Cisco Catalyst SD-WAN AppQoE コンフィギュレーション ガイド、Cisco IOS XE Catalyst SD-WAN リリース 17.x

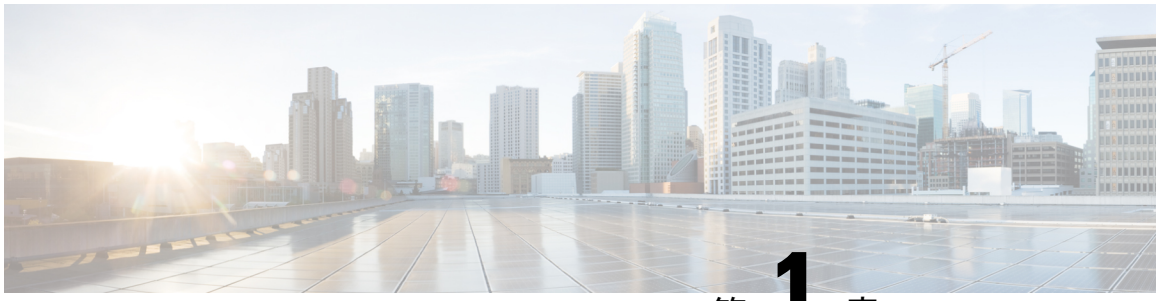
初版：2020 年 12 月 19 日

最終更新：2023 年 8 月 22 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

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

参考資料

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations [英語]
- Cisco Catalyst SD-WAN Device Compatibility [英語]

ユーザーマニュアル

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17 [英語]

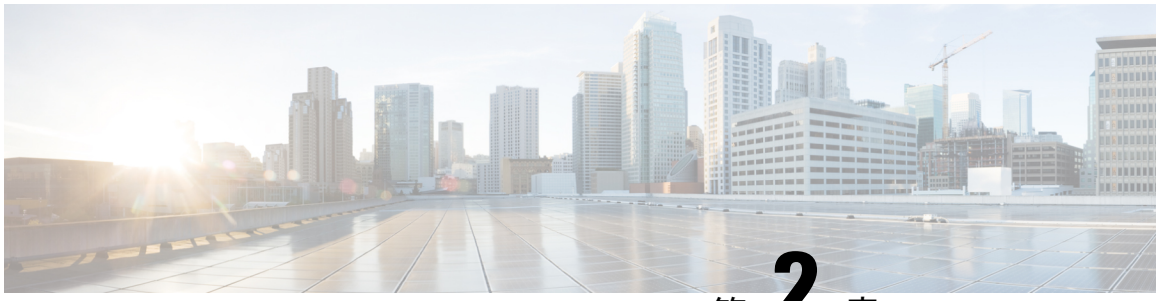
通信、サービス、およびその他の情報

- 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。



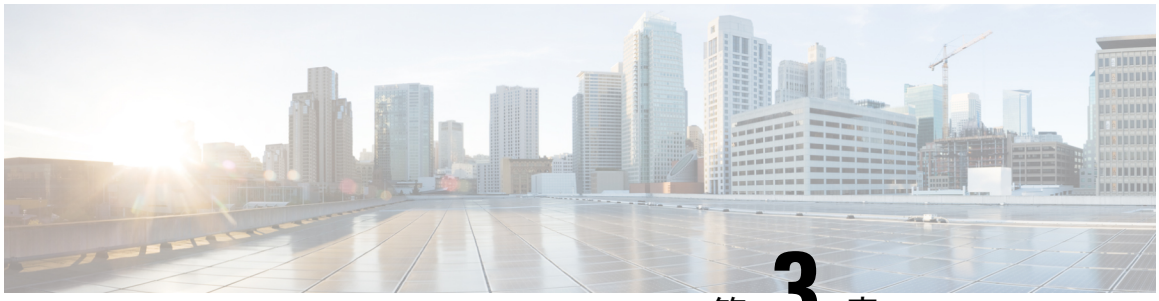
第 2 章

Cisco IOS XE（SD-WAN）の新機能

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

（注） シスコでは、リリースごとに Cisco Catalyst 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。次の表に、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新機能と変更された機能を示します。Cisco Catalyst 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 Catalyst SD-WAN Release 17.x [英語]



第 3 章

Cisco Catalyst SD-WAN 向け AppNav-XE

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

表 *1*：機能の履歴

機能名	リリース情報	説明
AppNav-XE	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能を使用すると、Cisco IOS XE Catalyst SD-WAN デバイス での WAN 最適化のために、WAAS ノードへの LAN から WAN 方向および WAN からLAN 方向のトラフィックフローのポリシーベース リダイレクションを設定できます。 この機能は、Cisco IOS XE プラットフォームですでに使用可能でしたが、このリリースでは Cisco IOS XE Catalyst SD-WAN プラットフォームまで拡張されています。

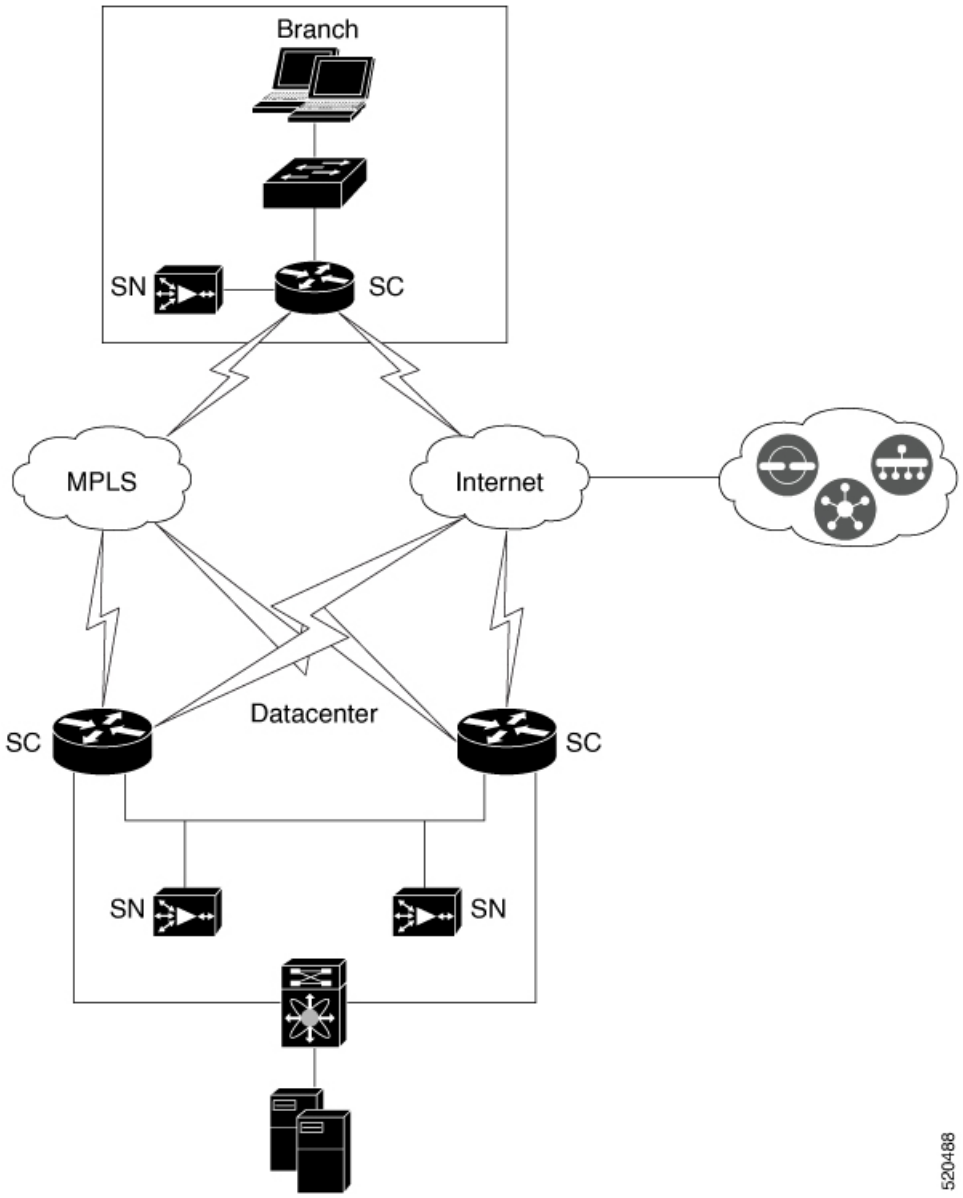
AppNav-XE の概要

AppNav-XE 機能は、WAAS デバイスへのトラフィックフローのインテリジェントな分散を促進します。WAAS デバイスは、WAN 最適化に使用されます。

AppNav-XE は、クラスおよびポリシーメカニズムを使用し、WAAS デバイス間でトラフィックを分散して最適化することで、代行受信スイッチやルータへの依存を低減します。WAAS ノード（WN）を使用して、サイトやアプリケーションに基づいてトラフィックを最適化できます。AppNav-XE ソリューションは、ノード間でトラフィックを分散させる際に WAAS デバイスの使用率を考慮することで、使用可能なキャパシティまで拡張することができます。このソリューションは、ノードの過負荷状態を監視し、設定可能なエラーや過負荷のポリシーを提供することで、最適化キャパシティの高可用性を実現します。

トポロジの例

図 *1* : トポロジの例



*SN：サービスノードまたは WAAS ノード（最大 64）
*SC：サービスコントローラとして機能する Cisco IOS XE Catalyst SD-WAN デバイス（最大 4）

上の図は、AppNav-XE を使用した Cisco Catalyst SD-WAN 展開の例を示しています。データセンターとブランチの Cisco IOS XE Catalyst SD-WAN デバイス は、AppNav-XE 機能を使用して有効化され、WAAS ノードを使用した AppNav クラスタを形成します。

AppNav-XE の利点

- 企業がサービスを効率的に費用対効果の高い仕方で拡張することを可能にします。
- 柔軟なポリシー定義の使用をサポートします。
- Cisco Catalyst SD-WAN ネットワークサービスと統合されているため、ハードウェアを追加する必要がありません。
- 各サービスノードの負荷に基づいて、インテリジェントに新しいフローをリダイレクトします。これには、個々の L7 アプリケーション アクセラレータの負荷が含まれます。
- 最適化を必要としないフローの場合、サービスノードは、AppNav コントローラに対してパケットを直接パススルーするよう通知することにより、遅延やリソース使用量を最小化します。
- サービスノードを追加または除去する際のトラフィックへの影響が最小限になります。
- VRF をサポートすることで、トラフィックがサービスノードから戻るときに VRF 情報が維持されるようにします。
- AppNav コントローラグループを介した非対称フローの最適化をサポートします。

（注） 非対称フローとは、単方向のトラフィックが AppNav コントローラを通過するときに、戻るトラフィックが別の AppNav コントローラを通過することです。ただし、両方の AppNav コントローラはトラフィックを同じサービスノードにリダイレクトします。

- 1 台のルータがダウンした場合に、トラフィックが AppNav コントローラグループ内の異なるルータに再ルーティングされるため、トラフィックフローの中断が発生しないルータ間高可用性を実現します。

AppNav-XE のコンポーネント

- AppNav クラスタ：サイトのすべての AppNav コントローラと WAAS ノードのグループ。通常、ブランチやデータセンターなどの各企業サイトには、AppNav クラスタがあります。
- AppNav コントローラ：ネットワークトラフィックを代行受信し、AppNav ポリシーに基づき、そのトラフィックを 1 つまたは複数の WAAS ノード（WN）に配信するデバイス。このコンテキストのデバイスは、AppNav-XE を実行している Cisco IOS XE Catalyst SD-WAN デバイス です。
- WAAS ノード：Wide Area Application Services（WAAS）ノードまたはサービスノードは、デバイスで設定された最適化ポリシーに基づいてトラフィックを最適化および高速化する WAAS 最適化エンジンまたは vWAAS インスタンスです。

（注） WAAS サービスノードは、このドキュメントの範囲外です。

- WAAS Central Manager（WCM）：WCM デバイスは、ネットワーク内の AppNav コントローラと WAAS ノードを設定、管理、モニターするための Web ベースのインターフェイスである WAAS Central Manager GUI を搭載しています。Cisco Catalyst SD-WAN 向け AppNav-XE では、WCM は、Cisco IOS XE Catalyst SD-WAN デバイス の設定に使用されるネットワーク管理システムである Cisco SD-WAN Manager と通信します。次に、Cisco SD-WAN Manager は AppNav-XE 設定を Cisco IOS XE Catalyst SD-WAN デバイス にプッシュします。ただし、AppNav クラスタ内の WAAS ノードは、引き続き WCM 経由で設定を受信します。Cisco IOS XE Catalyst SD-WAN デバイス の WAAS ノードと AppNav-XE のモニタリングは、WCM を介して直接実行されます。
- Cisco SD-WAN Manager：これは Cisco Catalyst SD-WAN でのプライマリ管理システムです。したがって、WCM は AppNav-XE 設定を Cisco SD-WAN Manager に送信し、次にその設定を AppNav-XE コントローラにプッシュします。

サポートされるプラットフォーム

次のプラットフォームは、Cisco Catalyst SD-WAN 向け AppNav-XE をサポートします。

- Cisco 1000 シリーズ アグリゲーション サービス ルータ
- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco Cloud Services Router 1000V シリーズ
- C8500-12X4QC および C8500-12X シリーズ アグリゲーション サービス ルータ
- C8300 シリーズ サービス統合型ルータ

Cisco Catalyst SD-WAN での AppNav-XE の管理

AppNav-XE 機能は、すでに IOS XE プラットフォームでサポートされていました。とはいえ、Cisco IOS XE SD-WAN リリース 17.2 以降、この機能は Cisco IOS XE Catalyst SD-WAN プラットフォームまで拡張されています。この機能を動作させるには、Cisco SD-WAN Manager がリリース 20.1.1 以降を実行している必要があることに注意してください。

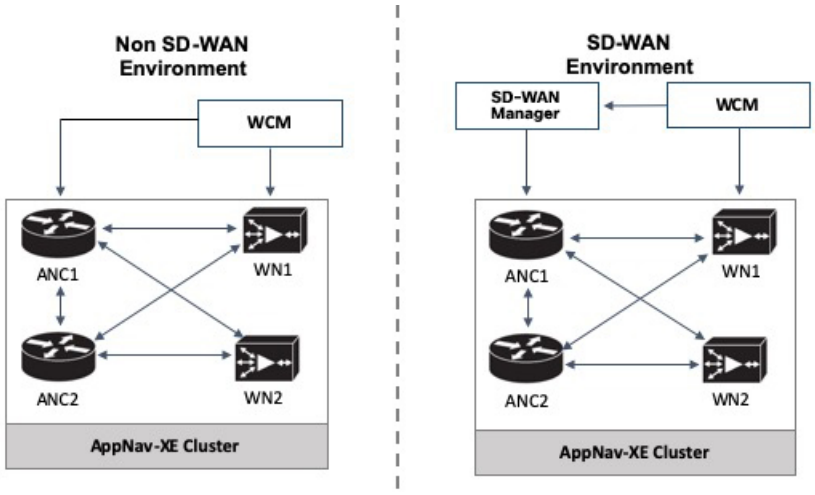
SD-WAN 環境と非 SD-WAN 環境における AppNav-XE

SD-WAN での AppNav-XE の設定方法は、非 SD-WAN 環境での設定方法とは異なります。主な違いは、WCM と AppNav-XE コントローラ間の仲介デバイスとして機能する Cisco SD-WAN Manager が AppNav ポリシー設定を Cisco IOS XE Catalyst SD-WAN デバイス にプッシュするこ

とです。Cisco IOS XE Catalyst SD-WAN デバイス は AppNav-XE コントローラとして機能します。

次の図は、SD-WAN 環境と非 SD-WAN 環境での AppNav-XE 展開の違いを示しています。

図 *2*：比較：*SD-WAN* 環境と非 *Catalyst SD-WAN* 環境における *AppNav-XE*



IOS XE での AppNav-XE：WCM GUI は、AppNav クラスタ内の AppNav コントローラ（ANC）および WAAS ノード（WN）と直接通信して、設定をプッシュします。

IOS XE SD-WAN での AppNav-XE：主な違いは、AppNav ポリシー設定を AppNav コントローラ（ANC）にプッシュする方法です。こちらでは、該当する機能が WCM GUI と Cisco SD-WAN Manager の両方を使用して設定されます。引き続き WCM で AppNav-XE 機能を設定します。その後、WCM は Cisco SD-WAN Manager に設定を送信します。次に、設定が AppNav コントローラにプッシュされます。WCM と Cisco SD-WAN Manager の間の通信は、Cisco SD-WAN Manager でサードパーティ製コントローラとして WCM を登録することによって達成されます。WCM は、引き続き設定を WAAS ノードに直接送信します。

Cisco IOS XE Catalyst SD-WAN デバイス での AppNax-XE の設定

Cisco IOS XE Catalyst SD-WAN デバイス で AppNav-XE を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager での WCM の登録
2. WCM パートナーへの Cisco IOS XE Catalyst SD-WAN デバイス のアタッチ
3. Cisco XE SD-WAN デバイスの WCM への登録
4. SD-WAN 向け AppNav-XE クラスタの構成 （14 ページ）

Cisco SD-WAN Manager での WCM の登録

このトピックでは、Cisco WAAS Central Manager（WCM）にアクセスし、Cisco SD-WAN Manager のサードパーティ製コントローラとして WCM を登録する方法について説明します。また、Cisco SD-WAN Manager を介して WCM パートナーに Cisco IOS XE Catalyst SD-WAN デバイスを接続する方法についても説明します。

WCM GUI へのアクセス

WAAS Central Manager GUI にアクセスするには、ブラウザで次の URL を入力します。

https:// *WAE_Address* :8443/

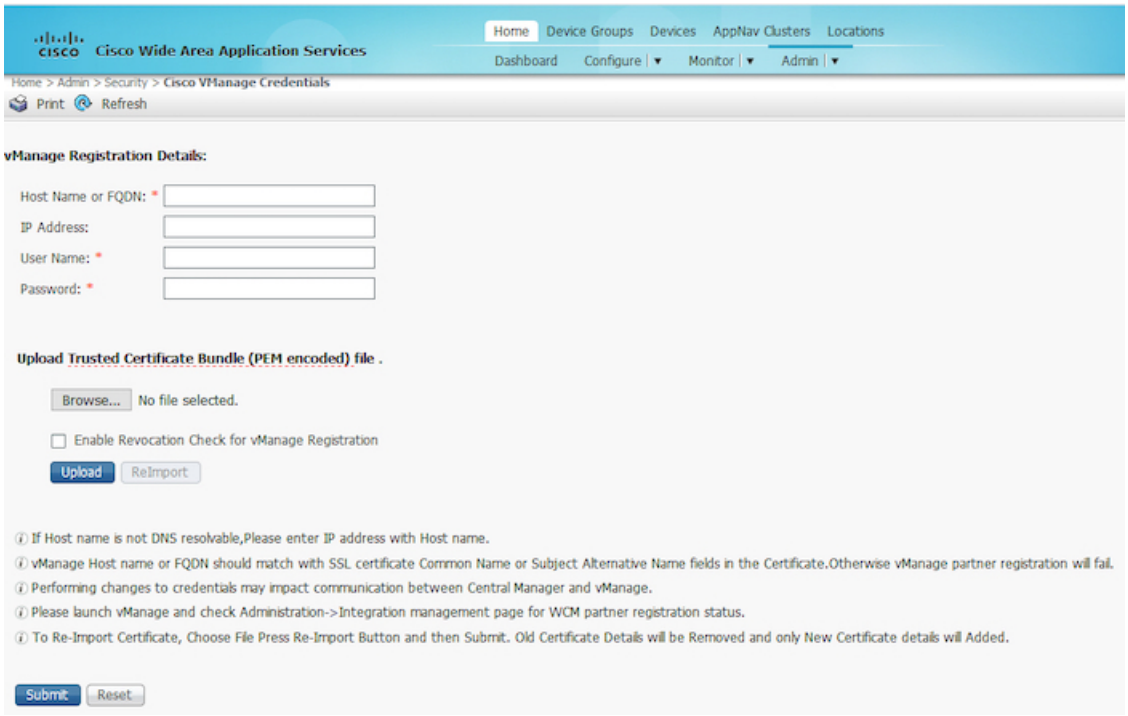
WAE_Address の値は、WAAS Central Manager デバイスの IP アドレスまたはホスト名です。

管理者のデフォルトのユーザ名は *admin*、パスワードは *default* です。

WCM と Cisco SD-WAN Manager の統合

1. WCM GUI ホームページから、[管理（Admin）] を選択します。
2. 次に、**[セキュリティ（Security）] > [Cisco vManageログイン情報（Cisco vManage Credentials）]** を選択します。
3. 必要な情報を入力します。

図 *3 : WCM GUI*



完全修飾ドメイン名（FQDN）を使用して登録するには、[ホスト名（Host Name）] フィールドに FQDN を入力します。[IP アドレス（IP Address）] フィールドは空のままにする必要があります。

4. Cisco SD-WAN Manager Web サーバー証明書の信頼できる発行元証明書バンドルを PEM 形式でアップロードします。

（注） [再インポート（re-import）] ボタンを使用して、信頼できる発行元証明書バンドルを再アップロードします。この操作により、既存の証明書バンドルが置き換えられます。

5. Cisco SD-WAN Manager Web サーバー証明書の失効チェックを有効にするには、[失効チェック（Revocation Check）] オプションを選択します。

   OSCP ベースの失効チェックのみがサポートされていることに注意してください。

6. [Submit] をクリックします。`

統合した後、**[管理（Administration）] > [統合管理（Integration Management）]** を選択することにより、WCM パートナーを Cisco SD-WAN Manager メニューから表示できます。

WCM パートナーへの Cisco IOS XE Catalyst SD-WAN デバイス のアタッチ

1. Cisco SD-WAN Manager メニューで、**[管理（Administration）] > [統合管理（Integration Management）]** を選択します。

   Cisco SD-WAN Manager に登録されているサードパーティ製コントローラのリストが表示されます。

2. 目的のWCMパートナーについて、[...] をクリックし、[デバイスのアタッチ（Attach Devices）] を選択します。

3. 左側の [使用可能なデバイス（Available Devices）] 列で、リストからデバイスを選択します。

4. [Attach] をクリックします。

5. デバイスで AppNav-XE を設定するには、次にCisco XE SD-WAN デバイスの WCM への登録。

Cisco XE SD-WAN デバイスの WCM への登録

前提条件

- 登録するデバイスは、Cisco SD-WAN Manager GUI で vManage モードになっている必要があります。詳細については、「Change Configuration Modes in Cisco SD-WAN Manager」[英語] を参照してください。
- 登録するデバイスには、HTTPS 設定がアタッチされている必要があります。HTTPS 設定は、Cisco SD-WAN Manager のグローバル設定テンプレートを使用してデバイスにアタッチできます。

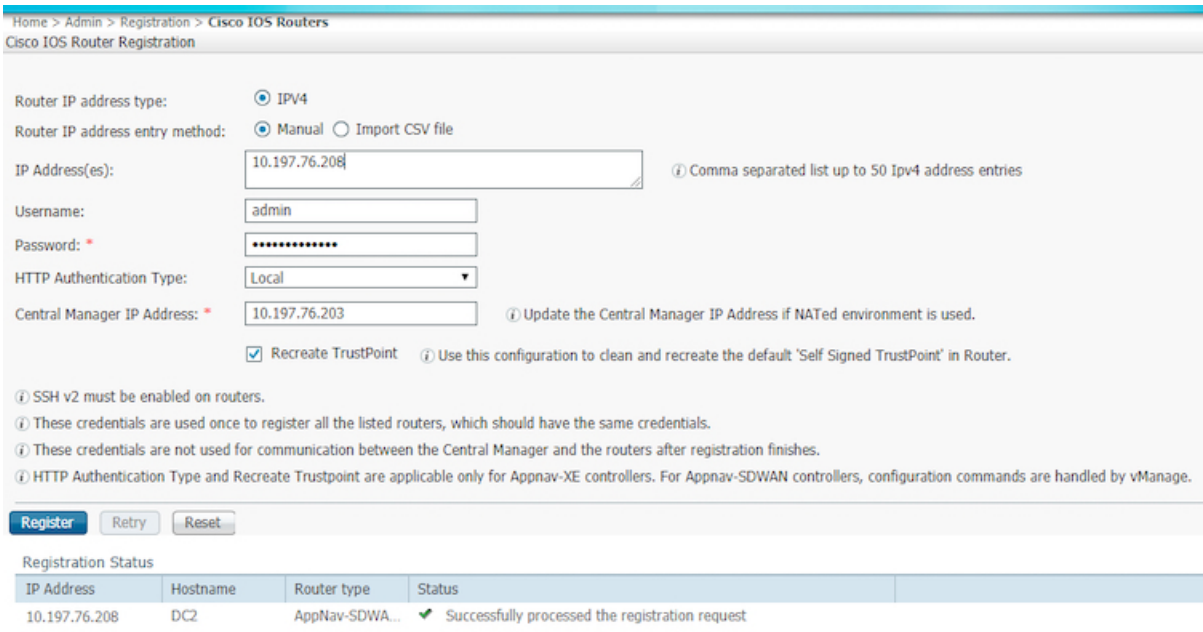
1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Templates]** を選択します。
2. [機能テンプレート（Feature Templates）] をクリックしてから、[テンプレートの追加（Add Template）] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. 右側ペインの [基本情報（Basic Information）] エリアで、[グローバル設定（Global Settings）] テンプレートを選択します。
4. [Services] をクリックします。
5. [HTTPサーバー（HTTP Server）] フィールドと [HTTPSサーバー（HTTPS Server）] フィールドの両方で、ドロップダウンリストから [グローバル（Global）] を選択し、[オン（On）] を選択します。

WCM でのデバイスの登録

1. WCM で、[管理（Admin）] セクションに移動します。
2. **[登録（Registration）]** > **[Cisco IOSルータ（Cisco IOS Routers）]** の順に選択します。
3. 必要な詳細情報を入力して、[登録（Register）] をクリックします。



デバイスの登録ステータスが画面下部に表示されます。

4. [送信（Submit）] をクリックします。

SD-WAN 向け AppNav-XE クラスタの構成

WCM を介した Cisco Catalyst SD-WAN 環境向けの AppNav-XE クラスタの構成は、いくつかの異なる手順を除き、非 Cisco Catalyst SD-WAN 環境の構成と同じです。AppNav-XE コンフィギュレーション ガイドの次のリンクを参照してください。Cisco Catalyst SD-WAN の設定に違いがある場合は、注記で示されています。

- Create a Cisco AppNav-XE Cluster with the AppNav Cluster Wizard [英語]
- Configure a Class Map on an AppNav-XE Cluster [英語]
- Configure AppNav-XE Policy Rules on an AppNav-XE Cluster [英語]
- Configure AppNav Controller Settings for an AppNav-XE Device [英語]
- Manage AppNav-XE Policies [英語]
- Enable Cisco WAAS Service Insertion on AppNav-XE Device Interfaces [英語]

AppNav-XE のモニターとトラブルシュート

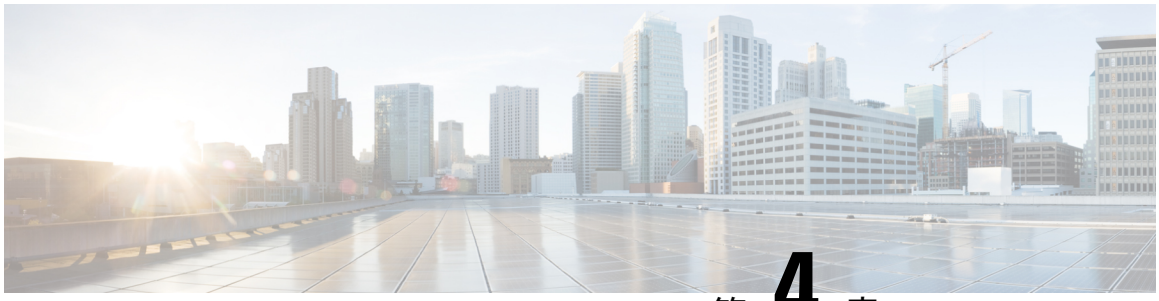
Cisco IOS XE Catalyst SD-WAN デバイス の AppNav-XE コンポーネントは、デバイスの CLI および WCM GUI を使用してモニターできます。

AppNav-XE のモニター

- **CLI を使用**：「Monitoring the AppNav-XE Component」[英語] を参照してください。
- **WCM GUI を使用**：「Monitoring an AppNav Cluster」[英語] を参照してください。

AppNav-XE のトラブルシュート

一般的な問題と、さまざまな debug コマンドを使用したトラブルシュート方法については、「Troubleshooting AppNav-XE」[英語] を参照してください。



第 4 章

TCP 最適化

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

表 *2*：機能の履歴

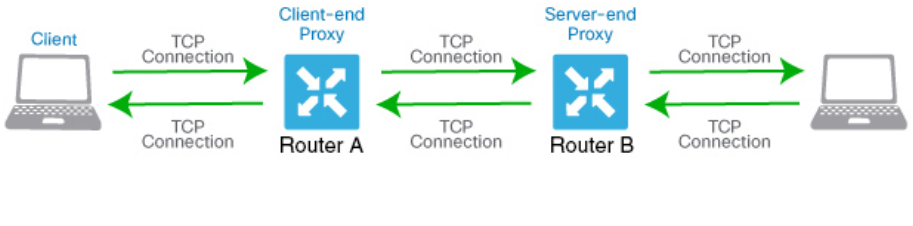
機能名	リリース情報	説明
TCP 最適化	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a	TCP 最適化のサポートが拡張され、Cisco ISR4221、Cisco ISRv、および Cisco 1000 シリーズ サービス統合型ルータで使用できるようになりました。詳細については、「Supported Platforms」[英語] を参照してください。
	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1d	この機能は、ラウンドトリップ遅延を短縮し、スループットを向上させることで、TCP データトラフィックを最適化します。

TCP最適化により、データトラフィックの処理を微調整して、ラウンドトリップの遅延を短縮し、スループットを向上させます。

この記事では、Cisco IOS XE Catalyst SD-WAN デバイスのサービス側 VPN での TCP トラフィックの最適化について説明します。

TCP トラフィックの最適化は、大陸間リンクや VSAT 衛星通信システムで使用される高遅延のトランスポートリンクなど、遅延の長いリンクで TCP トラフィックのパフォーマンスを向上させるのに特に役立ちます。TCP 最適化により、Software as a Service（SaaS）アプリケーションのパフォーマンスも向上させることが可能です。

TCP 最適化では、次の図に示すように、ルータは TCP フローを開始しているクライアントと TCP フローをリッスンしているサーバーの間で TCP プロキシとして機能します。



この図は、プロキシとして機能する 2 台のルータを示しています。ルータ A はクライアントのプロキシであり、クライアントプロキシと呼ばれます。ルータ B はサーバーのプロキシで、サーバープロキシと呼ばれます。TCP 最適化を使用しない場合、クライアントはサーバーへの TCP 接続を直接確立します。2 つのルータで TCP 最適化を有効にすると、ルータ A は、クライアントからの TCP 接続を終了し、ルータ B との TCP 接続を確立します。その後 ルータ B は、サーバーへの TCP 接続を確立します。2 つのルータは、TCP 接続がタイムアウトすることなく、クライアントからのトラフィックがサーバーに到達するように、TCP トラフィックをバッファにキャッシュします。

クライアントに近い方のルータとサーバーに近い方のルータの両方で、TCP 最適化を設定することを推奨します。この設定は、デュアルエンドプロキシと呼ばれることもあります。クライアントに近いルータでのみ TCP 最適化を設定できます。このシナリオはシングルエンドプロキシと呼ばれますが、TCP 最適化プロセスが侵害されるため、この設定は推奨されません。TCP は双方向プロトコルであり、接続開始メッセージ（SYN）が ACK メッセージによってタイムリーに確認応答された場合にのみ動作します。

クライアントとサーバーの両方が同じルータに接続されている場合、TCP 最適化は実行されません。

TCP 最適化を使用するには、まずルータでこの機能を有効にします。次に、最適化する TCP トラフィックを定義します。TCP 最適化を設定する前に、設定トランザクションを開始するために、次のようなコマンドを使用できます。

```
ntp server 198.51.241.229 source GigabitEthernet1 version 4
```


トポロジと役割

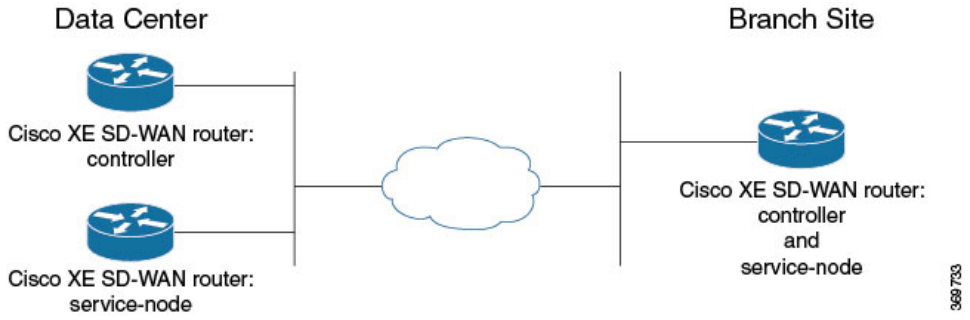
ブランチの場合、Cisco IOS XE Catalyst SD-WAN デバイス はコントローラとサービスノード両方の役割を果たします。

データセンター

データセンターの場合、コントローラのロールとサービスノードのロールは別々の Cisco IOS XE Catalyst SD-WAN デバイス によって実行されます。その結果、パフォーマンスが最適化され、より多くのトラフィックを処理できるようになります。

サービスノードは、設定を受信するための Cisco SD-WAN Manager への制御接続を持つ外部ノードです。

（注） AppNav トンネルを確立するには、サービスノード Cisco IOS XE Catalyst SD-WAN デバイス にグローバル VRF 上のコントローラへのアンダーレイ接続が必要です。



サポートされるプラットフォーム

リリース	サポートされるプラットフォーム
Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降	• Cisco 4331 サービス統合型ルータ（ISR 4331） • Cisco 4431 サービス統合型ルータ（ISR 4431） • Cisco 4321 サービス統合型ルータ（ISR 4321） • Cisco 4351 サービス統合型ルータ（ISR 4351） • Cisco 4451 サービス統合型ルータ（ISR 4451） • Cisco 4461 サービス統合型ルータ（ISR 4461） • Cisco CSR 1000v クラウドサービスルータ（CSRv）

リリース	サポートされるプラットフォーム
Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降	• Cisco 4221 サービス統合型ルータ（ISR 4221） • シスコサービス統合型仮想ルータ（ISRv） • Cisco 1000 シリーズ サービス統合型ルータ （注） このサポートは、8 GB 以上の RAM を搭載した Cisco 1000 シリーズ サービス統合型ルータにのみ適用されます。プラットフォーム仕様については、『Cisco 1000 Series Integrated Services Routers Data Sheet』[英語]を参照してください。
Cisco IOS XE Catalyst SD-WAN リリース 17.3.2	• Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a	• Cisco ISR 1100X シリーズ サービス統合型ルータ • Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V） • Cisco Catalyst 8200 シリーズ エッジ プラットフォーム • Cisco Catalyst 8300 シリーズ エッジ プラットフォーム

TCP 最適化は、DNS トラフィックおよびC8200L プラットフォームではサポートされません。

最小リソース要件

- これらのプラットフォームには、少なくとも 8 GB の DRAM が必要です。
- これらのプラットフォームには4つ以上のデータコアが必要です。ただし、Cisco 4321 サービス統合型ルータ（ISR 4321）は例外で、4 つ未満のデータコアでもサポートされます。
- Cisco CSR1000V および Cisco Catalyst 8000V プラットフォームには、8 つのデータコアが必要です。

制限事項と制約事項

- Cisco Catalyst SD-WAN での TCP 最適化では、輻輳制御にボトルネック帯域幅とラウンドトリップ時間（BBR）アルゴリズムを使用します。BBR が使用されるため、クライアントが明示的輻輳通知（ECN）を要求すると、プロキシは ECN を無効にします。サポートされていないためです。

TCP 最適化の設定例

CLI を使用したサービス挿入の設定例：ブランチルータ

この例では、コントローラおよびサービスノードとして機能するようにブランチ Cisco IOS XE Catalyst SD-WAN デバイス を設定します。

（注） デフォルトでは、Cisco SD-WAN Manager を使用して、VPG0 と VPG1（UTD）に使用されるサブネット 192.168.1.1/30 と 192.0.2.1/30 と、VPG2（AppQoE）に使用される 192.168.2.1/24 が設定されます。これらのネットマスク以外のトランスポートおよびサービス VPN の設定には、任意の RFC 1918 サブネットを使用します。

```
service-insertion appnav-controller-group ACG-APPQOE
 appnav-controller 192.3.3.1
!
service-insertion service-node-group SNG-APPQOE
 service-node 192.3.3.2
!
service-insertion service-context appqoe/1
 appnav-controller-group ACG-APPQOE
 service-node-group      SNG-APPQOE
 enable
 vrf global
!

interface VirtualPortGroup2
 no shutdown
 ip address 192.3.3.1 255.255.255.0
 service-insertion appqoe
exit
```

Cisco SD-WAN Manager を使用したサービス挿入の設定例：ブランチルータ

ブランチの場合、Cisco IOS XE Catalyst SD-WAN デバイス はコントローラとサービスノード両方の役割を果たします。

この例では、ブランチ Cisco IOS XE Catalyst SD-WAN デバイス をコントローラおよびサービスノードとして設定します。

（注） Cisco SD-WAN Manager を使用してデバイスで AppQoE 機能を有効にする場合は、設定にすでに **service-insertion appqoe** が含まれており、Cisco SD-WAN Manager 経由でプッシュするものとは異なる IP アドレスを持つ仮想ポートグループ（VPG）を削除していることを確認してください。VPG に既存の **service-insertion appqoe** 設定が含まれているデバイスで AppQoE を有効にすると、設定の競合が発生する可能性があります。この競合により、AppQoE ステータスが不明確なままになる場合があります。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。

2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. 表示されるデバイスオプションからデバイスを選選択します。
4. 右側ペインの [その他のテンプレート（Other Templates）] で、[AppQoE] を選択します。
5. テンプレートの名前と説明を入力します。
6. [コントローラ（Controller）] オプションをクリックします。
7. コントローラオプションで次の詳細を入力します。
   - [コントローラIP（Controller IP）]：CLI での設定時に service-insertion appnav-controller-group コマンドで設定される appnav-controller 値に対応します。
   - [内部（Internal）]：このチェックボックスをオンにします。
   - [サービスノードIP（Service Node IP）]：CLI での設定時に service-insertion service-node-group コマンドによって設定される service-node 値に対応します。
8. [Save] をクリックします。
9. 前の手順で作成した機能テンプレートをデバイステンプレートページに追加します。[AppQoE] ドロップダウンメニューで、機能テンプレートの名前を選択します。次の手順に従って、前の手順で作成した AppQoE テンプレートを追加します。
   1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
   2. [Device Templates] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート（Device Templates）] は [デバイス（Device）] と呼ばれます。

   3. ウィンドウに表示されているデバイスから、AppQoE テンプレートをアタッチするデバイスの [...] をクリックします。[Edit] をクリックします。
   4. [追加のテンプレート（Additional Templates）] をクリックし、[AppQoE] ドロップダウンリストで、作成した AppQoE テンプレートを選択します。
10. [Update] をクリックします。

Cisco SD-WAN Manager を使用したサービス挿入の設定例：データセンターコントローラ

1. Cisco SD-WAN Manager から、**[設定（Configuration）]** > **[テンプレート（Templates）]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. [デバイスの選択（Select Devices）] で、設定するブランチデバイスを選択します。
4. 右側ペインの [その他のテンプレート（Other Templates）] で、[AppQoE] を選択します。
5. テンプレートの名前と説明を入力します。
6. [コントローラ（Controller）] オプションをクリックします。
7. コントローラとして機能する Cisco IOS XE Catalyst SD-WAN デバイス の機能テンプレートを作成します。以下を入力します。
   - [コントローラIP（Controller IP）]：CLI での設定時に service-insertion appnav-controller-group コマンドで設定される appnav-controller 値に対応します。
   - [内部（Internal）]：このオプションはオフのままにします。
   - [サービスノードIP（Service Node IP）]：CLI での設定時に service-insertion service-node-group コマンドによって設定される service-node 値に対応します。
8. [Save] をクリックします。
9. 前の手順で作成した機能テンプレートをデバイステンプレートに追加します。[AppQoE] ドロップダウンメニューで、機能テンプレートの名前を選択します。次の手順に従って、すでに作成した AppQoE テンプレートを追加します。
   1. Cisco SD-WAN Manager メニューから、**[設定（Configuration）]** > **[テンプレート（Templates）]** を選択します。
   2. [Device Templates] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート（Device Templates）] は [デバイス（Device）] と呼ばれます。

   3. ページに表示されているデバイスから、AppQoE テンプレートを添付するデバイスを選択し、選択したデバイスの横にある [その他のオプション（More Options）] アイコン（[…]）をクリックします。[Edit] をクリックします。

4. [追加のテンプレート（Additional Templates）] をクリックし、[AppQoE] ドロップダウンメニューで、作成した AppQoE テンプレートを選択します。

10. [Update] をクリックします。

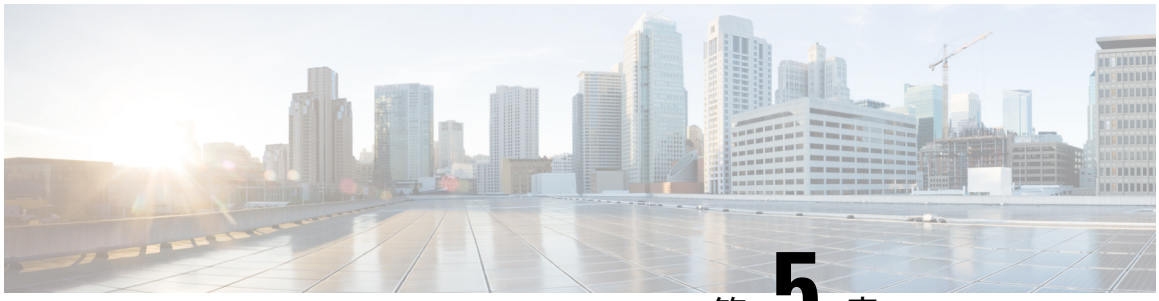
Cisco SD-WAN Manager を使用したサービス挿入の設定：データ センター サービス ノード

（注） Cisco SD-WAN Manager を使用してデバイスで AppQoE 機能を有効にする場合は、設定にすでに **service-insertion appqoe** が含まれており、Cisco SD-WAN Manager 経由でプッシュするものとは異なる IP アドレスを持つ仮想ポートグループ（VPG）を削除していることを確認してください。VPG に既存の **service-insertion appqoe** 設定が含まれているデバイスで AppQoE を有効にすると、設定の競合が発生する可能性があります。この競合により、AppQoE ステータスが不明確なままになる場合があります。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. [デバイスの選択（Select Devices）] で、設定するブランチデバイスを選択します。
4. 右側ペインの [その他のテンプレート（Other Templates）] で、[AppQoE] を選択します。
5. [サービスノード（Service Node）] ボタンをクリックします。
6. サービスノードとして機能する Cisco IOS XE Catalyst SD-WAN デバイス の機能テンプレートを作成します。以下を入力します。
   - テンプレート名
   - [サービスノードIP（Service Node IP）]：CLI での設定時に service-insertion service-node-group コマンドによって設定される appnav-controller 値に対応します。
   - [仮想ポートグループIP（Virtual Port Group IP）]：CLI での設定時に interface VirtualPortGroup2 コマンドによって設定される service-node 値に対応します。
7. [Save] をクリックします。
8. 前の手順で作成した機能テンプレートをデバイステンプレートページに追加します。[AppQoE] ドロップダウンリストで、機能テンプレートの名前を選択します。
9. [作成（Create）] をクリックします。



第 5 章

AppQoE サービス用の外部サービスノード

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

表 *3*：機能の履歴

機能名	リリース情報	説明
複数の外部 AppQoE サービスノードのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能を使用すると、代行受信するエッジルータまたは AppQoE サービスコントローラの外部にある複数の AppQoE サービスノードを設定できます。AppQoE のサポートを、AppQoE を統合サービスノードとして実行できないエッジルータまで拡張します。この機能により、統合された AppQoE ではスループットと接続数に制限がある場合に、AppQoE を拡張することもできます。複数の AppQoE サービスノードを設定するための機能は、データセンターなどの大規模な企業サイトのスケールとスループットの要件を満たすのに役立ちます。

機能名	リリース情報	説明
AppQoE サービスノードのコントローラとしての追加プラットフォームのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	このリリースでは、サービスコントローラのロールが追加のデバイスモデル（C8500L-8S4X および ASR1006-X）まで拡張されています。
トンネル隣接関係に関する自動 MTU 設定のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a	この機能により、サービスコントローラとサービスノードを接続するネットワークの最大伝送ユニット（MTU）サイズを 1500 にプログラム設定できます。この自動化により、スループット要件を低下させる可能性があるパケットのフラグメンテーションによる通信の中断が防止されます。

- AppQoE コントローラおよび外部サービスノードでサポートされるデバイス （27 ページ）
- 外部 AppQoE サービスノードの制約事項 （28 ページ）
- 外部 AppQoE サービスノードに関する情報 （29 ページ）
- AppQoE コントローラおよびサービスノードの設定 （33 ページ）
- CLI を使用した AppQoE サービスコントローラおよびノードの設定 （35 ページ）
- AppQoE サービスコントローラおよびノードのモニター （38 ページ）
- CLI を使用した AppQoE サービスコントローラおよびノードのモニター （38 ページ）

AppQoEコントローラおよび外部サービスノードでサポートされるデバイス

サービスコントローラとしてサポートされるデバイス

リリース	サポートされるデバイス数
Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降	• **Cisco ASR 1000** シリーズ アグリゲーション サービス ルータ • ASR1001X • ASR1002X • ASR1001-HX • ASR1002-HX • **Cisco Catalyst 8500** シリーズ エッジ プラットフォーム： • C8500-12X4QC • C8500-12X • Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V） （注） Cisco Catalyst 8000V をサービスコントローラとして設定する場合、同じインスタンスをサービスノードとして使用することはできません。
Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降	• **Cisco Catalyst 8500** シリーズ エッジプラットフォーム • C8500L-8S4X • **Cisco ASR 1000** シリーズ アグリゲーション サービス ルータ • ASR1006-X

外部サービスノードとしてサポートされるデバイス

リリース	サポートされるプラットフォーム
Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降	• Cisco Catalyst 8000V • **最小 RAM 要件**：16 GB（service plane heavy として設定） • **最小 CPU**：8 コア （注） Cisco Catalyst 8000V をサービスノードとして設定する場合、同じインスタンスをサービスコントローラとして使用することはできません。

（注） Cisco Catalyst 8000V をサービスノードとして設定する場合、同じインスタンスをサービスコントローラとして使用することはできません。

（注） データ冗長性排除（DRE）用の外部サービスノードとしてサポートされるプラットフォームの詳細については、「Traffic Optimization with DRE」[英語] を参照してください。

外部 AppQoE サービスノードの制約事項

- サービスノードロールを設定できるのは Cisco Catalyst 8000V インスタンスのみです。
- Cisco Catalyst 8000V がサービスノードとして設定されている場合、Cisco Catalyst 8000V がサービスコントローラロールをサポートしていても、サービスコントローラの役割を果たすことはできません。
- サイトごとにサポートされるサービスクラスタは 1 つのみです。
- サイトごとにサポートされるサービス コントローラ グループは 1 つのみで、サービス コントローラ グループには 8 つまでのサービスコントローラを含めることができます。サイトあたり最大 8 つのサービスコントローラがサポートされ、各サービスコントローラには最大 64 のサービスノードを接続できます。
- AppQoE クラスタごとにサポートされるサービスノードグループは 1 つのみです。
- VRRP は、サービスコントローラからサービスノードへの接続ではサポートされていません。
- サービスノードとサービスコントローラに専用の VRF を設定する必要があります。

- 非対称フローの処理機能は AppQoE に組み込まれていませんが、Cisco SD-WAN Manager のすべてのステートフル機能に対してフロー対称性を設定する必要があります。
- サービスコントローラに障害が発生すると、そのサービスコントローラによって処理されるフローがリセットされます。
- AppQoE サービスノードとして設定されている Cisco Catalyst 8000V インスタンスのブートストラップ設定が次のように変更されていることを確認します。
  - TLOC インターフェイスからコントローラグループを除外（**exclude-controller-group** *0*）
  - 設定に **omp shutdown** が含まれていることを確認

（注） この設定により、AppQoE サービスノードは SD-WAN データプレーンに参加できなくなります。ブートストラップ設定でこの変更が行われていない場合、Cisco SD-WAN Manager で OMP および制御接続がダウンしていることを示すアラームが生成されます。ただし、このアラームは無害であり、推奨される設定がブートストラップ設定に含まれていない場合は無視できます。

外部 AppQoE サービスノードに関する情報

外部 AppQoE サービスノードの概要

複数の外部 Application Quality of Experience（AppQoE）サービスノードの設定のサポートにより、TCP および DRE の最適化に高可用性が提供されます。AppQoE サービスノードがサービスコントローラとして機能するエッジルータの外部にある場合、この代行受信ルータへの依存性が低下します。この機能がリリースされる前は、AppQoE サービスインスタンスをサービスコントローラ自体で設定する必要がありました。サポートされているデバイスにAppQoEサービスノードロールを設定して、サイトとアプリケーションに基づいてトラフィックを最適化できるようになりました。このソリューションは、より高いスループットとより多くの接続を必要とする大企業の要件に対応します。

（注） サポートされる Application Optimization Interconnect Manager（AOIM）ピアの最大数は 255 です。DRE ノードが接続できるピアの最大数は 255 です。

外部サービスノードを使用した AppQoE ソリューションのコンポーネント

- **AppQoE クラスタ**：サイトの AppQoE コントローラと、AppQoE サービスノードのグループ。

通常、より高い集約スループットを必要とするデータセンターまたは地域のデータセンターサイトには、TCP および DRE 最適化のための外部サービスノードを含む AppQoE クラスタがあります。

- **AppQoE コントローラ**：ネットワークトラフィックを代行受信するサポート対象 Cisco IOS XE Catalyst SD-WAN デバイス。このデバイスは、AppQoE ポリシーに基づいて、ネットワークトラフィックを 1 つ以上の AppQoE サービスノードに分散させます。
- **AppQoE サービスノード**：AppQoE サービスノードとして設定されたデバイスで、トラフィックを最適化および高速化する TCP 最適化インスタンスです。最適化は、制御ポリシーの設定に基づいています。

  Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、サービスノードは、DRE 機能を実行して、データの冗長性を排除し、帯域幅の使用範囲を削減することもできます。詳細については、「Traffic Optimization with DRE」[英語] を参照してください。

外部サービスノードとスタンドアロンコントローラの動作の仕組み

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a からの外部サービスノードの作成をサポートする Cisco Catalyst SD-WAN を使用すると、サービスノードは代行受信エッジルータまたはサービスコントローラから分離されます。サポート対象のデバイスをスタンドアロン サービス コントローラとして設定し、サービスノードロールで設定されたデバイスに接続するオプションが追加されました。

Cisco SD-WAN Manager デバイステンプレートを使用すると、サポート対象のデバイスで次のロールを設定できます。

- サービスノード
- サービスコントローラ

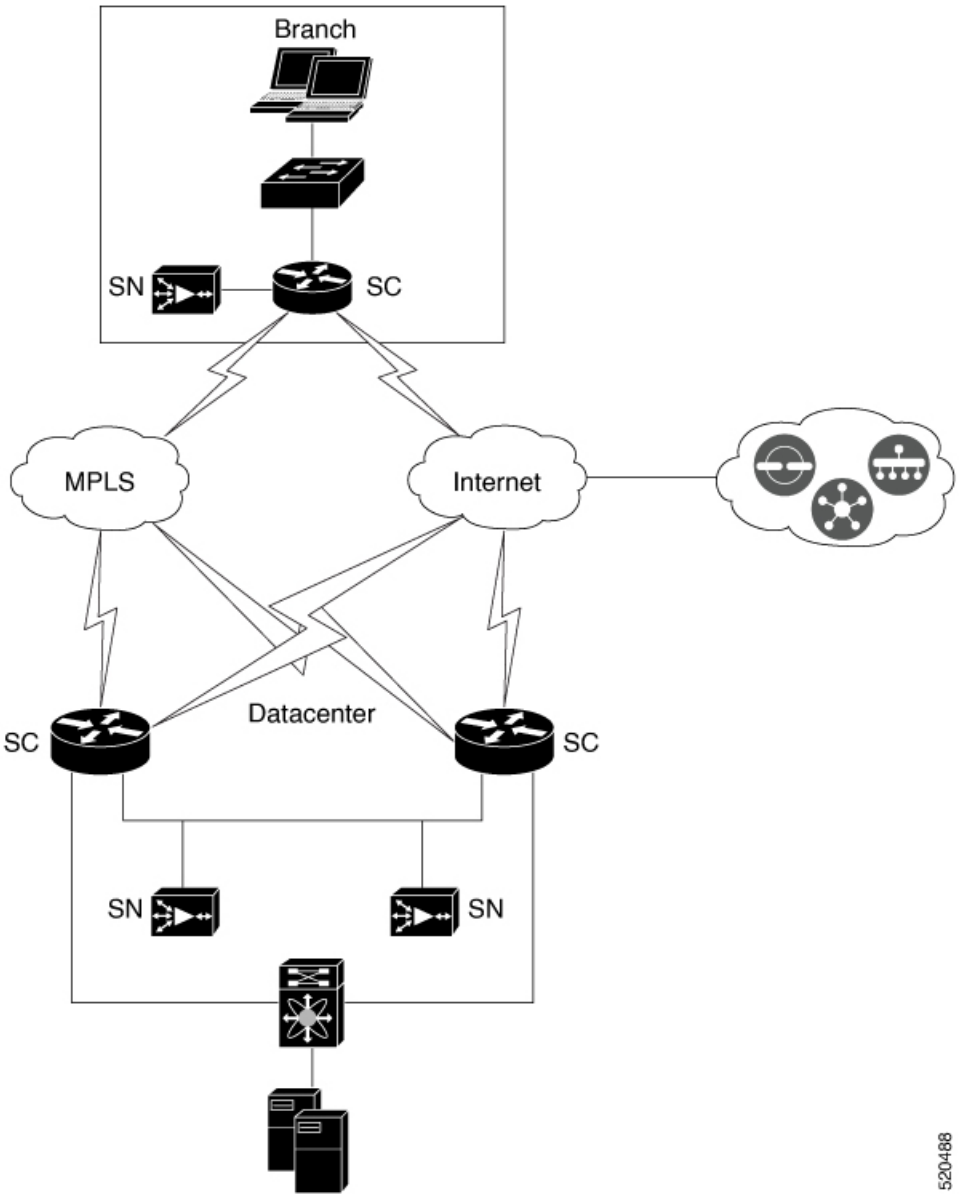
サービスコントローラとサービスノードの連携方法

- Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a では、Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V）のみにサービスノードロールを設定できます。Cisco Catalyst 8000V インスタンスにサービスノードロールを設定すると、デフォルトの AppQoE テンプレートがインスタンスにアタッチされます。これは変更できません。
- サイト内のサービスノードと、サービスクラスタを形成するために接続されているサービスコントローラ。
- サービスノードは相互に通信せず、クラスタ内の他のサービスノードを認識しません。
- サービスコントローラは、接続されているサービスノードとの通信を開始します。この設定は、サービスコントローラロールが定義されているデバイステンプレートに関連付けられた AppQoE 機能テンプレートで設定されます。
- サービスコントローラとサービスノードは、互いに隣接していたり、ネクストホップだったり、複数ホップ離れていたりする場合があります。

- サービスコントローラは、サービス VPN を介してサービスノードと通信します。他方、サービスノードは、トランスポート VPN または VPN 0 を介してサービスコントローラと通信します。
- サービスノードは、接続されているサービスコントローラにのみ応答します。
- Cisco SD-WAN Manager では、各 AppQoE サービスノードの正常性が緑色または黄色で表示されます。ステータスが緑色のノードのみが、新しいフローの配信対象と見なされます。黄色で表示されているサービスノードへの進行中のフローはリダイレクトされます。

トポロジの例

図 *4:* 外部サービスノードを使用したトポロジの例



*SN：サービスノード（コントローラあたり最大 64）
*SC：サービスコントローラ（サイトあたり最大 8）

上の図は、サービスコントローラの外部にあるサービスノードを使用した Cisco Catalyst SD-WAN 展開の例を示しています。この図は、ブランチサイトとデータセンター両方での展開を示しています。データセンターとブランチの Cisco IOS XE Catalyst SD-WAN デバイスは、それぞれのサイトのサービスノードで AppQoE クラスタを形成します。

ベストプラクティスと推奨事項

- サービスノードでAppQoEサービスに十分なキャパシティを確保するため、サービスノードロールが設定されているデバイスに他の機能を設定しないでください。
- サービスコントローラとサービスノードを含むAppQoEクラスタを作成する場合は、すべてのクラスタメンバーがサイトと同じ ID を持っていることを確認します。
- クラスタを形成するサービスコントローラとサービスノードが同じCisco Catalyst SD-WANサイト ID を共有していることを確認します。サイト ID に不一致がある場合、コントローラ上で該当するサービスノードが黄色の表示付きで報告されます。その後、これらのサービスノードは最適化のためのフロー分散で無視されるようになります。
- サービスコントローラとサービスノードを接続するネットワークの最大伝送ユニット（MTU）サイズが、トラフィックパス全体で均一であることを確認します。均一でない場合、パケット フラグメンテーションが原因で通信が切断される可能性があります。

AppQoE コントローラおよびサービスノードの設定

AppQoE サービスノードの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. [デバイステンプレート（Device Template] で、[テンプレートの作成（Create Template）] をクリックし、[機能テンプレートから選択（From Feature Template）] を選択します。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート（Device Templates）] は [デバイス（Device）] と呼ばれます。

3. [デバイスモデル（Device Model）] フィールドで、[C8000v] を選択します。

（注） Cisco Catalyst 8000V インスタンスのみを AppQoE サービスノードとして設定できます。他のデバイスを選択した場合、[デバイスロール（Device Role）] フィールドで [サービスノード（Service Node）] オプションは選択できません。

4. [デバイスロール（Device Role）] フィールドで、ドロップダウンリストから [サービスノード（Sevice Node）] を選択します。
5. [テンプレート名（Template Name）] と [説明（Description）] に入力します。
6. [Additional Templates] をクリックします。[AppQoE] フィールドで、工場出荷時のデフォルトとして [AppQoE外部サービスノード（AppQoE External Service Node）] テンプレートがアタッチされていることに注意してください。

AppQoEサービスノードとして設定されたデバイスに、これ以上の設定は必要ありません。サービスノードをサービスノードコントローラに接続するための追加設定は、Cisco SD-WAN Manager の AppQoE コントローラ設定画面で行います。

7. デバイステンプレートをデバイスに添付します。

AppQoE サービスコントローラの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. [デバイステンプレート（Device Template] で、[テンプレートの作成（Create Template）] をクリックし、[機能テンプレートから選択（From Feature Template）] を選択します。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート（Device Templates）] は [デバイス（Device）] と呼ばれます。

3. [デバイスモデル（Device Model）] フィールドで、サービスコントローラロールをサポートするデバイスのいずれかを選択します。サービスコントローラロールをサポートするデバイスの完全なリストについては、この章の「サポートされているプラットフォーム」セクションを参照してください。
4. [デバイスロール（Device Role）] フィールドで、ドロップダウンリストから [SDWAN エッジ（SDWAN Edge）] を選択します。

（注） [SDWANエッジ（SDWAN Edge）] オプションは、サービスコントローラロールをサポートするデバイスにのみ表示されます。

5. [テンプレート名（Template Name）] と [説明（Description）] に入力します。
6. [Additional Templates] をクリックします。[AppQoE] フィールドで、既存の AppQoE 機能テンプレートを選択するか、新しいテンプレートを作成できます。この手順には、サービスコントローラロールで設定されているデバイス用の新しい AppQoE テンプレートを作成する手順が含まれています。
7. [AppQoE] フィールドのドロップダウンリストをクリックしてから、[テンプレートの作成（Create Template）] をクリックします。
8. [テンプレート名（Template Name）] フィールドと [説明（Description）] フィールドに、テンプレートの名前と説明をそれぞれ入力します。
9. [コントローラ（Controller）] エリアで、要求される詳細情報を入力します。
    1. [コントローラIPアドレス（Controller IP Address）]：コントローラのサービス側インターフェイスの IP アドレスを入力します。これは、コントローラがサービスクラスタ内で接続されているサービスノードと通信するために使用するIPアドレスです。

2. [サービスVPN（Service VPN）]：サービスノードの LAN 側接続が存在するサービス VPN ID を指定します。VPN ID は、1 ～ 511、または 513～65527 の範囲で任意に指定できます。
3. [サービスノードIP 1（Service Node IP 1）]：サービスノードの IP アドレスを入力して、サービスコントローラがサービスノードと通信できるようにします。

（注） [サービスノードIP（Service Node IP）] フィールドの横にある [+] をクリックして、サービスノードをさらに追加します。1 つのサービスコントローラに最大 64 のサービスノードを追加できます。

（注） Cisco vManage リリース 20.6.1 から AppQoE 機能テンプレートを使用して、複数のサービスノードグループを設定し、設定したグループに外部サービスノードを追加できます。クラスタごとに最大 32 のサービスノードグループを設定できます。サービスノードグループの名前の範囲は、SNG-APPQOE0 ～ SNG-APPQOE31 です。

ただし、サービスコントローラとして設定しているデバイスのバージョンが Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 未満で、該当するデバイスの AppQoE テンプレートの設定に Cisco vManage リリース 20.6.1 を使用している場合、そのテンプレートで複数のサービスノードグループを設定可能な場合でも、設定できるのは 1 つのサービスノードグループのみになります。

10. デバイステンプレートをデバイスに添付します。

CLI を使用した AppQoE サービスコントローラおよびノードの設定

このセクションでは、外部サービスノードと、外部サービスノードに接続されたスタンドアロン サービス コントローラを使用して、TCP 最適化を CLI 設定する例を示します。

外部サービスノードの設定

1. TCP 最適化を有効にします。

```
Device# config-transaction
Device(config)# sdwan appqoe tcpopt enable
Device(config-appqoe)# no sslproxy enable
```

2. 仮想ポート グループ インターフェイスを作成します。

```
Device(config)# interface VirtualPortGroup virtual-port-group-number
```

```
Device(config-if)# service-insertion appqoe
Device(config-if)# ip address ip-address mask
```

3. サービスノードグループを作成します。

```
Device(config)# service-insertion service-node-group appqoe
service-node-group-name
Device(config-service-insertion-sng)# service-node service-node-ip-address
```

4. サービスノードを service plane heavy として設定します。

```
Device(config)# platform resource service-plane-heavy
```

（注） Cisco Catalyst 8000V を service plane heavy として設定する場合は、リロードしてサービスプレーンを有効にする必要があります。

サービスノードを作成するための完全な設定例を次に示します。

```
config-transaction

 sdwan appqoe tcpopt enable
  no sslproxy enable
  !

 service-insertion service-node-group appqoe SNG-APPQOE

  device-role service-node
  service-node 192.168.2.2
  !

 interface VirtualPortGroup1
  ip address 192.168.2.1 255.255.255.0
  service-insertion appqoe
  !

  interface GigabitEthernet 2
   description SN_LAN_Interface in VPN0
   ip address 192.0.2.1 255.255.255.0
   !

 platform resource service-plane-heavy

 system
  system-ip 198.51.100.1
  site-id 78200
 !
```

サービスコントローラの設定

1. サービスコントローラを作成し、サービス コントローラ グループに割り当てます。

```
Device# config-transaction
Device(config)# service-insertion appnav-controller-group appqoe
```

```
appqoe-controller-group-name
Device(config-service-insertion-acg)# appnav-controller controller-ip-address
```

2. サービスノードグループを作成し、サービスノードを追加します。

```
Device(config)# service-insertion service-node-group appqoe
service-node-group-name
Device(config-service-insertion-sng)# service-node service-node-ip-address
```

（注） 1つのサービスノードグループに複数の外部サービスノードを設定できます。

3. コントローラとサービスノードグループのサービスコンテキストを設定します。

```
Device(config)# service-insertion service-context appqoe/1
Device(config-service-insertion-context)# appnav-controller-group
appqoe-controller-group-name
Device(config-service-insertion-context)# service-node-group
service-node-group-name
Device(config-service-insertion-context)# enable
Device(config-service-insertion-context)# vrf default
```

サービスコントローラを作成するための完全な設定例を次に示します。

```
config-transaction

 service-insertion appnav-controller-group appqoe Test-ACgroup
  appnav-controller 198.51.100.1 vrf 200
  !

 service-insertion service-node-group appqoe Test-SNGroup
  service-node 192.0.2.2
  service-node 192.0.2.3
  service-node 192.0.2.4
  service-node 192.0.2.5
  !

 service-insertion service-context appqoe/1
  appnav-controller-group ACG-APPQOE
  service-node-group SNG-APPQOE
  cluster-type service-controller
  enable
  vrf default
  !

  interface GigabitEthernet 1
   description SC_To_SN_LAN_Interface in VPN200
   ip address 192.0.2.1 255.255.255.0
   vrf forwarding 200
   !

  system
   sytem-ip 198.51.100.10
   site-id 78200
   !
```

AppQoE サービスコントローラおよびノードのモニター

デバイスロールの確認

デバイステンプレートを使用してロールを設定した後、デバイスのデバイスロール（サービスコントローラまたはサービスノード）を確認するには、次の手順に従います。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. [デバイステンプレート（Device Templates）] エリアが表示されていることを確認します。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート（Device Templates）] は [デバイス（Device）] と呼ばれます。

使用可能なすべてのデバイステンプレートのリストが表示されます。

3. デバイスのロールを把握するには、[デバイスロール（Device Role）] 列を確認します。[SDWANエッジ（SDWAN Edge）] は、デバイスがサービスコントローラとして設定されていることを意味します。

サービスコントローラでのトラフィックのモニター

アラームおよびイベント

クラスタが形成されていない、または動作していない場合、デバイスは Cisco SD-WAN Manager に通知を送信します。このようなイベント通知は、Cisco SD-WAN Manager の [モニター（Monitor）] ページで確認できます。これらのイベントの一部について、Cisco SD-WAN Manager もアラームを生成します。デバイスのアラームとイベントを表示する方法については、「Alarms, Events, and Logs」[英語] を参照してください。

CLI を使用した AppQoE サービスコントローラおよびノードのモニター

AppQoE サービスコントローラ、サービスノード、およびクラスタの統計情報を表示するには、次の CLI コマンドを使用します。

次の出力例は、サービスノードグループ内のサービスノードの設定詳細を示しています。

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name : SNG-APPQOE
Service Context : appqoe/1
Member Service Node count : 2


Service Node (SN) : 10.1.1.1
```

```
Auto discovered : No
SN belongs to SNG : SNG-APPQOE
Current status of SN : Alive
System IP : 192.168.1.11
Site ID : 101
Time current status was reached : Wed Sep 23 11:01:49 2020

Cluster protocol VPATH version : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1601432656
Cluster protocol last received sequence number: 715749
Cluster protocol last received ack number : 1601432655
```

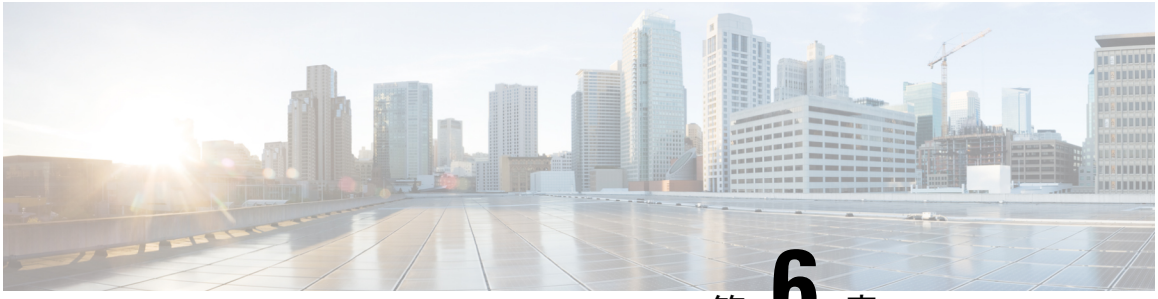
次の出力例は、サービスノードグループ内のサービスノードのトラフィック統計情報を示しています。

```
Device# show service-insertion type appqoe statistics service-node-group
Service Node Group: SNG-APPQOE
Number of Service Node(s): 2
Member Service Nodes:
IP Address
10.1.1.1
10.1.1.2

Aggregate of statistics from all SNs of the SNG:
-----------------------------------------------
Time since statistics were last reset/cleared:

Aggregate number of probe requests sent to SN : 1435070
Aggregate number of probe responses received from SN: 715915
Aggregate number of invalid probe responses received
Total : 0
Incompatible version : 0
Authentication failed : 0
Stale response : 0
Malformed response : 0
Unknown response : 0
Aggregate number of times liveliness was lost with the SN : 1
Aggregate number of times liveliness was regained with the SN:2
Aggregare number of version probes sent to SN: 719033
Aggregate number of version probes received from SN: 2
Aggregate number of healthprobes sent to SN: 716037
Aggregate number of healthprobes received from SN: 715913


Aggregate traffic distribution statistics
-----------------------------------------
Packet and byte counts-
-----------------------
Redirected Bytes : 1558757923174
Redirected Packets : 1945422189
Received Bytes : 1582477555093
Received Packets : 1908965233
```

次の出力例は、コントローラグループ内のサービスコントローラの設定詳細を示しています。

```
Device# show service-insertion type appqoe appnav-controller-group
All AppNav Controller Groups in service context
Appnav Controller Group : ACG-APPQOE
Member Appnav Controller Count : 1
Members:
IP Address
10.1.1.100
```

```
AppNav Controller : 99.1.1.100
Local AppNav Controller : Yes
Current status of AppNav Controller : Alive
Time current status was reached : Mon Sep 21 19:09:08 2020
Current AC View of AppNav Controller
IP Address
10.1.1.100

Current SN View of AppNav Controller
IP Address
10.1.1.1
```



第 6 章

DRE を使用したトラフィック最適化

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

表 *4*：機能の履歴

機能名	リリース情報	説明
DRE を使用したトラフィック最適化	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	このリリースでは、DRE 機能が Cisco Catalyst SD-WAN まで拡張されています。DRE は、WAN を介して送信されるデータのサイズを削減し、WAN をより効果的に使用できるようにする圧縮テクノロジーです。
DRE プロファイル	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、S、M、L、XL などのプロファイルを適用することで、接続要件に基づいて DRE のリソースを柔軟に使用できます。

機能名	リリース情報	説明
Cisco Catalyst 8000V 展開のための UCS E シリーズ サーバーのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能では、UCS E シリーズ ブレード サーバー モジュールを使用して、サポートされているルータで Cisco Catalyst 8000V インスタンスを展開するためのサポートが導入されています。この機能を使用すると、サポート対象のルータを、統合サービスノード、外部サービスノード、または内部サービスノードと外部サービスノードの両方を備えたハイブリッドクラスタとして設定できます。
Cisco Catalyst 8000V 展開のための UCS E シリーズ次世代サポート	Cisco vManage リリース 20.11.1 Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a	この機能では、UCS E1100D-M6 サーバーモジュールを使用して、サポート対象のルータに Cisco Catalyst 8000V エッジソフトウェアを展開するためのサポートが導入されています。

DRE でサポートされるデバイス

統合型サービスノードおよびコントローラ

デバイス	リリース	メモリ要件
Cisco Catalyst 8300 シリーズ エッジ プラットフォーム： • C8300-1N1S-6T • C8300-1N1S-4T2X • C8300-2N2S-6T • C8300-2N2S-4T2X	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降	• RAM：16 GB • ストレージ：600 GB
Cisco Catalyst 8200 シリーズ エッジ プラットフォーム： • C8200-1N-4T	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降	• RAM：16 GB • ストレージ：600 GB
Cisco Catalyst 8000V Edge ソフトウェア（Cisco Catalyst 8000V）	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降	• RAM：16 GB • ストレージ：600 GB • vCPU：8

外部サービスノードおよびコントローラ

デバイス	リリース	メモリ要件
Cisco Catalyst 8000V	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a	• RAM：32 GB • ストレージ：2 TB • vCPU：16
	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a	• RAM：16 GB • ストレージ：600 GB • vCPU：8

デバイス	リリース	メモリ要件
C8500L-8S4X	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a	• RAM：32 GB • ストレージ：2 TB
	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a	• RAM：16 GB • ストレージ：600 GB

DRE のディスク推奨事項

DRE および他の AppQoE サービスの展開には、SSD ディスクを使用することを推奨します。

Cisco Integrated Controller Manager（IMC）から、次の推奨パラメータを設定してください。一部の設定ではディスクのフォーマットが必要な場合があるため、ハイパーバイザをインストールする前に推奨パラメータを設定してください。

表 *5:* 推奨されるディスクパラメータ

パラメータ	値
RAID レベル	RAID10
Read Policy	常に先読み
ディスク キャッシュ ポリシー	ディセーブル
Write Policy	Write Back Good BBU
ストリップ サイズ	256 KB
I/O キャッシュポリシー	直接

Cisco Catalyst 8000V 展開のためのディスクプロビジョニングの推奨事項

Cisco Catalyst 8000V インスタンスの展開時に、ディスク形式として [シックプロビジョニング Eager Zeroed（Thick Provision Eager Zeroed）] を選択します。

サポート対象のハイパーバイザでの Cisco Catalyst 8000V インスタンスの展開については、次を参照してください。

- ESXi
- KVM

サポートされている DRE プロファイル

次の表にこの情報を示します。

- DRE 機能をサポートするデバイスとそのデフォルトの DRE プロファイル。
- デバイスでサポートされている DRE プロファイル。
- サポートされている UTD プロファイルと設定済みの DRE プロファイルサイズ。
- サポートされている DRE プロファイルの推奨最小リソース。
- サポートされているデバイスで DRE プロファイルによって提供される最大接続数。
- デバイスで設定されている DRE プロファイルに対応する FanOut 値。FanOut は、DRE サービスを形成するためにデバイスが通信できるピアの数を指します。

表 *6 : DRE* プロファイル、リソース要件、およびサポートされる接続と *FanOut*

デバイスとデフォルトの DRE プロファイル	DRE プロファイル	サポートされている UTD プロファイル	最小展開に関する推奨事項		最大接続数	FanOut
			RAM	ディスク		
C8200-1N-4T (S)	S	—	8 GB	120 GB	750	35
C8300-2N2S-6T (M) C8300-1N1S-4T2X (M) C8300-1N1S-6T (M)	S	S	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
C8300-2N2S-4T2X (M)	S	S、M	8 GB	120 GB	750	35
	M	S	8 GB	280 GB	5000	70
	L	—	16 GB	500 GB	10,000	256
C8500L-8G4X (M)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	32 GB	500 GB	22,000	256
	XL	—	32 GB	1600 GB	36,000	256

デバイスとデフォルトの DRE プロファイル	DRE プロファイル	サポートされている UTD プロファイル	最小展開に関する推奨事項		最大接続数	FanOut
			RAM	ディスク		
Cisco Catalyst 8000V：6 コア（S）	S	—	8 GB	120 GB	750	35
Cisco Catalyst 8000V：8 コア（S）	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
Cisco Catalyst 8000V：12 コア（S）	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	16 GB	500 GB	10,000	256
Cisco Catalyst 8000V：16 コア（S）	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	32 GB	500 GB	22000	256
	XL	—	32 GB	1600 GB	36000	256

（注） UCS E シリーズ サーバーは、6 コア、8 コア、および 12 コア Cisco Catalyst 8000V インスタンスのみをサポートします。詳細については、『Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V』[英語] を参照してください。

次の表にこの情報を示します。

- サポートされているデバイスで設定された DRE プロファイルに基づいて割り当てられたメモリ、ディスク、およびキャッシュ。

表 *7:* プロファイルごとのリソース割り当て

デバイスとデフォルトの DRE プロファイル	DRE プロファイル	リソース割り当て（GB）		
		メモリ	ディスク	Cache Size
C8200-1N-4T (S)	S	2	80	60

デバイスとデフォルトの DRE プロファイル	DRE プロファイル	リソース割り当て（GB）		
		メモリ	ディスク	Cache Size
C8300-2N2S-6T (M) C8300-1N1S-4T2X (M) C8300-1N1S-6T (M)	S	2	80	60
	M	4	250	230
C8300-2N2S-4T2X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
C8500L-8G4X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180
Cisco Catalyst 8000V：6 コア（S）	S	2	80	60
Cisco Catalyst 8000V：8 コア（S）	S	2	80	60
	M	4	250	230
Cisco Catalyst 8000V：12 コア（S）	S	2	80	60
	M	4	250	230
	L	8	480	460
Cisco Catalyst 8000V：16 コア（S）	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180

（注） UCS E シリーズ サーバーは、6 コア、8 コア、および 12 コア Cisco Catalyst 8000V インスタンスのみをサポートします。詳細については、『Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V』[英語] を参照してください。

Cisco Catalyst 8000V 展開のための UCS E シリーズ サーバーモジュールのサポート

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降、Cisco Catalyst 8000V インスタンスは、Cisco 4000 シリーズ サービス統合型ルータおよび Cisco Catalyst 8300 シリーズ エッジ プラットフォーム内に存在する UCS E シリーズ サーバーモジュールに展開できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降、Cisco Catalyst 8000 シリーズ エッジ プラットフォームにインストールされている UCS E シリーズ UCS E1100D-M6 サーバーモジュールに Cisco Catalyst 8000V インスタンスを展開できます。

デバイス ファミリ	デバイス モデル	サポートされている UCS E モジュールおよび DRE プロファイル
Cisco 4000 シリーズ サービス統合型ルータ	Cisco 4461	UCS E180D-M3/K9（S、M） UCS-E1120D-M3/K9（S、M、L）
	Cisco 4451	UCS E180D-M3/K9（S、M） UCS E1120D-M3/K9（S、M、L）
	Cisco 4351	UCS E160S-M3/K9（S）
	Cisco 4331	UCS E160S-M3/K9（S）
Cisco Catalyst 8300 シリーズ エッジ プラットフォーム	C8300-2N2S-4T2X	UCS E180D-M3/K9（S、M） UCS E1120D-M3/K9（S、M、L） UCS E1100D-M6（S）
	C8300-2N2S-6T	UCS E180D-M3/K9（S、M） UCS E1120D-M3/K9（S、M、L） UCS E1100D-M6（S）
	C8300-1N1S-4T2X	UCS E160S-M3/K9（S）
	C8300-1N1S-6T	UCS E160S-M3/K9（S）

DRE の制約事項

- DRE はデュアルサイド ソリューションです。したがって、DRE 最適化を設定するには、フローの対称性が必要です。DRE は非対称フローではサポートされません。

- DRE は、Cisco Catalyst SD-WAN オーバーレイトンネルの両端に統合サービスノードまたは外部サービスノードが展開されている場合にのみサポートされます。
- DREは、サービスコントローラとして設定されているデバイスではサポートされません。
- 統合脅威防御（UTD）がルータにインストールされており、トラフィックを外部サービスノードにリダイレクトするデータポリシーが存在するシナリオでは、トラフィックが特定の VRF の UTD によって学習された場合、同じトラフィックを外部サービスノードにリダイレクトすることはできません。
- Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降、SSL プロキシのデフォルトモードはシングルサイドです。ただし、DRE はデュアルサイド ソリューションであるため、トラフィックの送信側と受信側の両方で SSL が必要です。このデュアルサイド使用例の SSL パフォーマンスを最適化するには、Cisco SD-WAN Manager CLI テンプレートの `dual-side optimization enable` コマンドを使用して、デュアルサイド SSL 最適化を有効にします。WAN 経由で GRE トンネルを使用する場合、デュアルサイド SSL を有効にすることは推奨されません。
- Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以降、暗号化トラフィックの SMB 311 自動バイパスが DRE に対して有効になります。Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以前のデバイスで実行されているサービスノードに関して、SMB311 暗号化トラフィック バイパス ポリシーを DRE に対して手動で有効にすることも可能です。
- Cisco Catalyst 8000V が Cisco Enterprise Network Function Virtualization Infrastructure Software（NFVIS）に展開されている場合、DRE 最適化はサポートされません。

UCS E シリーズ サーバーでの Cisco Catalyst 8000V インストールの制約事項

（注） UCS E シリーズ サーバーのサポートは、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a からの外部サービスノードとしての Cisco Catalyst 8000V のインストールにのみ適用されます。

- UCS E シリーズ サーバーモジュールでの Cisco Catalyst 8000V インスタンスの展開では、VMware vSphere ESXi（リリース 6.7）ハイパーバイザのみがサポートされます。
- VMware vSpehere ESXi ハイパーバイザでは、ハイパースレッディングを無効にする必要があります。
- ハイパースレッディングは、UCS E シリーズ サーバーに展開された Cisco Catalyst 8000V の app-heavy コア割り当てプロファイルではサポートされていません。
- UCS E シリーズ サーバーモジュールの Cisco Catalyst 8000V インスタンスは、6、8、または 12 コアのみを搭載できます。
- UCS E シリーズ サーバーモジュールの Cisco Catalyst 8000V インスタンスは、app-heavy コア割り当てプロファイルを使用して設定し、DREサービスを実行できるようにする必要があります。

- サポート対象の UCS E シリーズ サーバーにインストールできる Cisco Catalyst 8000V インスタンスは 1 つのみです。
- デバイスに適用されている DRE プロファイルを変更するには、DRE をアンインストールし、再インストールしてから、新しい DRE プロファイルを適用する必要があります。

（注） DRE をアンインストールすると、キャッシュデータが失われます。

DRE について

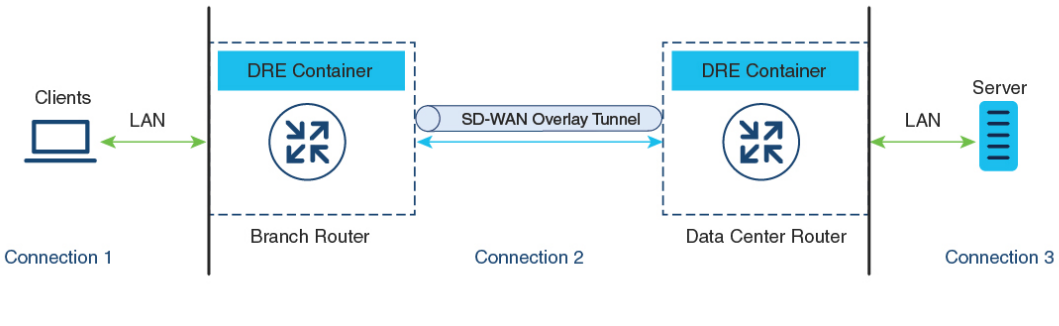
DRE の概要

データ冗長性排除（DRE）は、WAN を経由で送信されるデータのサイズを削減する圧縮テクノロジーです。DRE は、WAN 経由でデータストリームを送信する前に冗長な情報を削除して、送信データのサイズを削減します。DREの圧縮方式は、各ピアが圧縮に参加する共有キャッシュアーキテクチャに基づいており、圧縮解除も同じ冗長性キャッシュを共有します。DRE と Cisco Catalyst SD-WAN の統合により、DRE は、ストリーム内で繰り返されるデータを大幅に短い参照に置き換え、SD-WAN オーバーレイを介して短縮されたデータストリームを送信します。受信側端末は、ローカルの冗長性キャッシュを使用して、宛先クライアントまたはサーバーへ転送する前にデータストリームを再構築します。

（注） Cisco IOS XE Catalyst SD-WAN デバイス は、Cisco Catalyst SD-WAN オーバーレイ トンネルの両端に展開する必要があります。

DRE と TCP 最適化の連携の仕組み

図 *5: TCP* トラフィックの代行受信



DRE が設定されている場合、TCP トラフィックは代行受信され、次の 3 つの接続に分割されます。

接続タイプ	ネットワーク
クライアントからブランチ Cisco IOS XE Catalyst SD-WAN デバイスへ：この接続はローカルエリアネットワーク（LAN）に存在します。	LAN
ブランチルータからデータセンタールータへ	Cisco Catalyst SD-WAN オーバーレイトンネル経由
リモートブランチまたはデータセンタールータからサーバーへ	LAN

ローカルエリアネットワーク（LAN）の TCP 接続は、引き続き元のデータを送信します。ただし、Cisco Catalyst SD-WAN オーバーレイトンネル経由の TCP 接続は、DRE によって圧縮されたデータを送信します。トンネルの一方の側にある Cisco IOS XE Catalyst SD-WAN デバイスの DRE コンテナは、オーバーレイトンネル経由で送信される前にデータを圧縮します。トンネルの反対側にある Cisco IOS XE Catalyst SD-WAN デバイス の DRE コンテナは、リモートブランチまたはデータセンター側のサーバーに送信される前にデータを圧縮解除します。

DRE のコンポーネント

DRE キャッシュ：DRE キャッシュは、大量のデータを保存できるようにセカンダリストレージを使用します。DRE キャッシュは WAN の両側で保存され、エッジデバイスによってデータを圧縮解除するために使用されます。両方のデバイス（ブランチとデータセンター）の DRE キャッシュが同期されます。つまり、一方の側にチャンク署名がある場合、もう一方の側にもチャンク署名があります。

DRE 圧縮：DRE は、Lempel-Ziv-Welch（LZW）圧縮アルゴリズムを使用してデータを圧縮します。DRE は、大型のデータストリーム（数十から数百バイト）に作用し、はるかに大きな圧縮履歴を維持します。

DRE プロファイルの概要

DRE プロファイルは、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a で導入された機能です。この機能により、ブランチのサイズと必要な接続数に基づいて、DRE サービスにリソースを柔軟に割り当てることができます。DRE プロファイルは、接続要件に基づいたリソース割り当てを可能にする、リソース要件と割り当ての組み合わせです。

次の DRE プロファイルがサポートされています。

- 小規模（S）
- 中規模（M）
- 大規模（L）
- 超大規模（XL）

DRE 機能をサポートするデバイスでサポートされるプロファイルを確認するには、この章の「サポートされている *DRE* プロファイル」セクションを参照してください。

Cisco Catalyst 8000V 展開のための UCS E シリーズ サーバーのサポート

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降、Cisco Catalyst 8000V インスタンスは、サポート対象の UCS E シリーズ サーバーモジュールで外部サービスノードとして設定できます。該当するサーバーモジュールは、Cisco 4000 シリーズ サービス統合型ルータ（Cisco 4000 シリーズ ISR）および Cisco Catalyst 8000 シリーズ エッジ プラットフォームに搭載されています。これらのルータには統合サービスノードが付属しています。さらに、サポート対象の UCS E シリーズ サーバーを使用して、これらのルータに Cisco Catalyst 8000V インスタンスを展開することで、統合サービスノードと外部サービスノードを含むハイブリッドクラスタとして機能させることができます。この機能により、大容量の CPU を必要とする DRE などの AppQoE サービスを、CPU および RAM が低容量のルータで実行できるようになります。

Cisco UCS E シリーズ サーバーでの Cisco Catalyst 8000V の動作

- VMware vSphere ESXi 6.7 ハイパーバイザは、Cisco 4000 シリーズ ISR および Cisco Catalyst 8000 シリーズ エッジ プラットフォームに存在する UCS E シリーズ サーバーモジュールにインストールできます。
- その後、これらのサーバーに Cisco Catalyst 8000V をインストールできます。
- インストールされた Cisco Catalyst 8000V インスタンスは、app-heavy プロファイルを使用して設定する必要があります。この操作により、より多くのコアがサービスプレーンに割り当てられます。app-heavy プロファイルは、サービスプレーンコアとデータプレーンコアを分離するため、サービスプレーンのパフォーマンスが向上します。

DRE の設定

ソフトウェアリポジトリへの DRE コンテナイメージのアップロード

前提条件

シスコのソフトウェア ダウンロードページから、DRE コンテナイメージファイルをダウンロードします。DRE コンテナイメージをダウンロードするには、[Catalyst 8000Vエッジソフトウェア（Catalyst 8000V Edge Software）] ページに移動し、[IOS XE SD-WANソフトウェア（IOS XE SD-WAN Software）] を選択します。Cisco 8000 プラットフォーム全体で同じコンテナイメージを使用できます。

Cisco SD-WAN Manager へのコンテナイメージのアップロード

1. Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Repository]**を選択します。

2. [Virtual Images] をクリックします。
3. [仮想イメージのアップロード（Upload Virtual Image）] で、[vManage] を選択します。
4. ローカルマシンにダウンロードしたコンテナイメージを見つけて、[アップロード（Upload）] をクリックします。

   アップロードが完了すると、[仮想イメージ（Virtual Images）] ウィンドウにイメージが表示されます。

DRE コンテナ仮想イメージのアップグレード

コンテナイメージをアップグレードするには、「Upgrade Software Image on a Device」[英語] を参照してください。

DRE 最適化の有効化

DRE の AppQoE テンプレートの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [機能テンプレート（Feature Templates）] をクリックしてから、[テンプレートの追加（Add Template）] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. [選択されたデバイス（Selected Devices）] リストから、DRE でサポートされるデバイスを選択します。
4. [その他のテンプレート（Other Templates）] で、[AppQoE] をクリックします。
5. [テンプレート名（Template Name）] と [説明（Description）] に入力します。
6. 次のいずれかのデバイスロールを選択します。

   - [コントローラ（Controller）]：統合サービスノードを備えたコントローラとしてデバイスを設定する場合は、[コントローラ（Controller）] を選択します。統合サービスノードをサポートするデバイスでは、[有効化（Enable）] チェックボックスを使用できます。このオプションは、統合サービスノード機能をサポートしていないデバイスではグレー表示されます。
   - [サービスノード（Service Node）]：デバイスを外部サービスノードとして設定する場合は、[サービスノード（Service Node）] オプションを選択します。[外部サービスノード（External Service Node）] チェックボックスはデフォルトでオンになっています。

選択したデバイスを外部サービスノードとして設定できない場合、[サービスノード（Service Node）] オプションは表示されません。

7. [詳細（Advanced）] で、[DRE最適化（DRE Optimization）] を有効にします。

8

（注） [リソースプロファイル（Resource Profile）] フィールドは、DRE プロファイルに適用できます。DRE プロファイルは Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a で導入されました。したがって、このオプションは以前のリリースでは使用できません。

（オプション）[リソースプロファイル（Resource Profile）] フィールドで、ドロップダウンリストから [グローバル（Global）] を選択します。次に、使用可能なオプションからプロファイルサイズを選択します。

[リソースプロファイル（Resource Profile）] を設定しない場合は、デバイスのデフォルトの DRE プロファイルサイズが適用されます。デフォルトプロファイルの詳細については、「サポートされている DRE プロファイル」を参照してください。

9. （オプション）HTTPS、FTPS、またはその他の暗号化トラフィックを最適化するには、[SSL復号（SSL Decryption）] を有効にします。

（注） [SSL復号（SSL Decryption）] を有効にする場合は、TLS サービスがトラフィックを DRE コンテナに送信する前に復号し、トラフィックが最適化された後に再度暗号化できるように、SSL/TLS 復号セキュリティポリシーを設定する必要があります。

10. [Save] をクリックします。

SSL 復号のセキュリティポリシーの作成

この手順は、AppQoE 機能テンプレートを設定して DRE 最適化を有効にする際、SSL 復号を有効にする場合に適用されます。

SSL プロキシの CA の設定

SSL プロキシの認証局を設定するには、「Configure CA for SSL/TLS Proxy」[英語] を参照してください。

SSL 復号のセキュリティポリシーの設定

1. Cisco SD-WAN Manager メニューから、**[モニター（Monitor）]** > **[セキュリティ（Security）]** の順に選択します。
2. [セキュリティポリシーの追加（Add Security Policy）] をクリックします。

3. [アプリケーションのQuality of Experience（Application Quality of Experience）] を選択し、[続行（Proceed）] をクリックします。
4. [TLS/SSL複合ポリシーの追加（Add TLS/SSL Decryption Policy）] をクリックし、[新規作成（Create New）] を選択します。
5. [SSL復号の有効化（Enable SSL Decryption）] をクリックします。または、[SSL復号（SSL Decryption）] オプションを切り替えて有効にします。
6. [ポリシー名（Policy Name）] とその他の必要な詳細情報を入力します。
7. [TLS/SSL復号ポリシーの保存（Save TLS/SSL Decryption Policy）] をクリックします。新しいポリシーがウィンドウに表示されます。
8. **[Next]** をクリックします。
9. [セキュリティポリシー名（Security Policy Name）] と [セキュリティポリシーの説明（Security Policy Description）] を入力します。
10. ポリシーの CLI 設定を表示するには、[プレビュー（Preview）] をクリックします。それ以外の場合は、[保存（Save）] をクリックします。

デバイステンプレートの更新

DRE 設定を有効にするには、DRE を有効にした AppQoE ポリシーを、DRE を使用して AppQoE ポリシーを作成したデバイスのデバイステンプレートにアタッチします。

1. 新しいデバイステンプレートを作成するか、既存のテンプレートを更新するには、「Create a Device Template from Feature Templates」を参照してください。
2. [AppQoE] の [追加テンプレート（Additional Templates）] 領域で、[DRE用AppQoEテンプレートの設定（Configure AppQoE Template for DRE）] セクションで作成したテンプレートを選択します。

（注） DRE サービスを非アクティブ化するには、デバイステンプレートから AppQoE テンプレートを切り離します。

TCP および DRE 最適化のための集中管理型ポリシーの作成

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [集中管理型ポリシー（Centralized Policy）] で、[ポリシーの追加（Add Policy）]をクリックします。

（注） 詳細については、「Configure Centralized Policies Using Cisco vManage」[英語] を参照してください。

3. ポリシー設定ウィザードで、[トラフィックルールの設定（Configure Traffic Rules）] ウィンドウが表示されるまで、[次へ（Next）] をクリックします。
4. [トラフィックデータ（Traffic Data）] をクリックしてから、[ポリシーの追加（Add Policy）] をクリックします。
5. ポリシーの名前と説明を入力します。
6. [シーケンスタイプ（Sequence Type）] をクリックし、[データポリシーの追加（Add Data Policy）] ダイアログボックスから [カスタム（Custom）] を選択します。
7. [シーケンスルール（Sequence Rule）] をクリックします。
8. [一致（Match）] オプションでは、送信元データプレフィックス、アプリケーション/アプリケーションファミリリストなど、データポリシーに適用可能な一致条件を選択できます。
9. [アクション（Actions）] オプションで、[承認（Accept）] を選択します。オプションから [TCP最適化（TCP Optimization）] と [DRE最適化（DRE Optimization）] を選択します。

（注） すべての一致条件ですべてのアクションを使用できるわけではありません。使用可能なアクションは、選択した一致条件によって異なります。詳細については、「Configure Traffic Rules」[英語] を参照してください。

10. [一致とアクションの保存（Save Match and Actions）] をクリックします。
11. [データポリシーの保存（Save Data Policy）] をクリックします。
12. トラフィックフローに対して DRE 最適化をトリガーする必要があるサイトのエッジデバイスに、集中管理型データポリシーを適用します。
13. 集中管理型ポリシーをアクティブ化します。

DRE 最適化のための UCS E シリーズ サーバーモジュールでの Cisco Catalyst 8000V の設定

Cisco Catalyst 8000V インスタンスは、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a から、特定のルータモデルに存在するサポート対象の UCS E シリーズ サーバーに外部サービスノードとしてインストールできます。この機能により、ルータは、統合されたサービスノードと外部サービスノードを備えたハイブリッドクラスタとして動作することが可能になります。

設定ワークフロー

1. サポート対象のルータで UCS E シリーズ サーバーを設定します。
2. サポート対象の UCS E シリーズ サーバーに Cisco Catalyst 8000V を展開します。
3. Cisco SD-WAN Manager で、UCS E シリーズ サーバー上の Cisco Catalyst 8000V インスタンスの AppQoE 機能テンプレートを設定します。
4. Cisco SD-WAN Manager で、サービスコントローラの AppQoE 機能テンプレートを設定し、Cisco SD-WAN Manager CLI テンプレートおよび CLI アドオン機能テンプレートを使用して設定を追加します。

UCS E シリーズ サーバーの設定

はじめる前に

UCS E シリーズ サーバーモジュールをサポート対象のデバイスに挿入し、前面パネルから 2 つのインターフェイス（TE2 および TE3）を接続します。詳細については、『UCS-E Series Servers Hardware Installation Guide』[英語] を参照してください。

サポート対象ルータでの UCS E シリーズ サーバーの設定

次に、サポート対象ルータで UCS E シリーズ サーバーを有効にする設定例を示します。

```
Device(config)# ucse subslot 1/0
Device(config-ucse)# imc access-port shared-lom <ge1/te2/te3>
Device(config-ucse)# imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x
Device(config-ucse)# exit
Device(config)# interface ucse1/0/0
Device(config-if)# ip address x.x.x.1 255.255.255.0
```

UCS E シリーズ サーバーでの Cisco Catalyst 8000V の展開

はじめる前に

- UCS E サーバーモジュールにハイパーバイザをインストールします。
- シスコのソフトウェア ダウンロード ページから、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 用の Cisco Catalyst 8000V 17.6.1 OVA ファイルをダウンロードしてインストールします。

Cisco Catalyst 8000V の IP アドレスの設定

次に、UCS E シリーズ サーバーでの Cisco Catalyst 8000V の IP アドレスの設定例を示します。

```
Device(config)# interface GigabitEthernet1
Device(config-if)# description Mgmt
Device(config-if)# ip addeess x.x.x.x x.x.x.x
Device(config)# int GigabitEthernet2
Device(config-if)# description WAN-CONTROLLER
```

```
Device(config-if)# ip address x.x.x.x x.x.x.x
Device(config-if)# exit
Device(config)# int GigabitEthernet3
Device(config-if)# description UCSE-INTF
Device(config-if)# ip addeess x.x.x.x x.x.x.x
```

Cisco Catalyst 8000V インスタンスの AppQoE 機能テンプレートの設定

はじめる前に

UCS E シリーズ サーバーの Cisco Catalyst 8000V インスタンスは、app-heavy リソース割り当てプロファイルを使用して設定する必要があります。このプロファイルにより、Cisco Catalyst 8000V インスタンスは DRE 最適化に参加できます。

次の例は、Cisco SD-WAN Manager CLI アドオン機能テンプレートを使用して、デバイスを app-heavy として設定する方法を示しています。

```
Device(config)# platform resource app-heavy
```

Cisco Catalyst 8000V インスタンスの DRE 最適化の有効化

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [機能テンプレート（Feature Templates）] をクリックしてから、[テンプレートの追加（Add Template）] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. [選択されたデバイス（Selected Devices）] リストから、[C8000v] を選択します。
4. [その他のテンプレート（Other Templates）] で、[AppQoE] をクリックします。
5. [テンプレート名（Template Name）] と [説明（Description）] に入力します。
6. [サービスノード（Service Node）] オプションを選択します。
7. [詳細（Advanced）] セクションで、[DRE最適化（DRE Optimization）] を有効にします。
8. [Save] をクリックします。

コントローラクラスタタイプの設定

Cisco SD-WAN Managerでの UCS E シリーズ サーバー設定の追加

Cisco SD-WAN Manager で、CLI アドオン機能テンプレートを作成し、UCS E シリーズ サーバー設定を使用して更新します。

次に、CLI アドオン機能テンプレートに追加できる UCS E シリーズ サーバーの設定例を示します。

```
ucse subslot 1/0
imc access-port shared-lom te2
imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x

interface ucse1/0/0
vrf forwarding 5
```

オプション 1：クラスタタイプをサービスコントローラに設定する

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [機能テンプレート（Feature Templates）] をクリックしてから、[テンプレートの追加（Add Template）] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. [選択されたデバイス（Selected Devices）] リストで、UCS E シリーズ サーバーに展開されている Cisco Catalyst 8000V を含むルータを選択します。
4. [その他のテンプレート（Other Templates）] で、[AppQoE] をクリックします。
5. [テンプレート名（Template Name）] と [説明（Description）] に入力します。
6. [統合型サービスノード（Integrated Service Node）] チェックボックスはオフのままにします。
7. [コントローラIPアドレス（Controller IP Address）] フィールドに、コントローラの IP アドレスを入力します。

   または、ドロップダウンリストから [デフォルト（Default）] を選択します。AppQoE コントローラのアドレスがデフォルトで選択されます。
8. [サービスVPN（Service VPN）] フィールドに、サービス VPN 番号を入力します。

   または、ドロップダウンリストから [デフォルト（Default）] を選択します。AppQoE サービス VPN がデフォルトで選択されます。
9. [サービスノード（Service Nodes）] エリアで、[サービスノードの追加（Add Service Nodes）] をクリックして、AppQoE サービスノードグループにサービスノードを追加します。
10. [Save] をクリックします。
11. UCS E シリーズ サーバーに展開された Cisco Catalyst 8000V を含むルータのデバイステンプレートに、次をアタッチします。
    - UCS E シリーズ サーバー設定を使用した CLI アドオン機能テンプレート
    - AppQoE 機能テンプレート

DRE サービスを有効にするには、統合サービスノードとして個別に設定された Cisco Catalyst 8000V インスタンスで DRE を起動します。詳細については、「Enable DRE Optimization」[英語] を参照してください。

オプション 2：クラスタタイプをハイブリッドに設定する

UCS E シリーズ サーバーで展開されている Cisco Catalyst 8000V インスタンスを含むルータは、クラスタタイプをサービス コントローラまたはハイブリッドに設定できます。

1. Cisco SD-WAN Manager メニューから、**[設定（Configuration）] > [テンプレート（Templates）]** を選択します。
2. [機能テンプレート（Feature Templates）] をクリックしてから、[テンプレートの追加（Add Template）] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[機能テンプレート（Feature Templates）] は [機能（Feature）] と呼ばれます。

3. [選択されたデバイス（Selected Devices）] リストから、UCS E シリーズ サーバーに展開されている Cisco Catalyst 8000V を含むルータを選択します。
4. [その他のテンプレート（Other Templates）] で、[AppQoE] をクリックします。
5. [テンプレート名（Template Name）] と [説明（Description）] に入力します。
6. [統合サービスノード（Integrated Service Node）] フィールドで、[有効（Enable）] チェックボックスをオンにします。
7. [Save] をクリックします。
8. CLI テンプレートを作成して、クラスタタイプ ハイブリッド設定を追加します。

   次に、UCS E シリーズ サーバーに展開された Cisco Catalyst 8000V を含むルータでクラスタタイプをハイブリッドに設定する設定例を示します。

```
interface VirtualPortGroup2
 vrf forwarding 5
 ip address 192.168.2.1 255.255.255.0

interface ucse1/0/0
 vrf forwarding 5
 ip address 10.40.17.1 255.255.255.0
service-insertion service-node-group appqoe SNG-APPQOE
 service-node 192.168.2.2
service-insertion service-node-group appqoe SNG-APPQOE1
 service-node 10.40.17.5
!
service-insertion appnav-controller-group appqoe ACG-APPQOE
 appnav-controller 10.40.17.1 vrf 5

service-insertion service-context appqoe/1
 cluster-type hybrid
 appnav-controller-group ACG-APPQOE
 service-node-group SNG-APPQOE
```

```
service-node-group SNG-APPQOE1
vrf global
enable
```

9. UCS E シリーズ サーバーに展開された Cisco Catalyst 8000V を含むルータのデバイステンプレートに、次をアタッチします。
   - AppQoE 機能テンプレート
   - UCS E シリーズ サーバー設定を使用した CLI アドオン機能テンプレート
   - ハイブリッドクラスタ設定を含む CLI テンプレート

   DREサービスを有効にするには、統合サービスノードとして個別に設定されたCisco Catalyst 8000V インスタンスで DRE を起動します。詳細については、「Enable DRE Optimization」[英語] を参照してください。

CLI を使用した DRE の設定

DRE コンテナパッケージのインストール

DRE コンテナパッケージをインストールするには、次のコマンドを使用します。

```
app-hosting install appid < name > package bootflash:<name>.tar
```

仮想ポートグループの設定と DRE に対するマッピング

次に、仮想ポートグループを設定してDREサービスにマッピングした後にDREサービスを開始する例を示します。

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252

Device(config-if)# app-hosting appid dre


Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

仮想ポートグループの設定と DRE に対するマッピング、および DRE プロファイルの割り当て

（注） DRE プロファイル機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a からのみ使用できます。この機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a より前のリリースには適用されません。

次に、仮想ポートグループを設定して DRE サービスにマッピングし、DRE プロファイルをデバイスに割り当てる例を示します。この例は、小規模（S）プロファイルの割り当てを示しています。

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252

Device(config-if)# app-hosting appid dre
Device(config-app-hosting)# app-resource profile-package small



Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

DRE サービスのアクティブ化

次に、Bangalore という名前のアプリケーションの DRE サービスをアクティブ化する例を示します。

```
Device# app-hosting activate appid Bangalore
```

（注） DRE アプリケーションをすでに設定しているものの、有効にしていない場合は、**app-hosting activate appid** コマンドを使用します。または、前のセクションの例で示されているように、アプリケーション ホスティング ゲートウェイ コンフィギュレーション モードで **start** コマンドを使用することもできます。

DRE のアンインストール

DRE サービスを非アクティブ化してアンインストールするには、次の手順を実行します。

1. DRE サービスを停止するには、特権 EXEC モードで次のコマンドを使用します。

   ```
   Device# app-hosting stop appid Bangalore
   ```

   この例の Bangalore は、停止する DRE アプリケーションの名前です。

2. DRE サービスを非アクティブ化するには、特権 EXEC モードで次のコマンドを使用します。

   ```
   Device# app-hosting deactivate appid Bangalore
   ```

   この例の Bangalore は、非アクティブ化する DRE アプリケーションの名前です。

3. DRE サービスをアンインストールするには、特権 EXEC モードで次のコマンドを使用します。

   ```
   Device# app-hosting uninstall appid Bangalore
   ```

   この例の Bangalore は、アンインストールする DRE アプリケーションの名前です。

DRE のモニター

Cisco SD-WAN Manager を使用して、DRE によって最適化されたトラフィックまたはアプリケーションをモニターできます。

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

   Cisco vManage リリース 20.6.1 以前のリリース：Cisco SD-WAN Manager のメニューから **[モニター（Monitor）]** > **[ネットワーク（Network）]** の順に選択します。

2. モニターするデバイスのホスト名をクリックします。
3. [サービス（Service）] で、[AppQoE DRE最適化（AppQoE DRE Optimization）] を選択します。
4. モニター対象に応じて、[最適化されたトラフィック（Optimized Traffic）] または [アプリケーション（Application）] を選択します。
5. [コントローラ（Controller）] または [サービスノード（Service Node）] を選択します。

   選択したデバイスに統合サービスノードがある場合は、コントローラロールまたはサービスノードロールのデータを表示できます。選択したデバイスが外部 AppQoE サービスノードの場合は、外部サービスノードのモニタリングデータと、接続されているコントローラを表示できます。

チャートビューおよびテーブルビューオプション

選択したデバイスのモニタリングデータがチャート形式で表示され、その後にテーブルが表示されます。2 つのオプションを切り替えることで、グラフまたは棒グラフの形式でデータを表示できます。

- [グラフオプション（Chart Options）] ドロップダウンリストから、[バイト（Bytes）] または [削減率（Percentage Reduction）] でデータを表示できます。
- 指定した時間範囲（1 時間、3 時間、6 時間など）のデータをフィルタリングするか、[Custom] をクリックして時間範囲を定義できます。

CLI を使用した DRE のモニターとトラブルシュート

DRE 最適化ステータス

次に、**show sdwan appqoe dreopt status** コマンドの出力例を示します。

```
Device# show sdwan appqoe dreopt status

DRE ID                                          : 52:54:dd:d0:e2:8d-0176814f0f66-93e0830d

DRE uptime                                        : 18:27:43
```

```
Health status                                    : GREEN
Health status change reason                      : None
Last health status change time                   : 18:25:29
Last health status notification sent time        : 1 second
DRE cache status                                 : Active
Disk cache usage                                 : 91%
Disk latency                                     : 16 ms
Active alarms:
  None

Configuration:
  Profile type                                   : Default
  Maximum connections                            : 750
  Maximum fanout                                 : 35
  Disk size                                      : 400 GB
  Memory size                                    : 4096 MB
  CPU cores                                      : 1
  Disk encryption                                : ON
```

ステータスの詳細を表示するには、**show sdwan appqoe dreopt status detail** コマンドを使用します。

```
Device# show sdwan appqoe dreopt statistics detail
Total connections                 : 325071
Max concurrent connections        : 704
Current active connections        : 0
Total connection resets           : 297319
Total original bytes              : 6280 GB
Total optimized bytes             : 2831 GB
Overall reduction ratio           : 54%
Disk size used                    : 93%
Cache details:
  Cache status                      : Active
  Cache Size                        : 406573 MB
  Cache used                        : 93%
```

```
  Oldest data in cache               : 17:13:53:40
  Replaced(last hour): size          : 0 MB
  Cache created at                   : 27:14:13:43
  Evicted cache in loading cache     : 149610430464
Connection reset reasons:
  Socket write failures                              : 0
  Socket read failures                               : 0
  DRE decode failures                                : 0
  DRE encode failures                                : 0
  Connection init failures                           : 0
  WAN unexpected close                               : 297319
  Buffer allocation or manipulation failed           : 0
  Peer received reset from end host                  : 0
  DRE connection state out of sync                   : 0
  Memory allocation failed for buffer heads          : 0
  Other reasons                                      : 0
Connection Statistics:
  Alloc                                              : 325071
  Free                                               : 325071
Overall EBP stats:
  Data EBP received                                  : 1921181978
  Data EBP freed                                     : 1921181978
  Data EBP allocated                                 : 218881701
  Data EBP sent                                      : 218881701
  Data EBP send failed                               : 0
  Data EBP no flow context                           : 0
  Data EBP requested more than max size              : 46714730
```

DRE 自動バイパスステータス

次に、DRE 最適化の自動バイパスステータスの例を示します。

```
Device# show sdwan appqoe dreopt auto-bypass

      Server IP   Port       State    DRE LAN BYTES    DRE WAN BYTES    DRE COMP   Last
 Update   Entry Age
-------------------------------------------------------------------------------------------------
```

```
      10.0.0.1    9088       Monitor      48887002724      49401300299   0.000000
13:41:51   03:08:53
```

DRE 最適化統計情報

次に、DRE 最適化統計情報の例を示します。

```
Device# show sdwan appqoe dreopt statistics

Total connections                  : 3714

Max concurrent connections         : 552

Current active connections         : 0

Total connection resets            : 1081

Total original bytes               : 360 GB

Total optimized bytes              : 164 GB

Overall reduction ratio            : 54%

Disk size used                     : 91%

Cache details:

  Cache status                       : Active

  Cache Size                         : 407098 MB

  Cache used                         : 91%

  Oldest data in cache               : 03:02:07:55

  Replaced(last hour): size          : 0 MB
```

次に、ピアデバイスの DRE 最適化統計情報の例を示します。

```
Device# show sdwan appqoe dreopt statistics peer

  Peer No.  System IP          Hostname    Active connections    Cummulative connections

-------------------------------------------------------------------------------------

         0  209.165.201.1       dreopt                    0                       3714
```

DRE 復号ステータス

次に、復号要求を DRE に送信し、要求が正常に受信されたかどうかを確認する方法の例を示します。

```
Device# show sdwan appqoe dreopt crypt

Status: Success

Atempts: 1

1611503718:312238        DECRYPT REQ SENT
```

```
1611503718:318198        CRYPT SUCCESS

ENCRYPTION:

-------------------------------------------------

BLK NAME        :  No of Oper  | Success | Failure

-------------------------------------------------

SIGNATURE BLOCK |     210404     210404          0

SEGMENT BLOCK   |     789411     789411          0

SECTION BLOCKS  |      49363      49363          0

-------------------------------------------------

DECRYPTION:

-------------------------------------------------

BLK NAME        :  No of Oper  | Success | Failure

-------------------------------------------------

SIGNATURE BLOCK |     188616     188616          0

SEGMENT BLOCK   |          1          1          0

SECTION BLOCKS  |     366342     366342          0

-------------------------------------------------
```

DRE のトラブルシュート

次の出力例は、ピアデバイスの自動検出に関する統計情報を示しています。接続がDREによって最適化されていない場合は、次のコマンドを実行し、出力をシスコテクニカルサポートと共有します。

```
Device# show sdwan appqoe ad-statistics

============================================================

              Auto-Discovery Statistics

============================================================

 Auto-Discovery Option Length Mismatch       : 0

 Auto-Discovery Option Version Mismatch      : 0

 Tcp Option Length Mismatch                  : 6

 AD Role set to NONE                         : 0

 [Edge] AD Negotiation Start                 : 96771

 [Edge] AD Negotiation Done                  : 93711

 [Edge] Rcvd SYN-ACK w/o AD options          : 0

 [Edge] AOIM sync Needed                     : 99
```

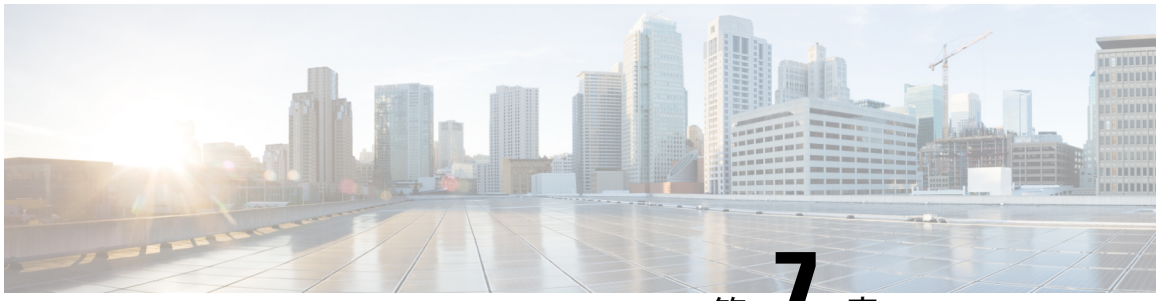
```
 [Core] AD Negotiation Start                : 10375
 [Core] AD Negotiation Done                 : 10329
 [Core] Rcvd ACK w/o AD options             : 0
 [Core] AOIM sync Needed                    : 0
```

次の出力例は、ピアデバイス間での 1 回の情報交換に関する統計情報を示しています。

```
Device# show sdwan appqoe aoim-statistics
============================================================
              AOIM Statistics
============================================================
 Total Number Of Peer Syncs      : 1
 Current Number Of Peer Syncs in Progress      : 0
 Number Of Peer Re-Syncs Needed      : 1
 Total Passthrough Connections Due to Peer Version Mismatch   : 0
 AOIM DB Size (Bytes): 4194304

 LOCAL AO Statistics
----------------------------------------
 Number Of AOs      : 2
 AO             Version   Registered
 SSL             1.2        Y
 DRE             0.23       Y

 PEER Statistics
----------------------------------------
 Number Of Peers      : 1
 Peer ID: 203.203.203.11
 Peer Num AOs      : 2
 AO             Version   InCompatible
 SSL             1.2        N
 DRE             0.23       N
```

次に、すべてのDREキャッシュをクリアする例を示します。キャッシュをクリアすると、DRE サービスが再起動します。

```
Device# clear sdwan appqoe dreopt cache

DRE cache successfully cleared
```



第 7 章

HTTP CONNECT

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

表 *8*：機能の履歴

機能名	リリース情報	説明
HTTP CONNECT	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、AppQoE での HTTP CONNECT メソッドの処理がサポートされるようになります。このサポートにより、SSL プロキシや DRE などのサービスで、HTTP CONNECT 暗号化トラフィックが最適化されます。

HTTP CONNECT に関する情報

HTTP CONNECT メソッドを使用すると、送信元サーバーは、明示的なプロキシサーバーを使用して宛先サーバーとの双方向通信を開始できます。HTTP CONNECT を使用して、送信元サーバーと宛先サーバー間の TCP 接続を介した HTTP プロキシトンネルを作成できます。HTTP CONNECT トラフィック処理により、SSL プロキシと DRE は、HTTP トンネル内の暗号化データを最適化できます。

SSL/TLS プロキシの詳細については、「Information about SSL/TLS Proxy」[英語] を参照してください。

HTTP CONNECT の前提条件

- Cisco IOS XE Catalyst SD-WAN デバイス が Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a を実行していることを確認します。
- HTTP CONNECT 要求をブロードキャストするには、リモートサーバーでホストされている明示的なプロキシが必要です。

HTTP CONNECT に関する制約事項

- HTTP CONNECT 要求は、プロキシサーバーにのみ送信されることを目的としています。
- HTTP CONNECT 要求は、標準ポートであるポート 80、8080、および 8088 を使用してのみ送信できます。
- HTTP CONNECT は、United Threat Defense（UTD）ではサポートされていません。そのため、UTD が有効になっている場合、設定はブロックされます。

HTTP CONNECT の使用例

HTTP CONNECT を使用しない SSL プロキシトラフィック

データの復号化がない Cisco IOS XE Catalyst SD-WAN リリース 17.x リリースの場合、DRE がフロー内の繰り返しパターンを把握できず、DRE圧縮は効果的ではありません。そのため、フローに対して DRE をバイパスすることが必須になります。あるいは、DRE に流れ込むデータをクリアテキストにする必要があります。HTTP CONNECT 要求が送信されるときに、SSL プロキシは HTTP CONNECT SSL トラフィックを復号しないため、暗号化されたトラフィックが DRE に流れ込みます。その結果、トラフィックの最適化に失敗します。

HTTP CONNECT を使用した SSL プロキシトラフィック

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以降、AppQoE での HTTP CONNECT の処理により、SSL プロキシはクリアテキストデータを復号化して DRE に送信するようになり、さらなる最適化が可能になります。

CLI アドオンテンプレートを使用した HTTP CONNECT の設定

はじめる前に

新しい CLI アドオンテンプレートを作成するか、既存の CLI アドオンテンプレートを編集します。

CLI Add-on Feature Templates の詳細については、「CLI Add-on Feature Templates」を参照してください。

CLI を使用した HTTP CONNECT の設定

1. コンフィギュレーション モードを入力します。

   ```
   config-transaction
   ```

2. HTTP CONNECT を有効にします。

   ```
   sdwan appqoe http-connect enable server-port <port-number>
   ```

（注） HTTP CONNECT を有効にするために入力できる標準サーバーポート番号は、80、8080、および 8088 のみです。

標準ポート番号を入力しない場合、サーバーポート番号 80 がデフォルトと見なされます。

3. 変更を確定します。

   ```
   commit
   ```

   次に例を示します。

   ```
   sdwan appqoe http-connect enable server-port80
   ```

4. CLI アドオンテンプレートをそれぞれのデバイスにアタッチします。

HTTP CONNECT 設定の確認

次に、**show sslproxy statistics** コマンドの出力例を示します。

```
Device# show sslproxy statistics
============================================================

              SSL Proxy Statistics

============================================================

Connection Statistics:

Total Connections                  : 3

Proxied Connections                : 0

Non-proxied Connections            : 3

Clear Connections                  : 0

Active Proxied Connections         : 0

Active Non-proxied Connections     : 2

Active Clear Connections           : 0

Max Conc Proxied Connections       : 0

Max Conc Non-proxied Connections   : 2

Max Conc Clear Connections         : 0

Tunneled Proxied Connections       : 2

Tunneled Non-proxied Connections   : 0

Active Tunneled Proxied Flows      : 1

Active Tunneled Non-proxied Flows  : 0

Max Conc Tunneled Proxied Flows    : 1

Max Conc Tunneled Non-proxied Flows: 0

SSL Encrypted marked Non SSL Flows : 0

Total Closed Connections           : 2
```

この出力で、**Tunnel Proxied Connections** と **Tunneled Non-proxied Connections** は、HTTP CONNECT 要求が成功したことを示しています。

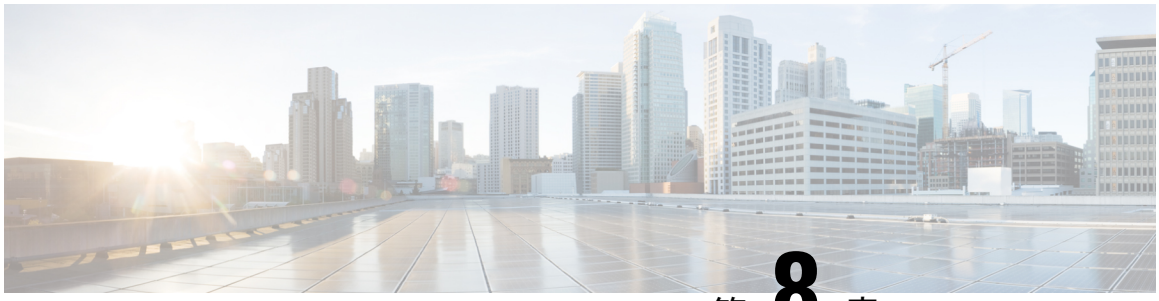
CLI を使用した HTTP CONNECT のモニター

デバイスの HTTP CONNECT をモニターするには、**show sdwan appqoe flow flow-id** コマンドを使用します。次に出力例を示します。

```
Device# show sdwan appqoe flow flow-id 4278327056727738
Flow ID: 4278327056727738
VPN: 1  APP: 0 [Client 192.0.2.0:49470 - Server 192.0.2.24:8080]

HTTP Connect: 1
TCP stats
---------
```

```
Client Bytes Received   : 215
Client Bytes Sent       : 46
Server Bytes Received   : 208
Server Bytes Sent       : 193

Client Bytes sent to SSL: 215
Server Bytes sent to SSL: 168

C2S HTX to DRE Bytes    : 0
C2S HTX to DRE Pkts     : 0
S2C HTX to DRE Bytes    : 152
S2C HTX to DRE Pkts     : 4
C2S DRE to HTX Bytes    : 70
C2S DRE to HTX Pkts     : 3
S2C DRE to HTX Bytes    : 46
S2C DRE to HTX Pkts     : 2

C2S HTX to HTTP Bytes   : 0
C2S HTX to HTTP Pkts    : 0
S2C HTX to HTTP Bytes   : 0
S2C HTX to HTTP Pkts    : 0
C2S HTTP to HTX Bytes   : 0
C2S HTTP to HTX Pkts    : 0
S2C HTTP to HTX Bytes   : 0
S2C HTTP to HTX Pkts    : 0

C2S SVC Bytes to SSL    : 129
S2C SVC Bytes to SSL    : 46
C2S SSL to TCP Tx Pkts  : 6
C2S SSL to TCP Tx Bytes : 193
S2C SSL to TCP Tx Pkts  : 2
S2C SSL to TCP Tx Bytes : 46
```

この出力で、**HTTP Connect: 1** は HTTP CONNECT 要求が成功したことを示します。



第 8 章

AppQoE の検証とトラブルシューティング

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

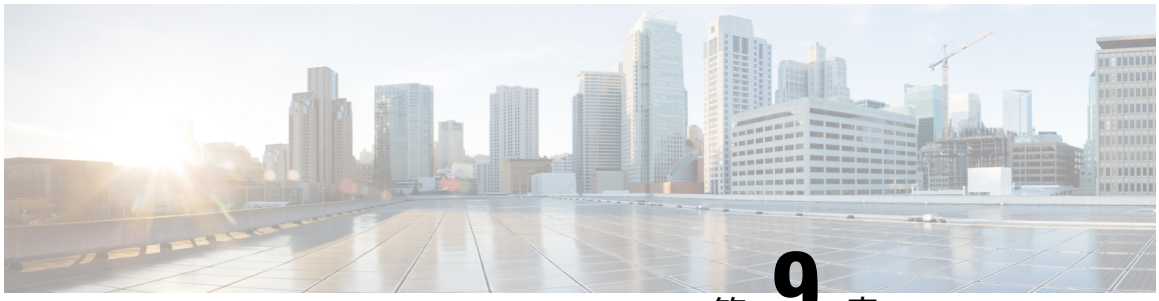
表 *9*：機能の履歴

機能名	リリース情報	説明
AppQoE の拡張トラブルシューティング	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a	このリリースでは、AppQoE機能の問題を確認しトラブルシュートするための付加的な show コマンドが導入されています。AppQoE の既存の show コマンドもいくつか拡張されました。 - show sdwan appqoe error recent - show sdwan appqoe status - show sdwan appqoe flow closed（キーワード error を含めるようにコマンドを変更） - show sslproxy status（コマンド出力の変更）

AppQoE の show コマンド

さまざまなAppQoE機能の設定を確認し、一般的な問題をトラブルシュートするには、次のコマンドを使用します。

- show sdwan appqoe
- show sdwan appqoe dreopt
- show sdwan appqoe dreopt statistics
- show sdwan appqoe error recent
- show sdwan appqoe status
- show sdwan appqoe flow closed
- show sdwan appqoe flow flow-id
- show sdwan appqoe flow vpn-id
- show sslproxy status



第 9 章

Cisco Catalyst SD-WAN AppQoE のトラブルシュート

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

概要

この章では、シスコの主題専門家（SME）が作成したドキュメントへのリンクを提供します。サポートチケットを必要とせずに技術的な問題を解決できるようにすることを目的としています。これらのドキュメントで問題を解決できない場合は、該当するシスココミュニティにアクセスすることをお勧めします。この問題をすでに経験し、解決策を提供している可能性のある他のシスコのお客様からは、豊富な情報とアドバイスを入手できます。コミュニティで解決策が見つからない場合は、シスコサポートでサポートチケットを提出するのが最善の方法です。サポートチケットを発行する必要がある場合、これらのドキュメントは、収集してサポートチケットに追加する必要があるデータに関するガイダンスを提供します。参照したサポートドキュメントを指定すると、TAC はドキュメントの所有者と改善要求を作成できます。

サポート記事

このセクションのドキュメントは、各記事の「使用するコンポーネント」セクションにリストされている特定のソフトウェアとハードウェアを使用して作成されています。ただし、これは、それらが使用されるコンポーネントにリストされているものに限定されるという意味ではなく、通常、ソフトウェアおよびハードウェアの新しいバージョンに関連し続けます。ソフトウェアまたはハードウェアに変更があり、コマンドが動作しなくなったり、構文が変更されたり、GUI や CLI がリリースごとに異なって見える可能性があることに注意してください。

このテクノロジーに関連したサポート記事は次のとおりです。

マニュアル	説明
Configure TCP Optimization Feature on Cisco IOS® XE SD-WAN cEdge Routers [英語]	このドキュメントでは、2019 年 8 月の 16.12 リリースで導入された Cisco IOS® XE SD-WAN ルータの Transmission Control Protocol（TCP）最適化機能について説明します。対象となるトピックは、前提条件、問題の説明、解決策、Viptela OS（vEdge）デバイスと XE SD-WAN デバイス間の TCP 最適化アルゴリズムの違い、設定、検証、および関連ドキュメントのリストです。

フィードバックのリクエスト

ユーザー入力が役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。
- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。