストラップ構成ファイルを選択するには、[Day 0 Configuration] をクリックし、[File Upload] をクリックし、ファイルを参照して選択します。

次の Day-0 構成プロパティを含めます。

表 *30 : Day-0* 構成

フィールド	必須またはオプション	説明
Mount	必須	ブートストラップファイルがマウントされるパス。
Parseable	必須	Day-0 構成ファイルを解析できるかどうか。 オプションは、[Enable] または [Disable] です。デフォルトでは、[Enable] が選択されています。
High Availability	必須	選択する Day-0 構成ファイルのハイアベイラビリティ。 サポートされている値は、スタンドアロン、HA プライマリ、HA セカンダリです。

（注） VNF にブートストラップ構成が必要な場合は、*bootstrap-config* または *day0-config* ファイルを作成します。

ステップ 6 Day-0 構成を追加するには、[Add] をクリックし、[Save] をクリックします。Day-0 構成が [Day 0 Config File] テーブルに表示されます。システム変数とカスタム変数を使用して、ブートストラップ構成変数をトークン化できます。Day-0 構成ファイルの変数をトークン化するには、目的の Day-0 構成ファイルの横にある [View Configuration File] をクリックします。[Day 0 configuration file] ダイアログボックスで、次のタスクを実行します。

（注） ブートストラップ構成ファイルは XML またはテキストファイルで、VNF と環境に固有のプロパティが含まれています。共有 VNF については、『Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide』のトピック「Additional References」でさまざまな VNF タイプに追加する必要があるシステム変数のリストについて参照してください。.

a) システム変数を追加するには、[CLI configuration] ダイアログボックスで、テキストフィールドからプロパティを選択して強調表示します。[System Variable] をクリックします。[Create System Variable] ダイアログボックスが表示されます。
b) [Variable Name] ドロップダウンリストからシステム変数を選択し、[Done] をクリックします。強調表示されたプロパティは、システム変数名に置き換えられます。
c) カスタム変数を追加するには、[CLI configuration] ダイアログボックスで、テキストフィールドからカスタム変数属性を選択して強調表示します。[Custom Variable] をクリックします。[Create Custom Variable] ダイアログボックスが表示されます。
d) カスタム変数名を入力し、[Type] ドロップダウンリストからタイプを選択します。
e) カスタム変数属性を設定するには、次の手順を実行します。
   - サービスチェーンの作成時にカスタム変数が必須になるようにするには、[Mandatory] の横にある [Type] をクリックします。

- VNF にプライマリとセカンダリの Day-0 ファイルの両方が含まれるようにするには、[Common] の横にある [Type] をクリックします。

f) [完了（Done）] をクリックしてから、[保存（Save）] をクリックします。強調表示されたカスタム変数属性は、カスタム変数名に置き換えられます。

ステップ 7 追加の VM イメージをアップロードするには、[Advance Options] を展開し、[Upload Image] をクリックして、追加の qcow2 イメージファイルを参照して選択します。ルートディスク、エフェメラルディスク 1、またはエフェメラルディスク 2 を選択し、[Add] をクリックします。新しく追加された VM イメージが [Upload Image] テーブルに表示されます。

（注） 追加の VM イメージをアップロードするときは、エフェメラルディスクとストレージボリュームを組み合わせないようにしてください。

ステップ 8 ストレージ情報を追加するには、[Add Storage] を展開し、[Add volume] をクリックします。次のストレージ情報を入力し、[Add] をクリックします。追加されたストレージの詳細が [Add Storage] テーブルに表示されます。

表 *31* : ストレージのプロパティ

フィールド	必須またはオプション	説明
Size	必須	VM 操作に必要なディスクサイズ。サイズ単位が GiB の場合、最大ディスクサイズは 256 GiB です。
Size Unit	必須	サイズ単位を選択します。 サポートされる単位は、MIB、GiB、TiB です。
Device Type	オプション	ディスクまたは CD-ROM を選択します。デフォルトでは、ディスクが選択されています。
Location	オプション	ディスクまたは CD-ROM の場所。デフォルトでは、ローカルです。
Format	オプション	ディスクイメージ形式を選択します。 サポートされている形式は、qcow2、raw、および vmdk です。デフォルトでは、raw です。

フィールド	必須またはオプション	説明
Bus	オプション	ドロップダウンリストから値を選択します。 バスでサポートされる値は、virtio、scsi、および ide です。デフォルトでは、virtio です。

ステップ 9 VNF イメージのプロパティを追加するには、[Image Properties] を展開し、次のイメージ情報を入力します。

表 *32 : VNF* イメージのプロパティ

フィールド	必須またはオプション	説明
SR-IOV Mode	必須	SR-IOV サポートを有効または無効にします。デフォルトでは有効になっています。
Monitored	必須	ブートストラップできる VM の VM ヘルスモニタリング。 オプションは enable または disable です。デフォルトでは有効になっています。
Bootup Time	必須	モニタリング対象 VM のモニタリングタイムアウト期間。デフォルトは 600 秒です。
Serial Console	オプション	サポートされているまたはされていないシリアルコンソール。 オプションは enable または disable です。デフォルトでは無効になっています。
Privileged Mode	オプション	プロミスキャスモードやスヌーピングなどの特別な機能を許可します。 オプションは enable または disable です。デフォルトでは無効になっています。

フィールド	必須またはオプション	説明
Dedicate Cores	必須	VM の低遅延（ルータやファイアウォールなど）を補う専用リソース（CPU）の割り当てを容易にします。それ以外の場合は、共有リソースが使用されます。 オプションは enable または disable です。デフォルトでは有効になっています。

ステップ 10 VM リソース要件を追加するには、[Resource Requirements] を展開し、次の情報を入力します。

表 *33 : VM* リソース要件

フィールド	必須またはオプション	説明
Default CPU	必須	VM でサポートされる CPU。サポートされる CPU の最大数は 8 です。
Default RAM	必須	VM でサポートされる RAM。RAM の範囲は 2 ～ 32 です。
Disk Size	必須	VM でサポートされるディスクサイズ（GB）。ディスクサイズの範囲は 4 ～ 256 です。
Max number of VNICs	オプション	VM に許可される VNIC の最大数。VNIC の数は 8 ～ 32 の範囲で指定でき、デフォルトの値は 8 です。
Management VNIC ID	必須	管理インターフェイスに対応する管理 VNIC ID。有効な範囲は、0 から VNIC の最大数までです。
Number of Management VNICs ID	必須	VNIC の数。
High Availability VNIC ID	必須	ハイアベイラビリティが有効になっている VNIC ID。有効な範囲は、0 から VNIC の最大数までです。管理 VNIC Id と競合してはなりません。デフォルトでは、値は 1 になっています。

フィールド	必須またはオプション	説明
Number of High Availability VNICs ID	必須	ハイアベイラビリティが有効になっている VNIC ID の最大数。有効な範囲は 0 ～（VNIC の最大数 - 管理 VNIC の数 - 2）で、デフォルトの値は 1 です。

ステップ 11 Day-0 構成ドライブオプションを追加するには、[Day 0 Configuration Drive options] を展開し、次の情報を入力します。

表 *34 : Day-0* 構成ドライブオプション

フィールド	必須またはオプション	説明
Volume Label	必須	Day-0 構成ドライブのボリュームラベル。 オプションは、V1 または V2 です。デフォルトでは、オプションは V2 です。V2 は、構成ドライブラベル config-2 です。V1 は、構成ドライブラベル cidata です。
Init Drive	オプション	マウント時のディスクとしての Day-0 構成ファイル。デフォルトのドライブは CD-ROM です。
Init Bus	オプション	初期バスを選択します。 バスでサポートされる値は、virtio、scsi、および ide です。デフォルトでは、ide です。

ソフトウェア リポジトリ テーブルにはカスタマイズされた VNF イメージが表示され、カスタムサービスチェーンを作成するときにイメージを選択できます。

VNF イメージの表示

ステップ 1 [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。

ステップ 2 [Virtual Images] をクリックします。

ステップ 3 検索結果をフィルタリングするには、検索バーのフィルタオプションを使用します。

[Software Version] 列には、ソフトウェアイメージのバージョンが表示されます。

[Software Location] 列は、ソフトウェアイメージが保存されている場所を示します。ソフトウェアイメージは、Cisco vManage サーバー上のリポジトリまたはリモートロケーションのリポジトリに格納できます。

[Version Type Name] 列には、ファイアウォールのタイプが表示されます。

[Available Files] 列には、VNF イメージファイル名が一覧表示されます。

[Update On] 列は、ソフトウェアイメージがリポジトリに追加された場合に表示されます。

ステップ 4 該当するイメージで […] をクリックし、[Show Info] を選択します。

リポジトリからのソフトウェアイメージの削除

Cisco vManage のソフトウェアリポジトリからソフトウェアイメージを削除するには、次の手順を実行します。

ステップ 1 Cisco vManage のメニューから、**[Maintenance]** > **[Software Repository]**を選択します。

ステップ 2 目的のソフトウェアイメージで […] をクリックし、[Delete] を選択します。

ソフトウェアイメージをルータにダウンロードしている場合、ダウンロードプロセスが完了するまでイメージを削除することはできません。

VNF イメージの削除

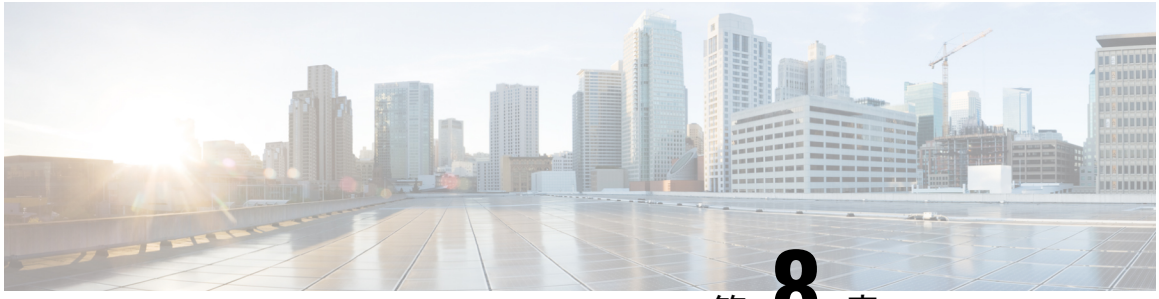
ステップ 1 [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。

ステップ 2 [Virtual Images] をクリックします。リポジトリ内のイメージが表に表示されます。

ステップ 3 目的のイメージの […] をクリックし、[Delete] を選択します。

（注） VNF イメージをデバイスにダウンロードしている場合、ダウンロードプロセスが完了するまで VNF イメージを削除することはできません。

（注） VNF イメージがサービスチェーンによって参照されている場合、それを削除することはできません。



第 8 章

ソフトウェアアップグレードワークフロー

表 *35* : 機能の履歴

機能名	リリース情報	説明
ソフトウェア アップグレード ワークフロー	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1 Cisco SD-WAN リリース 20.8.1	この機能により、Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス のソフトウェアイメージをアップグレードし、ソフトウェアアップグレードのステータスを監視するためのガイド付きワークフローが導入されます。 このワークフローでは、新しいソフトウェアイメージのダウンロード、インストール、およびアクティブ化を個別に実行することも、一括で実行することもできます。
ソフトウェア アップグレード ワークフローのスケジュール	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1 Cisco SD-WAN リリース 20.9.1	この機能には、Cisco vManage を使用してエッジデバイスのソフトウェアアップグレードをスケジュールするオプションが導入されています。
追加プラットフォームのソフトウェアアップグレードワークフローのサポート	Cisco vManage リリース 20.9.1	Cisco Enterprise NFV インフラストラクチャ ソフトウェア（NFVIS）および Cisco Catalyst セルラーゲートウェイのサポートが追加されました。

- ソフトウェア アップグレード ワークフローについて （172 ページ）
- ソフトウェア アップグレード ワークフローのサポート対象デバイス （172 ページ）

ソフトウェア アップグレード ワークフローについて

ソフトウェア アップグレード ワークフローを使用すると、サポート対象の各種シスコデバイスでソフトウェアイメージをダウンロードしてアップグレードできます。また、アップグレードプロセスを適時スケジュールするオプションもあります。ワークフローには、ソフトウェアアップグレードのステータスも示されます。このワークフローには、ソフトウェアアップグレードを実行するための2つのオプションが用意されています。**ダウンロードとアップグレード**、および**ダウンロードのみ**です。

ソフトウェア アップグレード ワークフロー のメリット

- ソフトウェア アップグレード ワークフローは、デバイスアップグレードのステータスを表示することで、デバイスソフトウェアのアップグレード時のさまざまなエラーを防ぐのに役立ちます。たとえば、アップグレードプロセスの特定の段階でエラーが発生した場合、ワークフローでは**エラー**のフラグが立てられます。
- このワークフローでは、新しいソフトウェアイメージのダウンロード、インストール、およびアクティブ化を個別に実行することも、一括で実行することもできます。また、ワークフローを随時スケジュールすることもできます。

ソフトウェアアップグレードワークフローのサポート対象デバイス

デバイス	サポート対象の最小リリース	注
Cisco IOS XE SD-WAN デバイスについて	Cisco vManage： Cisco vManage リリース 20.8.1 デバイス：Cisco IOS XE リリース 17.8.1a	Cisco IOS XE リリース 17.9.1a 以降では、ソフトウェアのアップグレードをスケジュールできます。
Cisco vEdge デバイスについて	Cisco vManage： Cisco vManage リリース 20.8.1 デバイス：Cisco SD-WAN リリース 20.8.1	Cisco SD-WAN リリース 20.9.1 以降では、ソフトウェアアップグレードのスケジュール機能を使用できます。

デバイス	サポート対象の最小リリース	注
Cisco Catalyst 8200 uCPE シリーズ エッジ プラットフォーム	Cisco vManage： Cisco vManage リリース 20.9.1 デバイス：Cisco IOS XE リリース 17.9.1a	なし
Cisco 5400 シリーズ エンタープライズ ネットワーク コンピューティング システム（ENCS）	Cisco vManage： Cisco vManage リリース 20.9.1 デバイス：Cisco IOS XE リリース 17.9.1a	なし
Cisco Catalyst セルラーゲートウェイ	Cisco vManage： Cisco vManage リリース 20.9.1 デバイス：Cisco IOS CG リリース 17.9.1	ソフトウェアアップグレードのスケジュール機能は使用できません。

ソフトウェアアップグレードワークフロー使用の前提条件

ソフトウェアアップグレードワークフロー機能を使用するために必要なソフトウェアバージョンがシスコデバイスで実行されていることを確認します。それぞれのデバイス要件については、「ソフトウェアアップグレードワークフローのサポート対象デバイス（172ページ）」を参照してください。

ソフトウェアアップグレードワークフローへのアクセス

はじめる前に

進行中のソフトウェア アップグレード ワークフローがあるかどうかを確認するには、次の手順を実行します。

Cisco vManage のツールバーから、[Task-list] アイコンをクリックします。Cisco vManage には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。

ソフトウェア アップグレード ワークフローへのアクセス

1. Cisco vManage のメニューで**[Workflows]** > **[Workflow Library]**を選択します。

（注） Cisco vManage リリース 20.8.1 では、[Workflow Library] のタイトルは [Launch Workflows] になります。

2. **[Library]** > **[Software Upgrade]**を選択して、新しいソフトウェア アップグレード ワークフローを開始します。

   または

   [In-progress] > **[Software Upgrade]**を選択して、進行中のソフトウェア アップグレード ワークフローを再開します。

3. 画面の指示に従って、新しいソフトウェア アップグレード ワークフローを開始します。

（注） [Exit]をクリックして進行中のソフトウェアアップグレードワークフローを終了します。進行中のワークフローを随時再開できます。

（注） マルチノードクラスタ構成の場合、デバイスのアップグレード中に制御接続が Cisco vManage から別のノードに切り替わると、NetConf セッションタイムアウトが原因でアップグレードが影響を受ける可能性があります。次に、デバイスは別のノードへの制御接続を確立します。アップグレード アクティビティを再度トリガーする必要があります。

ソフトウェア アップグレード ワークフローのステータスの確認

ソフトウェア アップグレード ワークフロー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 のツールバーから [Task-list] アイコンをクリックします。

   Cisco vManage には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。

2. [+] アイコンをクリックして、タスクの詳細を表示します。

   Cisco vManage でペインが開き、タスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

ソフトウェアアップグレードワークフローのスケジュール

Cisco vManage リリース 20.9.1 で導入されたソフトウェア アップグレード ワークフローのスケジューラを使用すると、ワークフローを適時スケジュールし、ソフトウェア アップグレード プロセスによるダウンタイムを回避できます。スケジューラを使用すると、アップグレード ワークフローを**今すぐ**または**後で**実行するかをスケジュールできます。後でアップグレードを実行するようにスケジュールする場合は、**開始日**、**開始時刻**、および**タイムゾーンの選択**を入力できます。

ソフトウェア アップグレード ワークフローのスケジュール

次の手順を使用して、ソフトウェア アップグレード ワークフローをスケジュールします。

1. Cisco vManage のメニューで**[Workflows]** > **[Workflow Library]**を選択します。

   または

   Cisco vManage リリース 20.9.1 以降では、**[Workflows]** > **[Popular Workflows]** > **[Software Upgrade]** をクリックします。.

2. **[Workflow Library]** > **[Software Upgrade]**を選択して、新しいソフトウェア アップグレード ワークフローを開始します。

   または

   [In-progress] > **[Software Upgrade]**を選択して、進行中のソフトウェア アップグレード ワークフローを再開します。

3. [Scheduler] セクションで、[Later] を選択します。

（注） 選択したデバイスのソフトウェアアップグレードをすぐに実行するには、[Now] オプションを使用します。

4. [Start Date]、[Start Time]、[Select Timezone] を選択します。

（注） 開始日時は、常に Cisco vManage サーバーの日時よりも後にする必要があります。

5. [Next] をクリックします。
6. ソフトウェア アップグレード ワークフローがスケジュールされています。

スケジュールしたソフトウェアアップグレードワークフローのキャンセル

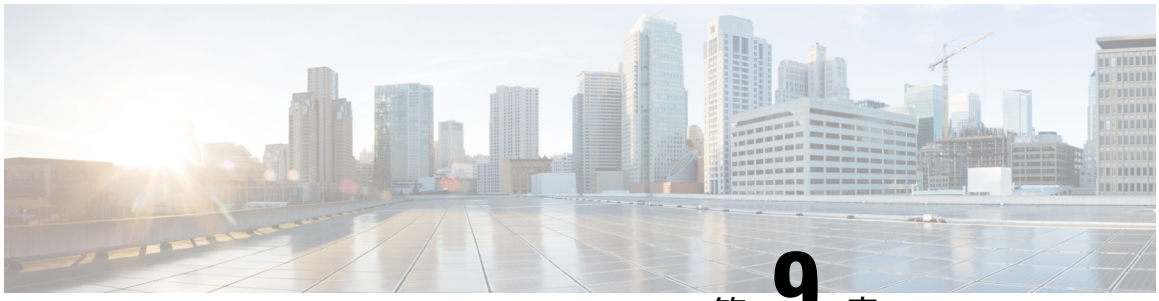
スケジュールしたソフトウェア アップグレード ワークフローをキャンセルするには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Maintenance]** > **[Software Upgrade]**をクリックします。
2. デバイスのリストから、ソフトウェアアップグレードがスケジュールされているデバイスを選択します。
3. [Cancel Software Upgrade] をクリックします。

ダウンロードしたソフトウェアイメージの削除

Cisco IOS XE SD-WAN デバイス と Cisco vEdge デバイス からダウンロードしたソフトウェアイメージを削除するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. [WAN Edge] をクリックします。
3. [Delete Downloaded Images] をクリックします。
4. [Delete Downloaded Images] ダイアログボックスで、削除するイメージを選択します。
5. [Delete] をクリックします。



第 9 章

接続障害管理について

表 *36* : 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス におけるイーサネット接続障害管理サポート	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	イーサネット接続障害管理機能は、キャリア イーサネット ネットワーク リンクのモニタリングに役立ちます。

イーサネット CFM について

イーサネット接続障害監理（CFM）は、サービスインスタンスごとのエンドツーエンド イーサネット レイヤの運用、保守、管理プロトコルです。大規模なイーサネット メトロポリタン エリア（MAN）およびワイドエリアネットワーク（WAN）向けのプロアクティブな接続モニタリング、障害検証、および障害分離機能が組み込まれています。サービスプロバイダーのネットワークは大規模で複雑であり、幅広いユーザーベースがありますOAM プロトコルは、障害を切り分け、タイムリーに障害に対処するのに役立ちます。

Cisco SD-WAN での CFM の仕組み

プロバイダーエッジルータと顧客宅内機器（CPE）がキャリア イーサネット ネットワークを介して接続されているネットワークでは、リンクの切断を監視する必要があります。キャリア イーサネット ネットワークで CFM がサポートされているため、CFM メッセージがプロバイダーエッジと CPE 間で交換され、CFM プロトコルはプロバイダーエッジがネットワーク内のリンク障害を認識できるようにします。

Cisco SD-WAN の CFM は、次のインターフェイスタイプでサポートされています。

- VDSL インターフェイス
- SHDSL インターフェイス
- GigabitEthernet インターフェイス

次のコンポーネントは、Cisco SD-WAN で CFM の機能をサポートします。

ダウン メンテナンス エンド ポイント

メンテナンスドメインは、ネットワークの管理を行うための管理空間です。ドメインは、単一のエンティティによって所有および運用され、一連の内部ドメインポートとその境界によって定義されます。メンテナンスアソシエーションとは、メンテナンスドメイン内で一意に識別されるサービスを指します。CFM プロトコルは、メンテナンス アソシエーション内で動作します。

メンテナンスエンドポイント（MEP）は、メンテナンスドメイン内でCFMに参加するインターフェイス上の境界点です。MEP より低いレベルのフレームはすべて廃棄され、高いレベルのフレームはすべて転送されます。MEP はメンテナンスドメイン（レベル）およびサービス（S-VLANまたはイーサネット仮想回線（EVC））ごとに定義されます。ドメインのエッジに存在して境界を定義し、CFM メッセージをその境界内に限定します。MEP は CFM 連続性チェックメッセージ（CCM）をプロアクティブに送信し、管理者の要求に応じてトレースルートとループバックメッセージを送信できます。

ダウンMEPは、MEPが設定されているポートに接続された回線を経由して、CFMフレームを送受信します。リレー側からのCFMフレームの場合、ダウンMEPはそのレベル以下のフレームを破棄します。回線側からCFMフレームを受信した場合、ダウンMEPは他の下位レベルのダウン MEP へのトラフィックを除いて、同じレベルのすべてのフレームは処理し、それより低いレベルのフレームは廃棄します。より高いレベルの CFM フレームはすべて、リレー側と回線側のどちらから受信した場合も、透過的に転送します。

サブインターフェイスごとにダウン MEP を展開するには、最初に EVC+VLAN メンテナンスアソシエーションを作成し、サブインターフェイスで VLAN ID を設定してから、そのサブインターフェイスの親インターフェイスでダウン MEP を設定する必要があります。

イーサネット CFM とイーサネット OAM の相互作用

イーサネット仮想回線

Metro Ethernet Forumによって定義されているように、イーサネット仮想回線（EVC）は、ポートレベルのポイントツーポイントまたはマルチポイントツーマルチポイントのレイヤ2回線です。エッジデバイスはEVC ステータスを使用して、サービス プロバイダー ネットワークへの代替パスを検索したり、場合によっては、イーサネット経由や非同期転送モード（ATM）などの別の代替サービス経由でバックアップパスにフォールバックしたりします。

OAM マネージャ

OAMマネージャは、OAMプロトコル間でデータのやりとりを効率化するためのインフラストラクチャ要素です。OAMマネージャには、2つのインターワーキングOAMプロトコル（ここ

では、イーサネット CFM とイーサネット OAM）が必要です。相互作用は、OAM マネージャから CFM プロトコルへの単方向で、ユーザ ネットワーク インターフェイス（UNI）のポートステータス情報のみが交換されます。その他に、次のポートステータスの値を利用できます。

- REMOTE_EE：リモート超過エラー
- LOCAL_EE：ローカル超過エラー
- TEST：リモートまたはローカル ループバック

CFM は、ポート ステータス情報を受信した後、CFM ドメイン全体にこのステータスを伝達します。

SNMP トラップ

MEP は 2 種類の Simple Network Management Protocol（SNMP）トラップを生成します。連続性チェック（CC）トラップとクロスチェックトラップです。

連続性チェックトラップ：

- MEP up：新しい MEP が検出されたとき、リモートポートのステータスが変更されたとき、または検出済みの MEP との接続が中断後、回復したときに送信されます。
- MEP down：タイムアウトまたは last gasp イベントの発生時に送信されます。
- Cross-connect：サービス ID が VLAN と一致しない場合に送信されます。
- Loop：MEP が独自の連続性チェックメッセージ（CCM）を受信したときに送信されます。
- Configuration error：MEP が重複する MPID を持つ連続性チェックを受信したときに送信されます。

クロスチェックトラップ：

- Service up：予定のリモート MEP が、すべて時間どおりに起動した場合に送信されます。
- MEP missing：予定の MEP がダウンしている場合に送信されます。
- Unknown MEP：予期しない MEP から CCM が受信された場合に送信されます。

イーサネット CFM の設定に関する制約事項

- CFM は Cisco vManage の CLI を介してのみ設定できます。したがって、CFM 実行ファイルにアクセスして、デバイスの SSH ターミナルにおけるリンク障害の検出、検証、および分離に対応できます。
- UP MEP およびメンテナンス中間ポイント（MIP）はサポートされていません。
- CFM によるレイヤ 2 トレースルートや ping などの CFM トラブルシューティング機能は、Cisco vManage でサポートされていません。この機能はデバイス上でのみ実行できます。

Cisco vManage の CLI テンプレートを使用したイーサネット CFM の設定

次のコマンドを使用して、イーサネット CFM を設定します。

1. CFM の CFM IEEE バージョンを有効にする場合：

   Device(config)# **ethernet cfm ieee**

2. デバイスの CFM 処理をグローバルに有効にする場合：

   Device(config)# **ethernet cfm global**

3. トレースルートメッセージによって取得された CFM データのキャッシングを有効にする場合：

   Device(config)# **ethernet cfm traceroute cache**

4. イーサネット CFM の syslog メッセージを有効にする場合：

   Device(config)# **ethernet cfm logging**

5. イーサネット CFM 連続性チェックイベントで SNMP トラップの生成を有効にする場合：

   Device(config)# **snmp-server enable traps ethernet cfm cc**

6. 静的に設定された MEP と CCM 経由で取得された MEP の間でのクロスチェック操作に関連した、イーサネット CFM 連続性チェックイベントで、SNMP トラップの作成を有効にする場合：

   csnmp-server enable traps ethernet cfm crosscheck

7. EVC を定義し、EVC コンフィギュレーション モードを開始する場合：

   Device(config)# **ethernet evc *evc-id***

8. 特定のメンテナンスレベルで CFM メンテナンスドメインを定義し、CFM コンフィギュレーション モードに切り替える場合：

   Device(config)# **ethernet cfm domain *domain-name* level *level-id***

9. 送信元 ID TLV とネイバー デバイスのタイプ、長さ、値などの属性を指定する場合：

   Device(config)# **sender-id chassis**

10. メンテナンスドメイン内にメンテナンスアソシエーションを設定し、イーサネット CFM サービスのコンフィギュレーション モードに切り替える場合：

    Device(config-ecfm)# **service *short-ma-name* evc *evc-name* vlan *vlanid* direction down**

11. オフロードサンプリングを設定する場合：

    Device(config)# **offload sampling *sample***

12. CCM の送信を有効にする場合：

    Device(config-ecfm-srv)# **continuity-check**

13. CCM の送信間隔を設定する場合（デフォルトの間隔は 10 秒）：

    Device(config-ecfm-srv)# **continuity-check [interval *cc-interval*]**

14. インターフェイスで MEP ドメインと ID を設定する場合：

    Device(config)# **interface *interface-name***

    Device(config-if)# **cfm mep domain *domain-name* mpid *id* service *service-name***

各コマンドの実行目的の詳細については、『Configuring Ethernet CFM』[英語] を参照してください。

設定例

次の設定例は、EVC+VLAN メンテナンス アソシエーションのサブインターフェイスごとに CFM を設定する方法を示しています。

```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet evc USER-SERVICE
 !
 ethernet cfm domain USER level 7
  service USER-SERVICE evc USER-SERVICE vlan 112 direction down
   continuity-check
   continuity-check interval 10s
   continuity-check loss-threshold 3
 !
 ethernet cfm logging
 !
 interface GigabitEthernet0/0/1
  no ip address
  speed 100
  no negotiation auto
  ethernet cfm mep domain USER mpid 1562 service USER-SERVICE
   cos 2
 !
 interface GigabitEthernet0/0/1.112
  description NAME 2286884663
   encapsulation dot1Q 112
   ip address 192.0.2.1 255.255.255.0
```

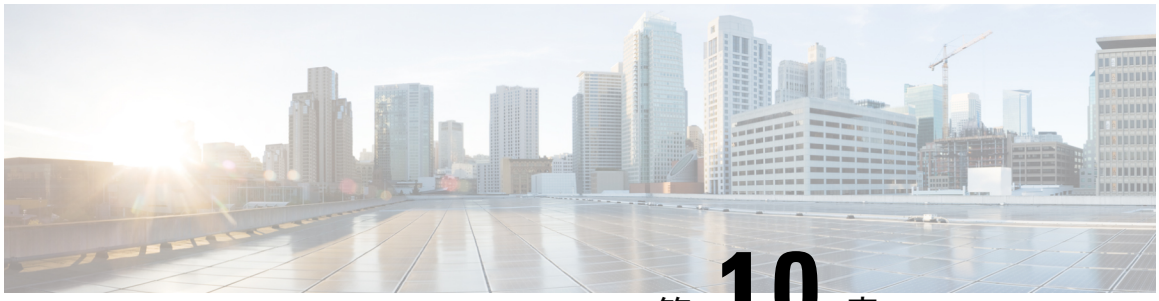
次の設定例は、ポート メンテナンス アソシエーションの物理インターフェイスごとに CFM を設定する方法を示しています。

```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet cfm traceroute cache
 ethernet cfm domain USER level 1
  sender-id chassis
  service USER-SERVICE port
   continuity-check
   continuity-check interval 1m
   sender-id chassis
```

```
!
ethernet cfm logging
!
interface Ethernet0/1/0
 no ip address
 load-interval 30
 speed [10/100/1000]
 duplex [half/full]
 ethernet oam mode passive
 ethernet oam remote-loopback supported
 ethernet oam
 ethernet cfm mep domain USER mpid 101 service USER-SERVICE
  alarm notification all
!
interface Ethernet0/1/0.101
 encapsulation dot1Q 101
 pppoe enable group global
 pppoe-client dial-pool-number 1
 no cdp enable
 ethernet loopback permit external
```

この設定は、Cisco vManage の CLI テンプレートおよび CLI アドオンテンプレートで使用できます。

Cisco vManage の CLI アドオンテンプレートの詳細については、「Create a CLI Add-On Feature Template」[英語] を参照してください。



第 10 章

トラブルシューティング

一般的なセルラーインターフェイス問題のトラブルシュート

セルラーインターフェイスの問題解決

ここでは、ルータからセルラーネットワークへのセルラー接続で発生する最も一般的な問題やエラーメッセージ、およびそれらを解決する手順について説明します。

無線信号強度が不十分

問題に関する説明

ルータのセルラーモジュールが、サービス プロバイダー ネットワークからの無線信号を検出できない。

問題の特定

- [Cisco vManage Cellular Status] 画面、**show cellular status** CLI コマンド、[Cellular Radio] 画面、**show cellular radio** コマンドで、「no signal」、「poor」、または「good」と表示されます。信号強度は「excellent」である必要があります。信号強度の範囲を次の表で示します。

表 37 :

信号	Excellent	Good	Fair	Poor	No Signal
受信信号強度インジケータ（RSSI）	> –58 dBm	–81 ～ –58 dBm	—	–82 ～ –95 dBm	< –96 dBm

信号	Excellent	Good	Fair	Poor	No Signal
基準の受信信号強度（RSRP）	–44 ～ –90 dBm	–91 ～ –105 dBm	–106 ～ –120 dBm	–121 ～ –140 dBm	< –140 dBm
基準の受信信号品質（RSRQ）	–3 ～ –8 dB	–9 ～ –12 dB	—	–13 ～ –20 dB	< –20 dB
SNR	> 10 dB	6 ～ 10 dB	0 ～ 5 dB	< 0 dB	—

- ルータのワイヤレス LED が赤、オレンジ、黄色で点灯（点灯または点滅）しているか、緑で点滅しています。緑色に点灯している必要があります。

問題の解決方法

1. ルータを調べて、両方の基本アンテナが正しく取り付けられていることを確認します。
2. サービスプロバイダーに連絡して、その場所がサービスエリアであるかを確認します。
3. ルータを建物内の別の場所に移動します。
4. 追加の外部ケーブルアンテナを入手し、ルータに接続します。

モデムのステータスが低電力モードのままになる

問題に関する説明

エンドユーザーがセルラーネットワークに接続できず、モデムのステータスは低電力モードのままです。

問題の特定

- エンドユーザーはセルラーネットワークに接続できません。
- 「Missing or unknown APN」というエラーメッセージが生成されます。
- 信号強度が「excellent」より低いです。

問題の解決方法

1. 十分な無線信号強度があることを確認します。無線信号強度が不十分な場合は、「無線信号強度が不十分」のセクションの指示に従います。
2. cellular0 インターフェイスが動作していることを確認します。セルラーインターフェイスがシャットダウンされている場合、モデムのステータスは低電力モードに設定されます。確認するには、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。

   次に、[Real Time] をクリックし、[Device Options] ドロップダウンリストで [Interface] を選択します。

CLI でこれを実行するには、**show interface** コマンドを使用します。[Admin Status] および [Oper Status] の値が共に「Up」であることを確認します。

3. モデムの温度がしきい値の温度から外れていないことを確認します。モデムの温度を表示するには、Cisco vManage のメニューから**[Monitor]** > **[Devices]** を選択し、次にルータを選択します。

   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。

   次に、[Real Time] をクリックし、[Device Options] ドロップダウンリストで [Cellular Modem] を選択します。

   CLI から **show cellular modem** コマンドを実行します。

4. cellular0 インターフェイスのプロファイルにあるアクセスポイント名（APN）が、サービスプロバイダーが想定している名前と一致していることを確認します。一部のサービスプロバイダーでは、APN の設定を要件にしており、SIM カードパッケージに設定手順が記載されています。

   1. 設定されている APN 名を確認するには、Cisco vManage のメニューから**[Monitor]** > **[Devices]**を選択し、次にルータを選択します。

      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。

      次に、[Real Time] をクリックし、[Device Options] ドロップダウンリストで [Cellular Profiles] を選択します。

      CLI から **show cellular profiles** コマンドを実行します。[APN] 列に APN の名前が表示されます。各プロファイルによりアクセスポイント名（APN）が指定されます。APN はサービスプロバイダーが正しい IP アドレスを判断して、正しいセキュアゲートウェイに接続するために使用されます。一部のプロファイルでは、APN の設定が必要です。

   2. APN がサービスプロバイダーで必要とされているものと異なる場合、正しい APN を設定します。Cisco vManage のメニューから **[Configuration]** > **[Templates]**の順に選択し、[Cellular Profile] 機能テンプレートを使用します。

      CLI からこれを設定するには、**cellular cellular0 profile apn** コマンドを使用します。

5. ここまでに示した手順でうまくいかない場合は、セルラーインターフェイスをリセットします。

エラーメッセージ

セルラーインターフェイスに関する最も一般的なエラーメッセージを次の表に示します。

表 *38 :*

エラーメッセージ	問題に関する説明	問題の修正方法
Authentication failed	サービスプロバイダーがユーザーの SIM カードまたは Cisco vEdge デバイス の SIM カードを認証できないため、エンドユーザーの認証に失敗しました。	セルラーサービスのプロバイダーにお問い合わせください。
Illegal ME	エンドユーザーがネットワークからブロックされているため、サービスプロバイダーはエンドユーザーに対してアクセスを拒否しました。	セルラーサービスのプロバイダーにお問い合わせください。
Illegal MS	エンドユーザーが認証チェックに失敗したため、サービスプロバイダーはエンドユーザーに対してアクセスを拒否しました。	セルラーサービスのプロバイダーにお問い合わせください。
Insufficient resources	リソースが不足しているため、サービスプロバイダーのネットワークで輻輳が発生しており、要求されたサービスをエンドユーザーに提供できません。	Cisco vEdge デバイス は自動的に再接続を試みます（再試行の間隔は、サービスプロバイダーによって異なります）。問題が自然に解決しない場合は、セルラーサービスのプロバイダーにお問い合わせください。
IPV4 data call throttled	Cisco vEdge デバイス で使用されている SIM カードでは、静的 APN を設定する必要があります。	SIM カードに関連付けられているデータプランに静的 APN が必要かどうかを確認します。必要な場合は、上記の「モデムのステータスが低電力モードのままになる」の説明に従って、APN 名を SIM カードの手順で指定した名前に変更します。
Missing or unknown APN	APN が必須であるにもかかわらず、セルラープロファイルに指定されていないか、または APN がサービスプロバイダーによって解決されなかったため、エンドユーザーはセルラーネットワークに接続できません。	上記の「モデムのステータスが低電力モードのままになる」の説明に従って、プロファイルの APN を確認してください。
MS has no subscription for this service	エンドユーザーがサブスクリプションを持っていないため、サービスプロバイダーはエンドユーザーに対してアクセスを拒否しました。	セルラーサービスのプロバイダーにお問い合わせください。

エラーメッセージ	問題に関する説明	問題の修正方法
Network failure	サービスプロバイダーのネットワークで問題が発生しています。	Cisco vEdge デバイス は自動的に再接続を試みます（再試行の間隔は、サービスプロバイダーによって異なります）。問題が自然に解決しない場合は、セルラーサービスのプロバイダーにお問い合わせください。
Network is temporarily out of resources	リソースが不足しているため、サービスプロバイダーのネットワークで輻輳が発生しており、要求されたサービスをエンドユーザーに提供できません。	Cisco vEdge デバイス は自動的に再接続を試みます（再試行の間隔は、サービスプロバイダーによって異なります）。問題が自然に解決しない場合は、セルラーサービスのプロバイダーにお問い合わせください。
Operator has barred the UE	オペレータがエンドユーザーを禁止したため、サービスプロバイダーはエンドユーザーに対してアクセスを拒否しました。	セルラーサービスのプロバイダーにお問い合わせください。
Requested service option not subscribed	Cisco vEdge デバイス で使用されている SIM カードでは、静的 APN エントリを設定する必要があります。	SIM カードに関連付けられているデータプランに静的 APN が必要かどうかを確認します。必要な場合は、上記の「モデムのステータスが低電力モードのままになる」の説明に従って、APN 名を SIM カードの手順で指定した名前に変更します。
Service not supported by the PLMN	Public Land Mobile Network（PLMN）はデータサービスをサポートしていません。	セルラーサービスのプロバイダーにお問い合わせください。

Wi-Fi 接続のトラブルシュート

ここでは、Wi-Fi クライアントが Wi-Fi ルータ経由で Wi-Fi ネットワークに接続した際に発生した問題を確認して解決する方法について説明します。ここで説明する手順は、Wi-Fi のみをサポートするデバイスを対象としています。

Wi-Fi 接続の問題を確認する

ルータが Wi-Fi ネットワークを提供しているときに Wi-Fi クライアントが Wi-Fi ネットワークに接続できない場合は、次の手順に従って問題の原因を特定します。各手順を実行する際、Wi-Fi クライアントに適した方法を使用してください。

1. Wi-Fi クライアントがルータによってアドバタイズされたサービス識別子（SSID）を見つけられることを確認します。クライアントが SSID を見つけられない場合は、「SSID が見つからない」のセクションを参照してください。
2. Wi-Fi クライアントがルータによってアドバタイズされた SSID に接続できることを確認します。クライアントが SSID に接続できない場合は、「SSID 接続に失敗する」のセクションを参照してください。
3. Wi-Fi クライアントに IP アドレスが割り当てられていることを確認します。クライアントが IP アドレスを取得できない場合は、「IP アドレスの欠如」のセクションを参照してください。
4. Wi-Fi クライアントがインターネットにアクセスできることを確認します。クライアントがインターネットに接続できない場合は、「インターネット接続障害」のセクションを参照してください。
5. W-iFi クライアント接続速度が遅い場合、または頻繁に切断される場合は、「Wi-Fi 速度が遅い」のセクションを参照してください。

Wi-Fi 接続の問題を解決する

このセクションでは、Wi-Fi クライアントとルータ間の Wi-Fi 接続で発生する最も一般的な問題と、問題の解決手順について説明します。

SSID が見つからない

問題に関する説明

Wi-Fi クライアントは、ルータによってアドバタイズされた SSID を見つけることができません。

問題の解決方法

1. SSID の基本サービスセット識別子（BSSID）アドレスが有効であるかを確認します。
   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 [WiFi] を選択します。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。
   4. 右ペインで SSID を見つけます。この SSID の BSSID の値が 00:00:00:00:00:00 ではないことを確認します。
   5. BSSID が 00:00:00:00:00:00 の場合、この SSID の WLAN（VAP）インターフェイスが正しく設定されていない可能性があります。設定プロセスで WLAN インターフェイスがブリッジに追加されていることを確認します。デバイスの実行コンフィギュレーショ

ンを表示するには、Cisco vManage のメニューから**[Configuration]** > **[Devices]**の順に選択します。目的のデバイスで [...] をクリックし、[Running Configuration] を選択します。

CLI からデバイスの実行コンフィギュレーションを表示するには、**show running-config** コマンドを使用します。WLAN インターフェイスをブリッジに追加するには、Cisco vManage から**[Configuration]** > **[Templates]**の順に選択します。

[Feature Templates] をクリックし、[Bridge] 機能テンプレートを選択します。

（注） Cisco vManage リリース 20.7.x 以前では、[Feature Templates] のタイトルは [Feature] です。

2. 静的チャネルを削除します。静的チャネルは、ルータによって最適な無線チャネルが自動的に選択されるのではなく、ユーザーが明示的に無線チャネルを設定します。低速の静的チャネルは、到達不能な SSID のように見える場合があります。
   1. ルータの現在の SSID チャネル設定を表示します。これを実行するには、Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。次に、[Real Time] をクリックし、[Device Options] ドロップダウンリストで [WLAN Clients] または [WLAN Radios] を選択します。

      CLI から **show wlan clients** または **show wlan radios** コマンドを実行します。
   2. チャネルが特定の番号に設定されている場合は、値を「auto」に変更します。これを実行するには、Cisco vManage の Wi-Fi 無線機能テンプレートを使用します。

      CLI から **wlan channel auto** コマンドを実行します。

3. Wi-Fi クライアントがルータと同じ無線帯域を使用していることを確認します。IEEE 802.11b/g/n の場合は 2.4 GHz、IEEE802.11a/n/ac の場合は 5 GHz です。
   1. Wi-Fi クライアントがサポートする無線帯域を確認します。
   2. ルータの無線選択の設定を確認します。これを実行するには、Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。次に、[Real Time] をクリックし、[Device Options] ドロップダウンリストで [WLAN Radios] を選択します。

      CLI から **show wlan radios** コマンドを実行します。
   3. ルータと Wi-Fi クライアントの無線帯域の設定が一致しない場合は、一致するように Wi-Fi クライアントの無線帯域を変更するか、ルータの設定を変更します。これを実行するには、Wi-Fi 無線機能テンプレートを使用します。

      CLI から **wlan** コマンドを実行します。

SSID 接続に失敗する

問題に関する説明

Wi-Fi クライアントは、ルータによってアドバタイズされた SSID を見つけることはできますが、接続できません。

問題の解決方法

1. ルータでローカルにパスワードを設定する場合は、Wi-Fi クライアントのパスワードと SSID のパスワードが一致していることを確認します。
2. Radius サーバーを使用している場合は、Radius サーバーが到達可能であり、Wi-Fi クライアントのユーザー名とパスワードが Radius の設定と一致していることを確認します。
    1. ルータから RADIUS サーバーに到達できることを確認するには、サーバーに ping を実行します。Cisco vManage でこれを行うには、デバイスに ping を実行します。CLI から **ping** コマンドを実行します。
    2. Radius サーバーと Wi-Fi クライアントでパスワードが一致していることを確認します。
3. この SSID についてクライアントの最大数を超えていないことを確認します。
    1. 使用されているクライアント数とクライアントの最大数を確認します。
        - Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。左ペインで [WiFi] を選択します。右ペインで SSID を見つけます。[No. of Clients] フィールドを確認します。使用されている数と最大値が等しい場合、この SSID にこれ以上クライアントを接続できません。
        - CLI から **show wlan interfaces detail** コマンドを実行します。
    2. 必要に応じて、SSID の最大クライアント数の設定を増やします。これを実行するには、Cisco vManage の Wi-Fi SSID 機能テンプレートを使用します。

        CLI から **max-clients** コマンドを実行します。
4. Wi-Fi クライアントが WPA2 管理セキュリティをサポートしていることを確認します。
    1. 管理セキュリティの設定を確認します。これを実行するには、Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。次に、[Real Time] をクリックし、[Device Options] ドロップダウンリストで [WLAN Interfaces] を選択します。

        CLI から **show wlan interfaces** コマンドを実行します。管理セキュリティの値が「required」に設定されている場合、Wi-Fi クライアントは WPA2 セキュリティをサポートしている必要があります。
    2. 必要に応じて、SSID の管理セキュリティの設定を「optional」または「none」に変更します。Cisco vManage でこれを実行するには、Wi-Fi SSID 機能テンプレートを使用します。

        CLI から **mgmt-security** コマンドを実行します。

IP アドレスの欠如

問題に関する説明

Wi-Fi クライアントは SSID に接続できますが、IP アドレスを取得できません。

問題の解決方法

DHCP サーバーが到達可能であり、そのアドレスプールに使用可能な IP アドレスがあることを確認します。

1. ルータが DHCP ヘルパー（DHCP リレーエージェント）として機能している場合は、DHCP サーバーに ping を実行して、ルータから到達可能であるかを確認します。CLI から **ping** コマンドを実行します。
2. リモート DHCP サーバーを使用している場合は、リモート DHCP サーバーのアドレスプールに使用可能な IP アドレスがあることを確認します。
3. ルータがローカル DHCP サーバーとして機能している場合：
    1. 使用されているアドレスの数を表示します。Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。次に、[Real Time] をクリックし、[Device Options] ドロップダウンリストで [DHCP Servers] を選択します。

        CLI から **show dhcp server** コマンドを実行します。
    2. 設定済みの DHCP アドレスプールサイズと、DHCP アドレスプールから除外されたアドレスの数に基づいて、プール内の IP アドレスの数を計算します。Cisco vManage でこれらの値を表示するには、Cisco vManage のメニューから**[Configuration]** > **[Devices]** の順に選択します。目的のルータで [...] をクリックし、[Running Configuration] を選択します。

        CLI から表示するには、**show running-config** コマンドを使用します。
    3. 必要に応じて、Cisco vManage の DHCP サーバー機能テンプレートを使用して、ルータの DHCP アドレスプールのアドレス範囲を拡張します。

インターネット接続障害

問題に関する説明

Wi-Fi クライアントは SSID に接続され、IP アドレスがありますが、インターネットに接続できません。

問題の解決方法

Wi-Fi クライアントが DHCP サーバーから正しいデフォルトゲートウェイと DNS 設定を受け取っているかを確認します。

1. DHCP サーバーがリモートの場合は、サーバーの設定を確認します。
2. ルータが DHCP サーバーの場合は、デフォルトゲートウェイと DNS サーバーの設定が Wi-Fi クライアントの設定と同じであるかを確認します。Cisco vManage で設定を表示する

には、Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。[Real Time] をクリックし、[Device Options] ドロップダウンリストで [DHCP Interfaces] を選択します。

CLI から **show dhcp interface** コマンドを実行します。

Wi-Fi 速度が遅い

問題に関する説明

Wi-Fi クライアントはインターネットに接続できますが、接続速度が遅いです。

問題の解決方法

ルータが最適な Wi-Fi チャネンルを選択できるようにします。

1. ルータの現在の SSID チャネルの設定を表示します。Cisco vManage でこの設定を表示するには、Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。[Real Time] をクリックし、[Device Options] ドロップダウンリストで [WLAN Clients] を選択します。

   CLI から **show wlan clients** または **show wlan radios** コマンドを実行します。

2. チャネルが特定の番号に設定されている場合は、値を「auto」に変更します。Cisco vManage でこれを実行するには、Wi-Fi 無線機能テンプレートを使用します。

   CLI から **wlan channel auto** コマンドを実行します。

デバイスのトラブルシューティング

オーバーレイネットワーク内のすべてのデバイスについて、接続やトラフィックの状態に関する問題をトラブルシューティングできます。

デバイス起動の確認

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 [Troubleshooting] をクリックします。
4. [Connectivity] 領域で [Device Bringup] をクリックします。

[Device Bringup] ウィンドウが開きます。

デバイスに対する ping の実行

デバイスがネットワーク上で到達可能であることを確認するには、デバイスに ping を実行して ICMP ECHO_REQUEST パケットを送信します。

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. [Connectivity] 領域で [Ping] をクリックします。
5. [Destination IP] フィールドに、ping を実行するデバイスの IP アドレスを入力します。
6. [VPN] フィールドで、デバイスに到達するために使用する VPN を選択します。
7. [Source/Interface] フィールドで、ping 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。
8. [Probes] フィールドで、ping パケットの送信に使用するプロトコルタイプを選択します。
9. [Source Port] フィールドに送信元ポート番号を入力します。
10. [Destination Port] フィールドに宛先ポート番号を入力します。
11. [Advanced Options] をクリックして、追加のパラメータを指定します。
    1. [Count] フィールドには、送信する ping 要求数を入力します。指定できる範囲は 1 ～ 30 です。デフォルトは 5 です。
    2. [Payload Size] フィールドには、送信するパケットのサイズを入力します。デフォルトは 64 バイトです。56 バイトのデータと 8 バイトの ICMP ヘッダーで構成されます。データの有効範囲は 56 ～ 65507 バイトです。
    3. [MTU] を入力します。
    4. [Rapid] スライダをクリックすると、5 つの ping 要求がすばやく連続して送信され、送受信されたパケットのみを対象にした統計情報とパケット損失率が表示されます。
    5. [Type of Service] フィールドには、ping パケットに含めるサービスタイプ（ToS）フィールドの値を入力します。
    6. [Time to Live] フィールドには、この ping パケットを送信してから応答を受信するまでの往復時間をミリ秒単位で入力します。
    7. ping パケットをフラグメント化しない場合は、[Don't Fragment] オプションをオンにします。
12. [Ping] をクリックします。

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。

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。

オンデマンドのトラブルシューティング

表 *39 :* 機能の履歴

機能名	リリース情報	説明
オンデマンドのトラブルシューティング	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	この機能を使用すると、デバイスからのトラフィックフローに関する詳細情報を表示できます。この情報は、トラブルシューティングに役立てることができます。

オンデマンドのトラブルシューティングについて

オンデマンドのトラブルシューティングでは、デバイスからのトラフィックフローに関する詳細情報を表示できます。

デフォルトでは、Cisco vManage がフローに関する集約情報をキャプチャします。オンデマンドトラブルシューティングのエントリを追加することで、特定のデバイスや特定の履歴期間の詳細情報を取得できます。エントリを追加すると、Cisco vManage では設定したパラメータに従って詳細情報が編集されます。

システムリソースの節約のため、エントリを追加して詳細情報を要求した場合にのみ、Cisco vManage で詳細情報が編集されます。また、Cisco vManage では情報が一定期間（デフォルトでは 3 時間）保存された後に削除されます。必要に応じて、同じ情報を再度要求できます。

オンデマンド トラブルシューティングの制約事項

オンデマンド トラブルシューティングの使用中は、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。

ページ要素

[On Demand Troubleshooting] ウィンドウには、オンデマンド トラブルシューティングのエントリを設定および追加するためのオプションがあります。[On Demand Troubleshooting] ウィンドウには、既存のオンデマンドトラブルシューティングのエントリに関する情報が表示され、次の情報とオプションが提供されます。

項目（フィールド）	説明
ID	システムによって割り当てられたエントリの識別子。
Device ID	エントリで適用されるデバイスのシステム IP。
Data Type	エントリにより詳細情報が提供されるデータのタイプ。
Creation Time	エントリを追加した日時。
Expiration Time	エントリの有効期限が切れる日時。 この有効期限が切れると、エントリはテーブルから自動的に削除され、対応する詳細情報は利用できなくなります。 デフォルトでは、エントリは作成から 3 時間後に削除されます。
Data Backfill Start Time	データバックフィル期間の開始日時。
Data Backfill End Time	データバックフィル期間の終了日時。

項目（フィールド）	説明
Status	エントリのステータス： • **IN_PROGRESS**：詳細なトラブルシューティング情報を編集中です。 • **QUEUED**：詳細なトラブルシューティング情報は編集用のキュー内にあります。 • **COMPLETED**：詳細なトラブルシューティング情報の編集が完了しました。

オンデマンド トラブルシューティングの設定

Cisco vManage の**[Tools]** > **[On Demand Troubleshooting]** ウィンドウから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できます。このウィンドウには、オンデマンド トラブルシューティングのエントリを追加するためのオプション、および既存のエントリを管理するためのオプションがあります。

Cisco vManage リリース 20.6.x 以前：Cisco vManage の**[Monitor]** > **[On Demand Troubleshooting]** ウィンドウから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できます。

また、デバイスの**[Monitor]** > **[Devices]** ウィンドウでは、さまざまな場所からオンデマンド トラブルシューティングを開始できます。デバイスのオンデマンド トラブルシューティング情報の表示 （199 ページ）を参照してください。

Cisco vManage リリース 20.6.x 以前：デバイスの**[Monitor]** > **[Network]** ウィンドウでは、さまざまな場所からオンデマンド トラブルシューティングを開始できます。

オンデマンド トラブルシューティングは、同時に最大 10 台のデバイスのトラブルシューティング エントリに対応できます。

オンデマンド トラブルシューティングのエントリの追加

[On Demand Troubleshooting] ウィンドウにエントリを追加すると、設定したパラメータを使用して、指定したデバイスの詳細なトラブルシューティング情報を編集するようにCisco vManageに対して指示されます。

オンデマンド トラブルシューティングのエントリを追加するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Tools]** > **[On Demand Troubleshooting]**の順で選択します。

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

2. [Select Device] ドロップダウンリストから、オンデマンド トラブルシューティングを有効にする Cisco IOS XE SD-WAN デバイス または Cisco vEdge デバイス を選択します。

3. [Select Data Type] ドロップダウンリストから [SAIE] または [ConnectionEvents] を選択します。

4. データバックフィル期間のオプションを選択します。

- [Last 1 hour]：トラブルシューティングのエントリを追加した 1 時間前からエントリを追加した時点までの詳細なストリーム情報を提供します。
- [Last 3 hours]：トラブルシューティングのエントリを追加した 3 時間前からエントリを追加した時点までの詳細なストリーム情報を提供します。
- [Custom Date and Time Range]：[Start date and time] および [End date and time] フィールドを使用して、必要なバックフィル期間を指定します。[End date and time] の値は、現在の日時より後にすることはできません。

5. [Add] をクリックします。

   トラブルシューティングのエントリがエントリテーブルに表示されます。エントリの [Status] フィールドの値が **Completed** の場合は、「デバイスのオンデマンドトラブルシューティング情報の表示 （199 ページ）」で説明されているように、**[Monitor]** > **[Devices]** ウィンドウからトラブルシューティング情報を表示できます。

オンデマンド トラブルシューティングのエントリの更新

設定を変更するには、オンデマンドトラブルシューティングのエントリを更新します。たとえば、エントリを更新してバックフィル期間を調整できます。

更新できるのは、ステータスが「QUEUED」のエントリのみです。

オンデマンド トラブルシューティングのエントリを更新するには、次の手順を実行します。

1. Cisco vManage のメニューから **[Tools]** > **[On Demand Troubleshooting]** の順で選択します。

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

2. エントリのテーブルで、更新するエントリの隣にある [...] をクリックし、[Update] を選択します。

3. [Update Troubleshoot Status] ダイアログボックスが表示されたら、必要に応じて設定を行い、[Add] をクリックします。

オンデマンド トラブルシューティングのエントリの削除

オンデマンド トラブルシューティングのエントリを削除すると、Cisco vManage からエントリが削除されます。エントリを削除すると、その詳細情報を表示できなくなります。

エントリの削除は、Cisco vManage のリソース解放に役立ちます。

オンデマンド トラブルシューティングのエントリを削除するには、次の手順を実行します。

1. Cisco vManage のメニューから **[Tools]** > **[On Demand Troubleshooting]** の順で選択します。

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

2. エントリのテーブルで、削除するエントリの隣にある [...] をクリックし、[Delete on demand queue] を選択します。

3. [Delete On Demand Status] ウィンドウが表示されたら、[OK] をクリックします。

デバイスのオンデマンド トラブルシューティング情報の表示

デバイスの [Network] ウィンドウからデバイスのオンデマンド トラブルシューティング情報を表示できます。

この情報を表示するには、デバイスのオンデマンド トラブルシューティング エントリが少なくとも 1 つは設定されている必要があります。「オンデマンド トラブルシューティングのエントリの追加」の説明に従って [On Demand Troubleshooting] ウィンドウからエントリを追加するか、次の手順に従って [Network] ウィンドウからエントリを追加します。

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. [Hostname] 列で、情報を表示するデバイスをクリックします。
3. 次のいずれかの操作を行います。
   - SAIE アプリケーションのトラブルシューティング情報を表示する場合：
     1. [SAIE Applications] をクリックします。

（注） 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。

     2. [Applications Family] テーブルで、アプリケーションファミリをクリックします。
     3. [Applications] テーブルで、アプリケーションファミリをクリックします。

   - 特定のメトリックに関するトラブルシューティング情報を表示するには、左ペインの [ON-DEMAND TROUBLESHOOTING] でオプションをクリックします。すべてのオプションがすべてのデバイスタイプに適用されるわけではありません。
     - FEC Recovery Rate
     - SSL Proxy
     - AppQoe TCP Optimization
     - AppQoE DRE Optimization
     - WAN Throughput
     - Flows
     - **Top Talkers**

デバイスにオンデマンドトラブルシューティングが設定されている場合、トラブルシューティングの詳細情報が表示されます。この情報には、トラフィック統計と送信元IPアドレス、宛先IPアドレス、パケット数、バイト数などのメトリックが含まれます。利用可能なオプションを使用し、カーソルをグラフ要素の上に置くと、必要な情報が表示されます。

（注） Cisco IOS XE リリース 17.9.1a 以降では、**policy ip visibility features enable** コマンドを使用して、Flexible Netflow（FNF）の機能フィールドを手動で有効または無効にします。**show sdwan policy cflowd-upgrade-status** コマンドを使用すると、バージョンアップのグレード前に有効になっている機能を確認できます。バージョンのアップグレード後に機能を手動で制御する必要性が生じた場合は、disable または enable コマンドを使用します。

詳細については、「policy ip visibility」のコマンドページを参照してください。

オンデマンドトラブルシューティング情報が設定されていない場合は、[Enable On Demand Troubleshooting] オプションが表示されます。ステップ 4 に進みます。

4. [Enable On Demand Troubleshooting] オプションが表示される場合は、次の操作を実行して、選択したデバイスに対してこの機能を開始します。

   1. [Enable On Demand Troubleshooting] をクリックします。
   2. 次のいずれかのオプションを選択します。

      - [Quick Enable]：3 時間のバックフィル期間でオンデマンド トラブルシューティングのエントリを開始します。このオプションを使用すると、過去 3 時間の詳細なストリーム情報が利用可能になります。

        このオプションを選択した後に [Refresh] をクリックすると、詳細なトラブルシューティング情報を表示できます。この情報が表示されるまで数分かかることがあります。または、[Go to On Demand Troubleshooting] をクリックして、追加したエントリが記載された [On Demand Troubleshooting] ウィンドウを表示します。

      - [Go to On Demand Troubleshooting]：[On Demand Troubleshooting] ウィンドウを表示します。「オンデマンド トラブルシューティングのエントリの追加」の説明に従って、このウィンドウでエントリを追加します。詳細情報を表示するには、この手順のステップ 1 からステップ 3 を繰り返します。

詳細な上位ソースデータの表示

オンデマンドトラブルシューティングを設定すると、デバイスの上位アプリケーションの使用状況に関する詳細情報を表示できます。これを行うには、次の手順を実行します。

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

2. [SAIE Application] タブで、チャート内にあるアプリケーションの使用状況バーをクリックします。

（注） 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。

3. 選択したアプリケーションのチャートで、デバイスの使用状況バーをクリックします。

   デバイスにオンデマンドトラブルシューティングが設定されている場合、詳細な上位ソースデータが表示されます。

   オンデマンド トラブルシューティング情報が設定されていない場合は、[Go to On Demand Troubleshooting] オプションが表示されます。ステップ 4 に進みます。

4. [Go to On Demand Troubleshooting] オプションが表示された場合は、次の操作を実行します。

   1. [Go to On Demand Troubleshooting] をクリックして、[On Demand Troubleshooting] ウィンドウを表示します。
   2. 「オンデマンド トラブルシューティングのエントリの追加」の説明に従って、[On Demand Troubleshooting] ウィンドウでエントリを追加します。
   3. 詳細情報を表示するには、この手順のステップ 1 からステップ 3 を繰り返します。

第 11 章

パケットトレース

表 *40* : 機能の履歴

機能名	リリース情報	説明
パケットトレースの双方向サポート	Cisco IOS XE リリース 17.8.1a Cisco SD-WAN リリース 20.8.1 Cisco vManage リリース 20.8.1	この機能により、データパケットが両方向のエッジデバイスによってどのように処理されるかを詳細に把握できます。双方向デバッグを実行することで、問題の診断とトラブルシュートを効率化できます。

パケットトレースについて

パケットトレース機能を使用すると、エッジデバイスでのパケット損失をデバッグし、ネットワーク内にあるデバイスでのトラフィックフローの転送動作を検査できます。パケットフローがどのように分離され、トレース用にキャプチャされるかに基づいて、さまざまな条件でパケットトレーサを設定できます。これにより、問題の診断とトラブルシュートを効率化できます。

パケットトレーサには、パスデータのコピーに使用される 2048 バイトの内部メモリが組み込まれています。このメモリは、トレースの循環モード中に上書きされます。

パケットトレース機能は、アカウンティング、サマリー、パスデータという 3 つのレベルのパケット検査を提供します。各レベルは、一部のパケット処理機能を犠牲にして、パケット処理の詳細なビューを提供します。ただし、パケットトレースは、**debug platform condition** ステー

トメントに一致するパケットの検査を制限し、大量のトラフィックが発生する環境下でも実行可能なオプションです。

Cisco IOS XE リリース 17.8.1a では、条件付きデバッグ一致フィルタ用に、双方向サポートがエッジデバイスに追加されています。条件付きデバッグにより、エッジデバイスでデバッグ情報の一部を除外できます。特定のインターフェイス、MAC アドレス、またはユーザー名に一致するデバッグ情報を確認できます。

表 *41* : パケットトレースレベル

パケット トレース レベル	説明
アカウンティング	パケットトレースのアカウンティングでは、ネットワークプロセッサに出入りするパケット数が示されます。パケットトレースのアカウンティングは負荷の軽いパフォーマンス アクティビティであり、無効化されるまで継続的に実行されます。
サマリー	パケットトレースのサマリーレベルでは、限られた数のパケットデータが収集されます。パケットトレースのサマリーは、入力インターフェイスと出力インターフェイス、最終的なパケットの状態、消費されたパケットの状態、およびパケットのパント、ドロップ、インジェクションを随時追跡します。サマリーデータの収集は、通常のパケット処理と比較してパフォーマンスが高く、問題のあるインターフェイスを分離するのに役立ちます。

パケット トレース レベル	説明
パスデータ	パケットトレースのパスデータレベルでは、パケットトレースが最も詳細なレベルで実行されます。限られた数のパケットを対象にデータが収集されます。パケットトレースのパスデータでは、条件付きデバッグIDを含むデータがキャプチャされます。このデータは、機能デバッグ、タイムスタンプ、および機能固有のパストレースデータと関連付ける際に役立ちます。 パスデータには、パケットコピーと Feature Invocation Array（FIA）トレースという2つのオプション機能もあります。パケットコピーオプションを使用すると、パケットの各種レイヤ（レイヤ2、レイヤ3、レイヤ4）で入力パケットや出力パケットをコピーできます。FIA トレースオプションは、パケット処理中に呼び出されたすべての機能エントリを追跡します。このオプションは、パケット処理中に何が起こっているかを把握する際に役立ちます。 （注） パスデータの収集では、多くのパケット処理リソースが消費されます。また、オプション機能はパケットパフォーマンスに徐々に影響を及ぼします。パスデータレベルは限定的に使用するか、またはパケットパフォーマンスの変化が許容できる状況で使用することを推奨します。

パケットトレースの設定に関する使用上のガイドライン

パケットトレースを設定する際には、次のベストプラクティスを考慮してください。

- パケットをより包括的に表示するには、パケットトレースを使用する際に入力条件を使用することを推奨します。
- パケットトレースの設定には、データプレーンメモリが必要です。データプレーンメモリが制限されているシステムでは、パケットトレース値をどのように選択するかを慎重に検討してください。パケットトレースによって消費されるメモリ量の概算値は、次の式で求められます。

  必要なメモリ＝（統計オーバーヘッド）＋（パケット数）＊（サマリーサイズ＋データサイズ＋パケットコピーサイズ）。

パケットトレース機能を有効にすると、統計用に少量の固定メモリが割り当てられます。同様に、パケットごとのデータをキャプチャする場合、サマリーデータ用に各パケットに少量の固定メモリが必要です。ただし、式が示すように、トレース対象に選択したパケット数や、パスデータとパケットのコピーを収集するかどうかによって、消費されるメモリ量が大きく影響される可能性があります。

（注） パケットトレース機能によって消費されるメモリの量は、パケットトレース設定の影響を受けます。他のルータサービスの中断を避けるために、パケットごとのパスデータとコピーバッファのサイズ、およびトレースするパケット数を慎重に選択する必要があります。

制限事項

- IPパケットのみがサポートされます。L2（ARP）パケット、ブリッジパケット、フラグメント化されたパケット、およびマルチキャストパケットはサポートされていません。
- IPv6 はサポートされていません。
- パケットの複製はサポートされていません。
- 再送信されたパケット（例：IPsecまたはGRE暗号化パケット）が内部パケット（復号されたパケット）と外部パケット（暗号化されたパケット）の両方で設定されたフィルタに一致する場合、そのパケットには、個別のトレースエントリがあります。パケットトレーサをより効率的に使用するには、問題のデバッグで利用できる情報に基づき、できるだけ多くのフィルタを設定する必要があります。

パケットトレースの設定

debug platform packet-trace コマンドを使用すると、双方向、VPN、ラウンドロビン、宛先IP、送信元IP、インターフェイス、開始、停止、ロギング、クリアなどのさまざまな条件でエッジデバイスでパケットトレーサを設定できます。

Cisco IOS XE SD-WAN デバイスでのパケットトレースの設定

1. トラフィックのパケットトレースを有効にし、パケットの最大数を指定します。

   ```
   Device# debug platform packet-trace packet [number of traced packets]
   ```

2. パケットをトレースする際の一致基準を指定します。一致基準には、プロトコル、IPアドレスとサブネットマスク、インターフェイス、方向によるフィルタリング機能があります。

   ```
   Device# debug platform condition [interface interface name] {match ipv4|ipv6|mac src
    dst}  {both|ingress|egress} [bidirectional]
   ```

3. 指定した一致基準を有効にして、パケットトレースを開始します。

```
Device# debug platform condition start
```

4. 条件を非アクティブにし、パケットトレースを停止します。

```
Device# debug platform condition stop
```

5. 特権 EXEC モードを終了します。

```
exit
```

Cisco vEdge デバイス でのパケットトレースの設定

次の例は、パケットトレースの条件を設定する方法を示しています。

```
Device# debug packet-trace condition source-ip 10.1.1.1
Device# debug packet-trace condition vpn-id 0
Device# debug packet-trace condition interface ge0/1
Device# debug packet-trace condition stop
```

詳細については、debug packet-trace condition のコマンドページを参照してください。

パケットトレースのモニタリング

パケットトレース設定は、指定した条件の AND 演算に基づいており、設定したすべての条件に一致するパケットがトレースされます。

Cisco vEdge デバイス でのパケットトレースのモニタリング

Cisco vEdge デバイス で **show packet-trace statistics** コマンドを使用すると、指定した条件と一致するすべてのパケットの概要が表示されます。

次の例では、パケットトレース用に設定したすべての条件が表示されます。

```
Device# show debugs
debugs packet-trace condition source-ip 10.1.1.1
debugs packet-trace condition vpn-id 0
debugs packet-trace condition interface ge0/1
debugs packet-trace condition state Stopped
```

Cisco vEdge デバイス で **show packet-trace statistics** コマンドを使用すると、指定した条件と一致するすべてのパケットの概要が表示されます。

次の例では、指定したインターフェイス（この場合は ge 0）のパケットトレース統計が表示されます。

```
Device# show packet-trace statistics source-interface ge0_0
packet-trace statistics 0
source-ip 10.1.15.13
source-port 0
destination-ip 224.0.0.5
destination-port 0
source-interface ge0_0
destination-interface loop0.0
decision PUNT
duration 40
```

詳細については、show packet-tracer のコマンドページを参照してください。

詳細なパケットビュー：

以下は、**show packet-trace details** コマンドの出力例です。指定されたトレース ID 10 について表示されます。

```
Device# show packet-trace details 10

Pkt-id     src_ip(ingress_if)     dest_ip(egress_if)     Duration     Decision
10         10.1.15.15:0 (ge0_0)   192.168.255.5:0 (ge0_0)     15 us          PUNT
INGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b 0a 01 0f
0f e0
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00 00 ff ff
ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00 00 00 00
00
00 00 00 00 00
EGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b 0a 01 0f
0f e0
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00 00 ff ff
ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00 00 00 00
00
00 00 00 00 00
Feature Data
-------------------------------------
TOUCH : fp_proc_packet
-------------------------------------
TOUCH : fp_proc_packet2
-------------------------------------
TOUCH : fp_send_to_host
-------------------------------------
FP_TRACE_FEAT_PUNT_INFO:
icmp_type : 0
icmp_code : 0
qos : 7
-------------------------------------
TOUCH : fp_hw_x86_pkt_free
```

show packet-trace details コマンドを使用すると、指定したトレース ID に関する詳細情報が表示されます。詳細なパケットビューの出力では、概要データセクション、パケットダンプセクション、および機能データセクションの 3 つのセクションが表示されます。

Cisco IOS XE SD-WAN デバイスでのパケットトレースのモニタリング

概要ビュー：

Cisco IOS XE SD-WAN デバイスで **show platform packet-trace summary** コマンドを使用すると、指定した条件と一致するすべてのパケットの概要が表示されます。

次の例では、Cisco IOS XE SD-WAN デバイスのパケットトレースの概要が表示されます。

```
Device# show platform packet-trace summary

Pkt   Input                    Output                   State  Reason
0     INJ.12                   Gi2                      FWD
1     Gi2                      internal0/0/rp:0         PUNT   5
2     INJ.1                    Gi2                      FWD
3     INJ.1                    Gi2                      FWD
4     Gi2                      internal0/0/rp:0         PUNT   5
```

```
5     Gi2                     internal0/0/rp:0          PUNT   5
6     INJ.1                   Gi2                       FWD
7     INJ.1                   Gi2                       FWD
8     Gi2                     internal0/0/rp:0          PUNT   5
9     Gi2                     internal0/0/rp:0          PUNT   5
10    Gi2                     internal0/0/rp:0          PUNT   5
11    INJ.1                   Gi2                       FWD
12    Gi2                     internal0/0/rp:0          PUNT   5
13    INJ.1                   Gi2                       FWD
14    INJ.1                   Gi2                       FWD
```

詳細なパケットビュー：

以下は、Cisco IOS XE SD-WAN で **show packet trace details** コマンドを実行した場合の出力例です。指定されたトレース ID 10 について表示されます。

```
Device# show platform packet-trace packet 10

Packet: 10          CBUG ID: 116
Summary
  Input     : GigabitEthernet2
  Output    : internal0/0/rp:0
  State     : PUNT 5   (CLNS IS-IS Control)
  Timestamp
    Start   : 2427641145361169 ns (02/23/2022 00:14:58.869057 UTC)
    Stop    : 2427641145374580 ns (02/23/2022 00:14:58.869071 UTC)
Path Trace
  Feature: DEBUG_COND_INPUT_PKT_EXT
    Entry       : Input - 0x813e9f60
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 176 ns
  Feature: LAYER2_INPUT_LOOKUP_PROCESS_EXT
    Entry       : Input - 0x81419e2c
    Input       : GigabitEthernet2
    Output      : internal0/0/rp:0
    Lapsed time : 896 ns
  Feature: LAYER2_INPUT_GOTO_OUTPUT_FEATURE_EXT
    Entry       : Input - 0x813ed9e8
    Input       : GigabitEthernet2
    Output      : internal0/0/rp:0
    Lapsed time : 553 ns
  Feature: LAYER2_OUTPUT_QOS_EXT
    Entry       : Output - 0x81420930
    Input       : GigabitEthernet2
    Output      : internal0/0/rp:0
    Lapsed time : 748 ns
  Feature: LAYER2_OUTPUT_DROP_POLICY_EXT
    Entry       : Output - 0x8142092c
    Input       : GigabitEthernet2
    Output      : internal0/0/rp:0
    Lapsed time : 947 ns
  Feature: INTERNAL_TRANSMIT_PKT_EXT
    Entry       : Output - 0x813eaa6c
    Input       : GigabitEthernet2
    Output      : internal0/0/rp:0
    Lapsed time : 6575 ns
Packet Copy In
  0180c200 00140050 569a8a44 0062fefe 03831b01 00120100 00005f04 af200020
  00200000 00000000 0a0aee03 01040349 00018101 cc890b61 6c706861 2d637372
  2d31020c 000a0000 00200020 00200001 84046400 00018018 0a808080 0a000a00
  ffffff00 00808080 64000001 ffffffff
Packet Copy Out
```

```
  01010000 00110070 00b80028 200a0000 00000000 00000006 00000000 80010500
  02065900 00000001 01010000 000e003c 00000000 00000074 03f50000 00000005
  00000000 80010700 0180c200 00140050 569a8a44 0062fefe 03831b01 00120100
  00005f04 af200020 00200000 00000000 0a0aee03 01040349 00018101 cc890b61
  6c706861 2d637372 2d31020c 000a0000 00200020 00200001 84046400 00018018
  0a808080 0a000a00 ffffff00 00808080 64000001 ffffffff

IOSd Path Flow: Packet: 10    CBUG ID: 116
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE
```

show platform packet-trace summary コマンドを使用すると、指定したトレース ID に関する詳細情報が表示されます。詳細なパケットビューの出力では、概要データセクション、パケットダンプセクション、および機能データセクションの 3 つのセクションが表示されます。

- 概要データセクション：パケットトレースID、入力インターフェイス、出力インターフェイス、および指定したトレース ID のデバイスを通過するパケットに関して が取った転送の決定について表示されます。
- パケットダンプセクション：入力パケットと出力パケット情報が表示されます。パケットヘッダー詳細の最初の 96 バイトのみが表示されます。

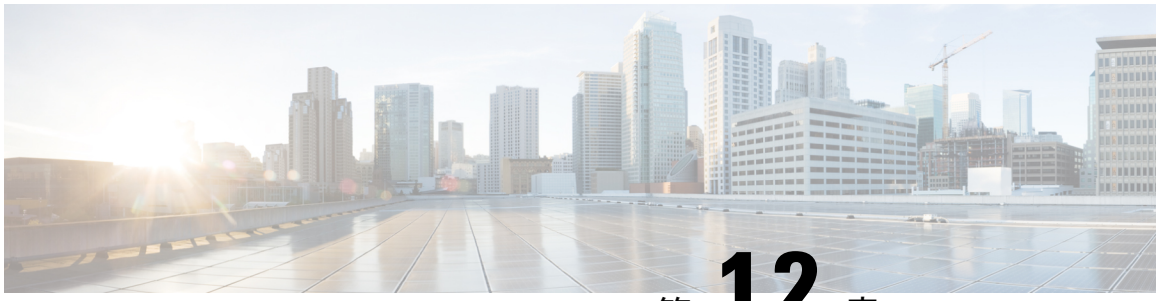
（注） トレーサメモリの制限により、完全なパケットダンプは表示されません。

- 機能データセクション：機能固有のトレースデータを生成し、機能データを復号化する転送プレーン機能が表示されます。これらの機能は、転送結果、ドロップ理由、その他の動作などのデバッグ情報をパケットトレーサに提供します。

パケットトレースの設定例

次の例は、パケットトレースの条件を設定および監視する方法を示しています。

```
Device# debug platform packet-trace packet 2048
Device# debug platform condition ingress
Device# debug platform condition start
Device# debug platform condition stop
Device# show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/2.3060 Gi0/0/2.3060 DROP 402
1 internal0/0/rp:0 internal0/0/rp:0 PUNT 21 2 internal0/0/recycle:0 Gi0/0/2.3060 FWD
```



第 12 章

付録

syslog メッセージ

Cisco vEdge デバイス および Cisco IOS XE SD-WAN デバイス によって生成される syslog メッセージを下記の表に示します。メッセージは生成元のソフトウェアモジュールに基づいてグループ化されます。通常、ソフトウェアモジュールはデバイス上で実行されるプロセス（デーモン）です。

特に指定がない限り、すべての syslog メッセージはすべてのデバイスで生成されます。

各 syslog メッセージには、対応する番号が付けられています。ヘッダーファイルで定義されているメッセージが、稼働中のソフトウェアで現在使用されていない場合でも、表にはすべての syslog メッセージとその番号が一覧で示されています。このようなメッセージの場合、「メッセージ形式」、「説明」、および「アクション」フィールドは空白です。

表の「アクション」フィールドは、syslog メッセージに対応して実行する必要がある推奨アクションを示しています。

- A：組織のサポートチーム内で自動的にチケットを開きます。
- AE：サポートチケットを自動的に開き、チケットをエスカレートします。
- E：組織内の担当チームに電子メールを送信します。

以下の表のいずれにも記載されていない syslog メッセージが表示された場合は、そのメッセージをデバイスとソフトウェアのバージョン情報とともにシスコサポートに送信してください。

CFGMGR：設定マネージャプロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
CFGMGR_SYSLOG_END	399999	Terminating cfgmgr	設定マネージャを停止しています	E
CFGMGR_SYSLOG_SPEED_DUPLEX_NOT_SUPPORTED	300003	—	インターフェイスがデュプレックスモードをサポートしていません	E
CFGMGR_SYSLOG_SPURIOUS_TIMER	300002	—	内部エラー	A
CFGMGR_SYSLOG_IF_STATE	300004	—	設定マネージャーによってインターフェイスの状態が報告されました	E
CFGMGR_SYSLOG_START	300001	Starting cfgmgr	設定マネージャを開始しています	E

CFLOWD：**Cflowd** トラフィックフローのモニタリングプロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
CFLOWD_SYSLOG_MSG	2200002	Received information about vpn_id %ld, vpn_id	Cflowd が VPN の変更を検出しました	E

優先度：**Notice**（通知）

メッセージ	番号	メッセージ形式	説明	アクション
CFLOWD_SYSLOG_END	2299999	Terminating module cflowd because sysmgr terminated	sysmgr の要求で Cflowd モジュールを停止しています	E
CFLOWD_SYSLOG_END	2299999	Terminating module cflowd with error code %d	Cflowd の初期化に失敗して cflowd が停止しようとしているか、cflowd モジュールは停止の途中です	A
CFLOWD_SYSLOG_START	2200001	Starting module cflowd	Cflowd モジュールが起動しています	E

CHMGR：シャーシマネージャ

シャーシマネージャのプロセスは、物理ルータでのみ実行されます。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_CHASSIS_INFO	100009	Chassis-Type %s max-modules %d	シャーシタイプとシャーシでサポートされるモジュール（PIM＋固定）の最大数を示す informational（情報提供）メッセージ	E
CHMGR_FAN_SPEED_HIGH	100003	—	ファン速度が速い	E
CHMGR_FAN_SPEED_NORMAL	100004	—	ファン速度が正常	E
CHMGR_FANTRAY_INSERTED	100052	Fantray %d inserted	ファントレイが挿入されました（vEdge 2000 のみ）	E
CHMGR_FANTRAY_REMOVED	100053	Fantray %d removed	ファントレイが取り外されました（vEdge 2000 のみ）	E
CHMGR_MODULE_INSERTED	100007	Module %d inserted - port type：%s, num_ports：%s	PIM モジュールが挿入されました	E
CHMGR_MODULE_REMOVED	100008	Module %d removed	PIM モジュールが取り外されました	E
CHMGR_PIM_OK	100057	—	PIM モジュールは正常な状態です	E

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_PORT_INSERTED	100005	Port %s inserted in module %d	SFP が挿入されました	E
CHMGR_PORT_REMOVED	100006	Port %s removed from module %d	SFP が取り外されました	E
CHMGR_SIGTERM	100024	Received sigterm, exiting gracefully	シャーシマネージャがダウンしていることを示すデバッグレベルのメッセージ	E
CHMGR_SYSLOG_START	100001	Starting chassis manager	シャーシマネージャのプロセスを開始しています	E
CHMGR_USB_INSERTED	100058	USB media inserted in slot %d	USB メディアが挿入されました	E
CHMGR_USB_REMOVED	100059	USB media removed from slot %d	USB メディアが取り外されました	E

優先度：**Notice**（通知）

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_EMMC_OK	100039	eMMC read successful	EMMC の読み取りに成功しました	E
CHMGR_FAN_OK	100041	Fan Tray %d Fan %d fault cleared, ftrayid, id	ファンの障害が解消されました	E
CHMGR_FANTRAY_OPER	100055	Fan tray '%d' up, ftrayid	ファントレイが検出されました	A
CHMGR_FLASH_OK	100037	Flash memory status read successful	フラッシュメモリの読み取りに成功しました	E
CHMGR_PEM_OK	100043	Power supply '%d' fault cleared	電源障害が解消されました	E
CHMGR_PEM_OPER	100045	Power supply '%d' up	電源が挿入または検出されました	E
CHMGR_SDCARD_OK	100047	SD card read successful	SD カードの読み取りに成功しました	E

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_SFP_UNSUPPORTED	10060	SFP %s is not supported	SFP はサポートされていません	E
CHMGR_SHORT_RESET_REQUEST	100018	—	シャーシマネージャがルータの再起動要求を受け取りました	E
CHMGR_TEMP_GREEN	100030	%s temperature (%d degrees C) is below yellow threshold (%d degrees C)	温度センサーの読み取り値が黄色のしきい値を下回っています	E
CHMGR_TEMP_OK	100027	%s temperature sensor fault cleared	前回の試行失敗後に温度センサーが正常に読み取られました	E

優先度：Warning（注意）

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_HOTSWAP_DIFF_MOD	100051	Hot-Insertion of a module of different type requires reboot. Module %d will remain down,	異なるタイプの PIM モジュールがスロットに挿入されました。モジュールは検出されましたが、次の再起動まで停止したままになります	E

優先度：Error（エラー）

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_CONFD_DATACB_REGISTER_FAILED	100023	Failed to register data cb	confd を使用したデータコールバック関数の登録中に内部エラーが発生しました	AE

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_CONFD_REPLY_FAILED	100022	Failed to send oper data reply - %s (%d)	**show** コマンドのシャーシマネージャ関連の設定を処理中に内部エラーが発生しました	A
CHMGR_EEPROM_READ_FAILED	100011	Failed to read module %d eeprom on chassis %s, module, chassis-name	挿入された PIM の詳細を読み取れませんでした	AE
CHMGR_EEPROM_VERSION_ERROR	100012	Unsupported eeprom format version for module %d	EEPROM バージョンの PIM モジュールがサポートされているため、モジュールが認識されません	AE
CHMGR_EMMC_FAULT	100038	eMMC fault detected	EMMC 情報の読み取り中にエラーが発生しました	A
CHMGR_FAN_FAULT	100040	Fan Tray %d Fan %d fault detected, ftrayid, id	ファン障害が検出されました	A
CHMGR_FANTRAY_DOWN	100054	Fan tray '%d' not present, ftrayid id	ファントレイが検出されませんでした	A

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_FLASH_FAULT	100036	Flash memory status fault	フラッシュメモリの読み取り中に内部エラーが発生しました	AE
CHMGR_GET_HWADDR_FAILED	100010	Failed to get macaddr for %s, p_ifname	インターフェイスの MAC アドレスの取得失敗による内部エラーが発生しました	A
CHMGR_GET_IFFLAG_FAILED	100016	Failed to get ifflags for %s err %d, p_port->kernel_name, errno	インターフェイスの初期化に失敗しました。インターフェイスが停止したままになるか、デバイスが再起動する可能性があります	A
CHMGR_IFFLAGS_SET_FAIL	100050	—	インターフェイスフラグの設定に失敗しました	E
CHMGR_IF_GSO_OFF_FAILED	100025	—	インターフェイスオプションの設定に失敗しました	E

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_PEM_DOWN	100044	Power supply '%d' down or not present	電源が取り外されているか、検出されません	A
CHMGR_PEM_FAULT	100042	Power supply '%d' fault detected	電源の障害が検出されました。	AE
CHMGR_PIM_FAULT	100056	PIM %d power fault	PIM 電源の障害が検出されました。	AE
CHMGR_PIM_FAULT	100056	PIM %d power fault cleared	PIM 電源の障害が解消されました	A
CHMGR_SDCARD_FAULT	100046	SD card fault detected (no present or unreadable)	SD カードの障害が検出されました	A
CHMGR_SET_IFFLAG_FAILED	100017	Failed to set ifflags to %x for %s err %d	インターフェイスの初期化に失敗しました。インターフェイスが停止したままになるか、デバイスが再起動する可能性があります	A
CHMGR_SHORT_RESET_CLEAR_FAILED	100019	—	再起動要求のクリアに失敗しました	A

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_SHORT_RESET_FAILED	100020	—	再起動によるルータのリセット要求に失敗しました	A
CHMGR_SPURIOUS_TIMER	100035	Spurious timer ignored what = %#x arg = %p	内部エラー	A
CHMGR_SYSOUT_OF_RESOURCES	100049	Timer add failed. Out of resources	内部エラー。致命的な場合、デバイスは復旧のために再起動する可能性があります	A
CHMGR_UNKNOWN_MODULE_TYPE	100013	Invalid module-type %x in module-slot %d on chassis %s,	スロットに認識されない PIM モジュールタイプがあります	AE
CHMGR_UNSUPPORTED_MODULE_TYPE	100014	Module-Type %s not supported in slot %d on chassis %s	PIM モジュールは、挿入されているスロットでサポートされていません	A

優先度：**Critical**（クリティカル）

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_IF_RENAME_FAILED	100015	Unable to rename %s to %s	インターフェイスの初期化に失敗しました。インターフェイスが停止したままになるか、デバイスが再起動する可能性があります	A
CHMGR_TEMP_FAULT	100026	%s temperature sensor fault detected. Unable to read temperature	温度センサーの読み取りに失敗しました。温度センサー故障の可能性があります	A
CHMGR_TEMP_RED	100028	%s temperature (%d degrees C) is above red threshold (%d degrees C).	温度センサーの読み取り値が赤色のしきい値を超えています	AE
CHMGR_TEMP_YELLOW	100029	%s temperature (%d degrees C) is above yellow threshold (%d degrees C),	温度センサーの読み取り値が黄色のしきい値を超えています	A

優先度：Alert（アラート）

メッセージ	番号	メッセージ形式	説明	アクション
CHMGR_CONFD_INIT_FAILED	100021	Initialization failed. vconfd_module_init returned %d	シャーシマネージャの初期化と開始に失敗しました	AE

CVMX：内部 Cavium ドライバプロセス

優先度：Informational（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
CVMX_SYSLOG_END	999999	Terminating Cavium drivers	内部 Cavium ドライバを終了しています	E
CVMX_SYSLOG_START	900001	Starting Cavium drivers	内部 Cavium ドライバを起動しています	E

CXP：**SaaS** プロセス向けの **Cloud onRamp**

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
CXP_SYSLOG_END	2799999	Terminating Cloud onRamp process	SaaS 向けの Cloud onRamp を終了しています	E
CXP_SYSLOG_START	2700001	Starting Cloud onRamp process	SaaS 向けの Cloud onRamp を開始しています	E

CONTAINER：コンテナ

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
CONTAINER_SYSLOG_END	2699999	Terminating container process	コンテナプロセスを終了しています	E
CONTAINER_SYSLOG_START	2600001	Starting container process	コンテナプロセスを開始しています	E

DBGD：デバッグプロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
DBGD_SYSLOG_END	2900001	Terminating debug process	デバッグプロセスを終了しています	E
DBGD_SYSLOG_START	2999999	Starting debug process	デバッグプロセスを開始しています	E

DHCPC：**DHCP** クライアント

DHCP クライアントプロセスは、Cisco vEdge デバイスでのみ実行されます。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
DHCP_SYSLOG_CLEAR_INTERFACE	1300006	Clearing dhcp state for interface %s,	DHCP クライアントで、インターフェイスの DHCP 状態がクリアされました	E
DHCP_SYSLOG_DISCOVER_TIMEOUT	1300005	No response for dhcp discover packets for interface %s,	DHCP ディスカバリに失敗しました	E
DHCP_SYSLOG_END	1300001	Terminating syslog process	syslog プロセスを終了します	E
DHCP_SYSLOG_IP_ADDR_ASSIGNED	1300002	Assigned address %s to interface %s	DHCP クライアントでインターフェイスにアドレスが割り当てられました	E
DHCP_SYSLOG_IP_ADDR_RELEASED	1300003	Released address for interface %s	DHCP クライアントでアドレスが解放されました	E
DHCP_SYSLOG_IP_ADDR_RENEWED	1300010	Renewed address %s for interface %s	DHCP クライアントでアドレスが更新されました	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [50%%] for interface %s address %s/%d	リース有効期限の 50% の時点での DHCP クライアント更新要求	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [85%%] for interface %s address %s/%d	リース有効期限の 85% の時点での DHCP クライアント更新要求	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [100%%] for interface %s address %s/%d	リース有効期限の 100% の時点での DHCP クライアント更新要求	E

メッセージ	番号	メッセージ形式	説明	アクション
DHCP_SYSLOG_START	1399999	Starting syslog process	syslog プロセスを開始しています	E

優先度：**Critical**（クリティカル）

メッセージ	番号	メッセージ形式	説明	アクション
DHCP_SYSLOG_IP_ADDR_CONFLICT	1300007	Interface %s IP Address %s conflict with interface %s,	DHCP クライアントで、別のインターフェイスとの IP アドレスの競合が検出されました	E

DHCP：**DHCP サーバー**

DHCP サーバープロセスは、Cisco vEdge デバイスでのみ実行されます。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
DHCP_SYSLOG_CLEAR_SERVER_BINDINGS	1300008	Clearing dhcp server bindings for interface %s, vpn %ld,	DHCP サーバーでインターフェイスのバインディングがクリアされました	E
DHCP_SYSLOG_CLEAR_SERVER_BINDINGS	1300008	Clearing dhcp server binding for interface %s, vpn %ld, mac addr %x:%x:%x:%x:%x:%x,	DHCP サーバーでインターフェイスのバインディングがクリアされました	E

FPMD：転送ポリシーマネージャプロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
FPMD_SYSLOG_ACL_PROGRAM_SUCCESS	1100005	Successfully reprogrammed access list - %s	アクセスリストが正常に作成されました	E
FPMD_SYSLOG_END	1199999	Terminating fpmd	転送ポリシーマネージャプロセスを終了しています	E
FPMD_SYSLOG_POLICY_PROGRAM_SUCCESS	1100004	Successfully reprogrammed policy %s - %s	ポリシーが正常に作成されました。	E
FPMD_SYSLOG_START	1100001	Starting fpmd	転送ポリシーマネージャプロセスを開始しています	E

優先度：**Alert**（アラート）

メッセージ	番号	メッセージ形式	説明	アクション
FPMD_SYSLOG_ACL_PROGRAM_FAILED	1100003	Failed to allocate memory for access list %s. Continuing without the access	アクセスリストを作成できませんでした	A
FPMD_SYSLOG_POLICY_PROGRAM_FAILED	1100002	Failed to allocate memory for policy %s - %s. Continuing without the policy	ポリシーを作成できませんでした	A

FTMD：転送テーブル管理プロセス

転送テーブル管理プロセスは、Cisco vEdge デバイスでのみ実行されます。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SLA_CLASS_ADD	1000020	SLA Class %s added at index %d: loss = %d%%, latency = %d ms	SLA クラスが追加されました	E
FTMD_SYSLOG_BFD_STATE	1000009	record with discriminator %u invalid	BFD が無効な状態です	E
FTMD_SYSLOG_BFD_STATE	1000009	BFD Session %s.%u->%s.%u %s:%u->%s:%u %s %s %s %d	BFD の状態に変化がありました	E
FTMD_SYSLOG_DBGD_STATE	1000036	Connection to DBGD came up Connection to DBGD went down DBGD FTM: Initialized message queue DBGD FTM oper %d vpn %u sip %s:%u dip %s %u DBGD FTM: oper %d vpn %lu localc %d remote %d remoteip %s	FTM デバッグプロセスに関連するメッセージ	E

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SYSLOG_DPI_FLOW_OOM	1000024	Out-of-memory status for DPI flows: %s	SAIE フローのメモリステータス （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。	E

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SYSLOG_DPI_WRITE_OFF	1000032	Turning off writing DPI records to disk	SAIE レコードをディスクに書き込むことができません （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。	E
FTMD_SYSLOG_END	1999999	Terminating FTM process	転送テーブル管理処理を終了しています	E
FTMD_SYSLOG_FIB_GROW	1000012	Growing FIB6 memory to accommodate larger tables):	IPv6 転送テーブルのサイズを拡張しています	E
FTMD_SYSLOG_FIB_GROW	1000012	Growing FIB memory to accommodate larger tables):	IPv4 転送テーブルのサイズを拡張しています	E
FTMD_SYSLOG_IF_STATE	1000001	VPN %lu Interface %s %s,	FTM がインターフェイスの状態の変化を検出しました	E

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SYSLOG_LR_ADD	1000027	LR: Adding Iface %s as LR	ラストリゾート インターフェイスが追加されています	E
FTMD_SYSLOG_LR_ADD	1000027	LR: Iface %s has become an LR	インターフェイスがラストリゾート インターフェイスになりました	E
FTMD_SYSLOG_LR_DEL	1000028	LR: Found iface %s while looking for iface %s	別のインターフェイスを検出中にラストリゾート インターフェイスが見つかりました	E
FTMD_SYSLOG_LR_DEL	1000028	LR: iface %s has become non-LR. Hence set OPER UP on that interface	ラストリゾート インターフェイスがアクティブインターフェイスになりました	E
FTMD_SYSLOG_LR_DEL	1000028	LR: Iface %s has become a non-LR LR: Removing Iface %s as LR	ラストリゾート インターフェイスではなくなったインターフェイスに関するメッセージ	E

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SYSLOG_LR_DOWN	1000030	LR: At least one bfd session of non-LR is active LR: At least one non-LR's bfd session in Up LF bfd session = SIP: %s DIP:%s SPORT:%u DPORT:%u PROTO:%u is Up for at least &u interval msecs LR: Bringing LR's wan if Down in %u msecs LR: Bringing LR's wan if Down right away LR: Cleared LR down_in-progress	ラストリゾート インターフェイスのシャットダウンに関するメッセージ	E
FTMD_SYSLOG_LR_UP	1000029	LR: All bfd sessions gone down. Setting LR %s's OPER state to UP	ルータ上でアクティブな回線が他にないため、ラストリゾートインターフェイスのステータスが稼働に設定されました	E
FTMD_SYSLOG_LR_UP	1000029	LR: Bring LR's wan if up immediately as no other circuit's bfd sessions are up	ルータ上でアクティブな回線が他にないため、ラストリゾートインターフェイスがアクティブ化されました	E

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SYSLOG_LR_UP	1000029	LR: Starting hold up timer immediately !!	ルータ上でアクティブな回線が他にないため、ラストリゾートインターフェイスのホールドタイマーがアクティブ化されました。	E
FTMD_SYSLOG_NAT_FLOW_ADD	1000039	NAT flow add: Private %s, Public %s	指定されたプライベート IP とパブリック IP アドレスを持つ NAT フローの追加が FTM によって検出されました	E
FTMD_SYSLOG_NAT_FLOW_DELETE	1000040	NAT flow delete: Private %s, Public %s	指定されたプライベート IP とパブリック IP アドレスを持つ NAT フローの削除が FTM によって検出されました	E
FTMD_SYSLOG_PIM_DOWN	1000017	—	FTM が PIM の終了を検出しました	E
FTMD_SYSLOG_PIM_UP	1000018	—	FTM が PIM の開始を検出しました	E
FTMD_SYSLOG_ROUTE_ADD_FAIL	1000004	Route Add for prefix %s Failed. Reason %s	FTM は RTM から受信したルートを追加できませんでした	E
FTMD_SYSLOG_ROUTE_VERIFY	1000033	Successfully verified RIB and FIB routes on the Cisco vEdge デバイス	FTM がルータの RIB および FIB でルートを確認しました	E
FTMD_SYSLOG_ROUTE_VERIFY_FAIL	1000034	—	RIB および FIB ルータの検証に失敗しました	E

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SYSLOG_SIGTERM	1000005	Received Cleanup signal. Exiting gracefully	FTM は sysmgr から終了信号を受信し、停止しようとしています	E
FTMD_SYSLOG_START	1000001	Starting FTM process	転送テーブル管理処理を開始しています	E
FTMD_SYSLOG_TCPD_STATE	1000035	Sent tcp_opt_disable successfully for vpn %ld	インターフェイスで TCP オプションが正常に無効化されました	E
FTMD_SYSLOG_TUNNEL_ADD_FAIL	1000015	Tunnel Add to TLOC %s.%s Failed. Reason %s	新しい TLOC の追加に失敗したことが、TTM によって報告されました	E
FTMD_SYSLOG_WWAN_STATE	1000025	Bring %s last resort circuit	ラストリゾートの回線の状態が、稼働または切断になっています	E
FTMD_SYSLOG_WWAN_STATE	1000025	Connection to WWAN came up	ラストリゾートの回線が稼働しました	E
FTMD_SYSLOG_WWAN_STATE	1000025	Connection to WWAN went down	ラストリゾートの回線が切断されました	E

優先度：Notice（通知）

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SLA_CLASS_DEL	1000022	Sla class %s at index %d removed: loss = %d%%, latency = %d ms, jitter = %d ms	SLA クラスが削除されました	A
FTMD_SLA_CLASS_MOD	1000021	Sla class %s at index %d modified: loss = %d%%, latency = %d ms, jitter = %d ms	SLA クラスが変更されました	A

FTMD_SLA_CLASS_VIOLATION	1000023	[%lu] SLA class violation application %s %2:%u._%s:&u protocol: %d dscp: %d %s, status - %s	送信元アドレスとポート、宛先アドレスとポート、プロトコル、DSCP、および理由が指定された VPN のアプリケーションに SLA クラス違反があります	A
FTMD_SYSLOG_DOT1X_HOST	1000031	Host %s denied access on interface %s in single host mode	シングルホストモードの 802.1X インターフェイスは、すでにクライアントへのアクセスを許可しているため、アクセスを拒否しています。	E
FTMD_SYSLOG_FLOW_LOG	1000026	%s	FTM は新しいフローを検出しました	E
FTMD_SYSLOG_FP_CORE_FAIL	1000013	FP core watchdog expired (rc = %d). %s, rc, action_str	FTM は、FP が機能していない可能性があることを検出しました。デバイスはすぐに再起動します	A
FTMD_SYSLOG_PMTU_LOWERED	1000016	Tunnel %s/%d -> %s/%d MTU Changed to %u due to Path-MTU Discovery,	パス MTU ディスカバリにより、トンネルの MTU サイズが変更されました	E
FTMD_SYSLOG_ZBFW_FLOW_ADD	1000037	ZBF flow created zone-air %s key %s src_vpn %d dst_vpn %d expiry secs %d state %s	FTM はゾーンペアの作成を検出しました	E
FTMD_SYSLOG_ZBFW_FLOW_DEL	1000038	ZBF flow deleted zone-air %s key %s src_vpn %d dst_vpn %d state %s	FTM はゾーンペアの削除を検出しました	E

優先度：Critical（クリティカル）

メッセージ	番号	メッセージ形式	説明	アクション

FTMD_SYSLOG_BUFFER_POOL_LOW （注） このエラーメッセージは、Cisco SD-WAN リリース 20.7.1 以降で生成されます。	1000041	Critical Alert: Buffer Pool <num>: available buffers are x% of total buffers	FTM は、指定されたバッファプールがキャパシティの 20% を下回ったことを検出しました	E

優先度：**Warning**（注意）

メッセージ	番号	メッセージ形式	説明	アクション
FTMD_SYSLOG_BUFFER_POOL_LOW （注） このエラーメッセージは、Cisco SD-WAN リリース 20.7.1 以降で生成されます。	1000041	Warning Alert: Buffer Pool <num>: available buffers are x% of total buffers	FTM は、指定されたバッファプールがキャパシティの 50% を下回ったことを検出しました	E
FTMD_SYSLOG_TTM_DOWN	1000008	Connection to TTM went down. p_msgq %p p_ftm %p,	TTM と FTM の接続が切断されました。 BFD セッションはクリアされます	E
FTMD_SYSLOG_TTM_UP	1000007	Connection to TTM came up. p_msgq %p p_ftm %p,	FTM と TTM が接続されました	E
FTMD_TUNNEL_SLA_CHANGED	1000019	SLA changed for session: %s.%u->%s:%u->%s:%u. New loss = %d%%, latency = %d ms, jitter = %d ms, SLA Classes: %s (ox%x) %s%s	FTM はトンネルで SLA の変更を検出しました	E

優先度：**Error**（エラー）

メッセージ	番号	メッセージ形式	説明	アクション

FTMD_SYSLOG_CONFD_FAIL	1000003	Failed to register bfd show data cb	FTM は、confd にデータコールバックを登録できませんでした。デバイスが再起動する場合があります	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	Failed to register policer show data cb	FTM は、confd にデータコールバックを登録できませんでした。デバイスが再起動する場合があります	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	%s: Failed to register data cb, __FUNCTION__	FTM は、confd にデータコールバックを登録できませんでした。デバイスが再起動する場合があります	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	%s: Failed to send oper data reply - %s (%d) : %s,	FTM は confd に正しく応答できませんでした。一部の **show** コマンドは機能しない場合があります	A
FTMD_SYSLOG_FP_COREDUMP	1000011	FP Core %d Died. Core file recorded at %s,	FTM が FP クラッシュを検出しました。デバイスはすぐに再起動します	AE
FTMD_SYSLOG_IFADD_FAIL	1000014	Failed to add interface %s in vpn %lu. Out of forwarding interface records	転送インターフェイスのデータベースレコードが不十分なため、インターフェイスが追加されませんでした	A
FTMD_SYSLOG_IFADD_FAIL	1000014	Failed to add interface %s in vpn %lu. Out of snmp interface indices	SNMP インターフェイスのインデックスが不十分なため、インターフェイスが追加されませんでした	A
FTMD_SYSLOG_INIT_FAIL	1000002	vconf_module_init returned %d	FTM は confd で開始できませんでした	A

FTMD_SYSLOG_LR_DEL	1000028	LR: LR is not enabled...while we are trying to remove iface %s as last resort	削除されるインターフェイスは、ラストリゾート インターフェイスとして設定されていません	A
FTMD_SYSLOG_LR_DEL	1000028	LR: Unable to remove iface %s as LR	インターフェイスがラストリゾート インターフェイスでないため、削除できません	A
FTMD_SYSLOG_RTM_DECODE_FAIL	1000006	Bad RTM Msg: Msg-Type %u Msg-Len %u len: %u decoded-len %u,	RTMからのルートまたはインターフェイス変更メッセージを処理できませんでした	A
FTMP_SYSLOG_SPURIOUS_TIMER	1000010	Spurious timer ignored what = %#x arg = %p,	内部エラー	A

GPS: Global Positioning System

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
GPS_SYSLOG_END	2599999	Terminating GPS	GPS プロセスを終了しています	E
GPS_SYSLOG_GGA_FIX	2500002	GGA %d:%d:%d lat=%f lon=%f alt=%f sat=%d hdop %f fix%d	GPS の修正情報	E
GPS_SYSLOG_GSA_FIX	2500004	GSA %s pdop=%.2f hdop=%.2f vdop=%.2f	GPS 衛星と精度の希釈（DOP）情報	E
GPS_SYSLOG_PSTOP	2500005	Polling disabled Stopping polling timers	GPS 情報のポーリングに関するメッセージ	E
GPS_SYSLOG_RMC_FIX	2500003	RMC %s %d %d lat=%f lon=%f speed %f course=%s status valid	GPS の基本情報	E
GPS_SYSLOG_START	2500001	Starting GPS	GPS プロセスを開始しています	E

IGMP：インターネットグループ管理プロトコル

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
IGMP_SYSLOG_END	1800001	Terminating IGMP	IGMP プロセスを終了しています	E
IGMP_SYSLOG_START	1899999	Starting IGMP	IGMP プロセスを開始しています	E

LIBBSS：**UNIX BSS** ライブラリ

未使用のメッセージ

メッセージ	番号	メッセージ形式	説明	アクション
LIBBSS_SYSLOG_END	1699999	Terminating libbss	UNIX BSS ライブラリプロセスを終了しています	E
LIBBSS_SYSLOG_START	1600001	Starting libbss	UNIX BSS ライブラリプロセスを開始しています	E

LIBCHMGR：シャーシマネージャのライブラリプロセス

未使用のメッセージ

メッセージ	番号	メッセージ形式	説明	アクション
LIBCHMGR_SYSLOG_END	1599999	Terminating libchmrg	シャーシマネージャのライブラリプロセスを終了しています	E
LIBCHMGR_SYSLOG_START	1500001	Starting libchmgr	シャーシマネージャのライブラリプロセスを開始しています	E

MSGQ：メッセージキュープロセス

未使用のメッセージ

メッセージ	番号	メッセージ形式	説明	アクション
MSGQ_SYSLOG_END	899999	Terminating msgq	メッセージキュープロセスを終了しています	E
MSGQ_SYSLOG_START	800001	Starting msgq	メッセージキュープロセスを開始しています	E

OMP：オーバーレイ マネジメント プロトコル

優先度：**Informational**（情報提供）またはその他

メッセージ	番号	メッセージ形式	説明	アクション
OMP_NUMBER_OF_CISCO_VSMARTS	400005	Number of Cisco vSmarts connected: %u	デバイスに接続されている Cisco vSmart コントローラ の数（Cisco vEdge デバイス のみ）	E
OMP_PEER_STATE_CHANGE	400002	%s peer %s state changed to %s,	OMP ピアの状態が稼働または停止に変更されました	E
OMP_POLICY_CHANGE	400007	Using policy from peer %s,	Cisco vSmart コントローラ から転送ポリシーを受信しました（Cisco vEdge デバイスのみ）	E
OMP_STATE_CHANGE	400003	Operational state changed to %s,	OMP の内部処理の状態に変化がありました	E
OMP_TLOC_STATE_CHANGE	400004	TLOC %s state changed to %s for address-family: %s,	TLOC の状態に変化がありました	E

優先度：**Notice**（通知）

メッセージ	番号	メッセージ形式	説明	アクション
OMP_SYSLOG_END	400006	Terminating	OMP プロセスを停止しています	E

メッセージ	番号	メッセージ形式	説明	アクション
OMP_SYSLOG_START	400001	Starting	OMP プロセスを開始しています	E

PIM：プロトコル独立型マルチキャストプロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
IGMP_SYSLOG_END	1900001	Terminating	PIM プロセスを終了しています	E
IGMP_SYSLOG_START	1999999	Starting	PIM プロセスを開始しています	E

優先度：**Notice**（通知）

メッセージ	番号	メッセージ形式	説明	アクション
PIM_SYSLOG_IF_STATE_CHANGE	1900003	VPN %lu Interface %s %s	指定された VPN で、インターフェイスの状態が稼働または停止に変更されました	E
PIM_SYSLOG_NBR_STATE_CHANGE	1900002	Neighbor %s state changed to up	PIM ネイバーが稼働しました	E
PIM_SYSLOG_TUNNEL_STATE_CHANGE	1900004	Tunnel %s state changed to %s	停止または稼働時に PIM でトンネルが使用されました	E

優先度：**Error**（エラー）

メッセージ	番号	メッセージ形式	説明	アクション
PIM_SYSLOG_NBR_STATE_CHANGE	1900002	Neighbor %s stated changed to down	PIM ネイバーがダウンしました	E

POLICY: ポリシープロセス

未使用のメッセージ

メッセージ	番号	メッセージ形式	説明	アクション
POLICY_SYSLOG_END	799999	Terminating policy	ポリシープロセスを終了しています	E
POLICY_SYSLOG_START	700001	Starting policy	ポリシープロセスを開始しています	E

RESOLV：レゾルバプロセス

未使用のメッセージ

メッセージ	番号	メッセージ形式	説明	アクション
RESOLV_SYSLOG_END	2000001	Terminating resolver	リゾルバプロセスを終了しています	E
RESOLV_SYSLOG_START	2099999	Starting resolver	リゾルバプロセスを開始しています	E

SNMP リスナープロセス

未使用のメッセージ

メッセージ	番号	メッセージ形式	説明	アクション
SNMP_SYSLOG_END	2100001	Terminating SNMP listener	SNMP リスナープロセスを終了しています	E
SNMP_SYSLOG_START	2199999	Starting SNMP listener	SNMP リスナープロセスを開始しています	E

SYSMGR：システムマネージャプロセス

システムマネージャプロセス（デーモン）は、システム内のすべてのプロセスを生成、監視、および終了します。また、メモリや CPU の状態といった重要なシステム情報を収集してログに記録します。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CONFD_PHASE1_INFO	200041	Generated authorized keys on %s, p_sysmgr->cfg.my_personality	Cisco vManage サーバーと Cisco SD-WAN デバイス間で SSH ベースのログイン用の認証キーが生成されました	E
SYSMGR_CONFD_PHASE2_SUCCESS	200007	Confd Phase2 Up	デバイスが正常に起動されました	E
SYSMGR_DAEMON_START	200017	Started daemon %s @ pid %d in vpn %lu,	システムマネージャが VPN でプロセスを開始しました	E
SYSMGR_DAEMON_UP	200011	Daemon %s @ pid %d came up in vpn %lu (%d %d)	システムマネージャによって開始されたデーモンが、想定通りに起動しました	E
SYSMGR_SIGTERM	200001	Received sigterm, stopping all daemons except confd	システムマネージャが終了シグナルを受け取ったため、すべてのプロセスの終了を開始します	E
SYSMGR_VPN_DESTROY	200022	vpn %lu destroy. lookup returned %p	VPN のすべてのプロセスを停止しています	E

優先度：**Notice**（通知）

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CLOCK_SET	200025	System clock set to %s	ユーザーがシステムクロックを設定しました	E
SYSMGR_CONFD_CDB_NOT_INITED	200031	Confd db initialization not complete. Deleting cdb and starting afresh.	設定データベースの初回の初期化	E
SYSMGR_CONFD_PHASE1_INFO	200041	Install successfully completed from %s to %s	インストール ID の読み取りに失敗しました。デフォルトにフォールバックします	E
SYSMGR_CORE_FILE_COMPRESSED	200045	—	コアファイルが圧縮されました	E
SYSMGR_DAEMON_EXIT_NORMAL	200021	—	プロセスが正常に終了しました	E
SYSMGR_DAEMON_RESTARTED	200043	—	プロセスが再開されました	E
SYSMGR_DISK_ALERT_OFF	200036	Disk usage is below 60%%.	ディスク使用率がしきい値を下回っています	E
SYSMGR_MEMORY_ALERT_OFF	200058	System memory usage is below 50%	システムメモリ使用率が 50%を下回っています	E
SYSMGR_MISC	200065	—	その他のメッセージ	E

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_REBOOT	200038	System going down for a reboot.. (%s), reason	システムマネージャがデバイスを再起動しています。おそらくプロセスエラーが原因です。	E
SYSMGR_SHM_FAIL	200042	Created shared memory %s	他のプロセスとの通信時に使用される共有メモリが正常に初期化されました	E
SYSMGR_SHUTDOWN	200040	System shutting down.. (%s), reason	システムマネージャがデバイスの電源を切断しています。物理的に電源を入れ直さない限り、デバイスは稼働状態に戻りません	A
SYSMGR_SYSTEM_GREEN	200050	System up with software version %s	システムステータスは緑です。すべてのプロセスが想定通りどおりに起動したことを示します	E
SYSMGR_SYSTEM_RED	200051	System status red (software version '%s')	システムステータスが赤です。プロセスエラーが原因の可能性があります	A
SYSMGR_SYSTEM_START	200002	Starting system with Cisco SD-WAN software version %s	システムからのメッセージです。通常、デバイス起動中の最初のメッセージの 1 つです。	E

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_TIMEZONE_SET	200028	System timezone changed from %s to %s	設定の変更により、システムのタイムゾーンが変更されました	E
SYSMGR_UPGRADE_AUTO_CONFIRMED	200063	—	ソフトウェアのアップグレードが自動的に確認されました	E
SYSMGR_UPGRADE_NOT_CONFIRMED	200049	—	ソフトウェアのアップグレードが確認されませんでした	E
SYSMGR_UPGRADE_PENDING_CONFIRMATION	200059	—	ソフトウェアのアップグレードは確認待ちです	E
SYSMGR_VDEBUG_LOG_CLEANUP_NEEDED	200066	Debug logs exceed expected storage quota. Performing age-based cleanup to restore debug logging operations.	スペースを作成するためにデバッグログが削除されました	A
SYSMGR_DAEMON_TERMINATED	200020	—	プロセスが停止されました	E
SYSMGR_WATCHDOG_EXPIRED	200062	—	ウォッチドッグプロセスが期限切れになりました	A

優先度：**Warning**（注意）

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CORE_FILE_DELETED	200044	—	コアファイルが削除されました	A
SYSMGR_DAEMON_RESTART_ABORTED	200060	—	プロセスの再起動が中止されました。	A
SYSMGR_DAEMON_STOP	200018	Stopping daemon %s @ pid %d. Sending signal %d	システムマネージャがデーモンを停止しました	E
SYSMGR_DISK_ALERT_ORANGE	200054	Disk usage is above 75%%. Please clean up unnecessary files.	ディスク使用率が 75% を超えています	E
SYSMGR_DISK_ALERT_YELLOW	200035	Disk usage is above 60%%. Please clean up unnecessary files.	ディスク使用率が 60% を超えています	E
SYSMGR_FILE_DELETED	200064	Deleted file %s (size %lu MB) to recover disk space	ディスク容量を解放するためにファイルが削除されました	A
SYSMGR_MEMORY_ALERT_ORANGE	200056	System memory usage is above 75%%	システムメモリ使用率が 75% を超えました	E
SYSMGR_MEMORY_ALERT_YELLOW	200057	System memory usage is above 60%%	システムメモリ使用率が 60% を超えました	E

優先度：**Error**（エラー）

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_BAUD_RATE_SET	200046	Console baud rate changed to '%d', baud_rate	コンソールボーレートが変更されました	E
SYSMGR_BAUD_RATE_SET_FAIL	200047	Failed to set console baud rate in OS to '%d'	Linus でユーザーが指定したコンソールボーレートを設定できませんでした	A
SYSMGR_BAUD_RATE_SET_FAIL	200047	Failed to set console baud rate in U-boot to '%d'	Uboot でユーザーが指定したコンソールボーレートを設定できませんでした	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CLOCK_SET_FAIL	200026	Cannot set system clock to %s	ユーザーが指定した時刻に合わせてシステムクロックを設定できませんでした	A
SYSMGR_CONFD_CDB_INIT_OPEN_FAIL	200030	Failed to open cdb init file (%s)	設定データベースを開けませんでした	A
SYSMGR_DAEMON_EXIT_FAIL	200023	—	プロセスを終了できませんでした	A
SYSMGR_CONFD_DATACB_REGISTER_FAIL	200010	Failed to register data cb	confd にデータコールバック関数を登録できませんでした。デバイスが再起動する場合があります	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CONFD_CDB_DEL_FAIL	200032	Failed to remove cbd directory '%s'	障害から回復するための設定データベースの再初期化に失敗しました	AE
SYSMGR_CONFD_FORK_FAILURE	200003	Cannot move confd to phase2 (err %s)	confd をフェーズ 2 に移行できませんでした。デバイスはすぐに再起動されます	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate archive keys	アーカイブ設定に必要なキーの生成に失敗しました	E

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate authorized keys on %s, p_sysmgr->cfg.my_personality	Cisco vManage サーバーと Cisco SD-WAN デバイス間で SSH ベースのログイン用の認証キーを生成できませんでした	E
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate SSH keys for archive	SSH キーの生成に失敗しました	E
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to get install id from file, using 00_00	以前のシステムバージョンを読み取れませんでした	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to get previous version, using 0.0	システムバージョンを読み取れませんでした	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to transition confd to phase1. Re-initializing CDB..	confd モジュールをフェーズ 1 に移行できませんでした。設定データベースに障害が発生した可能性があります。デバイスはすぐに再起動されます	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Verified that archive keys exist	設定アーカイブキーが確認されました	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to get current version, using 0.0	システムバージョンファイルを読み取れませんでした	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to open %s, version_file	システムバージョンファイルを開けませんでした	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to read %s, version_file	システムバージョンファイルを読み取れませんでした	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to transition confd to phase2	confd モジュールをフェーズ 2 に移行できませんでした。設定データベースに障害が発生した可能性があります。デバイスはすぐに再起動されます	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CONFD_REPLY_FAIL	200009	Failed to send oper data reply - %s (%d)	confd に応答できませんでした。一部の **show** コマンドは機能しない場合があります	A
SYSMGR_CONFD_SETPGID_FAILURE	200004	setpgid(0,0) failed: %d	プロセスグループを開始できませんでした	A
SYSMGR_DAEMON_DOWN	200012	Daemon %s [%u] went down in vpn %lu,	システムマネージャが開始したプロセスがダウンしました	A
SYSMGR_DAEMON_EXECV_FAILURE	200016	execv %s failed	プロセスの開始中に内部エラーが発生しました	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_DAEMON_FORK_FAILURE	200014	Cannot start daemon %s: %s	プロセスの開始中に内部エラーが発生しました	A
SYSMGR_DAEMON_INACTIVE	200033	Daemon %s[%lu] @ pid %d died. Rebooting device..	システムマネージャがプロセス障害を検出し、デバイスを再起動しようとしています	A
SYSMGR_DAEMON_MSGQ_FAILURE	200013	Could not start msgq to daemon %s. err %d	プロセスでメッセージキューを確立できませんでした。デバイスはすぐに再起動する場合があります	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_DAEMON_MSGQ_FAILURE	200013	Could not start msgq to quagga daemon %s. err %d	ルーティングプロセスでメッセージキューを確立できませんでした。デバイスはすぐに再起動する場合があります	A
SYSMGR_DAEMON_SETAFFINITY_FAILURE	200061	—	プロセスのスケジューリングに失敗しました	E
SYSMGR_DAEMON_SETPGID_FAILURE	200015	setpgid(0,0) failed	プロセスグループの設定中に内部エラーが発生しました	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_DAEMON_STOPPED	200019	Daemon %s @ pid %u terminated - %s	システムマネージャによって開始されたデーモンが終了しました。デバイスはすぐに再起動する場合があります（Cisco vBond オーケストレーションを除く）	A
SYSMGR_RTC_CLOCK_SET_FAIL	200027	Cannot set hardware clock to %s - %s (errno	ユーザーが指定したシステム時刻に合わせてハードウェアクロックを更新できませんでした	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_SHM_FAIL	200042	Failed to close shared memory %s with an error %d	他のプロセスとの通信時に使用される共有メモリのクローズが正常に実行されませんでした	E
SYSMGR_SHM_FAIL	200042	Failed to map shared memory %s	他のプロセスとの通信時に使用される共有メモリの初期化に失敗しました	E
SYSMGR_SHM_FAIL	200042	Failed to open shared memory %s with an error %d	他のプロセスとの通信時に使用される共有メモリをオープンできませんでした	E

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_SHM_FAIL	200042	Failed to truncate shared memory %s with an error %d	他のプロセスとの通信時に使用される共有メモリの初期化に失敗しました	E
SYSMGR_SHM_FAIL	200042	Failed to unmap shared memory %s	他のプロセスとの通信時に使用される共有メモリのクローズが正常に実行されませんでした	E
SYSMGR_SWITCHBACK_FAILED	200053	Software upgrade to version %s failed because of %s	ソフトウェアのアップグレードに失敗しました。	A

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_TIMEZONE_SET_FAIL	200029	Failed to set system timezone to %s (rc = %d)	ユーザーが指定したタイムゾーンに合わせてシステムのタイムゾーンを設定できませんでした	A
SYSMGR_TRACE_ERROR	200024	—	トレースエラーが発生しました	A

優先度：**Critical**（クリティカル）

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_CONFD_INIT_FAIL	200008	Sysmgr child in charge of migrating confd/ncs to phase2 exited with error code %d	システムマネージャが confd プロセスの障害を検出しました。デバイスが再起動する場合があります	AE
SYSMGR_DISK_ALERT_RED	200034	Disk usage is above 90%% (critically high). Please clean up unnecessary files.	ディスク使用率が 90% を超えています	AE
SYSMGR_MEMORY_ALERT_RED	200055	System memory usage is above 90%% (critically high)	システムメモリ使用率が 90% を超えています	AE

メッセージ	番号	メッセージ形式	説明	アクション
SYSMGR_REBOOT_HALTED	200039	Reboot (reason: %s) terminated...too many reboots	システムマネージャは、短期間に再起動が多すぎることを検出したため、デバイスの再起動を停止しました。	AE
SYSMGR_UPGRADE_FAILED	200052	Software upgrade to version %s failed because of reason	ソフトウェアのアップグレードに失敗しました。	AE

TCPD：TCP オプションプロセス

優先度：Informational（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
TCPD_MSGQ_SERVER	2800002	Server Exception: %s	プロキシサーバーで接続が許可されませんでした	E
TCPD_PROXY	2800004	Enabled TCP_OPT for vpn %lu: %s:%u %s Starting sysmgr_app object tcpd<->ftmd channel established tcpd<->ftmd = Will try connecting	プロキシの起動に関するメッセージ	E
TCPD_PROXY	2800004	tcpd error counters -%s	TCP オプションのエラー数	E
TCPD_SYSLOG_END	2800001	Terminating TCP options	TCP オプションプロセスを終了しています	E
TCPD_SYSLOG_START	2899999	Starting TCP options	TCP オプションプロセスを開始しています	E
TCPD_SYSMGR_APP	2800003	%s Exception: %s %s - Sysmgr app::connect -Exception - %s	システムマネージャと TCP プロキシプロセス間の接続に関するメッセージ	E

優先度：Debug（デバッグ）

メッセージ	番号	メッセージ形式	説明	アクション
TCPD_SYSMGR_APP	2800003	%s - Registering for send_hello-msg %s: Sending following register msg Sending msg of length %u %s - Sysmgr app::connect %s - Write %u bytes %s - Wrote register msg %u	システムマネージャと TCP プロキシプロセス間の接続に関するメッセージ	E

TRACKER：インターフェイス トラッカー プロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
TRACKER_SYSLOG_CONN_DOWN	1700003	Connection to %s %s Down	インターフェイスへの接続が切断されています	E
TRACKER_SYSLOG_CONN_UP	1700002	Connection to %s %s Up	インターフェイスへの接続が確立されています	E
TRACKER_SYSLOG_END	1700001	Terminating	インターフェイストラッカープロセスを終了しています	E
TRACKER_SYSLOG_START	1799999	Starting	インターフェイストラッカープロセスを開始しています	E

VCONFD：**Cisco SD-WAN** 設定プロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
VCONFD_SYSLOG_END	1400001	Terminating	設定プロセスを終了しています	E

メッセージ	番号	メッセージ形式	説明	アクション
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s process name: %s process id: %s reason: %s	指定された日時のプロセスの設定と理由	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s status: %s install id: %s message %s	指定された日時とステータス（Minor、Major）の設定	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s reason: %s	指定された日時の設定と理由	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s reboot reason: %s	指定された日時の設定と再起動の理由	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s username: %s remote host: %s	指定された日時のユーザー名とリモートホストの設定	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s vpn id: %s if name: %s mac addr: %s ip-addr:%s	指定された日時のVPN、インターフェイス、MACアドレス、IPアドレスの設定	E
VCONFD_SYSLOG_START	1499999	Starting	設定プロセスを開始しています	E

VDAEMON：**Cisco SD-WAN** ソフトウェアプロセス

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
VDAEMON_SYSLOG_DOMAIN_ID_CHANGE	500006	System Domain-ID changed from '%d' to '%d',	システムのドメインIDが変更されました	E
VDAEMON_SYSLOG_END	599999	—	プロセスを終了しています	E
VDAEMON_SYSLOG_ORG_NAME_CHANGE	500008	System Organization-Name changed from '%s' to '%s'	システムの組織名が変更されました	E
VDAEMON_SYSLOG_PEER_STATE	500003	Peer %s Public-TLOC %s Color %u %s,	ピアの状態が稼働または停止に変更されました	E
VDAEMON_SYSLOG_SITE_ID_CHANGE	500005	System Site-ID changed from '%d' to '%d'	システムのサイトIDが変更されました	E
VDAEMON_SYSLOG_START	500001	—	プロセスを開始しています	E
VDAEMON_SYSLOG_SYSTEM_IP_CHANGE	500007	System-IP changed from '%s' to '%s'	システムのIPアドレスが変更されました	E

優先度：**Error**（エラー）

メッセージ	番号	メッセージ形式	説明	アクション
VDAEMON_BOARD_ID_CHALLENGE_FAILED	500002	—	ボードIDを確認できませんでした	E
VDAEMON_BOARD_ID_INIT_FAILED	500001	—	ボードIDを確認できなかったため、ボードの初期化に失敗しました	E
VDAEMON_SYSLOG_CERT_STORE_FAIL	500009	Certificate store init failed	証明書が保存されていません	AE

メッセージ	番号	メッセージ形式	説明	アクション
VDAEMON_SYSLOG_PEER_AUTH_FAIL	500004	Peer %s Public-TLOC %s Color %u %s	vdaemon ピアによる認証に失敗しました	E
VDAEMON_SYSLOG_PEER_STATE	500003	Failed to read system host name	システムのホスト名の読み取り中に内部エラーが発生しました。デバイスが Cisco vManage サーバーに登録されないか、ZTP で障害が発生します	A

VRRP：**Virtual Router Redundancy Protocol**

VRRP プロセスは、Cisco vEdge デバイスでのみ実行されます。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
VRRPD_STATE_CHANGE	600002	Group %d, interface %s, vpn %lu state changed to %s	VRRP インターフェイスの状態が変更されました	E
VRRPD_SYSLOG_END	699999	Terminating VRRPD	VRRP プロセスを終了しています	E
VRRPD_SYSLOG_START	600001	Starting VRRPD	VRRP プロセスを開始しています	E

WLAN：**無線 LAN プロセス**

無線 LAN プロセスは、Cisco vEdge デバイスでのみ実行されます。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
WLAN_SYSLOG_END	2300001	Terminating wlan	WLAN プロセスを終了しています	E

メッセージ	番号	メッセージ形式	説明	アクション
WLAN_SYSLOG_START	2399999	Starting wlan	WLAN プロセスを開始しています	E

WWAND：セルラープロセス

無線 WAN プロセスは、Cisco vEdge デバイスでのみ実行されます。

優先度：**Informational**（情報提供）

メッセージ	番号	メッセージ形式	説明	アクション
WWAN_SYSLOG_ADMIN_DWL	2400010	Cellular%d interface is set for deletion	セルラーインターフェイスが削除されようとしています	E
WWAN_SYSLOG_ADMIN_DOWN	2400009	Cellular%d interface is set to admin down	セルラーインターフェイスが administratively down の状態です	E
WWAN_SYSLOG_ADMIN_UP	2400008	Cellular%d interface is set to admin up	セルラーインターフェイスが administratively up の状態です	E
WWAN_SYSLOG_CONNECT	2400002	Connected to Cellular%d modem	セルラーモデムへの接続が確立されました	E
WWAN_SYSLOG_CONNECT_DATA	2400006	—	—	E
WWAN_SYSLOG_DATA_MONITOR	2400032	Info: %lld bytes left Info: exceeded by %lld bytes	支払請求サイクルの残りデータ量に関する情報	E

メッセージ	番号	メッセージ形式	説明	アクション
WWAN_SYSLOG_DATA_SESSION	2400019	Data session started successfully	セルラーインターフェイスのデータセッションが正常に開始されました	E
WWAN_SYSLOG_DATA_SESSION_BEARER	2400028	Data bearer changed to %s (%lx)	データキャリアが変更されました	E
WWAN_SYSLOG_DATA_SESSION_DISCONNECT	2400023	Data session disconnect: restarting session	データセッションが切断されたため、再開しています	E
WWAN_SYSLOG_DATA_SESSION_DISC_REASON	2400024	Data session disconnect reason: %s	データセッション切断の理由	E
WWAN_SYSLOG_DATA_SESSION_DISC_VERB	2400025	Data session disconnect reason verbose: %s	データセッション切断の詳しい理由	E
WWAN_SYSLOG_DATA_SESSION_DOMAIN	2400026	Packet-switched domain state change to %s: registration: %s ran: %s if: %s	パケット交換ドメインが変更されました	E
WWAN_SYSLOG_DATA_SESSION_DORMANCY	2400029	Dormancy state changed to %s	セッションドーマンシーの状態が変更されました	E
WWAN_SYSLOG_DATA_SESSION_NETWORK	2400027	Network registration changed to %s: domain: %s ran: %s if: %s	ネットワーク登録が変更されました	E

メッセージ	番号	メッセージ形式	説明	アクション
WWAN_SYSLOG_DATA_SESSION_START	2400018	Starting data session on Cellular%e	セルラーインターフェイスのデータセッションを開始しています	E
WWAN_SYSLOG_DATA_SESSION_STATE	2400020	Data session state changed to %s	データセッションの状態	E
WWAN_SYSLOG_DATA_SESSION_STOP	2400022	Data session stopped successfully	データセッションが停止しました	E
WWAN_SYSLOG_DISCONNECT	2400003	Disconnected LTE modem %d	LTE モデムから切断されました	E
WWAN_SYSLOG_END	2400001	Terminating WWAND	WWAN プロセスを終了しています	E
WWAN_SYSLOG_FIRMWARE	2400007	Failed to get firmware details after upgrade on modem %d Firmware upgrade failed on modem %d Firmware upgrade successful on modem %d Upgrading firmware configuration on modem %d Upgrading firmware image on modem %d	セルラーモデムのファームウェア アップグレードに関するメッセージ	E

メッセージ	番号	メッセージ形式	説明	アクション
WWAN_SYSLOG_LR_DOWN	2400012	%s%d: bringing down	ラストリゾートインターフェイスをシャットダウンしています	E
WWAN_SYSLOG_LR_UP	2400011	%s%d: bringing up	ラストリゾートインターフェイスを開始しています	E
WWAN_SYSLOG_MODEM_ACTIVATION	2400039	Modem activation status: %s (%lu)	モデムの実際の状態とステータス	E
WWAN_SYSLOG_MODEM_PMODE	2400017	Modem is not in online mode Modem is not in online mode (tmp: %s degrees C) Modem power state is: %s (prev: %s) Modem set to %s (prev: %s) Powered off the modem %d	モデムの電源モードのステータスに関するメッセージ	E
WWAN_SYSLOG_MODEM_STATE	2400034	Modem device state changed to %s	モデムの状態に変化がありました	E
WWAN_SYSLOG_MODEM_TEMP	2400037	Modem temperature %d degree C: %s	モデムの温度と状態	E
WWAN_SYSLOG_MODEM_UP	2400035	WWAN cellular%d modem is back up	モデムが再接続されました	E

メッセージ	番号	メッセージ形式	説明	アクション
WWAN_SYSLOG_OMA_DM_DONE	2400041	Modem OMA DM configuration completed	モデムの OMA-DM 設定が完了しました	E
WWAN_SYSLOG_OPER_DOWN	2400014	Cellular%d set if down	セルラーインターフェイスの動作が停止しています	E
WWAN_SYSLOG_OPER_UP	2400013	Cellular%d set if up	セルラーインターフェイスは稼働中です	E
WWAN_SYSLOG_PROFILE_CHECK	2400030	Profile %lu with PDP: %s APN: %s Auth: %s User: %s	セルラープロファイル情報	E
WWAN_SYSLOG_REBOOT	2400040	Cellular%d modem mode updated: rebooting; %s reason	セルラーモデムが再起動した理由	E
WWAN_SYSLOG_SDK_DOWN	2400005	SDK got terminated: %s	ソフトウェア開発キットへの接続が終了しました	E
WWAN_SYSLOG_SDK_UP	2400004	Connected to Cellular%d sdk process	セルラーソフトウェア開発キットへの接続が確立されました	E
WWAN_SYSLOG_SIM_STATUS	2400033	SIM status changed to: %s	SIM ステータスに変化がありました	E
WWAN_SYSLOG_START	2499999	Starting WWAND	WWAN プロセスを開始しています	E

メッセージ	番号	メッセージ形式	説明	アクション
WWAN_SYSLOG_TRACK_GW_UP	2400015	Cellular%d gateway %s is reachable	セルラーゲートウェイに到達可能です	E

優先度：Error（エラー）

メッセージ	番号	メッセージ形式	説明	アクション
WWAN_SYSLOG_AUTO_PROFILE_MISS	2400031	Manually configure APN profile for the data connection	必要なAPNが見つからなかったため、データセッションを開始できませんでした	E
WWAN_SYSLOG_MODEM_DOWN	2400036	WWAN cellular%d modem went down	モデムが切断されました	E
WWAN_SYSLOG_MODEM_RESET	2400038	Failed to recover Cellular %d modem	モデムへの接続を再確立できませんでした	E
WWAN_SYSLOG_TRACK_GW_DOWN	2400016	Cellular%d gateway %s is not reachable	セルラーゲートウェイに到達できません	E

永続的なアラームとアラームフィールド

[Alarms] 画面では、オーバーレイネットワーク内のコントローラとルータによって生成されたアラームに関する詳細情報を表示できます。

Cisco vManage で生成されるアラーム

Cisco vManage ソフトウェアによって生成されるアラームを次の表に示します。ソフトウェアコンポーネントの起動時、停止から稼働への遷移、稼働から停止への遷移など、状態や条件が変化すると、このソフトウェアはアラームを生成します。シビラティ（重大度）はアラームの深刻度を示します電子メール通知を作成する際に、通知に設定するシビラリティ（重大度）によって、どのアラームに関する電子メール通知を受信できるかが決まります。

表 *42 :*

アラーム名	シビラティ（重大度）	説明
AAA管理者パスワードの変更	Critical	ルータまたはコントローラで AAA ユーザー **admin** のパスワードが変更されました。
サイト間の BFD が停止	Critical	2つのサイト間で、すべてのルータ上のすべてのBFDセッションが停止状態です。これは、この2つのルータ間でデータトラフィックを伝送できないことを意味します。
サイト間の BFD が稼働	Medium	2 つのサイト間でルータ上の BFD セッションが稼働状態に遷移しました。
BFD ノードが停止	Critical	ルータのすべてのBFDセッションが停止状態です。これは、そのルーターとの間でデータトラフィックを伝送できないことを意味します。
BFD ノードが稼働	Medium	ルータの BFD セッションが稼働状態に遷移しました。
BFD サイトが停止	Critical	サイト内のすべての Cisco vEdge デバイス で、すべてのBFDセッションが停止状態です。これは、そのサイトとの間でデータトラフィックを伝送できないことを意味します。
BFD サイトが稼働	Medium	サイト内のルータのBFDセッションが稼働状態に遷移しました。
BFD TLOC が停止	Major	TLOC（色で識別されるトランスポートトンネル）のすべての BFD セッションが停止状態です。これは、そのトランスポートトンネルとの間でデータトラフィックを伝送できないことを意味します。
BFD TLOC が稼働	Medium	TLOC の BFD セッションが稼働状態に遷移しました。
BGP ルータが停止	Critical	ルーターのすべての BGP セッションが停止状態です。
BGP ルータが稼働	Medium	ルータの BGP セッションが稼働状態に遷移しました。
インストールされている証明書の消去	Critical	公開キー、秘密キー、ルート証明書を含む、コントローラやデバイス上のすべての証明書が消去され、デバイスは工場出荷時のデフォルト状態に戻りました。

アラーム名	シビラティ（重大度）	説明
クローンされた Cisco vEdge の検出	Critical	同じシャーシ番号、シリアル番号、システム IP アドレスを持つ重複ルータが検出されました。
Cloud onRamp	Major	Cloud onRamp サービスがルータで開始されました。
すべての Cisco vSmart 制御接続が停止	Critical	オーバーレイネットワーク内のすべての Cisco vSmart コントローラ からの制御接続がすべて停止状態です。これは、オーバーレイネットワークが機能できないことを意味します。
制御ノードが停止	Critical	Cisco vEdge デバイス のすべての制御接続が停止状態です。
制御ノードが稼働	Medium	Cisco vEdge デバイス の 1 つ以上の制御接続が稼働状態に遷移しました。
サイトの制御接続が停止	Critical	サイト内にあるすべての Cisco SD-WAN デバイスからの制御接続が停止状態です。これは、そのサイトとの間で制御トラフィックやデータトラフィックを伝送できないことを意味します。
サイトの制御接続が稼働	Medium	サイト内の Cisco vManage や Cisco vBond オーケストレーション からの制御接続が稼働状態に遷移しました。
Cisco vBond 制御接続の状態の変化	Critical、Major	Cisco vBond オーケストレーション の制御接続が停止状態（Critical）または稼働状態（Major）に遷移しました。
TLOC 制御接続の停止	Major	TLOC のすべての制御接続が停止状態です。
TLOC 制御接続の稼働	Medium	TLOC の制御接続が稼働状態です。
Cisco vManage 制御接続の停止	Critical	Cisco vManage からのすべての制御接続が停止状態です。
Cisco vManage 制御接続の稼働	Medium	Cisco vManage からの制御接続が稼働状態に遷移しました。
Cisco vManage 制御接続の停止	Critical	オーバーレイネットワーク内の Cisco vSmart コントローラからの制御接続がすべて停止状態です。
Cisco vSmart 制御接続の稼働	Medium	オーバーレイネットワーク内の Cisco vSmart コントローラからの制御接続が稼働状態に遷移しました。

アラーム名	シビラティ（重大度）	説明
Cisco vSmart 制御接続の稼働	Medium	オーバーレイネットワーク内のすべてのCisco vSmartコントローラからの制御接続が稼働状態に遷移しました。
CPU 負荷	Critical、Medium	コントローラまたはデバイスのCPU使用率による負荷が、機能の低下やシャットダウンの可能性がある重大なレベル（Critical）に達しているか、機能の低下の可能性がある中程度のレベル（Medium）に達しています。
デフォルトのアプリケーションリストの更新	Major	アプリケーション認識型ルーティングポリシーで使用されるデフォルトのアプリケーションまたはアプリケーション ファミリ リストが変更されました。
デバイスアクティブ化の失敗	Critical	コントローラまたはデバイス上のソフトウェアイメージのアクティブ化に失敗しました。
デバイスアップグレードの失敗	Critical	ルータのソフトウェアアップグレードに失敗しました。
DHCP サーバーの状態の変化	Major	DHCP サーバーの状態に変化がありました。
ディスク使用率	Critical、Major	コントローラまたはデバイスのディスク使用率による負荷が、機能の低下やシャットダウンの可能性がある重大なレベル（Critical）に達しているか、機能の低下の可能性がある中程度のレベル（Medium）に達しています。
ドメイン ID の変更	Critical	オーバーレイネットワークのドメイン識別子が変更されました。
インターフェイス管理状態の変化	Critical、Medium	コントローラまたはルータのインターフェイスの管理ステータスが、稼働から停止（Critical）または停止から稼働（Medium）に変更されました。
インターフェイスの状態の変化	Medium	インターフェイスの管理ステータスまたは操作ステータスが変更されました。
メモリ使用率	Critical、Medium	コントローラまたはデバイスのメモリ使用率が、機能の低下やシャットダウンの可能性がある重大なレベル（Critical）に達しているか、機能の低下の可能性がある中程度のレベル（Medium）に達しています。

アラーム名	シビラティ（重大度）	説明
新しい CSR の生成	Critical	コントローラまたはルータで証明書署名要求（CSR）が生成されました。
すべての Cisco vSmart の OMP 接続の停止	Critical	オーバーレイネットワーク内にあるすべての Cisco vSmart コントローラからの OMP 接続が、すべて停止状態です。これは、オーバーレイネットワークが機能できないことを意味します。
Cisco vSmarts の OMP 接続が稼働		オーバーレイネットワーク内にあるすべての Cisco vSmart コントローラからの OMP 接続が、1 つ以上稼働状態です。
ノードの OMP 接続が停止		Cisco vEdge デバイス のすべての OMP 接続が停止状態です。
ノードの OMP 接続が稼働	Medium	Cisco vEdge デバイス の 1 つ以上の OMP 接続が稼働状態です。
サイトの OMP 接続が停止	Critical	サイト内のすべてのノードから Cisco vSmart コントローラ への OMP 接続が、すべて停止状態です。これは、サイトがオーバーレイネットワークに参加できないことを意味します。
サイトの OMP 接続が稼働	Medium	サイト内のすべてのノードから Cisco vSmart コントローラ への OMP 接続が、1 つ以上稼働状態です。
OMP の状態の変化	Critical、Medium	Cisco vSmart コントローラと Cisco vEdge デバイス の間の OMP セッションの管理ステータスまたは操作ステータスが、稼働から停止（Critical）または停止から稼働（Medium）に変更されました。
vSmarts の OMP 接続が稼働	Medium	オーバーレイネットワーク内のすべての Cisco vSmart コントローラ からの OMP 接続が、稼働状態に遷移しました。
組織名の変更	Critical	すべてのオーバーレイ ネットワーク デバイスの証明書で使用されている組織名が変更されました。
ルータの OSPF 接続が停止	Critical	ルータのすべての OSPF 接続が停止状態です。
ルータの OSPF 接続が稼働	Medium	ルータの OSPF 接続が稼働状態に遷移しました。
PIM インターフェイスの状態の変化	Major	PIM インターフェイスの状態に変化がありました。

アラーム名	シビラティ（重大度）	説明
プロセスの再起動	Critical	コントローラまたはルータのプロセス（デーモン）が再起動しました。
擬似コミットステータス	Minor	Cisco vManage は、コントローラまたはルータへのデバイス設定テンプレートのプッシュを開始しました。Cisco vManage は、仮の設定（疑似コミットと呼ばれる）をデバイスにプッシュし、ロールバックタイマーを開始します。新しい設定で、デバイスと Cisco vManage の間の制御接続が確立されると、仮設定が永続化されます。制御接続が確立されない場合、仮設定は削除され、デバイスの設定は以前の設定（最後に確認された有効な設定）にロールバックされます。
ルート証明書チェーンのインストール	Critical	ルート証明書キーチェーンを含むファイルが、コントローラまたはルータにインストールされました。
ルート証明書チェーンのアンインストール	Critical	ルート証明書キーチェーンを含むファイルが、コントローラまたはルータから削除されました。
サイト ID の変更	Critical	オーバーレイネットワーク内のサイト ID が変更されました。
システム IP の変更	Critical	コントローラまたはルータのシステム IP アドレスが変更されました。
システム IP の再利用	Critical	オーバーレイネットワーク内の複数のデバイスで同じシステム IP アドレスが使用されています。
システム再起動の開始	Critical、Medium	デバイスの再起動が、デバイス（Critical）またはユーザー（Medium）によって開始されました。
テンプレートのロールバック	Critical	設定されたロールバック時間内にルータへのデバイス設定テンプレートのアタッチが完了しなかったため、デバイスの設定は更新されず、代わりに以前の設定にロールバックされました。
サポートされていない SFP の検出	Critical	ハードウェアルータでサポートされていないトランシーバが検出されました。
Cisco vEdge シリアルファイルのアップロード	Critical	WAN エッジのシリアル番号ファイルが Cisco vManage サーバーにアップロードされました。

アラーム名	シビラティ（重大度）	説明
Cisco vSmart/Cisco vManage シリアルファイルのアップロード	Critical	Cisco vManage がオーバーレイネットワークにある Cisco vManage と Cisco vSmart コントローラ の証明書のシリアル番号を含むファイルをアップロードしました。
ZTP のアップグレードに失敗	Critical	コントローラまたはルータで、ZTP を使用したソフトウェアのアップグレードに失敗しました。

アラームフィールド

アラームメッセージには、次のフィールドを含めることができます。

表 *43*:

フィールド	説明
Acknowledged	アラームが表示され、確認されたかどうか。Cisco vManage はこのフィールドを使用して、すでに報告されているアラームとまだ対処されていないアラームを区別できます。アラームを確認するには、次の API ポストコールを使用します。 https://*vmanage-ip-address*:8443/dataservice/alarms/markviewed データを次のように指定します。 {“uuid”: [<確認するアラームの *UUID*>]}
Active	アラームがまだアクティブかどうか。自動的にクリアされるアラームの場合、ネットワーク要素が回復すると、アラームの [Active] フィールドの値は false になります。
Cleared By	現在のアラームをクリアするためのアラームの汎用一意識別子（UUID）。
Cleared Time	アラームが解除された時刻。[Active] フィールドの値が false のアラームの場合に、このフィールドが存在します。
Component	このアラームのソフトウェアコンポーネント。
Devices	対象デバイスのシステム IP アドレスまたはルータ ID のリスト。
Entry Time	アラームが発生した時刻（ミリ秒単位）。UNIX 時間で表されます。
Message	アラームを説明する短いメッセージ。
Possible Causes	イベントの考えられる原因。
Rule Name Display	アラームの名前。特定のタイプのアラームを照会する場合は、この名前を使用します。

フィールド	説明
Suppressed	このアラームが他のアラームによって抑制されているかどうか。
Tenant	テナント ID を示します。
Severity	アラームのシビラティ（重大度）：Critical（重大）、Major（やや重大）、Medium（中程度）、Minor（比較的重大でない）。
Severity Number	シビラレティ（重大度）を示す値：1（重大）、2（やや重大）、3（中程度）、4（比較的重大でない）
UUID	アラームの一意の識別子
Values	すべての対象デバイスの値セット。これらの値はアラームごとに異なり、[Devices] フィールドに表示される値を補足します。
Values Short Display	対象ネットワークデバイスの概要を示す値フィールドのサブセット。

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。