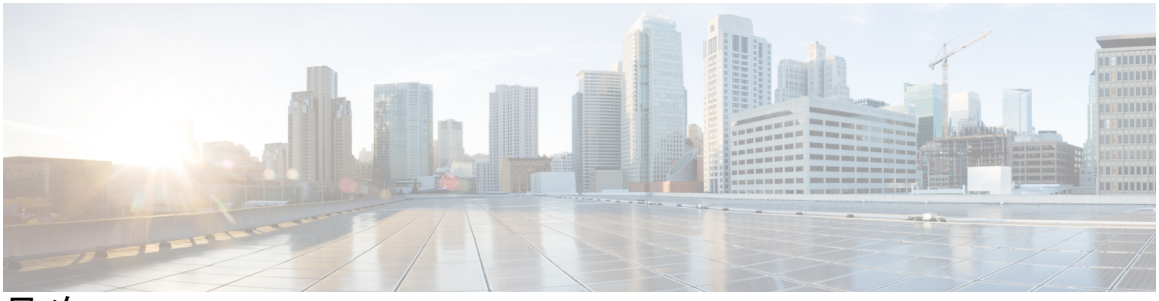
Cisco Catalyst 8000V エッジ ソフトウェア インストールおよびコンフィギュレーション ガイド

最終更新：2024 年 8 月 6 日

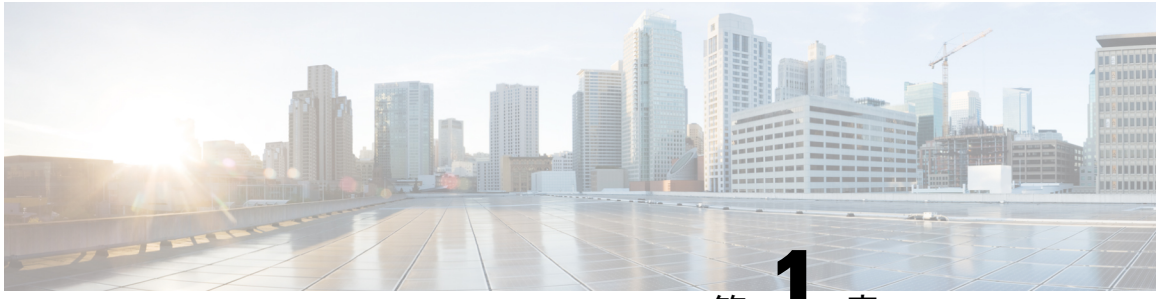
シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次

目 次

【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。



第 1 章

はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

対象読者および適用範囲

このドキュメントは、Cisco Enterprise ルータの設定担当者を対象としています。このドキュメントの対象者は、主に次のとおりです。

- ネットワーキングに関する技術的な背景知識と経験を持つお客様。
- ルータベースのインターネットワーキングに関する基本的な知識に精通しているが、Cisco IOS ソフトウェアについては経験の浅いシステム管理者。
- インターネットワーキング装置のインストールと設定を担当しているシステム管理者、および Cisco IOS ソフトウェアに精通しているシステム管理者。

機能の互換性

コンフィギュレーション ガイドで説明されているデバイスで使用可能な機能などの Cisco IOS XE ソフトウェアの詳細については、それぞれのルータのドキュメントセットを参照してください。

特定の機能のサポートを確認するには、Cisco Feature Navigator ツールを使用します。これは、特定のソフトウェアリリース、フィーチャセット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェアイメージを判別できるツールです。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または **Ctrl**	^ および **Ctrl** シンボルは、Ctrl キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、**Ctrl** キーを押しながら **D** キーを押すことを意味します。キーは大文字で表記されていますが、大文字と小文字の区別はありません。
string	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、SNMP コミュニティ ストリングとして public を設定する場合、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

コマンドシンタックスの説明には、次の表記法を使用しています。

表記法	説明
ボールド	ユーザが入力するコマンドおよびキーワードを示します。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
|	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1 つを選択します。
[x | y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x | y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。

省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。たとえば、次の表を参照してください。

表記法	説明
[x {y | z}]	角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

例では、次の表記法を使用しています。

表記法	説明
`screen`	画面に表示される情報の例は、Courier フォントで表します。
`bold screen`	ユーザの入力が必要なテキストの例は、太字の Courier フォントで表します。
< >	山カッコで囲まれたテキストは、パスワードなど、画面に出力されないテキストを表します。
!	行の先頭にある感嘆符（!）は、コメント行を表します。また、いくつかのプロセスでも、Cisco IOS XE ソフトウェアにより感嘆符が表示されることがあります。
[ ]	角カッコは、システム プロンプトに対するデフォルトの応答です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] 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、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 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。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

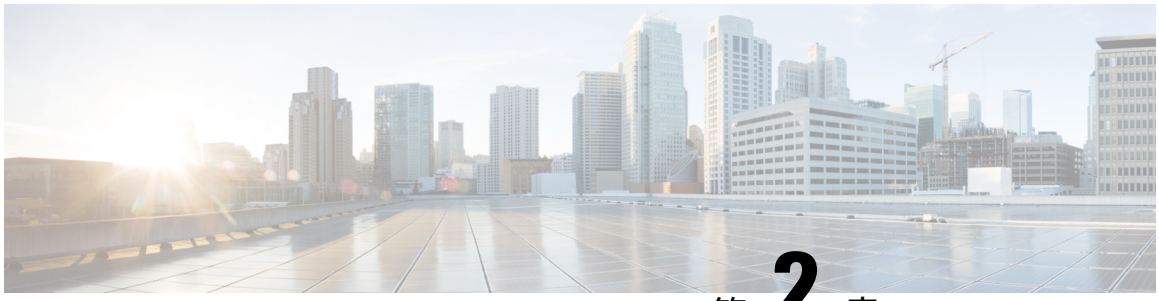
マニュアルに関するフィードバック

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。

トラブルシューティング

トラブルシューティングの最新の詳細情報については、
https://www.cisco.com/c/ja_jp/support/index.html にある Cisco TAC Web サイトを参照してください。

製品カテゴリに移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、**トラブルシュートおよびアラート**を参照してください。



第 2 章

Cisco Catalyst 8000V の概要

Cisco Catalyst 8000V エッジソフトウェア は、x86 サーバーハードウェアで実行されている仮想マシン（VM）に導入された仮想のフォームファクタルータです。このガイドでは、Cisco Catalyst 8000V の概要、インストール、アップグレード、および設定について説明します。

Cisco Catalyst 8000V は、それぞれ自律モードとコントローラモードを介して Cisco IOS XE と Cisco IOS XE SD-WAN の両方の機能をサポートします。Cisco Catalyst 8000V は、自律モードでは Cisco IOS XE ソフトウェアの機能とテクノロジーのサブセットをサポートし、仮想化プラットフォームで Cisco IOS XE セキュリティとスイッチング機能を提供します。コントローラモードでは、仮想環境とクラウド環境で包括的な SD-WAN、WAN ゲートウェイ、およびネットワークサービス機能を提供します。

VM 上に Cisco Catalyst 8000V を展開した場合、Cisco IOS XE ソフトウェアは、あたかも従来のシスコのハードウェアプラットフォーム上に展開されているかのように機能します。このルータには、アーキテクチャの一部として仮想ルートプロセッサと仮想フォワーディングプロセッサ（FP）が含まれており、ブランチオフィスやデータセンターなどの企業ロケーションからパブリッククラウドまたはプライベートクラウドへのセキュアな接続を提供します。

Cisco Catalyst 8000V は SSL VPN をサポートしています。Cisco IOS XE リリース 17.x 以降では、Cisco IOS-XE ルータを SSL VPN ゲートウェイとして実行している場合、TLS カプセル化により、余分な SSL VPN オーバーヘッドが追加されます。SSL VPN クライアントとサーバー間のパケットの IP フラグメンテーションとリアセンブルを防ぐには、TCP-MSS 値を最適に調整する必要があります。そうしないと、SSL VPN ゲートウェイで IPFragErr エラーによるパケットドロップが発生する可能性があります。

Cisco Catalyst 8000V ルータは、Enterprise Network Compute System（ENCS）プラットフォームおよび Cisco Cloud Services Platform 5000 シリーズでのルーティングおよび転送用の仮想 IOS XE オペレーティングシステムも提供します。

この仮想ルータの機能を使用するには、Cisco Catalyst 8000V ルータをハイパーバイザ上の仮想マシンとして展開する方法を確認してください。

Cisco Catalyst 8000V ルータを使用した仮想化のメリット

- **ハードウェアの独立性**：Cisco Catalyst 8000V ルータは、クラウドの仮想化の利点を活用してハードウェアの独立性を提供します。Cisco Catalyst 8000V は仮想マシン上で動作するため、仮想化プラットフォームでサポートされている任意の x86 ハードウェアでこのルータを使用できます。
- **リソースの共有**：Cisco Catalyst 8000V で使用されるリソースはハイパーバイザによって管理されており、これらのリソースは VM 間で共有できます。VM サーバーが特定の VM に割り当てるハードウェアリソースの量を調整できます。サーバー上の別の VM にリソースを再割り当てできます。
- **展開の柔軟性**：サーバー間で容易に VM を移動できます。したがって、ある物理的な場所にあるサーバーから別の物理的な場所にあるサーバーへハードウェアリソースを移動せずに Cisco Catalyst 8000V インスタンスを移動できます。
- **強化されたソフトウェアセキュリティ - セキュアなオブジェクトストア**：Cisco Catalyst 8000V では、NVRAM、ライセンス、およびその他のデータのストレージパーティションがオブジェクトストアとして作成されます。個々のオブジェクトストアはデータのセキュリティを確保するために暗号化されており、この製品は Cisco Secure Development ライフサイクル（CSDL）に準拠しています。さらに、Cisco Catalyst 8000V は 16G ディスクプロファイルをサポートします。

ルータ インターフェイス

Cisco Catalyst 8000V ルータインターフェイスはハードウェアベースのシスコ ルータと同じ機能を実行します。Cisco Catalyst 8000V インターフェイスは次のように機能します。

- インターフェイスは、論理的にギガビットイーサネット（GE）インターフェイスと呼ばれます。
- 使用可能なインターフェイスの番号付けは、Cisco Catalyst 8000V バージョンによって異なります。

デバイスを初めて起動すると、Cisco Catalyst 8000V ルータインターフェイスは、Cisco Catalyst 8000V への vNIC 列挙に基づいて VM 上の vNIC インターフェイスにマッピングされます。次回起動時に、Cisco Catalyst 8000V ルータインターフェイスが vNIC MAC アドレスにマッピングされます。

詳細については、「Cisco Catalyst 8000V Network Interfaces to the VM Network Interfaces」を参照してください。

インターフェイスの番号付け

- インターフェイスポートの番号付けは、1 からサポートされるインターフェイスの数までです。サポートされる vNIC と、各 VM インスタンスでサポートされる vNIC の最小数および最大数については、VMware 要件 （24 ページ）を参照してください。
- ギガビット イーサネット インターフェイス 0 はサポートされていません。
- 任意のインターフェイスを管理インターフェイスとして指定できます。ターゲット環境で使用可能な適切な Day0 ブートストラップメカニズムを実行することで、管理インターフェイスを指定できます。詳細については、デイゼロ設定 （75 ページ）を参照してください。

Cisco IOS XE および Cisco Catalyst 8000V

Cisco Catalyst 8000V は、Cisco IOS XE および Cisco IOS XE SD-WAN で動作する仮想ルータです。このガイドでは、Cisco IOS XE での Cisco Catalyst 8000V の概要、インストール、および設定情報について説明します。

次の方法で Cisco Catalyst 8000V を設定および管理できます。

- VM にシリアルポートをプロビジョニングして接続し、Cisco IOS XE CLI コマンドにアクセスします。

（注） 基盤となるハイパーバイザが VM とシリアルポートの関連付けをサポートしている場合にのみ、シリアルポートを使用して Cisco Catalyst 8000V VM を管理できます。詳細については、ハイパーバイザのドキュメンテーションを参照してください。

- Cisco IOS XE CLI コマンドにアクセスするには、リモート SSH または Telnet を使用します。

（注） デフォルトでは、Telnet はセキュリティ上の理由から無効になっています。SSH は、オンプレミス展開では無効になっています。リモートユーザー管理には SSH が推奨されますが、オンプレミス展開では SSH を手動で有効にする必要があります。

クラウド展開では、SSH はデフォルトで有効になっています。SSH にアクセスするには、クラウドセキュリティ設定でインバウンドトラフィックとアウトバウンドトラフィックの両方に SSH 接続が許可されていることを確認します。

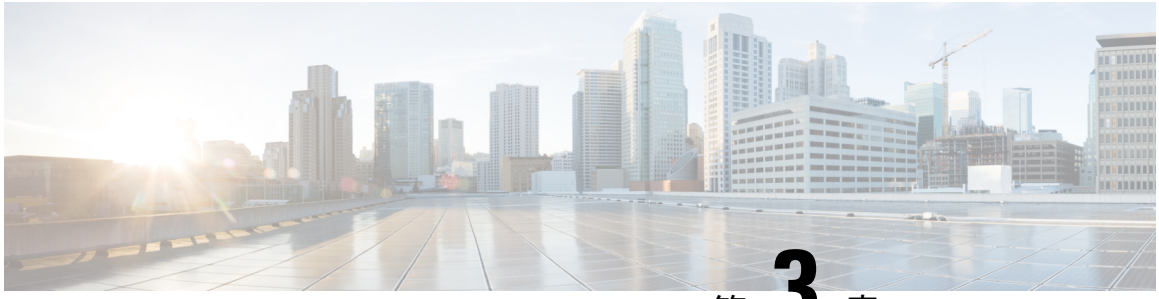
Cisco Catalyst 8000V のソフトウェアは、標準の Cisco IOS XE CLI コマンドと表記規則を使用します。コマンドは大文字と小文字を区別せず、コマンドおよびパラメータは、現在使用可能な

他のコマンドまたはパラメータと区別可能な文字数まで省略できます。Cisco IOS XE CLI のすべての機能とその使用方法にアクセスするには、『Configuration Fundamentals Configuration Guide』を参照してください。

Cisco Unified Computing System（UCS）製品

表 *1 : Cisco Catalyst 8000V* の *Cisco UCS* サーバーとの互換性

Cisco Unified Computing System（UCS）製品	Cisco UCS サーバーの要件は次のとおりです。 • VMware 認定済みである。 • 4 つ以上のコアが設定されている。 • 最低 16 GB の UCS メモリ。SDWAN/コントローラモードを使用する場合は、SDWAN vManage、vBond、および vSmart に対応するために少なくとも 128 GB のメモリが必要です。 • 最低 1 TB の UCS ストレージ。 • UCS C220 M5 以上を推奨します。 サポートされているハイパーバイザと互換性のある UCS ハードウェアおよびソフトウェアを確認するには、http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html を参照してください。



第 3 章

設置の概要

この章では、Cisco Catalyst 8000V をインストールする方法の概要を説明します。Cisco ハードウェアルータは、通常、Cisco IOS XE ソフトウェアをプレインストールして出荷されます。しかしながら、Cisco Catalyst 8000V はハードウェアベースのルータではないため、Cisco.com から Cisco IOS XE ソフトウェアをダウンロードして、仮想ルータを仮想マシンに直接インストールする必要があります。インストールに進む前に、Cisco Catalyst 8000V ソフトウェアをインストールして起動できるように、まず VM の属性をプロビジョニングする必要があります。

選択したハイパーバイザに依存するさまざまなインストールファイルとインストールオプションについては、次のセクションを参照してください。

インストール ファイル

次の表に、サポートされているハイパーバイザへの Cisco Catalyst 8000V のインストールに使用できるソフトウェアイメージを示します。

イメージ タイプ	ハイパーバイザ	モード	セキュアブート	ファイル名の例
bin	ESXi、KVM、AWS、Microsoft Azure、GCP	アップグレード（バンドルモード） アップグレード（インストールモード）	不可	c8000v-universalk9.17.04.01a.SPA.bin

イメージ タイプ	ハイパーバイザ	モード	セキュアブート	ファイル名の例
iso：VM にソフトウェアイメージをインストールするために使用されます。	ESXi、KVM	新規インストール	不可	c8000v-universalk9.17.04.01a.iso
ova：VM での OVA テンプレート（TAR 形式）の展開に使用されます。	ESXi	新規インストール	対応	c8000v-universalk9.17.04.01a.ova
qcow2：KVM 環境でソフトウェアイメージをインストールするために使用されます。	KVM	新規インストール	不可	c8000v-universalk9.17.04.01a.qcow2
serial.qcow2	KVM	新規インストール	不可	c8000v-universalk9.17.04.01a.efi.qcow2
efi.qcow2	KVM	新規インストール	対応	c8000v-universalk9.17.04.01a.efi.qcow2
serial.efi.qcow2	KVM	新規インストール	対応	c8000v-universalk9.17.04.01a-serial.efi.qcow2
tar.gz	NFVIS	新規インストール	対応	c8000v-universalk9.17.04.01a-tar.gz

（注） セキュアブートは特定のイメージタイプでサポートされますが、この機能はデフォルトでは有効になっていません。ハイパーバイザのセキュアブートを有効にする方法については、「VNF Secure Boot」を参照してください。

サポートされるハイパーバイザ

ハイパーバイザは、単一のハードウェア ホスト マシンを複数のオペレーティング システムで共有できるようにします。各オペレーティングシステムがホストのプロセッサ、メモリ、およびその他のリソースを専有していたとしても、ハイパーバイザは、各オペレーティングシステムに必要なリソースのみを制御して割り当てます。そうすることにより、オペレーティングシステム（VM）が相互に干渉しないようにします。

Cisco Catalyst 8000V でサポートされるハイパーバイザは次のとおりです。

- **VMware ESXi**：Cisco Catalyst 8000V は VMware ESXi ハイパーバイザ上で動作します。VMware ESXi ハイパーバイザは、仮想化拡張機能を含む x86 ハードウェア上で動作します。VMware の要件を確認し、ESXi 環境に Cisco Catalyst 8000V をインストールする方法を調べるには、「Installing in VMware ESXi Environment」を参照してください。
- **Red Hat KVM**：Cisco Catalyst 8000V は Red Hat Enterprise Linux（RHEL）上でも動作します。
- **パブリッククラウド**：上記のハイパーバイザとは別に、Cisco Catalyst 8000V を Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Alibaba Cloud で展開して使用することもできます。詳細については、それぞれのパブリッククラウド展開ガイドを参照してください。

仮想マシン処理リソース

Cisco Catalyst 8000V は低遅延アプリケーションであり、ホスト側の処理リソースがオーバーサブスクライブされている場合、正しく機能しない可能性があります。デフォルトでは、ほとんどのハイパーバイザは処理リソースのオーバーコミットをサポートしています。とはいえ、Cisco Catalyst 8000V では、仮想 CPU（vCPU）をオーバーサブスクライブしている状況で、確実にスケジュール設定しなかった場合、パケット処理のドロップ、エラーメッセージ、またはシステム停止が発生する可能性があります。

Cisco Catalyst 8000V vCPU は、実際の物理コアで動作するようにホストハイパーバイザによってスケジュール設定される必要があります。各ハイパーバイザには、物理コアへの vCPU のスケジュール設定に影響を及ぼすさまざまな制御機能があります。ベストプラクティスとして、vCPU と実際の物理コアの比率を 1:1 にすることを推奨します。

仮想マシン処理リソースの詳細については、ハイパーバイザが提示する各ハイパーバイザのチューニングガイドを参照してください。また、本ガイドの該当するハイパーバイザのセクションを参照できます。この資料は、パフォーマンスを向上させ、システム全体の確定性を改善させるために使用可能な設定について説明しています。

インストールファイルのダウンロード

ステップ 1 シスコの Software Download ページに移動します。

ステップ 2 ページの下部にある [Select a Product] フィールドで、Cisco Catalyst 8000V を検索します。

ステップ 3 Cisco Catalyst 8000V のリンクをクリックし、ダウンロードページに移動します。

ステップ 4 左側のペインから該当するリリースを選択します。たとえば、Bengaluru 17.4.1 を選択します。

ステップ 5 使用可能なイメージのリストで [Download] または [Add to Cart] をクリックします。手順に従ってソフトウェアをダウンロードしてください。

（注） ダウンロードするインストールファイルを確認するには、インストール ファイル （9 ページ）を参照してください。

注意事項と制約事項

ネットワークに Cisco Catalyst 8000V ルータをインストールする前に留意すべき一般的な注意事項と制限事項を以下に示します。

- ネストされた VM 内の Cisco Catalyst 8000V はテストされていないため、推奨されません。
- ハイパーバイザが vNIC ホット追加/削除をサポートしていない場合、VM の電源が入っているときに、VM のハードウェア（メモリ、CPU、ハードドライブのサイズなど）に変更を加えないでください。
- Gigabit Ethernet0 インターフェイスは使用できなくなりました。任意のインターフェイスを管理インターフェイスとして指定できます。
- 仮想 VGA コンソールまたは仮想シリアルポートのコンソールのいずれかを使用して、Cisco IOS XE CLI にアクセスできます。初回インストール中に GRUB モードからコンソールを選択するか、ルータの起動後に Cisco IOS XE **platform console** コマンドを使用してコンソールを変更します。詳細については、Cisco Catalyst 8000V を VM として起動 （167 ページ）を参照してください。
- I350 デバイスで仮想機能を実行している場合、HSRP/VRRP などの冗長プロトコルはサポートされません。
- .qcow2 ファイルの場合、インストール時に選択したイメージによって、選択できるコンソールのタイプが決まります。
- vNIC は、インターフェイスでのデュプレックス設定をサポートしていません。
- vNIC は自動ネゴシエーションをサポートしていません。

- Cisco IOS XE 17.9.1 以降、**show license udi** コマンドは Cisco Catalyst 8000Vでサポートされなくなりました。
- Cisco Catalyst 8000V は、L2TP クライアントや L2TP ネットワークサーバー（LNS）を含む L2TP 機能をサポートしていません。
- メモリが少ない Cisco Catalyst 8000V 展開では SDWAN の設定が厳しいため、コントローラモードで 8GB メモリで Cisco Catalyst 8000V を使用することをお勧めします。このため、Cisco Catalyst 8000V でメモリ使用率が高くなることがあります。

（注） 一部のハイパーバイザは、シリアルコンソールアクセスをサポートしない場合があります。ハイパーバイザのマニュアルを使用して、サポートを確認してください。

次の作業

インストールファイルをダウンロードしたので、展開に進むことができます。選択したハイパーバイザに応じて、展開手順は異なります。

適切なハイパーバイザ環境での Cisco Catalyst 8000V の展開方法については、このガイドの次の章を参照してください。

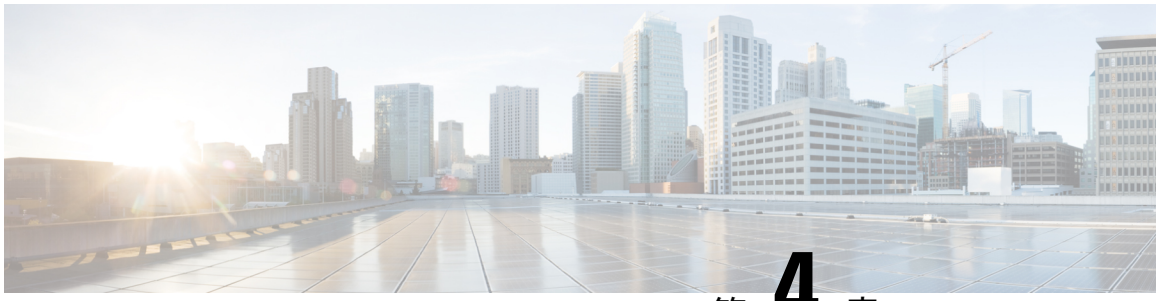
- VMware ESXi 環境でのインストール
- カーネル仮想マシンサポート（KVM）環境でのインストール

パブリッククラウドでの展開

- Amazon Web Services 環境での Cisco Catalyst 8000V 展開の詳細については、『Deploying Cisco Catalyst 8000V Edge Software on Amazon Web Services』を参照してください。
- Microsoft Azure 環境での Cisco Catalyst 8000V 展開の詳細については、『Deploying Cisco Catalyst 8000V on Microsoft Azure』を参照してください。
- Google Cloud Platform での Cisco Catalyst 8000V 展開の詳細については、『Deploying Cisco Catalyst 8000V on Google Cloud Platform』を参照してください。
- Alibaba Cloud での Cisco Catalyst 8000V の展開の詳細については、『Deploying Cisco Catalyst 8000V on Alibaba Cloud』を参照してください。

（注） インストールを続行する前に、次の章を参照してください。

- Day 0 Configuration
- VNF Secure Boot
- Configuring Console Access



第 4 章

パブリックおよびソブリン IaaS クラウドにおける Cisco Catalyst 8000V の互換性マトリックス

この章では、Cisco Catalyst 8000V ルータでサポートされているさまざまなパブリック クラウドコンピューティングインスタンスのサイズについて説明します。次のトピックでは、サポートされている各パブリッククラウドとソブリン IaaS クラウドのコンピューティング インスタンスの詳細について説明します。

AWS でサポートされるインスタンスタイプ

AMI は、さまざまなインスタンスタイプをサポートしています。インスタンスタイプによって、インスタンスのサイズと必要なメモリ容量が決まります。Cisco Catalyst 8000V では、次のインスタンスタイプがサポートされています。

リリース番号	サポートされているインスタンスタイプ
Cisco IOS XE 17.13.1a	• t3.medium • c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.18xlarge、c5n.4xlarge • c6in.8xlarge、c6in.2xlarge、c6in.xlarge、c6in.large

リリース番号	サポートされているインスタンスタイプ
Cisco IOS XE 17.12.2、 Cisco IOS XE 17.12.1	• t3.medium • c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large
Cisco IOS XE 17.11.1a	• t3.medium • c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large
Cisco IOS XE 17.10.1a	• t3.medium • c5.9xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large
Cisco IOS XE 17.9.4a Cisco IOS XE 17.9.4 Cisco IOS XE 17.9.3a Cisco IOS XE 17.9.2a Cisco IOS XE 17.9.1a	• t3.medium • c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.18xlarge、c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large
Cisco IOS XE 17.8.1a	• t3.medium • c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large
Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a	• t3.medium • c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large

リリース番号	サポートされているインスタンスタイプ
Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.6 Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	• t3.medium • c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large
Cisco IOS XE 17.5.1a	• t3.medium、t2.medium • c4.8xlarge、c4.4xlarge、c4.2xlarge、c4.xlarge、c4.large • c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large
Cisco IOS XE 17.4.2 Cisco IOS XE 17.4.1b Cisco IOS XE 17.4.1a	• t3.medium、t2.medium • c4.8xlarge、c4.4xlarge、c4.2xlarge、c4.xlarge、c4.large • c5.9xlarge、c5.4xlarge、c5.2xlarge、c5.xlarge、c5.large • c5n.9xlarge、c5n.4xlarge、c5n.2xlarge、c5n.xlarge、c5n.large

インスタンスタイプの詳細については、Amazon EC2 インスタンスタイプを参照してください。

Microsoft Azure でサポートされるインスタンスタイプ

次の 2、4、および 8 つの NIC ソリューションテンプレートは、現在、パブリッククラウドの Microsoft Azure マーケットプレイスで提供されています。

Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.13.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2 • D16_v5
Cisco IOS XE 17.12.2、 Cisco IOS XE 17.12.1	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2 • D16_v5
Cisco IOS XE 17.11.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2
Cisco IOS XE 17.10.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2
Cisco IOS XE 17.9.4a Cisco IOS XE 17.9.3a Cisco IOS XE 17.9.2a Cisco IOS XE 17.9.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2

Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.8.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2
Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2
Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.5a、 Cisco IOS XE 17.6.4a Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2a Cisco IOS XE 17.6.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2
Cisco IOS XE 17.5.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2
Cisco IOS XE 17.4.2 Cisco IOS XE 17.4.1b Cisco IOS XE 17.4.1a	• D4_v2 / DS4_v2 • D3_v2 / DS3_v2 • D2_v2 / DS2_v2 • F16s_v2 • F32s_v2

Google Cloud Platform でサポートされるインスタンスタイプ

Cisco IOS XE リリース	サポートされているインスタンスタイプ	注
Cisco IOS XE 17.13.1a	N1：n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.12.2 Cisco IOS XE 17.12.1a	N1：n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.11.1a	N1：n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.10.1a	N1：n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.9.4a Cisco IOS XE 17.9.3a Cisco IOS XE 17.9.2a Cisco IOS XE 17.9.1a	N1：n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.8.1a	N1：n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a	N1：n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	N1：n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ
Cisco IOS XE 17.5.1a	N1：n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ

Cisco IOS XE リリース	サポートされているインスタンスタイプ	注
Cisco IOS XE 17.4.2 Cisco IOS XE 17.4.1b Cisco IOS XE 17.4.1a	N1：n1-standard-1、n1-standard-2、n1-standard-4、n1-standard-8	BYOL のみ 自律モードとコントローラモードの両方をサポート

Sovereign Cloud でサポートされるインスタンスタイプ

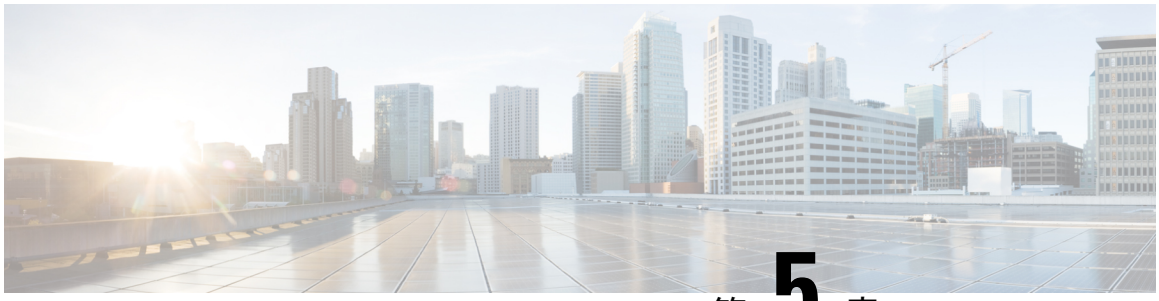
表 *2 : Alibaba Cloud*（中国）でサポートされるインスタンス

Cisco IOS XE リリース	インスタンスタイプ（BYOL のみ）
Cisco IOS XE 17.9.1a Cisco IOS XE 17.8.1a Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.6 Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	• ecs.g5.large • ecs.g5.4xlarge

表 *3 : AWS*（中国）でサポートされるインスタンス

Cisco IOS XE リリース	インスタンス タイプ
Cisco IOS XE 17.9.1a	• t3.medium • c4.large、 • c5.large、c5.xlarge、c5.2xlarge、c5.4xlarge、c5.9xlarge

Cisco IOS XE リリース	インスタンス タイプ
Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.6 Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	• t3.medium • c4.large、 • c5.large、c5.xlarge、c5.2xlarge、c5.4xlarge、c5.9xlarge



第 5 章

VMware ESXi 環境でのインストール

仮想マシンの基本的な作成と管理を可能にするハイパーバイザである VMware ESXi は、Cisco Catalyst 8000V によってサポートされるハイパーバイザの 1 つです。このハイパーバイザは、仮想化拡張機能を含む x86 ハードウェア上で動作します。同じハイパーバイザを使用して複数の VM を同時に実行できます。

Cisco IOS XE 17.12.1 リリース以降、Cisco Catalyst 8000V は、VMware ESXi 7.0.x 上の Intel x550 NIC を搭載した Intel Atom® C3000 プロセッサ（Denverton）CPU ベースのサーバーでサポートされます。異なるバージョンのハイパーバイザ オペレーティング システムを使用する他の x86 CPU で Cisco Catalyst 8000V を実行できますが、サポートは VMware ESXi 7.0.x でのみ使用できます。

この章では、ESXi での Cisco Catalyst 8000V の展開方法と、展開を成功させるための要件について説明します。要件と展開手順を読む前に、ESXi ハイパーバイザのさまざまな展開方法を示す次の情報を参照してください。

⚠

注意 ホストリソースのオーバーサブスクリプションは、パフォーマンスの低下につながり、インスタンスが不安定になる可能性があります。ホストハイパーバイザに関するガイドラインとベストプラクティスに従うことを推奨します。

VM に OVA テンプレートを展開します。

OVA ファイルを使用した展開：この方法では、ソフトウェア ダウンロード ページから .ova ファイルをダウンロードし、このファイルを展開に使用する必要があります。さらに、次の 2 つの方法を使用して OVA ファイルを展開できます。

- **vSphere クライアントを使用した展開**：この手順では、VMware vSphere クライアントまたは vSphere Web クライアントを使用して *.ova インストールファイルを展開する必要があります。VMware vSphere Web クライアントは、仮想拡張を含む x86 ハードウェア上で実行され、VMware vCenter サーバーにアクセスする Web アプリケーションです。VMware vSphere Web クライアントソフトウェアを使用して、VMware vCenter サーバー上で VM を作成、設定、管理したり、Cisco Catalyst 8000V インスタンスを起動または停止したりすることができます。

（注） Cisco Catalyst 8000V の展開にはこの方法を推奨します。

- **共通 OVF ツール（COT）を使用した展開**：COT は、Cisco Catalyst 8000V などの仮想アプライアンスを編集できるツールです。このツールを使用して、.ova ファイルを ESXi サーバーに展開し、VM をプロビジョニングすることもできます。

VMware vSphere 製品の詳細については、VMware 製品のマニュアルを参照してください。

.ISO ファイルの手動展開

ESXi ハイパーバイザの 3 番目の展開オプションは、.iso ファイルを使用した VM の手動作成と Cisco Catalyst 8000V のインストールです。シスコのソフトウェア ダウンロード ページから .iso ファイルをダウンロードし、このファイルをインストールに使用します。この方法では、VMware ESXi ホストに .iso ファイルをインストールし、vSphere GUI を使用して手動で VM を作成します。このオプションは、OVA を変更する場合にのみ使用することをお勧めします。ただし、手動展開ではサポートされている設定から逸脱する可能性があるため、このオプションは推奨されません。

重要 ESXi 6.5 以降を使用して VM を作成します。VM バージョン 13 以降を使用していることを確認します。EFI ファームウェアモードを選択するには、[VM Options] > [Boot Options] > [Firmware] > [EFI] の順に移動します。セキュアブート機能を有効にするには、このファームウェアモードを選択する必要があります。詳細については、VNF セキュアブートの有効化 （163 ページ）を参照してください。

重要 VM の作成後にファームウェアモードを（BIOS から EFI、またはその逆に）変更することはできません。

- VMware 要件 （24 ページ）
- サポートされている VMware 機能と操作 （27 ページ）
- vSphere を使用した VM への OVA の展開 （31 ページ）
- COT を使用した VM への OVA の展開 （34 ページ）
- .iso ファイルを使用した VM の手動作成 （40 ページ）
- VMware ESXi 構成でのパフォーマンスの向上 （42 ページ）

VMware 要件

次の表に、Cisco IOS XE 17.4.1 以降のリリースを使用する Cisco Catalyst 8000V でサポートされる VMware ツールを示します。これらのバージョンは完全にテスト済みで、パフォーマンスベンチマークに適合しています。

Cisco IOS XE リリース	vSphere Web Client	vCenter Server
Cisco IOS XE 17.15.1 リリース	VMware vSphere Web クライアントのバージョン 7.0 および 6.7 がサポートされています。	VMware ESXi 7.0
Cisco IOS XE 17.14.x リリース Cisco IOS XE 17.13.x リリース Cisco IOS XE 17.12.x リリース Cisco IOS XE 17.11.x リリース Cisco IOS XE 17.10.x リリース Cisco IOS XE 17.9.x リリース Cisco IOS XE 17.8.x リリース Cisco IOS XE 17.7.x リリース Cisco IOS XE 17.6.x リリース	VMware vSphere Web クライアントのバージョン 7.0 および 6.7 がサポートされています。	VMware ESXi 7.0 および ESXi 6.7
Cisco IOS XE 17.5.x リリース	VMware vSphere Web クライアントのバージョン 6.7 および 6.5 がサポートされています。	VMware ESXi 6.7 および ESXi 6.5
Cisco IOS XE 17.4.x リリース	VMware vSphere Web クライアントのバージョン 6.7 および 6.5 がサポートされています。	VMware ESXi 6.7 および ESXi 6.5

（注） ESXi サーバーの管理にスタンドアロンの vSphere クライアントを使用しないでください。ESXi 6.0 以降では、OVA を展開する場合、Cisco Catalyst 8000V を ESXi に直接展開することはできなくなりました。.ova ファイルを展開するには、vMware vCenter サーバーと vSphere クライアントが必要です。

- vCPU：次の vCPU 設定がサポートされています。
  - 1 vCPU：最低 4 GB の RAM 割り当てが必要
  - 2 vCPU：最低 4 GB の RAM 割り当てが必要
  - 4 vCPU：最低 4 GB の RAM 割り当てが必要
  - 8 vCPU：最低 4 GB の RAM 割り当てが必要
  - 16 vCPU：最低 8 GB の RAM 割り当てが必要（Cisco IOS XE 17.11.1a 以降でサポート）

（注） 必要な vCPU 設定は、インストールされているスループットライセンスとテクノロジーパッケージによって異なります。詳細については、使用中のリリースのデータシートを参照してください。

- 仮想ネットワーク インターフェイス カード（vNIC）：最大 8 つの vNIC がサポートされます。次の vNIC がサポートされています。
  - VMXNET3：Cisco IOS XE 17.4.1 以降でサポート
  - iXGBeVF：Cisco IOS XE 17.4.1 以降でサポート
  - i40eVF：Cisco IOS XE 17.4.1 から Cisco IOS XE 17.8.x でサポート
  - iavf：Cisco IOS XE 17.9.1 以降でサポート
  - ConnectX-5VF：Cisco IOS XE 17.9.1 以降でサポート
  - ixgbe：Cisco IOS XE 17.10.1 以降でサポート
- VMware vCenter：インストールツール
- VMware vSwitch：標準または分散型の vSwitch がサポートされています
- ハードドライブ：単一のハードディスクドライブのみがサポートされています。1 台の VM 上で複数のハードディスクドライブはサポートされません
- 仮想ディスク：16 GB と 8 GB 両方の仮想ディスクがサポートされています
- ESXi ハイパーバイザ：サポートされているバージョンについては、このセクションの表を参照してください
- 仮想 CPU コア：1 つの仮想 CPU コアが必要です。これには、ホストマシンの BIOS セットアップで仮想化テクノロジー（VT）が有効にされた 64 ビットプロセッサが必要です。
- 仮想ハードディスク領域：最小サイズは 8 GB です
- このインストールには、デフォルトのビデオ、SCSI コントローラセット、およびインストール済みの仮想 CD / DVD ドライブも必要です。

（注） サポートされている NIC ドライバのバージョンとファームウェアのバージョンは、ハイパーバイザパッケージに含まれているデフォルトのバージョンです。

ヒント インストールを進める前に、セキュアブート設定についてよく理解しておいてください。セキュアブートの詳細については、VNF セキュアブートの有効化（163 ページ）を参照してください。

サポートされている VMware 機能と操作

VMware では、仮想アプリケーションを管理したり、複製、移行、シャットダウン、復帰などの操作を実行したりするためのさまざまな機能と操作がサポートされています。

これらの操作の一部では、VM の実行時状態が保存され、再起動時に復元されます。ランタイム状態にトラフィック関連の状態が含まれている場合、ランタイム状態を再開または再生すると、追加のエラー、統計情報、またはメッセージがユーザーのコンソールに表示されます。設定のみに基づいて回復される保存状態の場合は、これらの機能と動作を問題なく使用できます。

「サポートされている VMware 機能と操作：ストレージオプション（vCenter Server と vSphere Client の両方）」の表に、Cisco Catalyst 8000V でサポートされる VMware の機能と操作を示します。VMware の機能と操作の詳細については、VMware のマニュアル を参照してください。

Cisco Catalyst 8000V のすべてのバージョンで次の VMware 機能および動作はサポートされていませんが、パケットのドロップ、接続の切断、およびその他のエラー統計が発生するリスクを承知の上であれば、サポート対象外のバージョンでも使用および実行できます。

- 分散リソース スケジューリング（DRS）
- 耐障害性
- 再開
- スナップショット
- 一時停止

一般的な機能（vCenter サーバー）

表 *4*：サポートされている *VMware* 機能および操作：一般機能（*vCenter Server* のみ）

サポートされているエンティティ	説明
複製	仮想マシンまたはテンプレートを複製したり、仮想マシンをテンプレートに複製したりできます。
移行	データ ストレージがまだ共有ストレージの同じ場所にある間でも、仮想マシンの状態全体および必要に応じた設定ファイルが新しいホストに移動されます。
VMotion	VM の実行中に、ある物理サーバから別の物理サーバに VM を移動できます。
テンプレート	テンプレートを仮想マシンとして複製することにより、テンプレートを使用して新しい仮想マシンを作成します。

操作（vCenter サーバーおよび vSphere Web クライアントの場合）

表 *5:* サポートされている *VMware* 機能と操作：操作（*vCenter Server* および *vSphere Client* の場合）

サポートされているエンティティ	説明
電源オン	仮想マシンの電源を投入し、ゲスト オペレーティング システムがインストールされていればゲスト オペレーティング システムをブートします。
電源オフ	電源が再度オンになるまで仮想マシンを停止します。電源オフ オプションは、「強制」電源オフを行います。これは、物理マシンの電源コードを引き抜くことに相当し、常に機能します。
シャットダウン	シャットダウン（「安全な」電源オフ）は、VMware ツールを使用してゲスト オペレーティング システムのグレースフル シャットダウンを実行します。特定の状況（VMware ツールがインストールされていない場合や、ゲスト オペレーティング システムが停止している場合など）では、正常にシャットダウンできないことがあり、電源オフ オプションを使用する必要があります。
一時停止	仮想マシンを一時停止します。
リセット/再起動	仮想マシンを停止し、再起動（リブート）します。
OVF の作成	ディレクトリ内の複数のファイルで構成される OVF パッケージは、圧縮形式で保存されたディスクファイルを含む仮想マシンの状態をキャプチャします。OVF パッケージをローカルコンピュータにエクスポートできます。
OVA の作成	OVF パッケージ/テンプレートから 1 つの OVA パッケージファイルを作成できます。そうすると、OVA の配布が容易になります。たとえば、Web サイトからダウンロードしたり、USB キーを介して移動したりすることができます。

表 *6:* サポートされている *VMware* 機能と操作：ネットワーク機能

サポートされているエンティティ	説明
カスタム MAC アドレス	vCenter Server と vSphere Client の両方から。仮想ネットワーク アダプタの MAC アドレスを手動で設定できます。
分散 VSwitch	vCenter Server からのみ。vCenter Server データセンター上の 1 台の vSphere 分散型スイッチで、データセンターのすべての関連ホストに対するネットワーク トラフィックを処理できます。
分散リソース スケジューラ	ホスト間の自動ロード バランシングを提供します。

サポートされているエンティティ	説明
NIC ロード バランシング	vCenter Server と vSphere Client の両方から。ロード バランシング ポリシーとフェールオーバー ポリシーにより、アダプタが故障した場合に、アダプタ間でネットワーク トラフィックを分散する方法と、トラフィックを再ルーティングする方法を指定できます。
NIC チーミング	vCenter Server と vSphere Client の両方から。各仮想スイッチが NIC チームを形作る 2 個のアップリンク アダプタに接続する環境をセット アップできます。これにより、NIC チームでは、メンバーの一部または全体をまたがって、物理ネットワークと仮想ネットワーク間のトラフィックの負荷を共有するか、ハードウェア障害やネットワーク障害の発生時にパッシブ フェールオーバーを提供します。 （注） NIC チーミングにより、多数の ARP パケットが Cisco Catalyst 8000V にフラッディングし、CPU が過負荷になるおそれがあります。この状況を回避するには、ARP パケットの数を減らし、アクティブ-アクティブではなく、アクティブ-スタンバイとして NIC チーミングを実装します。
vSwitch	vCenter Server と vSphere Client の両方から。vSwitch はレイヤ 2 物理スイッチの仮想化バージョンです。vSwitch では、仮想マシン間でトラフィックを内部的にルーティングでき、外部ネットワークにリンクできます。vSwitch を使用すると、複数ネットワーク アダプタの帯域幅を組み合わせ、このアダプタ間で通信トラフィックを分散できます。物理 NIC フェールオーバーを処理するように vSwitch を設定することもできます。

ハイ アベイラビリティ

（注） Cisco IOS ベースの高可用性は、Cisco Catalyst 8000V インスタンスではサポートされていません。高可用性は、VM ホストでのみサポートされます。

表 *7:* サポートされている *VMware* 機能および操作：ハイ アベイラビリティ

サポートされているエンティティ	説明
VM レベルのハイ アベイラビリティ	オペレーティング システムの障害をモニタするために、VM レベルのハイ アベイラビリティでは、VMware ハイ アベイラビリティ クラスタのハートビート情報をモニタします。ユーザ指定の間隔までに、指定した仮想マシンからハートビートが受信されていないと、障害が検出されます。VM レベルのハイ アベイラビリティは、VMware vCenter Server を使用して VM のリソース プールを作成することによって有効化されます。

サポートされているエンティティ	説明
ホストレベルのハイアベイラビリティ	物理サーバをモニタするために各サーバ上のエージェントでは、ハートビートが失われたときに、リソース プール内の他のサーバにある影響を受けるすべての仮想マシンの再起動を自動的に開始できるように、リソース プール内の他のサーバとのハートビートを維持します。ホスト レベルのハイ アベイラビリティは、サーバまたはホストのリソース プールを作成し、vSphere でハイ アベイラビリティをイネーブルにすることによってイネーブルになります。
耐障害性	ハイ アベイラビリティを使用することで、ESXi ホストの耐障害性が有効になります。Cisco Catalyst 8000V ルータを実行する VM の耐障害性を有効にすると、クラスタ内の別のホストにセカンダリ VM が作成されます。プライマリホストが停止すると、セカンダリホストの VM が Cisco Catalyst 8000V のプライマリ VM を引き継ぎます。

ストレージオプション（vCenter サーバーおよび vSphere Web クライアントの場合）

表 *8 :* サポートされている *VMware* 機能と操作：ストレージ オプション（*vCenter Server* と *vSphere Client* の両方）

サポートされているエンティティ	説明
ストレージオプション（vCenter Server および vSphere Client の両方）	
ローカル ストレージ	ローカル ストレージは ESXi ホスト内にある内部ハードディスクにあります。ローカル ストレージ デバイスは複数ホストにまたがる共有をサポートしません。ローカル ストレージ デバイス上のデータ ストアは 1 台のホストによってのみアクセスできます。
外部ストレージ ターゲット	外部ストレージに Cisco Catalyst 8000V インスタンスを展開できます。この外部ストレージとは、ストレージ エリア ネットワーク（SAN）のことです。

サポートされているエンティティ	説明
USB ストレージのマウントまたはパススルー	Cisco Catalyst 8000V に USB スティックを接続し、ストレージデバイスとして使用できます。ESXi では、USB コントローラを追加し、Cisco Catalyst 8000V にディスクデバイスを割り当てる必要があります。 • Cisco Catalyst 8000V はホットプラグをサポートしています。 • 一度に使用できる USB ディスクのホットプラグ対応デバイスは、2 台のみです。 • USB ハブはサポートされていません。

vSphere を使用した VM への OVA の展開

Cisco Catalyst 8000V OVA ファイルパッケージを使用して、Cisco Catalyst 8000V をVM に展開できます。OVA パッケージには、Cisco IOS XE リリースとサポート対象のハイパーバイザに基づいたデフォルトの VM 設定が入っている OVF ファイルが含まれています。

制限事項および要件

OVA パッケージを VM に展開する場合は、次の制限事項が適用されます。

仮想 CPU 設定を変更した場合は、Cisco Catalyst 8000V インスタンスをリブートする必要があります。RAM 割り当ての変更では、Cisco Catalyst 8000V インスタンスをリブートする必要はありません。

OVA パッケージには、仮想 CPU 設定を選択するオプションがあります。

OVA を展開する場合、VM には、OVF 環境ファイル用に 1 台と .iso ファイル用に 1 台の合計 2 台の仮想 CD/DVD ドライブが必要です。

VM への OVA の展開

VMware vSphere クライアントで次の手順を実行します。

ステップ 1 VMware vSphere Client にログインします。

ステップ 2 [vSphere Client] メニューバーから、[File] > [Deploy OVF Template] を選択します。

ステップ 3 OVA ウィザードで、展開する Cisco Catalyst 8000V OVA の送信元を指定します。[Next] をクリックします。

OVA に関する情報を示す [OVF Template Details] が表示されます。[Next] をクリックします。

ステップ 4 [Name and Inventory Location] で、VM の名前を指定し、[Next] をクリックします。

ステップ 5 [Deployment Configuration] で、ドロップダウンメニューから必要なハードウェア設定プロファイルを選択し、[Next] をクリックします。

ステップ 6 [Storage] で、VM に使用するデータストアを選択します。[Next] をクリックします。

ステップ 7 [Disk Format] で、ディスクフォーマットのオプションを選択します。

- Thick Provision Lazy Zeroed
- Thick Provision Eager Zeroed

（注） [Thin Provision] オプションはサポートされていません。[Thick Provision Eager Zeroed] オプションを指定すると、インストールに時間がかかりますが、優れたパフォーマンスを得られます。

[Next] をクリックします。

ステップ 8 [Network Mapping] で、ドロップダウン リストを使用して、宛先ネットワーク上に 1 つ以上の仮想ネットワーク インターフェイス カード（vNIC）を割り当てます。

OVA の展開時に作成された 3 つのデフォルト vNIC のネットワークマッピングを選択します。ブートストラッププロパティを設定するときに、ルータの管理インターフェイスにマッピングする vNIC を選択できます。

（注） ブートストラッププロパティを変更すると、システムはユーザーが新規の VM を開始しようとしていると判断します。そのため、VM を再起動すると、既存のネットワーキング設定がすべて削除されます。

ステップ 9 [Power On] 時に接続する vNIC を選択します。[Next] をクリックします。

OVA テンプレートを使用した Cisco Catalyst 8000V のインストールが完了すると、追加の 2 つの vNIC が割り当てられます。Cisco Catalyst 8000V は最大 10 の vNIC をサポートします。VM で追加の vNIC を手動で作成する必要があります。

ステップ 10 VM のプロパティを設定します。

（注） ブートストラッププロパティを変更すると、システムはユーザーが新規の VM を開始しようとしていると判断します。そのため、VM を再起動すると、既存のネットワーキング設定がすべて削除されます。

（注） VM 作成時のブートストラッププロパティはオプションです。これらのプロパティを設定して、起動する前の VM を簡単にプロビジョニングできます。

表 *9: OVA* ブートストラップのプロパティ

プロパティ	説明
ブートストラップのプロパティ	
コンソール	コンソールモードを設定します。 設定可能な値：virtual、serial
Login Username	ルータのログインユーザー名を設定します。

プロパティ	説明
ログイン パスワード（Login Password）	ルータのログインパスワードを設定します。
管理インターフェイス	Cisco Catalyst 8000V インスタンスの管理インターフェイスを指定します。形式は GigabitEthernetx または GigabitEthernetx.xxx である必要があります。 （注） GigabitEthernet0 インターフェイスはサポートされなくなりました。
管理 vVLAN	dot1Q VLAN インターフェイスを設定します。GigabitEthernetx.xxx 形式を使用して管理インターフェイスを設定する必要があります。
管理インターフェイス IPv4 アドレス/マスク	管理インターフェイスの IPv4 アドレスとサブネットマスクを設定します。
Management IPv4 Default Gateway	IPv4 管理デフォルト ゲートウェイ アドレスを設定します。DHCP を使用する場合は、フィールドに「dhcp」と入力します。
管理 IPv4 ゲートウェイ	IPv4 管理デフォルト ゲートウェイ アドレスを設定します。DHCP を使用する場合は、フィールドに「dhcp」と入力します。
管理 IPv4 ネットワーク	管理ゲートウェイがルーティングする IPv4 ネットワーク（「192.168.2.0/24」や「192.168.2.0 255.255.255.0」など）を設定します。デフォルトルート（0.0.0.0/0）が必要な場合は、空白のままにすることができます。
PNSC IPv4 アドレス	Cisco Prime Network Services Controller の IP アドレスを設定します。 この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V インスタンスをリモートで管理する場合に使用されます。
ルータ名	ルータのホスト名を設定します。
リソーステンプレート	リソーステンプレートを設定します。 設定可能な値：default、service_plane_medium、service_plane_heavy
機能	
SCP サーバーの有効化	IOS SCP 機能を有効にします。
SSH ログインの有効化と Telnet ログインの無効化	SSH を使用したリモートログインを有効にし、Telnet を介したリモートログインを無効にします。ログインユーザー名とパスワードを設定する必要があります。
追加の設定プロパティ	
Enable Password	特権（有効化）アクセス用のパスワードを設定します。
Domain Name	ネットワークドメイン名を設定します。

プロパティ	説明
License Boot Level	Cisco Catalyst 8000V インスタンスの起動時に使用可能なライセンス テクノロジー レベルを設定します。使用可能なライセンスレベルは次のとおりです。 • network-essentials • network-advantage • network-premier （注） Cisco DNAライセンスの詳細については、『Cisco DNA Software for SD-WAN and Routing』を参照してください。

ルータプロパティの設定を完了したら、[Next] をクリックします。テンプレートを展開するときに使用される設定を示す [Ready to Complete] 画面が表示されます。

ルータのブート後に、詳細プロパティも設定できます。

ステップ 11 VM の電源を自動的にオンにするには、[Power On After Deployment] を選択します。

ステップ 12 [Finish] をクリックして OVA を展開します。

OVA により .iso ファイルが展開され、[Power On After Deployment] 設定が選択されている場合は VM の電源が自動的にオンになります。VM の電源がオンになると、Cisco Catalyst 8000V デバイスによりインストールおよび起動プロセスが開始されます。ブートストラップ設定ファイルがOVAに含まれている場合は、ルータ設定が自動的に有効化されます。

詳細については、「Booting the Cisco Catalyst 8000V and Accessing the Console」を参照してください。

COT を使用した VM への OVA の展開

Cisco Catalyst 8000V OVA ファイルパッケージを使用して、Cisco Catalyst 8000V をVM に展開できます。OVA パッケージには、Cisco IOS XE リリースとサポート対象のハイパーバイザに基づいたデフォルトのVM設定が入っているOVFファイルが含まれています。VMware vSphere または COT または共通 OVF ツールを使用して OVA を展開できます。このセクションでは、COT を使用した展開方法について説明します。

共通 OVF ツールは、1 つ以上の VM の属性を作成し、Cisco Catalyst 8000V ソフトウェアをプレインストールして VM を迅速に展開できる、Cisco Catalyst 8000V ソフトウェアパッケージに含まれる Linux ベースのアプリケーションです。このツールを使用すると、複数の VM に Cisco Catalyst 8000V を展開するプロセスを高速化できます。

COTは、.ovaファイルにVMの属性を入力するためのシンプルなコマンドラインインターフェイスを提供します。COT は Linux シェルと Mac OS X のどちらでも実行できます。ただし、VMware OVF ツールがインストールされていることを確認してください。

危険　共通 OVF ツール（COT）は、シスコの正式なサポートなしで提供されます。自己責任で使用してください。

COT のダウンロード

http://cot.readthedocs.io/en/latest/installation.html GitHub サイトに示されている手順に従って、COT ライブラリとスクリプトをダウンロードしてインストールします。

COT を使用した Cisco Catalyst 8000V の基本的なプロパティの編集

COT を使用して Cisco Catalyst 8000V を展開する前に、COT を使用して OVA パッケージの Cisco Catalyst 8000V VM の基本プロパティまたはカスタムプロパティを編集できます。

OVA の基本プロパティを編集するには、**cot edit-properties** コマンドを使用します。

cot edit-properties

-p *key1=value1*, **--properties** *key1=value1*

このコマンドは、キーと値のペアを使用してプロパティを設定します。たとえば、**-p "login-username=cisco"** は、キーと値のペアを使用してログインユーザー名を設定します。

-o *output*

既存の OVA を更新する代わりに新しい OVA を作成する場合は、新しい OVA パッケージの名前またはパスを指定します。

cot edit-properties コマンドの詳細については、http://cot.readthedocs.io/en/latest/usage_edit_properties.html を参照してください。

COT を使用した Cisco Catalyst 8000V の基本プロパティの編集（サンプル）

```
cot edit-properties c8000v-universalk9.ova
-p "login-username=cisco"

-p "login-password=cisco"
-o c8000v-universalk9-customized.ova
\# save modifications to a new OVA
cot info c8000v-universalk9-customized.ova
  # verify the new values of properties in the OVA
(...)
Properties:
  <config-version>                                  "1.0"
  Router Name                                       ""
  Login Username                                    "cisco"
  Login Password                                    "cisco"
  Management Interface                              "GigabitEthernet1"
  Management VLAN                                   ""
  Management Interface IPv4 Address/Mask            ""
```

次の表に、上記の例で使用される **cot edit-properties** コマンドと引数を示します。

スクリプトステップ	説明
`cot edit propertie s c8000v-universalk9.ova`	OVA ファイルの基本的な環境プロパティを編集します。
`-p "login-username=cisco"`	ブートストラップ ログイン ユーザー名を設定します。
`-p "login-password=cisco"`	ブートストラップ ログイン パスワードを設定します。
`-o "c8000v-universalk9-customized.ova"`	テキストファイルからの設定コマンドを含む、変更された OVA を保存します。

カスタムプロパティの編集

vSphere GUI を使用して、Cisco IOS XE CLI コマンドに基づくカスタム属性を Cisco Catalyst 8000V インスタンスに追加できます。Cisco Catalyst 8000V インスタンスの起動前または後に、これらのプロパティを追加できます。Cisco Catalyst 8000V インスタンスの起動後にこれらのカスタム属性を設定した場合、プロパティ設定を有効にするには、ルータをリロードするか、VM の電源を再投入する必要があります。

vApp オプションを編集してカスタム Cisco Catalyst 8000V プロパティを追加するには、以下の手順を実行します。

ステップ 1 vSphere GUI で [Options] タブを選択します。

ステップ 2 [vApp Options] > [Advanced] を選択します。

ステップ 3 [Advanced Property Configuration] 画面で、[Properties] ボタンをクリックします。

ステップ 4 プロパティを追加するには、[New] をクリックします。

ステップ 5 [Edit Property Settings] 画面で、Cisco IOS XE CLI コマンドに基づく新しいカスタムプロパティを作成するための情報を入力します。

（注） カスタムプロパティを追加する前に、カスタムプロパティの基になる Cisco IOS XE コマンドが、使用中の Cisco Catalyst 8000V バージョンでサポートされていることを確認します。

a) （任意）ラベルを入力します。これはプロパティを説明する文字列です。
b) クラス ID として「com.cisco.c8000v」と入力します。
c) ID「ios-config-xxxx」をプロパティに割り当てます。「xxxx」は、カスタムプロパティを適用する順序を決定する 0001 ～ 9999 のシーケンス番号です。
d) （任意）プロファイルの説明を入力します。
e) プロパティタイプとして「string」と入力します。これは、サポートされる唯一のタイプです。
f) デフォルト値として、カスタムプロパティが基にする Cisco IOS XE CLI コマンドを入力します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Advanced Property Configuration] 画面で、[OK] をクリックします。

ステップ 8 Cisco Catalyst 8000V インスタンスを再起動します。

新規または編集されたプロパティを有効にするには、ルータを再起動する必要があります。

cot edit-properties

少数の設定コマンドを OVA に事前適用するには、**cot edit-properties** コマンドを使用します。

もっと多くのコマンドを使用するには、**cot inject-config** コマンドを使用します。

cot edit-properties コマンドの詳細については、
http://cot.readthedocs.io/en/latest/usage_edit_properties.html を参照してください。

概要と説明

cot edit-properties *ova-filename*

-o *output*

既存の OVA を更新する代わりに新しい OVA を作成する場合は、新しい OVA パッケージの名前またはパスを指定します。

-c *config-file*

OVA に追加する IOS XE コマンドを含むテキストファイルの名前を指定します。

例

この例では、以前に作成されたテキストファイル iosxe_config.txt（IOS XE config コマンドを含む）が、**cot edit-properties** コマンドを使用して OVA に追加されます。最後に、**cot info** コマンドを使用して、変更された OVA を表示します。

```
$ cat iosxe_config.txt

interface GigabitEthernet1
no shutdown
ip address 192.168.100.10 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.100.1
$ cot edit-properties c8000v-universalk9.ova \
     -o c8000v-universalk9-customized.ova \
     -c iosxe_config.txt
$ cot info c8000v-universalk9-customized.ova

...


Properties:
  <config-version>              "1.0"
  Router Name                   ""

...


  Intercloud Tunnel Interface Gateway IPv4 Address    ""
  <ios-config-0001>             "interface GigabitEthernet1"
  <ios-config-0002>             "no shutdown"
```

```
 <ios-config-0003>              "ip address 192.168.100.10 255.255.255.0"
 <ios-config-0004>            "ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.100.1"
```

次の表に、この例で使用する **cot edit properties** コマンドと引数を示します。

スクリプトステップ	説明
`cot edit properties c8000v-universalk9.ova`	OVA ファイルのカスタム環境プロパティを編集します。
`-o "c8000v-universalk9-customized.ova"`	テキストファイルからの設定コマンドを含む新しい OVA。
`-c iosxe_config.txt`	IOS XE 設定コマンドを含むテキストファイル。このファイルに含まれる各行の設定により、OVF の XML で com.cisco.productname.ios-config-xxxx などのエントリが生成されます。

cot inject-config

OVA に事前適用する設定コマンドが多数ある場合は、**cot inject-config** コマンドを使用します。たとえば、完全な実行コンフィギュレーションを追加する場合に使用します。このコマンドは、設定コマンドに（XML の代わりに）プレーンテキストを使用するため、ファイルサイズとロード時間の点で効率的です。**cot inject-config** コマンドの詳細については、http://cot.readthedocs.io/en/latest/usage_inject_config.html を参照してください。

概要と説明

cot inject-config ova-filename

-o *output*

既存の OVA を更新する代わりに新しい OVA を作成する場合は、新しい OVA パッケージの名前またはパスを指定します。

-c *config-file*

OVA に埋め込むテキストファイルの名前（iosxe_config.txt など）を指定します。

例

この例では、**cot inject-config** コマンドがテキストファイル iosxe_config.txt の Cisco IOS XE コマンドを OVA に追加します。

```
$ cat iosxe_config.txt
interface GigabitEthernet1
no shutdown
ip address 192.168.100.10 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.100.1
$ cot inject-config c8000v-universalk9.ova \

 -o c8000v-universalk9-customized.ova \
```

```
      -c iosxe_config.txt
$ cot info c8000v-universalk9-customized.ova
```

<..簡潔にするために、その他の出力が省略されています..>

```
Files and Disks:                        File Size  Capacity Device
                                        --------- --------- --------------------
  c8000v_harddisk.vmdk                 71.50 kB   8.00 GB harddisk @ SCSI 0:0
  bdeo.sh                               52.42 kB
  README-OVF.txt                         8.53 kB
  README-BDEO.txt                        6.75 kB
  cot.tgz                              116.78 kB
  c8000v-universalk9.iso               484.80 MB           cdrom @ IDE 1:0
  config.iso                           350.00 kB             cdrom @ IDE 1:1
```

次の表に、この例で使用する **cot inject-config** コマンドと引数を示します。

スクリプトステップ	説明
`cot inject-config c8000v-universalk9.ova`	OVA ファイルのカスタム環境プロパティを編集します。
`-o "c8000v-universalk9-customized.ova"`	テキストファイルからの config コマンドを含む、新規または変更された OVA の名前。
`-c iosxe_config.txt`	IOS XE 設定コマンドを含むテキストファイルの名前。

COT を使用した Cisco Catalyst 8000V VM の展開

Cisco Catalyst 8000V VM を展開するには、次の手順に示すように **cot deploy ... esxi** コマンドを使用します。以下の説明は一般的なガイダンスを示していることに注意してください。実行する必要のある正確な手順は、VMware 環境と設定の特性に応じて異なる場合があります。

cot deploy ... esxi コマンドを実行して Cisco Catalyst 8000V を展開します。スクリプトオプションについては、http://cot.readthedocs.io/en/latest/usage_deploy_esxi.html を参照してください。

（注） デフォルト値は、Cisco Catalyst 8000V のバージョンによって異なります。

例

次の表に、vCenter 環境での Cisco Catalyst 8000V VM の展開に使用する **cot deploy** コマンドとその引数の例を示します。

スクリプトステップ	説明
`cot deploy`	

スクリプトステップ	説明
`-s '10.122.197.5/UCS/host/10.122.197.38'`	vCenter サーバー 10.122.197.5、ターゲットホスト UCS/ホスト/10.122.197.38
`-u administrator -p password`	ESXi サーバーのログイン情報。指定しない場合、COT はユーザー ID を使用し、パスワードの入力を求めます。
`-n XE3.13`	新しく作成された Cisco Catalyst 8000V VM の名前。
`-c 1CPU-4GB`	OVF ハードウェア設定プロファイル。これが指定されていない場合、COT は使用可能なプロファイルのリストを表示し、プロファイルを選択するように求めます。

`-N "GigabitEthernet1=VM Network"`
`-N "GigabitEthernet2=VM Network"`
`-N "GigabitEthernet3=VM Network"`
	Cisco Catalyst 8000V OVA の各 NIC をサーバーの vSwitch にマッピングします。

`esxi`	ターゲットハイパーバイザ（現在は常に ESXi）
`~/Downloads/c8000v-universalk9.ova`	展開する OVA
`-ds=datastore38a`	ESXi 固有のパラメータ（ここでは、ディスクストレージ用に使用するデータストア）。

.iso ファイルを使用した VM の手動作成

以下の手順に従って、VMware ESXi ホストに .iso ファイルをインストールし、vSphere GUI を使用して手動で VM を作成します。この手順には、Cisco Catalyst 8000V の展開に関する一般的なガイドラインが記載されていますが、実行する必要がある正確な手順は、使用中の VMware 環境と設定の特性によって異なる可能性があります。この手順に含まれる指示は、VMware ESXi 5.0 に基づいています。

ステップ 1 Cisco Catalyst 8000V ソフトウェア インストール イメージ パッケージから C8000V_esxi.iso ファイルをダウンロードし、VM データストアにコピーします。

ステップ 2 vSphere クライアントで、[Create a New Virtual Machine] オプションを選択します。

ステップ 3 [Configuration] で、カスタム設定を作成するオプションを選択して [Next] をクリックします。

ステップ 4 [Name and Location] で、VM の名前を指定して [Next] をクリックします。

ステップ 5 [Storage] で、VM に使用するデータストアを選択します。[Next] をクリックします。

ステップ 6 [Virtual Machine Version] フィールドで、[Virtual Machine Version 15] またはそれ以降の使用可能なバージョンを選択します。[Next] をクリックします。

（注） Cisco Catalyst 8000V には、6.5 Update 2 より前のバージョンの ESXi サーバーとの互換性がありません。

ステップ 7 [Guest Operating System] で、[Linux] を選択し、ドロップダウンメニューから [Other 3.x Linux (64-bit)] 設定を選択します。[Next] をクリックします。

ステップ 8 [CPU] の下で、次の設定を選択します。

- 仮想ソケット（仮想 CPU）の数
- ソケットあたりのコア数

ソケットごとのコアの数は、選択されている仮想ソケットの数に関係なく、常に [1] に設定する必要があります。たとえば、4 vCPU 構成の Cisco Catalyst 8000V では 4 ソケット、ソケットあたり 1 コアとして設定する必要があります。

[Next] をクリックします。

ステップ 9 [Memory] で、**Cisco Catalyst 8000V** リリースでサポートされるメモリサイズを設定します。[Next] をクリックします。

ステップ 10 [Network] で、少なくとも 3 つの仮想ネットワーク インターフェイス カード（vNIC）を割り当てます。

a) 接続する vNIC の数をドロップダウンメニューから選択します。

（注） VMware ESXi インターフェイスでは、最初の VM の作成中は、vNIC を 4 個だけ作成できます。VM が作成され、Cisco Catalyst 8000V を最初に起動した後に、vNIC をさらに追加できます。

b) vNIC を追加します。

各 vNIC に異なるネットワークを選択します。

ドロップダウンメニューからアダプタタイプを選択します。使用中のリリースでサポートされているアダプタタイプについては、本ガイドの要件のセクションを参照してください。

c) すべての vNIC を選択して電源投入時に接続します。

d) [Next] をクリックします。

（注） Cisco Catalyst 8000V の実行中に、vSphere を使用して vNIC を VM に追加することができます。既存の VM に vNICS を追加する方法の詳細は、vSphere のマニュアルを参照してください。

ステップ 11 [SCSI Controller] で、[VMware Paravirtual] を選択します。[Next] をクリックします。

ステップ 12 [Select a Disk] で、[Create a New Virtual Disk] をクリックします。

ステップ 13 [Create a Disk] フィールドで、以下の項目を設定します。

a) [Capacity: Disk Size]：使用中のリリースで必要な仮想ハードディスクサイズについては、本ガイドの要件のセクションを参照してください。

b) [Disk Provisioning]：[Thick Provision Lazy Zeroed] または [Thick Provision Eager Zeroed] のいずれかを選択します。

（注） [Thin Provision] オプションはサポートされていません。[Thick Provision Eager Zeroed] オプションを指定すると、インストールにかかる時間が長くなりますが、優れたパフォーマンスが得られます。

c) [Location]：仮想マシンと同じ場所に保存します。

[Next] をクリックします。

ステップ 14 [Advanced Options] フィールドで、仮想デバイスノード用に [SCSI (0:0)] を選択します。

ステップ 15 [Ready to Complete] 画面で、完了前の [Edit the Virtual Machine] 設定をクリックします。[Continue] チェックボックスをオンにします。

ステップ 16 [Hardware] タブで、[New CD/DVD Drive] をクリックします。

a) VM の起動元の [Device Type] を選択します。

.iso ファイルから起動する [Datastore ISO file] オプションを選択します。ステップ 1 で設定したデータストア上の .iso ファイルの場所を参照します。

b) [Device Status] フィールドで、[Connect at Power On] チェックボックスをオンにします。

c) VM を起動するホスト上の [Virtual Device Node CD/DVD] ドライブを選択します。

ステップ 17 [Resources] タブで、[CPU] 設定をクリックします。

[Resource Allocation] 設定を [Unlimited] に設定します。

ステップ 18 [OK] をクリックします。

ステップ 19 [Finish] をクリックします。

Cisco Catalyst 8000V 用の VM が設定され、起動する準備が整いました。VM の電源がオンになると Cisco Catalyst 8000V が起動されます。「Booting the Cisco Catalyst 8000V VM and Accessing the Console」のセクションを参照してください。

（注） 手動でインストールした Cisco Catalyst 8000V にデイゼロを設定するには、上記のブートストラップ設定を含む ISO をポイントする 2 番目の CD/DVD ドライブを接続します。サポートされているブートストラップ ISO の内容の詳細については、デイゼロ設定 （75 ページ）を参照してください。

（注） 仮想 VGA コンソールの代わりに ESXi ホストのシリアルポートから Cisco Catalyst 8000V にアクセスして設定する場合は、VM の電源をオンにしてルータを起動する前に、この設定を使用するよう VM をプロビジョニングします。

VMware ESXi 構成でのパフォーマンスの向上

ホストと仮想マシンの設定を変更することで、ESXi 環境で実行される Cisco Catalyst 8000V のパフォーマンスを向上させることができます。

- ハイパーバイザのパフォーマンス設定を有効にします。

- サポートされている物理 NIC で SR-IOV を有効にして、vSwitch のオーバーヘッドを制限します。
- 物理 NIC と同じ NUMA ノードで動作するように VM の vCPU を設定します。
- [VM Latency Sensitivity] を [High] に設定します。

VMware バージョン 6.7 および 6.5 でのベストプラクティスの詳細については、https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/Perf_Best_Practices_vSphere65.pdf と https://www.vmware.com/techpapers/2019/vsphere-esxi-vcenter-server-67U2-performance-best-practices.html を参照してください。

ホスト設定の変更

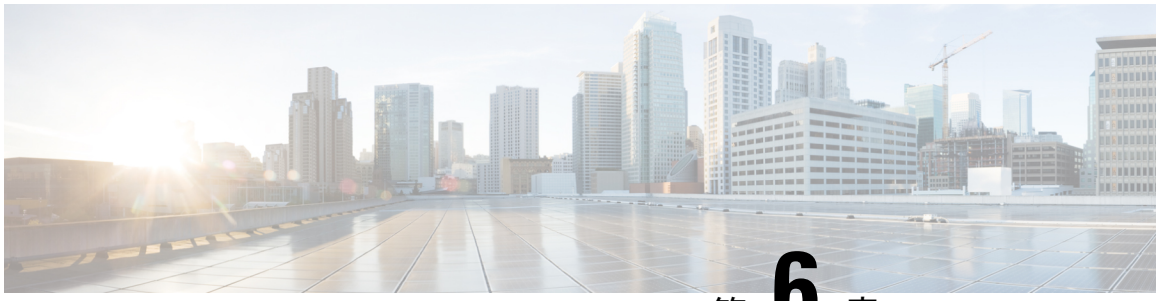
VMware ESXi 設定のパフォーマンスを向上させるには、ホスト設定で次の変更を行います。

- [Power Management] で [High Performance] オプションを選択します。
- [Hyperthreading] を無効にします。
- サポートされている物理アダプタの SR-IOV を有効にします。

仮想マシン設定の変更

VMware ESXi 設定のパフォーマンスを向上させるには、ホスト設定で次の変更を行います。

- ESXi バージョンが使用中の Cisco Catalyst 8000V バージョンと互換性があることを確認します。
- [Virtual Hardware: CPU] の予約を [Maximum] に設定します。
- [Virtual Hardware: Memory] ですべてのゲストメモリを予約します。
- [Virtual Hardware: SCSI Controller] から [VMware Paravirtual] を選択します。
- [Virtual Hardware: Network Adapter: Adapter Type] オプションから、サポートされている NIC の SR-IOV を選択します。
- [General Guest OS Version] > [VM Options] オプションを [Other 3.x or later Linux (64-bit)] に設定します。
- [Advanced Latency Sensitivity] の [VM Options] オプションを [High] に設定します。
- [VM Options] > [Advanced Edit Configuration] で、「numa.nodeAffinity」を SRIOV NIC と同じ NUMA ノードに追加します。



第 6 章

KVM 環境でのインストール

Red Hat Enterprise Linux（RHEL）は、Red Hat が製造するエンタープライズ仮想化製品です。カーネルベース仮想マシン（KVM）をベースとする RHEL は、仮想化拡張機能を搭載した x86 ハードウェア上の Linux 向けの、オープンソース完全仮想化ソリューションです。

Cisco IOS XE 17.12.1 リリース以降、Cisco Catalyst 8000V は、RHEL 8.4 KVM ハイパーバイザ上の Intel x550 NIC を搭載した Intel Atom® C3000 プロセッサ（Denverton）CPU ベースのサーバーでもサポートされます。異なるバージョンのハイパーバイザ オペレーティング システムを使用する他の x86 CPU で Cisco Catalyst 8000V を実行できますが、サポートはこれらのリストされているバージョンでのみ使用できます。

Cisco Catalyst 8000V 仮想ルータを Red Hat KVM 仮想化の仮想マシンとしてインストールできます。インストール手順では、最初に VM を手動で作成します。その後に、.iso ファイルまたは qcow2 ファイルを使用したインストールが続きます。次を使用して、KVM 環境に Cisco Catalyst 8000V をインストールできます。

- **GUI ツール**：KVM サーバーに virt-manager RPM パッケージをダウンロードしてインストールします。virt-manager は、仮想マシンを管理するためのデスクトップ ユーザー インターフェイスです。GUI を使用したインストールは、推奨されるインストール方法です。
- **コマンド ライン インターフェイス**：このインストール方法では、コマンド ライン インターフェイスを使用して Cisco Catalyst 8000V VM をインストールします。

（注） KVM 環境での OVA テンプレートの展開はサポートされていません。

Cisco Catalyst 8000V は、KVM 実装で Virtio vNIC タイプをサポートします。KVM は最大 26 の vNIC をサポートします。

KVM のインストール要件

Cisco IOS XE 17.4.x リリース以降を使用する Cisco Catalyst 8000V の KVM 要件は次のとおりです。

表 *10 : KVM* バージョン（*Red Hat Enterprise Linux* をベースとした *Linux KVM*）

Cisco IOS XE リリース	**KVM** バージョン
Cisco IOS XE 17.15.1 リリース	Red Hat Enterprise Linux 9.2 および 8.4 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.14.x リリース Cisco IOS XE 17.13.x リリース Cisco IOS XE 17.12.x リリース Cisco IOS XE 17.11.x リリース Cisco IOS XE 17.10.x リリース Cisco IOS XE 17.9.x リリース Cisco IOS XE 17.8.x リリース Cisco IOS XE 17.7.x リリース	Red Hat Enterprise Linux 7.7 および 8.4 をベースとした Linux KVM を推奨。
Cisco IOS XE 17.4.x リリース Cisco IOS XE 17.5.x リリース Cisco IOS XE 17.6.x リリース	Red Hat Enterprise Linux 7.5 および 7.7 をベースとした Linux KVM を推奨。

表 *11 : KVM* バージョン（*SUSE Linux® Enterprise Server*）

Cisco IOS XE リリース	**KVM** バージョン
Cisco IOS XE 17.14.x リリース Cisco IOS XE 17.13.x リリース Cisco IOS XE 17.12.x リリース Cisco IOS XE 17.11.x リリース Cisco IOS XE 17.10.x リリース Cisco IOS XE 17.9.x リリース Cisco IOS XE 17.6.3 リリース	SUSE Linux Enterprise Server バージョン 15 SP3 をサポート
Cisco IOS XE 17.15.1 リリース	SUSE Linux Enterprise Server バージョン 15 SP5 をサポート

表 *12* : サポートされている *VNIC*

vNIC	サポートされているリリース
Virtio	Cisco IOS XE リリース 17.4.1 以降
ixgbevf	Cisco IOS XE リリース 17.4.1 以降
i40evf	Cisco IOS XE リリース 17.4.1 から Cisco IOS XE 17.8.x リリース
iavf	Cisco IOS XE リリース 17.9.1 以降
ConnectX-5VF	Cisco IOS XE リリース 17.9.1 以降
Ixgbe	Cisco IOS XE リリース 17.10.1 以降

（注） i40evf ドライバを備えた vNIC を使用する場合、物理 VLAN の最大数は 512 に制限され、すべての（仮想機能）VF で共有されます。VF の VLAN の数は、信頼されていない VF のホスト（PF）ドライバによってさらに制限される場合があります。最新の Intel i40e PF ドライバは、信頼されていない VF を最大 8 つの VLAN/サブインターフェイスに制限します。

VM インスタンスあたりのサポートされる最大 vNIC 数：26

- vCPU。次の vCPU 設定がサポートされています。
  - 1 vCPU：最低 4 GB の RAM 割り当てが必要
  - 2 vCPU：最低 4 GB の RAM 割り当てが必要
  - 4 vCPU：最低 4 GB の RAM 割り当てが必要
  - 8 vCPU：最低 8 GB の RAM 割り当てが必要
  - 16 vCPU：最低 8 GB の RAM 割り当てが必要（Cisco IOS XE 17.11.1a 以降でサポート）
- 仮想 CPU コア：1 vCPU が必要
- 仮想ハードディスクサイズ：最低 8 GB
- 仮想 CD/DVD ドライブのインストール（.iso ファイルを使用してインストールする場合、または ISO を介してデイゼロ設定を提供する場合にのみ適用）：必須

KVM インスタンスの作成

GUI ツールを使用した VM の作成

始める前に

KVM サーバーに virt-manager RPM パッケージをダウンロードして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 .qcow2 イメージまたは .iso イメージをダウンロードし、ファイルをローカルデバイスまたはネットワークデバイスにコピーします。

ステップ 1 virt-manager GUI を起動します。

ステップ 2 [Create a New Virtual Machine] をクリックします。

ステップ 3 次のいずれかを実行します。

a) .qcow2 ファイルをダウンロードした場合は、[Import Existing Disk Image] を選択します。

b) .iso ファイルをダウンロードした場合は、[Local Install Media (ISO Image or CDROM)] を選択します。

ステップ 4 Cisco Catalyst 8000V qcow2 または iso ファイルの場所を選択します。

ステップ 5 メモリと CPU のパラメータを設定します。

ステップ 6 仮想マシンのストレージを設定します。

ステップ 7 （オプション）VM を作成する前にハードウェアを追加するには、[Customize configuration before install] を選択します。[Add Hardware] ボタンが表示されます。追加ディスクやシリアル ポート インターフェイスなど、さまざまなハードウェアオプションを追加するには、このボタンをクリックします。

ステップ 8 （オプション）シリアルコンソールを追加するには、シリアルコンソールの追加 （48 ページ）に記載されている手順に従います。

ステップ 9 （オプション）VM を作成する前に設定をカスタマイズする場合は、VM を作成する前の設定のカスタマイズ （49 ページ）を参照してください。

ステップ 10 [Finish] をクリックします。

ステップ 11 Cisco Catalyst 8000V コンソールにアクセスするには、次のいずれかのアクションを実行します。

a) 仮想コンソールを使用している場合は、VM インスタンスをダブルクリックして VM コンソールにアクセスします。

b) シリアルコンソールを使用している場合は、「Booting the Cisco Catalyst 8000V and Accessing the Console」を参照してください。

シリアルコンソールの追加

このタスクを実行し、シリアルコンソールを追加して Cisco Catalyst 8000V インスタンスへのアクセスを有効にします。

ステップ 1 [Add Hardware] をクリックします。
ステップ 2 メニューから [Serial] オプションを選択します。
ステップ 3 [Device Type] ドロップダウンメニューから、[TCP net console (tcp)] を選択します。
ステップ 4 ポート番号を指定し、[Use Telnet] チェックボックスをオンにします。
ステップ 5 [Finish] をクリックします。
ステップ 6 必要なハードウェアをすべて追加したら、[Begin Installation] をクリックします。

VM を作成する前の設定のカスタマイズ

始める前に

.qcow2 または .iso イメージを使用して GUI ツールを使用した VM の作成 （48 ページ） タスクを実行します。[Customize configuration before install] オプションをオンにしてから、[Finish] をクリックします。[Add Hardware] ボタンが表示されます。

[Customize Configuration Before Install] オプションを選択した後のオプションの手順を説明するこの手順に進みます。

ステップ 1 [Add Hardware] をクリックします。
ステップ 2 [Storage] オプションを選択します。
ステップ 3 [Select Managed Or Other Existing Storage] チェックボックスをオンにします。
ステップ 4 [Browse] をクリックし、**c8000v_config.iso** の場所に移動します。この手順は、デイゼロまたはブートストラップ設定を追加する場合にのみ適用されます。
ステップ 5 [Device-type] ドロップダウンメニューから、[IDE CDROM] を選択します。
ステップ 6 [Finish] をクリックします。
ステップ 7 必要なハードウェアをすべて追加したら、[Begin Installation] をクリックします。

ブートストラップ設定を実行するには、デイゼロ設定 （75 ページ）を参照してください。

CLI を使用した VM の作成

- KVM サーバーに virt-install RPM パッケージをダウンロードしてインストールします。
- Cisco Catalyst 8000V ソフトウェア インストール イメージ パッケージから **qcow2** イメージをダウンロードし、ローカルデバイスまたはネットワークデバイスにコピーします。

ステップ 1 .qcow2 イメージの VM を作成するには、virt-install コマンドを使用してインスタンスを作成し、起動します。次の構文を使用します。

例：

```
virt-install                    \
     --connect=qemu:///system   \
     --name=my_c8kv_vm           \
     --os-type=linux            \
     --os-variant=rhel4         \
     --arch=x86_64              \
     --cpu host                 \
     --vcpus=1,sockets=1,cores=1,threads=1   \
     --hvm                      \
     --ram=4096                 \
     --import                   \
     --disk path=<path_to_c8000v_qcow2>,bus=ide,format=qcow2   \
     --network bridge=virbr0,model=virtio                        \
     --noreboot
```

ステップ 2 .iso イメージの VM を作成するには、次の手順を実行します。

a) **qemu-img** コマンドを使用し、**.qcow2** 形式で 8 G のディスクイメージを作成します。

例：

```
qemu-img create -f qcow2 c8000v_disk.qcow2 8G
```

b) **virt-install** コマンドを使用して、Cisco Catalyst 8000V インスタンスをインストールします。これには、新しい VM を作成するための適切な権限が必要です。次の例では、4G の RAM、1 つのネットワークインターフェイス、および 1 つのシリアルポートを備えた 1 つの vCPU Cisco Catalyst 8000V を作成します。

例：

```
virt-install              \
 --connect=qemu:///system  \
 --name=my_c8000v_vm          \
 --description "Test VM"   \
 --os-type=linux           \
 --os-variant=rhel4        \
 --arch=x86_64             \
 --cpu host                \
 --vcpus=1,sockets=1,cores=1,threads=1    \
 --hvm                     \
 --ram=4096                \
 --cdrom=<path_to_c8000v_iso>          \
 --disk path=c8000v_disk.qcow2,bus=virtio,size=8,sparse=false,cache=none,format=qcow2   \
 --network bridge=virbr0,model=virtio     \
 --noreboot
```

virt-install コマンドで新しい VM インスタンスを作成し、Cisco Catalyst 8000V は指定したディスクファイルにイメージをインストールします。

インストールが完了すると、Cisco Catalyst 8000V VM はシャットダウンされます。**virsh start** コマンドを実行することで VM を起動できます。

（注） c8000v_config.iso ディスクイメージを使用してデイゼロ設定を指定する場合は、**virt-install** コマンドにパラメータを追加します。たとえば、`--disk path=/my/path/c8000v_config.iso,device=cdrom,bus=ide` です。詳細については、デイゼロ設定 （75 ページ）を参照してください。

Red Hat Enterprise Linux - ホストモードの設定

Red Hat Enterprise Linux に固有の問題により、**virt-install** を使用して Red Hat Enterprise Linux 環境で Cisco Catalyst 8000V を起動する場合は、次のようにホストモードを設定します。

- Red Hat Enterprise Linux 6 の場合は次を使用します。

```
--cpu host
```

- Red Hat Enterprise Linux 7 の場合は次を使用します。

```
--cpu host-model
```

VM のクローン作成

問題

KVM 環境では、**virt-manager** 仮想マシンマネージャを使用して Cisco Catalyst 8000V 仮想マシンの複製を作成すると、Cisco Catalyst 8000V 仮想マシンが起動できない場合があります。この問題は、**virt-manager** によって作成され複製されたイメージのサイズが、元の Cisco Catalyst 8000V VM イメージと比較して増加したことが原因で発生します。余分なバイト（KB 範囲）が原因で起動が失敗します。

回避策

次の 3 つの回避策があります。

- **virt-clone** コマンドを使用して、Cisco Catalyst 8000V VM イメージを複製します。
- ブートアップ中に **virt-manager** によって作成された複製の Cisco Catalyst 8000V VM イメージの場合は、packages.conf の代わりに起動する GOLDEN イメージを選択します。
- [Create a new virtual machine] ウィンドウで、新しい Cisco Catalyst 8000V VM を作成する前に、[Allocate Entire Disk Now] の選択を解除します。これにより、複製された Cisco Catalyst 8000V VM イメージが起動できるようになります。ただし、この回避策はネストされた複製をサポートしていません。この方法は、最初に複製された Cisco Catalyst 8000V VM イメージでのみ使用します。

KVM 構成のパフォーマンスの向上

KVM ホストの一部の設定を変更することによって、KVM 環境内で実行されている Cisco Catalyst 8000V のパフォーマンスを向上させることができます。これらの設定は、Cisco Catalyst 8000V インスタンスの IOS XE の構成時の設定とは無関係です。

KVM 設定のパフォーマンスを向上させるために、次のことを推奨します。

- vCPU のピン止めの有効化
- エミュレータのピン止めの有効化
- NUMA チューニングの有効化。すべての vCPU が同じソケットの物理コアにピン止めされていることを確認します。
- hugepage メモリバッキングの設定
- IDE ではなく virtio を使用
- SPICE ではなくグラフィック VNC を使用
- 未使用のデバイスの USB、タブレットなどの取り外し
- memballoon の無効化

（注） これらの設定は、サーバーでインスタンス化できる VM の数に影響を与える可能性があります。

調整手順は、ホストでインスタンス化する少数の VM に対して最も影響があります。

上記に加えて、次の手順を実行します。

CPU ピンニングの有効化

KVM CPU アフィニティオプションを使用して特定のプロセッサに仮想マシンを割り当てることで、KVM 環境のパフォーマンスを向上させます。このオプションを使用する場合は、KVM ホストで CPU ピンニングを構成します。

KVM ホスト環境で、次のコマンドを使用します。

- **virsh nodeinfo**：次のコマンドを使用して、ホストトポロジを確認し、ピン止めに使用できる vCPU の数を確認します。
- **virsh capabilities**：使用可能な vCPU の数を確認します。
- **virsh vcpupin** *<vmname> <vcpu#> <host core#>*：仮想 CPU をプロセッサコアのセットにピン止めします。

  この KVM コマンドは、Cisco Catalyst 8000V インスタンス上の vCPU ごとに実行する必要があります。次に、仮想 CPU 1 をホストコア 3 にピン止めする例を示します。

  virsh vcpupin c8000v 1 3

  次の例は、vCPU が 4 個の Cisco Catalyst 8000V 構成を使用し、ホストに 8 個のコアが搭載されている場合に必要になる KVM コマンドを示しています。

  virsh vcpupin c8000v 0 2

  virsh vcpupin c8000v 1 3

virsh vcpupin c8000v 2 4

virsh vcpupin c8000v 3 5

ホストのコア番号は、0 ～ 7 のどの番号でもかまいません。詳細については、KVM のドキュメンテーションを参照してください。

（注） CPU ピン止めを構成する場合は、ホストサーバーの CPU トポロジを検討してください。複数のコアがある Cisco Catalyst 8000V インスタンスを使用している場合は、複数のソケットにまたがる CPU ピン止めを設定しないでください。

BIOS 設定

次の表に示す推奨 BIOS 設定を適用して、KVM 設定のパフォーマンスを最適化します。

設定	推奨される設定
Intel Hyper-Threading Technology	無効
Number of Enable Cores	すべて
Execute Disable	有効
Intel VT	有効
Intel VT-D	有効
Intel VT-D coherency サポート	有効
Intel VT-D ATS サポート	有効
CPU パフォーマンス	高スループット
Hardware Prefetcher	無効
Adjacent Cache Line Prefetcher	無効
DCU Streamer Prefetch	無効
Power Technology	カスタム
[Enhanced Intel Speedstep Technology]	無効
[Intel Turbo Boost Technology]	有効
[Processor Power State C6]	無効
Processor Power State C1 Enhanced	無効
Frequency Poor Override	有効

設定	推奨される設定
P-State Coordination	HW_ALL
Energy Performance	パフォーマンス

Red Hat Enterprise Linux の要件については、後続のセクションを参照してください。

ホスト OS 設定

ホスト側では、hugepage を使用し、エミュレータのピン止めを有効にすることをお勧めします。次に、ホスト側の推奨設定の一部を示します。

- IOMMU=pt の有効化
- intel_iommu=on の有効化
- hugepage の有効化
- ネットワーキング パフォーマンスを向上させるためにシステムがサポートしている場合は、SR-IOV を使用。システムに存在する可能性のある SR-IOV の制限を確認してください。

hugepage とエミュレータのピン止めを有効にすることに加えて、次の設定も推奨されます。
nmi_watchdog=0 elevator=cfq transparent_hugepage=never

（注） VPP または OVS-DPDK で Virtio VHOST USER を使用する場合、QEMU のバージョンでサポートされていれば、バッファサイズを 1024 に増やすことができます（rx_queue_size='1024'）。

IO 設定

SR-IOV を使用してパフォーマンスを向上させることができます。ただし、これにより、仮想機能（VF）の数、QoS サポートなどの SR-IOV の OpenStack の制限、ライブ移行、セキュリティグループのサポートなど、いくつかの制限が発生する可能性があることに注意してください。

fd.io VPP や OVS-DPDK などの最新の vSwitch を使用する場合は、VPP ワーカースレッドまたは OVS-DPDK PMD スレッド用に少なくとも 2 つのコアを予約します。

コマンドラインから VPP を実行するには、次のパラメータを設定します。

- -cpu host：このパラメータにより、VM はホスト OS フラグを継承します。これを xml 設定に含めるには、libvirt 0.9.11 以降が必要です。
- -m 8192：最適なゼロパケットドロップ率を実現するには、8GB RAM が必要です。
- rombar=0：PXE 起動遅延を無効にするには、各デバイスオプションリストの最後に rombar=0 を設定するか、"<rom bar=off /> " をデバイスの xml 設定に追加します。

KVM パフォーマンス向上のためのサンプル XML

NUMA チューニングのサンプル XML

```
  <numatune>
    <memory mode='strict' nodeset='0'/>
  </numatune>
```

vCPU およびエミュレータのピン止めのサンプル XML

```
 <cputune>
    <vcpupin vcpu='0' cpuset='3'/>
    <emulatorpin cpuset='3'/>
  </cputune>
```

Hugepage のサンプル XML

```
 <currentMemory unit='KiB'>4194304</currentMemory>
  <memoryBacking>
    <hugepages>
      <page size='1048576' unit='KiB' nodeset='0'/>
    </hugepages>
    <nosharepages/>
  </memoryBacking>
```

IDE の代わりの virtio のサンプル XML

```
<devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/var/lib/libvirt/images/rhel7.0.qcow2'/>
      <backingStore/>
      <target dev='vda' bus='virtio'/>
      <boot order='1'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
    </disk>
```

VNC グラフィックのサンプル XML

```
<graphics type='vnc' port='5900' autoport='yes' listen='127.0.0.1' keymap='en-us'>
      <listen type='address' address='127.0.0.1'/>
    </graphics>
```

memballon を無効にするための XML

```
<memballon model='none'>
```

halt_poll_ns パラメータの設定

halt_poll_ns は、アイドル状態の KVM ゲスト仮想 CPU（vcpus）の処理方法の動作を変更できる KVM パラメータです。

KVM ゲストの仮想CPUに実行するスレッドがない場合、QEMUは従来、アイドル状態のCPUを停止します。この設定は、デフォルトで 400 ナノ秒の期間を指定します。この場合、仮想 CPU は CPU アイドル状態になる前に待機してポーリングします。

仮想 CPU が停止する前のポーリング期間中に新しい作業が到着すると、仮想 CPU はすぐに作業を実行できるようになります。新しい作業が到着したときに仮想CPUがアイドル状態であった場合は、新しい作業を開始する前に仮想 CPU をアイドル状態から戻す必要があります。アイドル状態から実行状態になるまでにかかる時間は、遅延の影響を受けやすいワークロードに悪影響を与える追加の遅延を引き起こします。

デフォルトのカーネルパラメータでは、ゲスト Cisco Catalyst 8000V ルータの CPU がホスト CPU の 100% を消費します。

halt_poll_ns は、次の 2 つの方法で設定できます。

- **Large Holt_poll_ns**：この場合、仮想 CPU をスリープ解除するイベントのビジースピンに多くの CPU が費やされ、acpi ディープスリープの発生が少なくなります。これは、より多くの電力が消費されることを意味します。ただし、ディープスリープ状態からのウェイクアップは少なく、設定されている状態によっては、キャッシュミスなどの問題が発生する可能性があります。
- **Small halt_poll_ns**：この場合、CPUをスリープ解除するイベントのビジースピンに費やされるCPU時間が少なくなり、より多くのacpiディープスリープが発生します。この場合、消費電力は少なくなりますが、ディープスリープ状態からのウェイクアップが多くなります。ウェイクアップが多いと、ディープ スリープ インスタンスが大量に発生する可能性があり、設定によっては大量のキャッシュミスが発生し、ウェイクアップ時間が長くなる可能性があります。

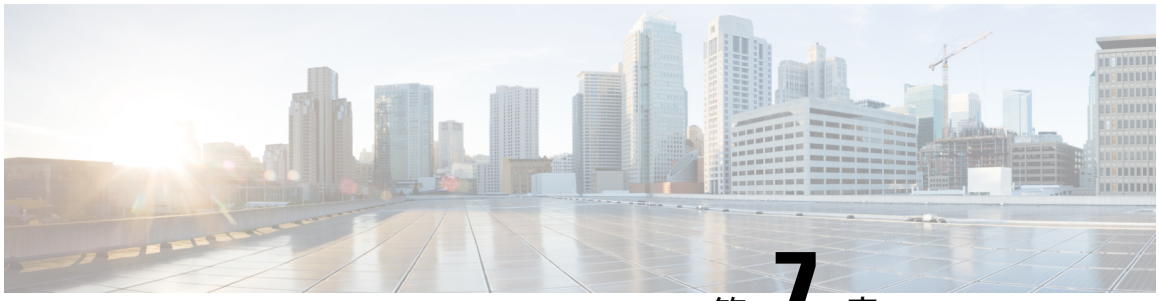
halt_poll_ns パラメータの設定

halt_poll_ns パラメータは次のように設定できます。

1. 実行時に、`echo 0 > /sys/module/kvm/parameters/halt_poll_ns` を実行します。
2. モジュールをロードする場合は、次の設定を実行します。

```
# rmmod kvm_intel
# rmmod kvm
# modprobe kvm halt_poll_ns=0
# mpdprobe kvm_intel
```

3. デバイスを起動するときに、grub2 のパラメータセクションに `kvm.halt_poll_ns=<specify value>` を追加します。



第 7 章

NFVIS 環境でのインストール

Cisco Enterprise Network Function Virtualization Infrastructure Software（Cisco Enterprise NFVIS）は、サービスプロバイダーや企業が仮想ルータ、ファイアウォール、WAN 加速化などの仮想化ネットワーク機能をサポート対象のシスコのデバイス上へ容易に動的に展開できるようにする Linux ベースのインフラストラクチャ ソフトウェアです。

Cisco Enterprise NFVIS ソリューションは、重要なネットワーク機能をソフトウェアに容易に変換できるようにし、ネットワークサービスを分散された場所に数分で展開できるようにします。このソリューションは、仮想デバイスと物理デバイスの両方から構成される多様なネットワーク上で実行できる、完全に統合されたプラットフォームを実現します。

この章では、シスコ サービス統合型仮想ルータ（ISRv）から Cisco Catalyst 8000V にアップグレードする方法について説明します。使用中のハードウェアが Cisco NFVIS で実行されているときに、この設定を Cisco Catalyst 8000V に展開する場合は、「*NFVIS* での *VM* のインストール」のセクションに記載されている手順を実行します。

（注） Cisco IOS XE 17.4.x 以降のリリースでは、ISRv は Cisco Catalyst 8000V に置き換えられます。

Cisco Catalyst 8000V の展開には NFVIS バージョン 4.4 以降が必要です。

NFVIS を実行しているサポート対象ハードウェア プラットフォーム

- 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）
- クラウド サービス プラットフォーム 5000 シリーズ（CSP）
- Cisco 8200 UCPE シリーズ

サポートされる NIM

- NIM-4G-LTE-VZ
- NIM-4G-LTE-ST
- NIM-4G-LTE-NA
- NIM-4G-LTE-GA

- NIM-4G-LTE-LA
- NIM-LTEA-EA
- NIM-LTEA-LA
- NIM-1MFT-T1/E1
- NIM-2MFT-T1/E1
- NIM-4MFT-T1/E1
- NIM-8MFT-T1/E1
- NIM-1CE1T1-PRI
- NIM-2CE1T1-PRI
- NIM-8CE1T1-PRI
- NIM-16A
- NIM-24A
- NIM-VA-B
- NIM-VAB-A
- NIM-VAB-M
- NIM-4SHDSL-EA
- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- NIM-ES2-8-P
- NIM-ES2-8 NIM-ES2-4

サポートされる NIC

ハードウェア	vNIC
ENCS	virtio、igbvf、i40evf
UCPE	virtio、igbvf、ixgbevf

ハードウェア	vNIC
CSP	• virtio、igbvf：Cisco IOS XE 17.4.1 以降でサポート • i40evf：Cisco IOS XE 17.4.1 ～ 17.8.x でサポート • ConnectX-5VF および iavf：Cisco IOS XE 17.9.1 以降でサポート • Ixgbe：Cisco IOS XE 17.10.1 以降でサポート

サポートされるプロファイル

- Mini：1vCPU
- Small：2vCPU
- Medium：4vCPU
- Large：4vCPU

（注） Cisco Catalyst 8000V は低遅延 VM として機能し、専用の vCPU コアで想定どおりに動作します。

- NFVIS での VM のインストール （59 ページ）
- NFVIS での VM のインストール（リリース 4.5.1 以降） （60 ページ）
- NFVIS での VM のインストール（リリース 4.5.0 以前） （63 ページ）
- 仮想マシンの監視 （67 ページ）
- Cisco ISRV と Cisco Catalyst 8000V の間でのアップグレードとダウングレード （67 ページ）

NFVIS での VM のインストール

Cisco IOS XE 17.4.1 リリース以降は、NFVIS に Cisco Catalyst 8000V VM を新規インストールするか、Cisco ISRv から Cisco Catalyst 8000V にアップグレードできます。インストールまたはアップグレードのために実行する必要がある主なタスクは次のとおりです。

- **VM イメージの登録**：VM イメージを登録するには、VM イメージを最初に NFVIS サーバーにコピーまたはダウンロードするか、あるいは HTTP または HTTPS サーバー上でイメージをホストする必要があります。ファイルをダウンロードしたら、登録 API を使用してイメージを登録します。この API を使用すると、tar.gz ファイルをホストする場所（HTTP または HTTPS サーバ上）へのファイル パスを指定することができます。イメージの登録

は1回限りのアクティビティです。イメージをHTTPまたはHTTPSサーバー上に登録し、登録がアクティブ状態になると、登録されたイメージを使用して複数のVM展開を実行できるようになります。

- **カスタムプロファイルの作成**：VMイメージを登録した後、必要に応じてVMイメージのカスタムプロファイルを作成できます。このプロファイルは、イメージファイルで定義されたプロファイルが要件に一致しない場合に特に役立ちます。カスタムプロファイルでは、VM が実行する仮想 CPU など、VM イメージの特定のプロファイリングの詳細や、VMが使用する仮想メモリの量を指定することができます。必要なトポロジに応じて、展開時に VM に接続する追加のネットワークやブリッジを作成できます。
- **VM の展開**：展開 API を使用して VM を展開します。この API では、導入時にシステムに渡すパラメータに値を指定できます。展開する VM に応じて、必須のパラメータとオプションのパラメータがあります。APIの詳細については、「VM Lifecycle Management APIs」を参照してください。
- **VM の管理と監視**：VM ステータスを取得したり、ログをデバッグしたりできるようにする API とコマンドを使用して VM を監視できます。VM 管理 API を使用すると、VM を起動、停止、またはリブートでき、CPU 使用率などの VM の統計情報を表示できます。VM プロファイルを変更または更新することもできます。VMプロファイルをイメージファイル内の既存のプロファイルのいずれかに変更できます。または、VM の新しいカスタムプロファイルを作成できます。VM 上の vNIC は追加または更新することもできます。

NFVIS での VM のインストール（リリース 4.5.1 以降）

NFVIS 環境での Cisco Catalyst 8000V のインストール

Cisco Catalyst 8000V を NFVIS バージョン 4.5.1 以降にインストールする場合は、このセクションの手順に従います。

NFVIS の以前のリリースに Cisco Catalyst 8000V をインストールするには、NFVIS 環境でのインストール （57 ページ）を参照してください。

NFVIS でのイメージのアップロード

ステップ 1 NFVIS ポータルにログインします。

ステップ 2 [Configuration] > [Virtual Machine] > [Images] > [Image Repository] の順に選択します。

ステップ 3 次のいずれかを実行して、インストールファイルをアップロードします。

- [Local] > [Select File] の順に選択し、デバイスからインストールファイルを見つけて選択します。
- [Remote] を選択します。

ステップ 4 [Remote] を選択した場合は、次の詳細を入力します。

a) [Image Name]：このフィールドでイメージファイルの名前を指定します。
b) [Protocol]：ドロップダウンリストからプロトコルを選択します。
c) [IP Address]：このフィールドでリモートロケーションの IP アドレスを指定します。
d) [Port]：このフィールドでリモートロケーションのポートを指定します。
e) [Image File Path]：このフィールドでイメージファイルへのファイルパスを指定します。

ネットワークの作成

ステップ 1 NFVIS ポータルで、[Configuration] > [Virtual Machine] > [Networking] > [Networks] の順に選択します。

ステップ 2 新しいネットワークを作成するには、[+] アイコンをクリックします。

ステップ 3 [Add Network] 領域で、次の詳細を入力します。

a) [Network]：このドロップダウンリストから、適切なネットワークを選択します。
b) [Mode]：VNF がブートするモードを入力します。
c) [VLAN]：VM の VLAN を選択します。
d) [VLAN-Range]：VM の VLAN の範囲を入力します。
e) [Native VLAN]：このフィールドから VM のネイティブ VLAN を選択します。
f) [Bridge]：VM の仮想ネットワーク インターフェイス コントローラ（vNIC）間のレイヤ 2 ドメインです。[Existing] または [Create New] オプションボタンを選択します。
g) [Interface]：このフィールドから VM のインターフェイスを選択します。

（注） このインストールでは Single Root Input/Output Virtualization（SR-IOV）はサポートされていません。

ステップ 4 [Submit] をクリックします。

VM パッケージの作成

ステップ 1 NFVIS ポータルで、[Configuration] > [Virtual Machine] > [Images] > [Image Package] の順に選択します。

ステップ 2 VM パッケージを作成するには、[+] アイコンをクリックします。

ステップ 3 [Image Packaging] 領域で、次の詳細を入力します。

a) [Name]：VM パッケージングに関連付けられている名前。
b) [Version]：パッケージのバージョン。
c) [VM Type]：パッケージを作成する VM のタイプ。
d) [Dedicate Cores (Optimize)]：コンテナに必要な専用コア。デフォルトでは、値は [False] です。

e) [Serial Console]：シリアルコンソールを介したアクセスを有効または無効にするフィールド。デフォルトでは、値は [Disable] です。
f) [SRIOV Driver]：VM インターフェイスでサポートされる SRIOV。
g) [Local]：バンドルするイメージが intdatastore で使用可能な場合に使用する必要があるオプション。
h) [Upload Raw Images]：ローカルマシンからパッケージ化するイメージをアップロードするオプション。
i) [Raw Disk File Bus]：このドロップダウンリストからルートディスクイメージバスを選択します。
j) [Thick Disk Provisioning]：ドロップダウンリストから [true] を選択して、シックプロビジョニングを有効にします。デフォルトでは、値は [false] です。

ステップ 4 ブートストラップファイルをアップロードするには、次のいずれかを実行します。

- [Local] を選択し、[Add Local File] オプションを選択して、ローカルで使用可能なブートストラップファイルを追加します。
- [Upload Bootstrap Files] オプションを選択して、コンピュータからブートストラップ設定ファイルを参照します。
- [Monitored] ドロップダウンフィールドから VM の追跡状態を選択します。デフォルトでは、値は [False] です。

ステップ 5 VM パッケージを生成するには、[Submit] をクリックします。

VM の展開

ステップ 1 NFVIS ポータルで、[Configuration] > [Deploy] の順に選択します。
ステップ 2 [VM Deployment] ウィンドウで、[Router] アイコンを選択します。
ステップ 3 VM をクリックします。VM の周囲に 4 つのドラッグハンドラが表示されます。これらのハンドラのいずれかから、いずれかのネットワークにドラッグし、詳細を入力します。
ステップ 4 [VM Details] エリアで、以下の詳細を入力します。

a) [VM Name]：VM の名前を指定します。
b) [Image]：ドロップダウンリストから適切な値を選択します。
c) [Profile]：ドロップダウンリストからプロファイルを選択します。デフォルトのプロファイルは、展開時にプロファイルが指定されていない場合に使用されます。
d) [Group Name]：この VM を特定のグループに関連付ける場合は、グループを選択します。
e) [VNC Password]：このフィールドに VNC パスワードを入力します。
f) [Controller]：自律モードで展開するには [non-vManage] を選択し、コントローラモードで VM を展開するには [vManage] を選択します。
g) [Tech Package]：ドロップダウンフィールドから、適切な技術パッケージを選択します。使用可能なオプションは、ネットワークエッセンシャル、ネットワークアドバンテージ、ネットワークプレミアです。

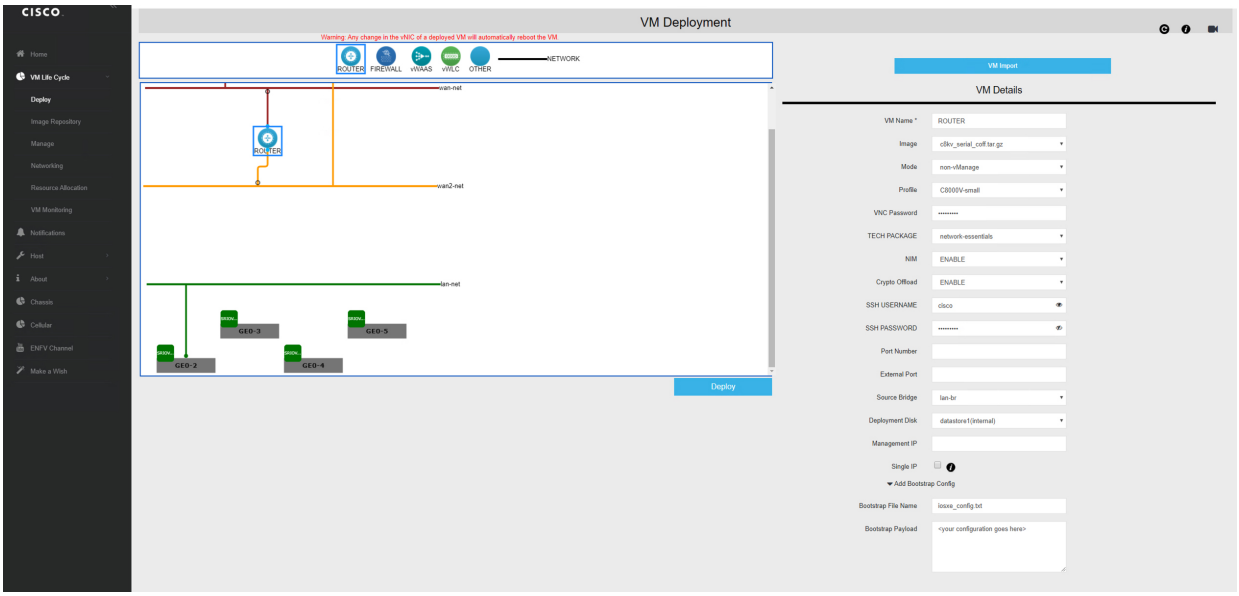
h) [NGIO]：VM で使用可能な NIM 有効化機能を決定する次世代入出力（NGIO）オプション。NGIO ドロップダウンリストから [ENABLE] を選択して NGIO を有効にします。
i) [SSH Username]：Cisco Catalyst 8000V VM にリモートでログインするためのユーザー名。
j) [SSH Password]：VM にアクセスするための SSH パスワード。
k) [Port Number]：VM への SSH 接続に必要なポート番号。
l) [External Port Number]：VM への SSH 接続に必要な外部ポート番号。

ステップ 5 [Deploy] をクリックします。

NFVIS での VM のインストール（リリース 4.5.0 以前）

NFVIS での仮想マシンの展開

ステップ 1 NFVIS ポータルから [VM Lifecycle] > [Deploy] を選択します。
ステップ 2 [VM Deployment] ウィンドウで、[Router] アイコンを下のペインにドラッグアンドドロップし、必要に応じて適切なネットワークにマッピングします。
ステップ 3 [VM Details] セクションで、[VM Name] を入力します。
ステップ 4 [Image] ドロップダウンフィールドから、適切な値を選択します。
ステップ 5 [Mode] ドロップダウンフィールドから、[non-vManage] オプションを選択します。
ステップ 6 [Profile] ドロップダウンリストから、プロファイル名を選択します。
ステップ 7 [Tech Package] ドロップダウンフィールドから、適切な技術パッケージを選択します。
ステップ 8 特定のネットワーク機能を持つ物理ハードウェアがインストールされている場合は、[NIM] ドロップダウンフィールドから [ENABLE] を選択して VM に渡すことができます。
ステップ 9 [Crypto Offload] ドロップダウンフィールドから [ENABLE] オプションを選択して、暗号化処理をハードウェアチップにオフロードします。
ステップ 10 Cisco Catalyst 8000V への SSH ログイン用のユーザー名とパスワードを入力します。
ステップ 11 必要に応じて、[VNC Password]、[Port Number]、[External Port]、[Source Bridge]、[Deployment Disk]、[Management IP] などの他の VM 詳細情報を追加します。
ステップ 12 VM を展開する前にブートストラップ設定ファイルを提供するため、[Add Bootstrap Config] オプションを選択します。ブートストラップ設定ファイルに「`iosxe_config.txt`」というファイル名が使用されていることを確認します。



（注） ギガビットイーサネット 1 インターフェイスは、NFVIS ホストとの管理通信用に予約されています。

ステップ 13 [Deploy] をクリックします。

次のタスク

VM インスタンスを展開したら、[Manage] タブでインスタンスの詳細を確認します。このタブには、VM インスタンスの概要が表示されます。

コンソールにアクセスするには、VM の横にある [Console] 記号をクリックします。次の NFVIS コマンドを使用して、VM の**シリアルコンソール**に接続することもできます。

```
vmConsole <ROUTER-NAME>
```

NFVIS 用 Cisco Catalyst 8000V イメージのダウンロード

ステップ 1 https://software.cisco.com/download/home に移動します。

ステップ 2 ページ下部の検索バーで Cisco Catalyst 8000V を検索します。

ステップ 3 リストから [Software Type] を選択します。たとえば、IOS XE ソフトウェアを選択します。

ステップ 4 ファイルのリストから、tar.gz 拡張子を持つ最新の Cisco Catalyst 8000V イメージファイルをダウンロードします。

（注） NFVIS で Cisco Catalyst 8000V イメージを展開するには、イメージをイメージプロパティファイルにパッケージ化する必要があります。

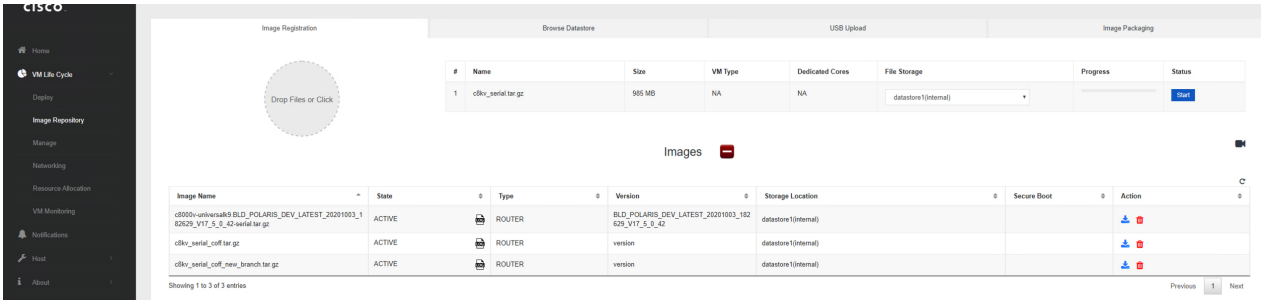
NFVIS でのイメージのアップロード

ステップ 1 NFVIS ポータルにログインします。

ステップ 2 [VM Lifecycle] > [Image Repository] を選択します。

ステップ 3 [Image Registration] タブをクリックし、[Images] オプションの横にあるアップロード矢印をクリックします。

ステップ 4 [Drop Files or Click] オプションから適切なファイルを選択します。



ステップ 5 [Start] をクリックしてイメージをアップロードします。

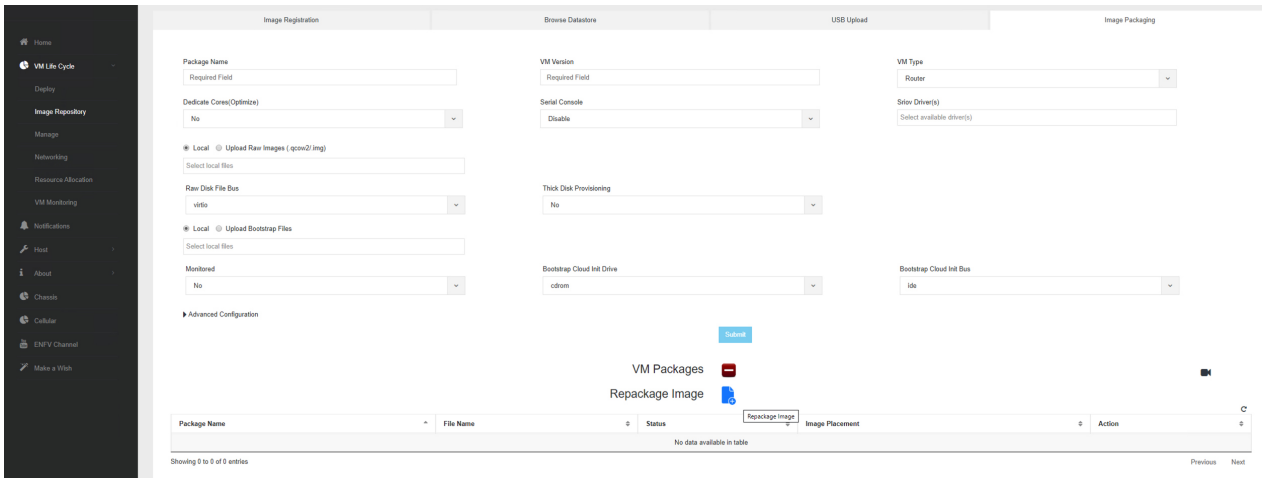
イメージをアップロードすると、NFVIS はそれぞれのプロファイルを作成し、イメージを登録します。選択したファイルは同じページの [Images] セクションに表示されています。

Web インターフェイスを使用した VM パッケージの作成

ステップ 1 NFVIS Web ポータルから、[Image Repository] > [Image Packageing] を選択します。[Create] アイコンをクリックします。

ステップ 2 [VM Packages] をクリックします。

ステップ 3 [Image Packaging] タブに詳細を入力します。[Dedicated Code] ドロップダウンリストから [Yes] を選択します。



ステップ 4 [Submit] をクリックします。ブートストラップ ファイルがアップロードされます。

イメージを作成したら、そのイメージを登録し、プロファイルが VFVIS に適切に入力されるようにする必要があります。

ステップ 5 作成したイメージを選択し、[Register] をクリックします。

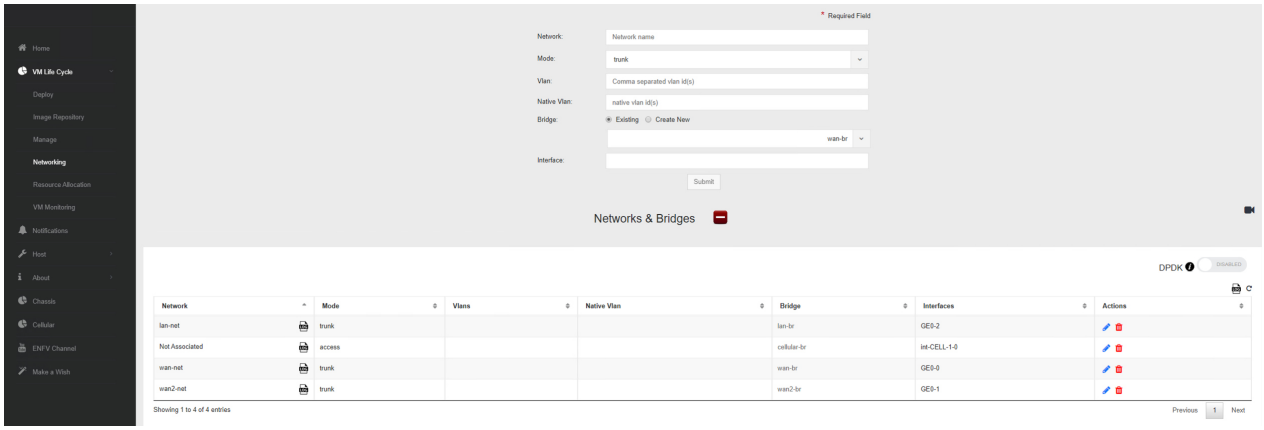
ネットワークの作成

ステップ 1 NFVIS ポータルから、[VM Lifecycle] > [Networking] を選択します。[Networks & Bridges] ページが表示されます。

ステップ 2 [Networks & Bridges] の横にある [Create] アイコンをクリックします。

ステップ 3 [Network]、[Mode]、[VLAN]、[Bridge]、および [Interface] の各フィールドに適切な値を入力します。

Single Root Input/Output Virtualization（SRIOV）はサポートされていません。



ステップ 4 [Submit] をクリックします。ネットワークが作成されました。

仮想マシンの監視

この手順では、VM を監視する手順を指定し、リソース割り当て、VM 統計情報などの動作情報を表示します。

ステップ 1 VM のリソース割り当てを表示するには、次のステップに従います。

a) NFVIS ポータルから、[VM Life Cycle] > [Resource Allocation] を選択します。全体的な CPU 割り当てが示された [VM CPU Allocation] タブが表示されます。

b) [VM Memory Allocation] をクリックして、全体的なメモリ割り当てを表示します。

c) [VM Disk Allocation] をクリックして、全体的なディスク割り当てを表示します。

ステップ 2 VM 統計情報を表示するには、次のステップを実行します。

a) NFVIS ポータルから、[VM Life Cycle] > [Resource Allocation] を選択します。

VM ごとの全体的な CPU 使用率が示された [VM CPU Utilization] タブが表示されます。

b) [Memory Allocation] をクリックして、VM ごとのメモリ使用率を表示します。

c) [VNC Utilization] タブをクリックして、VM ごとの VNIC 使用率を表示します。

d) [Disk Utilization] タブをクリックして、VM ごとのディスク使用率を表示します。

Cisco Catalyst 8000V の最初のインターフェイスは、Cisco NFVIS 管理ネットワーク（通常はギガビットイーサネット 1）用に常に予約されています。Cisco NFVIS は、このインターフェイスに IP アドレスを割り当て、インターフェイス経由で ICMP ping を使用して VM を周期的に監視します。

警告 インターフェイスをシャットダウンしたり、IP アドレスを変更したりすると、NFVIS VM のリカバリとリロードが発生する可能性があります。

Cisco ISRV と Cisco Catalyst 8000V の間でのアップグレードとダウングレード

Cisco IOS XE 17.4.x 以降のリリースでは、シスコのサービス統合型仮想ルータ（ISRV）が Cisco Catalyst 8000V に置き換えられます。ユーザーは、既存の ISRv ルータを Cisco Catalyst 8000V にアップグレードできます。Cisco Catalyst 8000V の最新リリースにアップグレードする方法については、Cisco IOS XE ソフトウェアのアップグレード （221 ページ）を参照してください。

（注）

- Cisco Catalyst 8000V から Cisco ISRV にダウングレードすることはできません。

- Cisco ISRV から Cisco Catalyst 8000V にアップグレードする場合、サポートされる Cisco ISRV の最小バージョンは 16.12.4、17.2.3、17.3.2 です。上記以外のバージョンが実行されている Cisco ISRV デバイスを使用している場合は、Cisco Catalyst 8000V にアップグレードできません。
- Cisco IOS XE 17.1.x 以前のリリースから Cisco IOS XE 17.4.x にアップグレードする場合、**install add file bootflash:c8000v-universalk9.XXX.bin activate commit** コマンドはサポートされません。Cisco ISRV を Cisco Catalyst 8000V にアップグレードするには、`c8000v-universalk9.XXX.bin` ファイルを Configuration フォルダの `bootflash:` にコピーします。次に、**write memory** コマンドを使用して設定をコピーし、アップグレードプロセスを開始します。
- Cisco IOS XE 16.12.3 以前のリリースを実行している既存の Cisco CSR1000V ユーザーが Cisco Catalyst 8000V にアップグレードする場合、Web UI を使用してアップグレードすることはできません。Cisco Catalyst 8000V にアップグレードする前に、まず Cisco CSR1000V リリース 16.12.4、17.2.3、または 17.3.2 にアップグレードする必要があります。
- すべてのライセンス情報は、Cisco Catalyst 8000V へのアップグレード後も保持されます。

サポートされているアップグレード パス

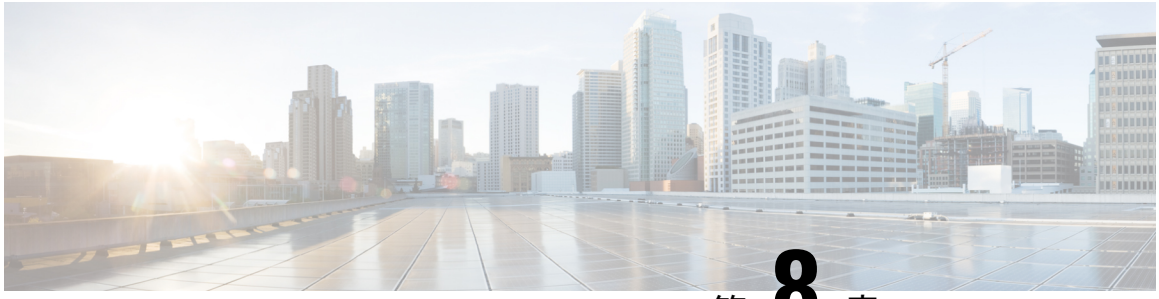
自律モード

- 16.12.x > 17.4 C8000V
- 17.2.x > 17.4 C8000V
- 17.3.x > 17.4 C8000V

コントローラモード

- 16.12.2 ISRV > 16.12.4 ISRV > 17.4 C8000V
- 16.12.3 ISRV > 16.12.4 ISRV > 17.4 C8000V
- 16.12.4 ISRV > 17.4 C8000V
- 17.1.1 ISRV > 17.3.x ISRV > 17.4 C8000V
- 17.2.1 ISRV > 17.2.2 ISRV > 17.4 C8000V
- 17.2.2 ISRV > 17.4 C8000V
- 17.3.x ISRV > 17.4 C8000V

（注） コントローラモードで Cisco ISRV を Cisco Catalyst 8000V にアップグレードする場合は、最初に Cisco IOS XE を 17.3.1 以降のリリースまたは 16.12.4 以降のリリースにアップグレードします。



第 8 章

OpenStack 環境へのインストール

Cisco IOS XE リリース 17.7.1 以降では、ハイパーバイザマネージャとして機能する OpenStack Train に Cisco Catalyst 8000V をインストールして起動できます。OpenStack Train リリースは、仮想マシン（VM）またはインスタンスを起動できるオープンソース クラウドインフラストラクチャ ソフトウェアの 20 番目のバージョンです。

このインストールでは、8 GB と 16 GB の両方のディスクがサポートされます。次のいずれかの方法を使用して、OpenStack に Cisco Catalyst 8000V VM をインストールできます。

- OpenStack ダッシュボードを使用して VM を手動で作成し、qcow2 イメージを使用してインストールする。
- Heat テンプレートを使用したインストールを実行する。OpenStack では、Heat は、OpenStack コア REST API を介してテンプレート形式を使用して複合クラウドアプリケーションをオーケストレーションするサービスです。Heat テンプレートは、クラウドアプリケーションのインフラストラクチャをテキストファイルで記述します。これらのテンプレートは、Heat が OpenStack API を呼び出すことを可能にするリソース間の関係を指定します。このアクションにより、アプリケーションを起動するための正しい順序ですべてのインフラストラクチャが作成されます。

Cisco Catalyst 8000V インスタンスをインストールして起動すると、指定したブートストラップまたはデイゼロ設定データに基づいて、ルータは自律モードまたはコントローラモードで起動します。

サポートされている機能

OpenStack の Cisco Catalyst 8000V インストールでサポートされる機能は次のとおりです。

- IPv6
- CDNA ライセンスモデル
- 自律モードでの vNIC のホット追加および削除

OpenStack のインストール要件

OpenStack に Cisco Catalyst 8000V をインストールするための要件は次のとおりです。

- OpenStack リリース：トレインリリース
- Red Hat Enterprise Linux（RHEL）8.2（Ootpa）
- RHEL OSP バージョン 16.1（トレイン）
- CVIM バージョン 4.2
- 仮想ディスク：8 GB と 16 GB 両方の仮想ディスクがサポートされています
- サポートされる最小プロファイル：4 GB のメモリと 8 GB または 16 GB の仮想ディスクを搭載した 1 vCPU

OpenStack へのインストールに関する制約事項

OpenStack heat デプロイメントによって生成されたコンソール URL には、トークンの存続可能時間（TTL）が適用され、デフォルト設定は 10 分です。使用する NoVNC URL は、特に低プロファイルのインスタンスの起動時や異なるセットアップの使用時など、特定の条件下では、このデフォルトの時間が経過すると期限切れになります。

この制限を克服するには、ポータルの組み込みインスタンス VNC コンソールを使用するか、コンピューティングノードの **virsh console** コマンドを使用してインスタンスのコンソールにアクセスします。

OpenStack への Cisco Catalyst 8000V のインストール

次のいずれかの方法で Cisco Catalyst 8000V をインストールすることができます。

- OpenStack GUI を使用します。これを行う方法については、インスタンスの起動 （71 ページ）を参照してください。
- Heat テンプレートを使用します。このインストールの実行方法については、Heat テンプレートを使用した VM のインストール （72 ページ）を参照してください。
- CLI を使用します。OpenStack CLI で **openstack server create** コマンドを実行することで VM を作成できます。詳細については、https://docs.openstack.org/python-openstackclient/train/cli/command-objects/server.html#server-create を参照してください。

インスタンスの起動

ステップ 1 OpenStack ポータルで、[Images] をクリックし、起動するイメージを選択します。

または、[Instances]、[Launch Instance] の順にクリックすることもできます。

ステップ 2 左側のペインで、[Details] をクリックし、次の詳細 を指定します。

- [Instance Name]：インスタンスの名前を入力します。
- [Description]：インスタンスの説明を入力します。このフィールドは任意です。
- [Availability Zone]：このフィールドは、クラウドの論理パーティションを指定します。このフィールドに **Nova** と入力します。
- [Count]：作成するインスタンスの数を入力します。同じ設定で複数のインスタンスを作成するには、数を増やします。

ステップ 3 [Next] をクリックします。

ステップ 4 左ペインで、[Source] をクリックします。

ステップ 5 [Select Boot Source] ドロップダウンフィールドから、[Image]、[Instance Snapshot]、[Volume]、または [Volume Snapshot] を選択します。

[Source] オプションでは、インスタンスの作成に使用するテンプレートを指定します。イメージ、インスタンスのスナップショット（イメージスナップショット）、ボリューム、またはボリュームスナップショット（有効な場合）を使用できます。新しいボリュームを作成して、永続ストレージを使用することもできます。

ステップ 6 インスタンスの削除時にボリュームを削除するには、[Delete Volume on Instance Delete] フィールドで [Yes] を選択します。

ステップ 7 左側のペインで [Flavor] をクリックします。

ステップ 8 メモリとストレージの要件に基づいてオプションを選択します。

ステップ 9 [Next] をクリックします。

ステップ 10 [Networks] オプションから、Cisco Catalyst 8000V VM とそのネットワーク内のサーバーを接続するネットワークを選択します。このオプションは、トポロジを設定する場合にも必要です。

（注） VM に接続する SRIOV ポートを選択する場合は、[Network Ports] ドロップダウンリストを使用して NIC を選択できます。

ステップ 11 [Next] をクリックします。

ステップ 12 [Security Groups] ドロップダウンリストから、インスタンスを起動するセキュリティグループを選択します。デフォルトのセキュリティグループも使用できます。

ステップ 13 [Next] をクリックします。

ステップ 14 [Configuration] セクションで、ユーザーデータをコピーして [Customization Script] フィールドに貼り付けます。次に、ユーザーデータ設定スクリプトの例を示します。

```
hostname c8kv-ios_cfg
license smart enable
username lab privilege 15 secret lab
ip domain-name cisco.com
interface GigabitEthernet1
ip address 10.0.0.5 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
line vty 0 4
login local
exit
```

ステップ 15 XML ファイルまたは iosxe_config.txt ファイルをアップロードして、ユーザーデータまたは設定データを提供することもできます。[Choose File] をクリックし、XML または .txt ファイルを参照します。

（注） デイゼロ設定の詳細については、デイゼロ設定 （75 ページ）を参照してください。

ステップ 16 [Configuration Drive] チェックボックスをオンにして、[Next] をクリックします。

ステップ 17 [Launch Instance] をクリックしてインスタンスを起動します。

（注） 自律モードからコントローラモードに切り替える場合は、ciscosdwan_cloud_init.cfg ファイルをブートフラッシュにコピーする必要があります。

Heat テンプレートを使用した VM のインストール

OpenStack の Heat テンプレートを使用すると、インスタンス、ボリューム、セキュリティグループなどの OpenStack リソースを作成できます。このテンプレートは、クラウドアプリケーションのインフラストラクチャをテキストファイルの形式で指定し、インフラストラクチャ、サービス、およびアプリケーションの展開を自動化できるようにします。

Heat テンプレートを使用して OpenStack VM をインストールするには、次の手順を実行します。

ステップ 1 OpenStack のポータルにログインします。

ステップ 2 上部のメニューオプションから、[Project] をクリックします。

ステップ 3 [Orchestration] をクリックし、[Stack] を選択します。

ステップ 4 [Stacks] ウィンドウで、[Launch Stack] をクリックします。

ステップ 5 [Template Source] ドロップダウンリストから、テンプレートの提供方法に基づいて、[File]、[URL]、または [Direct Input] を選択します。

ステップ 6 [File] オプションを選択した場合は、[Choose File] オプションをクリックし、テンプレートファイルを保存した場所を参照してこのファイルをアップロードし、[Next] をクリックします。

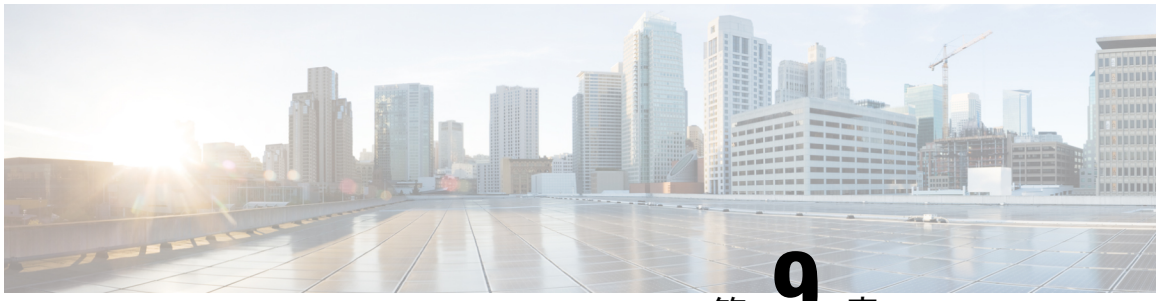
ステップ 7 [Stack Name] フィールドにスタックの名前を入力します。

ステップ 8 ロールバックを有効にするには、[Rollback on Failure] チェックボックスをオンにします。

ステップ 9 [Password for user “admin”] フィールドに、管理者のパスワードを入力します。

ステップ 10 [Launch] をクリックします。

起動が完了すると、[Stacks] ウィンドウの [Status] 列に「Create Complete」というメッセージが表示されます。



第 9 章

デイゼロ設定

Cisco Catalyst 8000V は、Cisco IOS XE と Cisco IOS XE SD-WAN の両方の機能をサポートします。自律モードでインスタンスを起動することで、Cisco IOS XE の機能にアクセスできます。同様に、Cisco SD-WAN 機能にアクセスして使用するには、インスタンスをコントローラモードで起動します。

自律モードは、Cisco Catalyst 8000V インスタンスが起動するデフォルトのモードです。自律モードでデイゼロの設定を続行する場合は、この章を参照してください。

（注） Cisco Catalyst 8000V インスタンスをコントローラモードで展開する場合は、「Install and Upgrade for Cisco Catalyst 8000V Controller Mode」を参照してください。

注目 システムが 4 つのパラメータ（OTP、UUID、VBOND、ORG）をいずれも検出できない場合、デバイスは自律モードで起動します。

ハイパーバイザとクラウド全体でのブートストラップのサポート

次の表に、自律モードでの Cisco Catalyst 8000V のハイパーバイザとクラウド全体のブートストラップサポートの概要を示します。

ハイパーバイザ	CD-ROM の iosxe_config.txt	CD-ROM の ovf-env.xml	OVA のインストール	Config-drive 形式	カスタムデータ	ユーザーデータ
VMware	対応	対応	対応	対応	非対応	非対応
KVM	対応	対応	非対応	対応	非対応	非対応
AWS	非対応	非対応	非対応	非対応	対応	対応
Azure	非対応	非対応	非対応	非対応	対応	対応
GCP	非対応	非対応	非対応	対応	対応	対応

デイゼロ設定の機能サポート

ハイパーバイザ	CD-ROM の iosxe_config.txt	CD-ROM の ovf-env.xml	OVA のインストール	Config-drive 形式	カスタムデータ	ユーザーデータ
raw 設定のコピーと貼り付け	対応	対応	非対応	対応	対応	対応
特定の設定フィールドの対応可否	非対応	対応	対応	対応	対応	対応
GUI の対応可否	非対応	非対応	対応	非対応	非対応	非対応
ゲストシェル ブートストラップ	対応（IOS の手動設定による）	対応（IOS の手動設定による）	非対応	対応（IOS の手動設定による）	対応	対応（IOS の手動設定による）

- パブリッククラウドには、VM にブートストラップ情報を提供できる入力メカニズムが 1 つあります。ただし、デバイス側では、カスタムデータ、ユーザーデータ、および SDWAN（vManage からダウンロードした ciscosdwan_cloud_init.cfg ファイルを使用）の 3 つのブートストラップ入力形式が各クラウドでサポートされます。たとえば、AWS では、EC2 ユーザー データ テキスト ボックスまたは [File Upload] オプションを使用して、起動時にインスタンスに上記のいずれかの形式でブートストラップ情報を提供できます。その後 Cisco Catalyst 8000V は、提供された設定情報を決定して処理します。
- 上記の表のカスタムデータとユーザーデータの列は、ブートストラップ入力形式を参照しており、元の名前の由来であるクラウドネイティブのブートストラップ入力メカニズムではありません。すべてのパブリッククラウドは両方の形式をサポートしていますが、カスタムデータ形式はより成熟しており、ほとんどのアプリケーションに推奨されるオプションです。
- プライベートクラウドの場合、`iosxe_config.txt` 形式または `ovf-env.xml` 形式の構成ファイルを指定することで、ブートストラップ構成を実行できます。Cisco Catalyst 8000V のインストール中に、付属の CD-ROM を使用して構成ファイルを VM にアップロードする必要があります。

- デイゼロ設定の前提条件 （77 ページ）
- デイゼロ設定の制約事項 （77 ページ）
- ブートストラップメカニズムの選択 （77 ページ）
- .txt または .xml ファイルを使用したデイゼロ設定 （78 ページ）
- OVF テンプレートのデイゼロ設定 （83 ページ）
- config-drive を使用したデイゼロ設定 （83 ページ）
- カスタムデータを使用したデイゼロ設定 （84 ページ）
- コントローラモードでのデイゼロ設定 （93 ページ）

デイゼロ設定の前提条件

• Cisco Catalyst 8000V インスタンスをコントローラモードで展開する場合は、vManage からブートストラップ設定ファイルを生成し、生成された設定ファイルの名前を ciscosdwan_cloud_init.cfg に変更します。デバイスがコントローラモードで自動的に起動し、vManage に登録されるようにするには、同じファイルを使用します。

vManage から自動生成された設定ファイルを手動で編集しないでください。これを行うと、コントローラが同期しなくなり、デバイスの最初の電源投入と起動が成功しない可能性があります。

デイゼロ設定の制約事項

• PayG ライセンスモデルを使用する場合、コントローラモードは PayG ライセンスモデルをサポートしていないため、モード切り替えを実行できません。

• 自律モードのみが Dual-IOSd をサポートします。

• ペイロード暗号化のないイメージと NO-LI イメージは、コントローラモードではサポートされていません。

• オンボーディングして動作モードを決定後、コントローラモードから自律モードに、またはその逆に切り替えると構成が失われます。

• 自律モードからコントローラモードに、またはその逆に切り替えると、Cisco Federal Licensing と Smart Licensing の登録が機能しなくなります。ライセンスを機能させるには、再登録する必要があります。

• GUI を使用して Cisco Catalyst 8000V VM を展開する場合、VM に追加されたネットワークインターフェイスの順序は、インターフェイスが作成された順序と一致しない場合があります。これは、インターフェイスの番号付け順序がドライバの名前と PCI アドレスに基づいているためです。この動作により、デイゼロ設定が一部のネットワーク インターフェイスに誤って適用される可能性があります。このシナリオが発生した場合は、VM の展開後に、影響を受けるネットワーク インターフェイスを手動で設定する必要があります。

ブートストラップメカニズムの選択

ハイパーバイザとクラウド全体でサポートされているブートストラップ方式がわかったので、次のステップは、デイゼロ設定を実行するために選択するメカニズムを決定することです。次を使用して、デバイスのデイゼロ設定を構成できます。

- **GUI ツール**：VMware に Cisco Catalyst 8000V をインストールし、OVA 展開を選択した場合は、OVA 展開ウィザードを使用して設定を実行できます。このウィザードはブートストラップ固有のフィールドをサポートしているため、ブートストラップ構成ファイルを手動で作成する必要はありません。
- **.txt ファイル/.xml ファイル**：プライベートクラウド内で、IOS 設定コマンドを使用してデイゼロ設定を行う場合は、iosxe_config.txt ファイルを選択することをお勧めします。この方法では、適用する CLI をファイルに貼り付け、CD-ROM として VM に提供できます。
- **カスタムデータ**：AWS、Microsoft Azure、または GCP に Cisco Catalyst 8000V を展開する場合は、推奨される方法はカスタムデータ形式のブートストラップ設定です。この設定方法は、ユーザーデータを使用した設定よりも機能的で柔軟性があります。ユーザーデータを使用して行うデイゼロ設定は、主に、すでに確立されたユーザーデータ展開を持つユーザーを対象としています。

これらの各メカニズムの詳細については、以下をお読みください。

.txt または .xml ファイルを使用したデイゼロ設定

新しいすぐに使用できるデバイスで、インストール中に自律モードでデバイスを起動する場合は、ブートストラップ関連の設定を指定できます。

KVM 環境などのプライベートクラウドでは、iosxe_config.txt ファイルまたは ovf-env.xml ファイルを指定してブートストラップ設定を実行できます。この方法では、CLI を介して適用する設定を収集し、ファイルに貼り付けて、このコンテンツを CD-ROM として VM に提供できます。ハイパーバイザ環境に応じて、データはブートストラップ設定に使用されます。

次の項では、このブートストラップ設定方法について詳しく説明します。

ブートストラップ ファイルの作成

この手順では、ブートストラップ構成ファイルを作成するために実行する必要がある手順について説明します。.txt または .xml 形式のこのファイルを使用すると、シンプルで柔軟な方法でデバイスのデイゼロ設定を指定できます。

この手順は、KVM などのハイパーバイザで仮想マシンを作成するときに実行できます。

ステップ 1 **iosxe_config.txt** または **ovf-env.xml** ファイルを作成します。

a) isoxe_config.txt ファイルを作成するには、IOS conf t コマンドを 1 行ずつ含むファイルをこの名前で作成します。

b) ovf-env.xml ファイルを作成するには、[Bootstrap Properties] から設定するプロパティを選択し、指定した名前のファイルに配置します。

（注） .xml ファイルの個々のプロパティの詳細については、ブートストラップのプロパティ （79ページ）を参照してください。

ステップ 2 .xml または .txt ファイルを仮想マシンで使用可能な形式に変換するには、次のコマンドを使用してファイルからディスクイメージを作成します。

例：

```
mkisofs -l -o /my/path/c8000v_config.iso <configuration_filename>
```

ステップ 3 Cisco Catalyst 8000V 仮想マシンの作成中に **c8000v_config.iso** を追加ディスクとしてマウントします。

ブートストラップのプロパティ

ovf-env.xml ファイルを作成できる個々のブートストラッププロパティについては、次の表を参照してください。

表 *13 :* ブートストラップのプロパティ

プロパティ	説明
console	コンソールモードを設定します。設定可能な値には、auto、virtual、serial などがあります。
domain-name	ルータのドメイン名。
enable-scp-server	IOS SCP 機能を有効にします。
enable-ssh-server	SSH を使用したリモートログインを有効にし、Telnet を介したリモートログインを無効にします。ログインユーザー名とパスワードを設定する必要があります。
hostname	ルータのホスト名。

ios-config	Cisco IOS コマンドの実行を有効にします。
	複数のコマンドを実行するには、複数の ios-config のインスタンスと各インスタンスに付加されている番号を使用します。たとえば、ios-config-1、ios-config-2 などです。コマンドは、付加された番号に従って番号順に実行されます。
	例
	`ios-config-1="username cisco priv 15 pass ciscoxyz"`
	`ios-config-2="ip scp server enable"`
	`ios-config-3="ip domain lookup"`
	`ios-config-4="ip domain name cisco.com”`

ライセンス	Cisco Catalyst 8000V インスタンスの起動時に使用可能なライセンス テクノロジー レベルを設定します。
login-password	ルータのログインパスワード。

プロパティ	説明
login-username	ルータのユーザー名。
mgmt-interface	Cisco Catalyst 8000V インスタンスの管理インターフェイスを指定します。形式は GigabitEthernetx または GigabitEthernetx.xxx である必要があります。
mgmt-ipv4-addr	GigabitEthernet0 管理インターフェイスの IPv4 形式の管理ゲートウェイアドレス/マスク。
mgmt-ipv4-gateway	IPv4 管理デフォルト ゲートウェイ アドレス。DHCP を使用している場合は、フィールドに **dhcp** と入力します。
mgmt-ipv4-network	管理ゲートウェイがルーティングする IPv4 ネットワーク（「192.168.2.0/24」や「192.168.2.0 255.255.255.0」など）を設定します。この値が指定されていない場合は、デフォルト ルート（0.0.0.0/0）が使用されます。
mgmt-vlan	dot1Q VLAN インターフェイスを設定します。GigabitEthernetx.xxx 形式を使用して管理インターフェイスを設定する必要があります。
pnsc-agent-local-port	（任意）サービスマネージャからポリシーを受信するように、ローカル Cisco Catalyst 8000V の Cisco Prime Network Services Controller サービス エージェント SSL ポートを設定します。 この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V をリモートで管理する場合に使用されます。
pnsc-ipv4-addr	Cisco Prime Network Services Controller の IP アドレスを設定します。 この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V インスタンスをリモートで管理する場合に使用されます。
pnsc-shared-secret-key	コントローラから SSL 証明書を設定するために、Cisco Prime Network Services Controller エージェントの Cisco Prime Network Services Controller 共有秘密キーを設定します。 この設定は、Cisco Prime Network Services Controller を使用して Cisco Catalyst 8000V インスタンスをリモートで管理する場合に使用されます。
privilege-password	特権（有効化）アクセス用のパスワードを設定します。
resource-template	リソーステンプレートを設定します。設定可能な値には、default、service_plane_medium、service_plane_heavy などがあります。

（注） **ovf-env.xml** ファイルのサンプルについては、ovf-env.xml ファイルの例 （81 ページ）を参照してください。

iosxe_config.txt ファイルの例

```
hostname ultra-ios_cfg
license smart enable
username lab privilege 15 password lab
ip domain-name cisco.com
crypto key generate rsa modulus 1024
interface GigabitEthernet1
ip address 10.0.0.5 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
line vty 0 4
 login local
exit
```

OpenStack 環境の iosxe_config.txt ファイルの例

```
hostname c8kv-ios_cfg
license smart enable
username lab priv 15 secret lab
ip domain-name cisco.com
interface GigabitEthernet1
ip address 10.0.0.5 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
line vty 0 4
login local
exit
```

ovf-env.xml ファイルの例

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
   xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
    <PropertySection>
        <Property oe:key="com.cisco.c8000v.license.1" oe:value="security"/>
        <Property oe:key="com.cisco.c8000v.console.1" oe:value="serial"/>

<Property oe:key="com.cisco.c8000v.config-version.1" oe:value="1.0"/>
        <Property oe:key="com.cisco.c8000v.domain-name.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.enable-scp-server.1" oe:value="False"/>
        <Property oe:key="com.cisco.c8000v.enable-ssh-server.1" oe:value="False"/>
        <Property oe:key="com.cisco.c8000v.hostname.1" oe:value="lab"/>
        <Property oe:key="com.cisco.c8000v.license.1" oe:value="ax"/>
        <Property oe:key="com.cisco.c8000v.login-password.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.login-username.1" oe:value="lab"/>
       <Property oe:key="com.cisco.c8000v.mgmt-interface.1" oe:value="GigabitEthernet1"/>

       <Property oe:key="com.cisco.c8000v.mgmt-ipv4-addr.1" oe:value="172.25.223.251/25"/>

       <Property oe:key="com.cisco.c8000v.mgmt-ipv4-gateway.1" oe:value="172.25.223.129"/>

        <Property oe:key="com.cisco.c8000v.mgmt-ipv4-network.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.mgmt-vlan.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.pnsc-agent-local-port.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.pnsc-ipv4-addr.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.pnsc-shared-secret-key.1" oe:value=""/>
```

```
        <Property oe:key="com.cisco.c8000v.privilege-password.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.remote-mgmt-ipv4-addr.1" oe:value=""/>
        <Property oe:key="com.cisco.c8000v.resource-template.1"
oe:value="service_plane_medium"/>
        <Property oe:key="com.cisco.c8000v.ios-config-0001" oe:value="logging buffered
10000"/>
       <Property oe:key="com.cisco.c8000v.ios-config-0002" oe:value="hostname uut-ovf"/>

        <Property oe:key="com.cisco.c8000v.ios-config-0003" oe:value="ip domain-name
cisco.com"/>
       <Property oe:key="com.cisco.c8000v.ios-config-0004" oe:value="crypto key generate
 rsa modulus 1024"/>
        <Property oe:key="com.cisco.c8000v.ios-config-0005" oe:value="interface
GigabitEthernet2"/>
       <Property oe:key="com.cisco.c8000v.ios-config-0006" oe:value="ip address 10.0.0.5
 255.255.255.0"/>
        <Property oe:key="com.cisco.c8000v.ios-config-0007" oe:value="no shut"/>
        <Property oe:key="com.cisco.c8000v.ios-config-0008" oe:value="exit"/>
        <Property oe:key="com.cisco.c8000v.ios-config-0009" oe:value="ip route 0.0.0.0
0.0.0.0 10.0.0.1"/>
    </PropertySection>
</Environment>
```

OpenStack の ovf-env.xml ファイルの例

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
   xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
    <PropertySection>
        <Property oe:key="com.cisco.c8000v.license.1" oe:value="network-premier addon
dna-premier"/>
        <Property oe:key="com.cisco.c8000v.console.1" oe:value="virtual"/>

<Property oe:key="com.cisco.c8000v.config-version.1" oe:value="1.0"/>
<Property oe:key="com.cisco.c8000v.domain-name.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.enable-scp-server.1" oe:value="False"/>
<Property oe:key="com.cisco.c8000v.enable-ssh-server.1" oe:value="False"/>
<Property oe:key="com.cisco.c8000v.hostname.1" oe:value="lab"/>
<Property oe:key="com.cisco.c8000v.login-password.1" oe:value="lab#123"/>
<Property oe:key="com.cisco.c8000v.login-username.1" oe:value="lab"/>
<Property oe:key="com.cisco.c8000v.mgmt-interface.1" oe:value="GigabitEthernet1"/>
<Property oe:key="com.cisco.c8000v.mgmt-ipv4-addr.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.mgmt-ipv4-gateway.1" oe:value="192.168.8.1"/>
<Property oe:key="com.cisco.c8000v.mgmt-ipv4-network.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.mgmt-vlan.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.pnsc-agent-local-port.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.pnsc-ipv4-addr.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.pnsc-shared-secret-key.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.privilege-password.1" oe:value="lab#123"/>
<Property oe:key="com.cisco.c8000v.remote-mgmt-ipv4-addr.1" oe:value=""/>
<Property oe:key="com.cisco.c8000v.resource-template.1" oe:value="service-plane-medium"/>
<Property oe:key="com.cisco.c8000v.ios-config-0001" oe:value="logging buffered 10000"/>
<Property oe:key="com.cisco.c8000v.ios-config-0002" oe:value="hostname uut-ovf"/>
<Property oe:key="com.cisco.c8000v.ios-config-0003" oe:value="ip domain name cisco.com"/>
<Property oe:key="com.cisco.c8000v.ios-config-0005" oe:value="interface GigabitEthernet2"/>
<Property oe:key="com.cisco.c8000v.ios-config-0006" oe:value="ip address dhcp"/>
<Property oe:key="com.cisco.c8000v.ios-config-0007" oe:value="no shut"/>
<Property oe:key="com.cisco.c8000v.ios-config-0008" oe:value="exit"/>
<Property oe:key="com.cisco.c8000v.ios-config-0009" oe:value="ip route 0.0.0.0 0.0.0.0
192.168.8.1"/>
<Property oe:key="com.cisco.c8000v.ios-config-0010" oe:value="interface GigabitEthernet1"/>
<Property oe:key="com.cisco.c8000v.ios-config-0011" oe:value="ip address dhcp"/>
<Property oe:key="com.cisco.c8000v.ios-config-0012" oe:value="no shut"/>
```

```
 </PropertySection>
</Environment>
```

OVF テンプレートのデイゼロ設定

デイゼロのブートストラップを完全にサポートする OVF 展開は、vCenter UI または COT ツールを介して VMware でのみサポートされます。ESXi ハイパーバイザで実行されている Cisco Catalyst 8000V のデイゼロ設定は、VM への OVA の展開 （31 ページ）で入手できます。

COT ツールを使用して展開のデイゼロ設定を実行する方法については、COT を使用した Cisco Catalyst 8000V の基本的なプロパティの編集 （35 ページ）を参照してください。

config-drive を使用したデイゼロ設定

Cisco Catalyst 8000V の起動時に設定がロードされるように指定するには、**--config-drive** オプションを使用します。CD-ROM および 2 番目のハードドライブには、config-drive 形式の設定情報を含めることもできます。いずれの場合も、この情報は、`iosxe_config.txt` ファイルまたは `ovf-env.xml` ファイルのいずれかの形式と一致する内容を持つファイルです。

デイゼロ設定に config drive オプションを使用するには、**--config-drive** オプションを **`true`** に設定し、起動するルータ設定を入力する構成ファイルの名前を指定します。次の方法で構成情報を指定できます。

XML/TXT ファイルとして

このオプションでは、次の 2 つの形式のいずれかで構成ファイルを指定する必要があります。

- ovf-env.xml ファイル形式の xml ファイルとして（OVF 展開の場合）
- iosxe_config.txt ファイル形式のテキストファイルとして

.txt ファイルまたは .xml ファイルのいずれか 1 つの構成ファイルタイプのみを使用し、両方は使用しないことを強く推奨します。

次の設定例を参照してください。次のいずれかの設定を使用して、ファイルシステムで構成ファイルを指定します。

```
nova boot c8000v-vm-174 --image c8000v-174 --flavor c8000v.2vcpu.4gb --nic
port-id=6773be11-7b95-48cd-b372-fb8a3cae2b50 --config-drive=true --file
ovf-env.xml=/home/stack/conf_files/ut/ovf-env.xml
```

または

```
nova boot c8000v-vm-174 --image c8000v-174 --flavor c8000v.2vcpu.4gb --nic
port-id=6773be11-7b95-48cd-b372-fb8a3cae2b50 --config-drive=true --file
iosxe_config.txt=/home/stack/conf_files/ut/iosxe_config.txt
```

（注） これらのファイル名はハードコードされており、config-drive 設定を起動するのに必要です。

ユーザーデータの使用

OpenStack などの特定の環境では、**user_data** オプションを使用して、config-drive 形式でファイルシステムにファイルを提供します。OpenStack 環境については、次のユーザーデータの例を参照してください。

```
openstack server create "admin-VK-C8KISOSerial-20210917"
--config-drive true
--image c8kv-image-176
--flavor m1.large
--network mgmt-nt
--network prod-nt
--block-device-mapping id=admin-VK-EmptyVolume-SerialTest:type=volume
--user-data userdata.txt
```

カスタムデータを使用したデイゼロ設定

Cisco Catalyst 8000V インストールファイルをダウンロードし、環境にイメージを展開した後、デバイスが完全に機能するようにするには、Cisco Catalyst 8000V インスタンスを手動で設定する必要があります。設定手順を自動化するため、またはオンプレミスサイトに接続するために、サポートされているすべてのパブリッククラウドとプライベートクラウドで Cisco Catalyst 8000V カスタムデータまたはユーザーデータをアップロードできます。

クラウド サービス プロバイダーまたはプライベートクラウドのカスタムデータをアップロードすることで、デイゼロ設定やブートストラップ設定を自動化できます。ブートストラップ構成ファイル（iosxe_config.txt ファイル）をアップロードまたはアタッチするか、ユーザーデータを提供してこれらのプロセスを自動化し、最小限の操作またはまったく操作せずにデバイスを機能状態にします。

デイゼロ ブートストラップ ファイルを使用すると、Cisco IOS XE 設定コマンドを実行したり、デイゼロのゲストシェルに Python パッケージをインストールしたり、デイゼロのゲストシェルでスクリプトを実行したり、必要なテクノロジーパッケージを使用して Cisco Catalyst 8000V インスタンスを起動するためのライセンス情報を提供したりできます。

カスタムデータを使用して Cisco Catalyst 8000V インスタンスを起動するには、次の手順を実行します。

デイゼロ ブートストラップ ファイルの編集

ブートストラップファイルを編集するには、IOS Configuration、Scripts、Script credentials、Python package、および Licensing の各プロパティを設定します。プロパティは、任意の順序でブートストラップファイルに配置できます。プロパティ間の依存関係は、次の各プロパティの説明に記載されています。https://github.com/csr1000v/customdata-examples にあるブートストラップファイルの例を参照してください。

ブートストラップファイルのプロパティを定義したら、ファイルをアップロードします。

IOS 設定プロパティの設定

デイゼロで特定の IOS 設定をブートストラップする場合は、IOS 設定プロパティを設定します。次の例を参照してください。

```
Section: IOS configuration
hostname C8000V1
interface  GigabitEthernet1
description “static IP address config”
ip address 10.0.0.1 255.255.255.0
interface GigabitEthernet2
description “DHCP based IP address config”
ip address dhcp
```

`Section: IOS configuration` という最初の行の後に、Cisco Catalyst 8000V ルータで実行する Cisco IOS XE 設定コマンドのリストを入力します。

このコマンドを実行すると、上記の IOS 設定がデイゼロの Cisco Catalyst 8000V ルータに適用されます。

スクリプトプロパティの設定

スクリプトプロパティは、展開を自動化し、他の自動化の目標を達成するのに役立ちます。ゲストシェルのコンテキストで Day0 に Python または bash スクリプトを実行する場合は、Scripts プロパティで Python または bash スクリプトのパブリック URL と引数を指定することで同じことを実現できます。

スクリプトには、スクリプトの最初の行にシバン（!）文字を含むコードを含める必要があります。この行は、スクリプトコードの解析に使用する必要があるスクリプトインタープリタ（Python または Bash）を Cisco IOS-XE に通知します。たとえば、Python スクリプトの最初の行には `#!/usr/bin/env python` を含めることができますが、bash スクリプトの最初の行には `#!/bin/bash` を含めることができます。この行により、Python または Bash スクリプトを Linux 環境で実行可能コードとして実行できます。

スクリプトを実行すると、Cisco Catalyst 8000V インスタンスのゲストシェルコンテナでスクリプトが実行されます。ゲストシェルコンテナにアクセスするには、**guestshell** EXEC モードコマンドを使用します。ゲストシェルコマンドの詳細については、『Programmability Configuration Guide』を参照してください。

Scripts プロパティを設定するには、次の形式に従います。

```
Section: scripts
public_url <arg1> <arg2>
```

このスクリプトでは、プロパティの最初の行に `Section: Scripts` と記載する必要があります。

プロパティの 2 行目に、スクリプトの URL とスクリプトの引数を入力します。スクリプトは、python または bash スクリプトのいずれかです。Cisco Catalyst 8000V インスタンスの作成時にブートストラップファイルがアップロードされると、最初の起動時にゲストシェルでスクリプトが実行されます。

スクリプトのその他の例については、https://github.com/csr1000v/customdata-examples の「Scripts」セクションを参照してください。また、次の 2 つの例も参照してください。

例 1

```
Section: Script
https://raw.githubusercontent.com/csr1000v/customdata-
examples/master/scripts/smartLicensingConfigurator.py --idtoken "<token_string>"
--throughput <throughput_value>
```

Scripts プロパティの 2 行は、指定された URL の `customdata-examples` リポジトリから `smartLicensingConfigurator.py` スクリプトを取得します。スクリプトは、引数 `idtoken` と `throughput` を使用して、Cisco Catalyst 8000V のゲストシェルコンテナで実行されます。

例 2

```
Section: Scripts
ftp://10.11.0.4/dir1/dir2/script.py -a arg1 -s arg2
```

Scripts プロパティのこれらの 2 行は、IP アドレス 10.11.0.4 の FTP サーバーから `script.py` スクリプトを取得し、引数 arg1 と arg2 を使用して Cisco Catalyst 8000V の ゲストシェルコンテナで `./script.py -a arg1 -s arg2` bash コマンドでスクリプトを実行します。

（注） Scripts プロパティのスクリプトで、標準の CentOS Linux リリース（ゲストシェルで使用される CentOS Linux リリース。現在は CentOS Linux リリース 7.1.1503）に含まれていない Python パッケージが必要な場合は、Python パッケージプロパティの Python パッケージに関する情報を含める必要があります。詳細については、Python パッケージプロパティの設定 （87 ページ）を参照してください。

ブートストラップファイルをアップロードして bash または Python スクリプトを実行する前に、Scripts プロパティで使用する予定の URL をテストすることをお勧めします。`ftp://10.11.0.4/dir1/dir2/script.py -a arg1 -s arg2` URL をテストするには、最初に curl ソフトウェアツールを実行してスクリプトファイルをダウンロードします。ゲストシェルで、次の例に示すように、curl コマンドを入力します。

```
curl -m 30 --retry 5 --user username:password
ftp://10.11.0.4/dir1/dir2/script_needs_credentials.py.
```

curl コマンドが成功すると、URL が正しいかどうかを確認する Python スクリプトのコピーがダウンロードされます。

スクリプトログイン情報プロパティの設定

Script プロパティで FTP サーバーを指定していて、そのサーバーにユーザー名とパスワードのログイン情報が必要な場合は、Script credentials プロパティを使用してログイン情報を指定します。FTP サーバーに匿名でアクセスできる場合は、Script credentials プロパティを使用する必要はありません。

Script credentials プロパティの URL とパラメータと一致する URL とパラメータを使用して、Scripts プロパティを設定します。Script credentials プロパティを設定するには、次の形式に従います。

```
Section: Script credentials
public_url <username> <password>
```

例 1

```
Section: Script credentials

ftp://10.11.0.4/dir1/dir2/script1.py userfoo foospass
```

Script credentials プロパティの 2 行目は、Python スクリプト `script1.py` のユーザー名（`userfoo`）とパスワード（`foospass`）のログイン情報の値を指定します。

Scripts プロパティにも含まれている FTP サーバーの名前を含めます。Scripts プロパティの行の例は、`ftp://10.11.0.4/dir1/dir2/script1.py -a arg1 -s arg2` です。スクリプトプロパティの設定 （85 ページ）の例 2 を参照してください。

Python パッケージプロパティの設定

Python パッケージが Scripts プロパティのスクリプトに必要であり、標準の CentOS Linux リリース 7.1.1503 の一部ではない場合は、Python パッケージプロパティにパッケージに関する情報を含める必要があります。ブートストラップファイルに Python パッケージプロパティを含めることで、Scripts プロパティで指定したスクリプトを実行する前に、Cisco Catalyst 8000V が必要な Python パッケージをダウンロードしてインストールするようにします。

（注） Cisco Catalyst 8000V はゲストシェルで Python 3 のみサポートします。

Python パッケージプロパティを設定するには、次で指定される形式に従います。

```
Section: Python package
package_name [ version ] [ sudo ] { [ pip_arg1 [ ..[ pip_arg9] ] ] }
```

引数：*version*、**sudo**、および *pip_arg1* ～ *pip_arg9* はオプションです。pip コマンドの引数は、「{」と「}」のかっこの間に配置する必要があります。

version 引数を指定すると、特定のバージョン番号がダウンロードされます。

sudo 引数を指定すると、パッケージは sudo ユーザーとしてダウンロードされます。

設定例（Microsoft Azure）

例 1

この例では、Python パッケージプロパティの 2 行目は、*package_name* が ncclient で、*version* が「0.5.2」であることを指定しています。ブートストラップファイルがアップロードされると、ncclient パッケージのバージョン 0.5.2 が Cisco Catalyst 8000V のゲストシェルコンテナにインストールされます。

```
Section: Python package

ncclient 0.5.2
```

例 2

```
Section: Python package

c8000v_azure_guestshell 1.1.2 sudo {--user}
```

この例では、Python パッケージプロパティの 2 行目で、*package_name* が「c8000v_azure_guestshell」、*version* が「1.1.2」と指定されています。ブートストラップファイルがアップロードされると、c8000v_azure_guestshell パッケージのバージョン 1.1.2 が Cisco Catalyst 8000V のゲストシェルコンテナにインストールされます。次のコマンドが sudo ユーザーとして実行されます。`sudo pip install c8000v_azure_guestshell==1.1.2 --user`。

（注） 引数を指定しない場合、--user がデフォルトの引数として使用されます。

設定例（Google Cloud Platform）

例 1

```
Section: Python package

ncclient 0.5.2
```

この例では、Python パッケージプロパティの 2 行目は、*package_name* が「ncclient」で、*version* が「0.5.2」であることを指定しています。ブートストラップファイルがアップロードされると、ncclient パッケージのバージョン 0.5.2 が Cisco Catalyst 8000V インスタンスのゲストシェルコンテナにインストールされます。

例 2

```
Section: Python package

c8000v_gcp_ha 3.0.0 sudo {--user}
```

この例では、Python パッケージプロパティの 2 行目は、*package_name* が「c8000v_gcp_ha」で、*version* が「3.0.0」であることを指定しています。ブートストラップファイルがアップロードされると、c8000v_gcp_ha package パッケージのバージョン 3.0.0 が Cisco Catalyst 8000V インスタンスのゲストシェルコンテナにインストールされます。次のコマンドが sudo ユーザーとして実行されます。`pip3 install c8000v_gcp_ha=3.0.0 --user`。

（注） 引数を指定しない場合、--user がデフォルトの引数として使用されます。

ライセンスプロパティの設定

Cisco Catalyst 8000V のライセンス テクノロジー レベルを指定するライセンスプロパティを設定します。

次のようにプロパティの最初の行を入力します。`Section: License`。次の形式を使用して、ライセンスの技術レベルを指定するプロパティの 2 行目を入力します。**TechPackage:***tech_level*。

（注） TechPackage: と tech_level の間にはスペースを入れないでください。設定可能な tech_level 値には、ax、security、appx、ipbase などがあります。

tech_level は小文字にする必要があります。

例 1

```
Section: License

TechPackage:security
```

デイゼロ ブートストラップ ファイルの提供

次の Azure CLI コマンドを実行して、Cisco Catalyst 8000V VM を作成するデイゼロ ブートストラップ ファイルを指定します。

```
az vm create --name C8000V-name --resource-group resource-group { [ arg1 [ ..[ arg9] ] ] } --custom-data bootstrap-file
```

az vm create コマンドの詳細については、https://docs.microsoft.com/en-us/cli/azure/vm?view=azure-cli-latest#az-vm-create を参照してください。

次の例を参照してください。

```
az vm create -n c8000V-VM-Name -g MyResourceGroup --image cisco:cisco-c8000v-1000v:16_6:16.6.120170804 --data-disk-sizes-gb 8 --availability-set myAvlSet --nics nic1 nic2 nic3 nic4 --admin-username azureuser --admin-password "+Cisco123456" --authentication-type password -l westus --size Standard_DS4_v2 --custom-data bootstrap.txt..
```

このコマンドを実行すると、Cisco Catalyst 8000V VM が作成されます。ルータは、ブートストラップファイル「bootstrap.txt」のコマンドを使用して設定されます。

カスタム データ ブートストラップ設定ファイルを指定するには、**Cisco C8000V Settings** オプションを使用します。

Linux VM の管理の詳細については、「Tutorial: Create and Manage Linux VMs with the Azure CLI 2.0」を参照してください。

カスタムデータ設定の確認（Microsoft Azure）

デイゼロ ブートストラップ ファイルをアップロードすると、VM が作成され、設定コマンドが実行されます。次のコマンドを実行して、各プロパティの設定コマンドを確認します。

ライセンスプロパティが機能しているかどうかを確認するには、Cisco Catalyst 8000V の Cisco IOS XE CLI で **show version** コマンドを入力します。たとえば、セキュリティライセンスへの参照が表示されます。

スクリプトプロパティでコマンドを実行した後にエラーが発生したかどうかを確認するには、`/home/guestshell/customdata` ディレクトリの customdata.log ファイルを調べます。*scriptname*.log ファイルには、スクリプトによって STDOUT に送信される出力が保存されます。

Python プロパティが機能したかどうかを確認するには、**pip freeze | grep***package-name* コマンドを入力して、現在インストールされている Python パッケージを表示します。目的のパッケージ *package-name* を検索します。

IOS の設定プロパティで Cisco IOS XE コマンドが成功したかどうかを確認するには、**show running-configuration** コマンドを入力します。次に、このコマンドの出力例を示します。

```
Router#show version
Cisco IOS XE Software, Version
Copyright (c) 1986-2020 by Cisco Systems, Inc.

Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 1 minute
Uptime for this control processor is 7 minutes
System returned to ROM by reload
System image file is "bootflash:packages.conf"
Last reload reason: Unknown reason



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: ipbase
License Type: N/A(Smart License Enabled)
Next reload license Level: ipbase

The current throughput level is 250000 kbps


Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C8000V (VXE) processor (revision VXE) with 2271486K/3075K bytes of memory.
Processor board ID 9MUG8CATY8R
Router operating mode: Controller-Managed
1 Gigabit Ethernet interface
32768K bytes of non-volatile configuration memory.
8106756K bytes of physical memory.
11530240K bytes of virtual hard disk at bootflash:.

Configuration register is 0x2102

[guestshell@guestshell ~]$ pip3 freeze | grep  gpg==1.10.0
```

```
gpg==1.10.0
[guestshell@guestshell ~]$
```

```
Router#show running-config
Building configuration...

Current configuration : 6982 bytes
!
! Last configuration change at 14:34:36 UTC Fri Nov 6 2020 by NETCONF
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! Call-home is enabled by Smart-Licensing.
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform console serial
!
hostname Router
!
boot-start-marker
boot-end-marker
!
vrf definition 65528
 !
 address-family ipv4
 exit-address-family
!
no logging buffered
no logging rate-limit
!
aaa new-model
!
aaa authentication login default local
aaa authentication enable default enable
aaa authorization console
aaa authorization exec default local
!
aaa session-id common
fhrp version vrrp v3
!
no ip dhcp use class
!
no ip igmp ssm-map query dns
login on-success log
ipv6 unicast-routing
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-2465303444
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2465303444
 revocation-check none
 rsakeypair TP-self-signed-2465303444
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-2465303444
```

```
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32343635 33303334 3434301E 170D3230 31313036 31343333
  35345A17 0D333031 31303631 34333335 345A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34363533
  30333434 34308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100B02F AD33A0FF 0C50D3F2 D06CFDC6 F3CB73BB 4070D649 E07D16CE
  E6271C90 34E86882 822C8D71 E4BAC29D 85285258 51E748E1 8C9FB2C5 12242A22
  7FB71551 02CB4DBC 64089D2F 8DBB6C4A D3E2F112 8E16E71F FE70D102 F59862A3
  E920E77E 52E62E02 1979F800 3D13601F 27C42F81 483BFB34 697F1C20 3952626A
  CA1F5805 26D50A39 33F264D6 1AD485A0 8EB45882 FC97DCA2 106C8FAD 8CDBC0E6
  FF609188 B4677AB0 FBBE77F2 359EA002 E1A5D37D EA895FF3 92732A2B 63465DFD
  4A2A277C 17E7F720 2007A6B6 A7C7296F D0CD2707 8C7C9690 F86B0642 1BA9F28C
  F729157B 8C472E40 78A4E6BE 70471018 4B62EE36 48193FCA 062DB09F 38BC420B
  687E5866 DFA10203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 14ABBD00 3D02C6E1 7706FA96 29B037A8 583E7B2E
  69301D06 03551D0E 04160414 ABBD003D 02C6E177 06FA9629 B037A858 3E7B2E69
  300D0609 2A864886 F70D0101 05050003 82010100 40C60BF0 2184CF86 08CACB66
  73E74D63 E87A6661 DC839037 D0DB08D0 33C4993C EC326432 E3573D1B EC3B42AF
  F410BF72 2AAB6D8F 1406B352 FE6B5365 CCA7E094 96980FC7 A4B77A02 49CB8C01
  3EC87F01 58BFEE33 0DA222DB 0A1BA130 0AC01F1F FDBF2085 D41EFA45 7A4C7F5E
  2D004D04 D11433BF 69337D90 117A86ED 2CF57A49 AD7DA227 129E53DF 55E12E03
  4D8E0097 A29DC365 11E8B386 891C310E F19EDF6D D9B3EA1E E26ABDBD EF82D8E9
  B0484E26 C0FC1D71 91B19B70 221E1A1A 090F8EA1 3A5FC4FD A4EF36CD EFD2F1F4
  6056C87D 8A76ED1A 68FB76F5 956C6B50 7EFA9D8C 90EA910F 187EBD13 0BF76E5A
  0B9CE20E AA5927C4 7AD13C28 58C6E920 76E36475
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
!
license udi pid C8000V sn 9MUG8CATY8R
diagnostic bootup level minimal
memory free low-watermark processor 69848
!
!
username admin privilege 15 secret 9
```

```
$14$vKLj$yfnFjRidlKJg9.$4obKgKyy4TsoUs0sJ2t3HXPnA3XjYWRBnnYKBwVeJrw
!
redundancy
!
interface Loopback65528
 vrf forwarding 65528
 ip address 192.168.1.1 255.255.255.255
!
```

カスタムデータ設定の確認（Google Cloud Platform）

カスタムデータスクリプトを実行すると、VM が作成され、設定コマンドが実行されます。同じことを確認するには、次のコマンドとスクリプトを使用します。

- **show version**：Cisco Catalyst 8000V インスタンスの Cisco IOS XE CLI でライセンスプロパティが機能したかどうかを確認するには、**show version** コマンドを入力します。たとえば、セキュリティライセンスへの参照が出力に表示されます。
- スクリプトプロパティでコマンドを実行した後にエラーが発生したかどうかを確認するには、`/bootflash/<cloud>/` ディレクトリの `customdata.log` ファイルを調べます。*scriptname*.log ファイルには、スクリプトによって STDOUT に送信される出力が保存されます。
- Python プロパティが機能したかどうかを確認するには、ゲストシェルから `pip freeze | grep <package-name>` コマンドを入力して、現在インストールされている Python パッケージを表示します。ここで、*package-name* は、特に検索するパッケージを指します。
- IOS 設定プロパティで Cisco IOS XE コマンドを確認するには、**show running-configuration** コマンドを実行します。

コントローラモードでのデイゼロ設定

コントローラ（SD-WAN）モードで Cisco Catalyst 8000V のデイゼロ設定を実行する場合は、vManage からダウンロードした ciscosdwan_cloud_init.cfg ファイルの内容を指定する必要があります。

コントローラモードに切り替える場合、または Cisco SD-WAN 機能で Cisco Catalyst 8000V をブートストラップする場合は、「Install and Upgrade for Cisco Catalyst 8000V Controller Mode」を参照してください。

（注） Cisco CSP-5000 ハイパーバイザで実行されている Cisco Catalyst 8000V インスタンスの場合、[Day Zero Config] 画面で設定を入力する場合は、次の形式を維持してください。

- [Source File Name]：このフィールドの値を day0_ciscosdwan_cloud_init.cfg の形式で入力します。
- [Destination File Name]：このフィールドの値を day0-dest-filename /openstack/content/ciscosdwan_cloud_init.cfg の形式で入力します。

（注） SD-WAN 形式の設定では、最初の起動時に confd が設定を正常に適用できない場合、ボックスではデイゼロで設定が機能していない可能性があります。これは、ログインに SSH が必要なパブリッククラウド環境では特に重要です。プロビジョニング時に問題が発生した場合は、設定を慎重に確認してください。

ルータの動作モードとデイゼロ設定の確認

IOS XE 17.4 以降のリリースに正常に展開またはアップグレードされたかどうかを確認するには、**show version** コマンドを実行します。このコマンドはインスタンスのバージョンを表示し、**operating device-mode** パラメータは Cisco Catalyst 8000V インスタンスが実行されているモードを表示します。

自律モードでの Cisco Catalyst 8000V インスタンスの設定出力例

```
Device# show version | inc operating
Router operating mode: Autonomous
Device# show platform software device-mode
Operating device-mode: Autonomous
Device-mode bootup status:
------------------------------------
Device# show platform software chasfs r0 brief | inc device_managed_mode
/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [autonomous]
/tmp/fp/chasfs/etc/device_managed_mode : [autonomous]
Device# show version | inc Last reload
Last reload reason: Enabling autonomous-mode
```

よく寄せられる質問

Q. これまでCisco IOS XEイメージを使用していました。これからどのモードを選択すればよいでしょうか。

A. これまで Cisco IOS XE universalk9 イメージを使用していた場合は、IOS XE 17.4 イメージを展開し、自律モードを開始します。

Q. Cisco Catalyst 8000V 17.4 リリースにアップグレードする場合、ブートストラップ設定を指定する必要がありますか。

A. 既存の非 SD WAN ユーザーであり、IOS XE 17.4 リリース（自律モード）にアップグレードする場合は、アップグレードを直接実行できます。デイゼロまたはカスタムデータの設定を再度実行する必要はありません。

Microsoft Azure または Google Cloud Platform で実行されている Cisco Catalyst 8000V インスタンスの場合、デバイスは、Cisco Catalyst 8000V インスタンスを初めて設定したときに指定したカスタムデータを使用します。

AWS で実行されている Cisco Catalyst 8000V インスタンスの場合、デバイスはクラウド サービス プロバイダーからカスタムデータを取得します。

Q. モードを切り替えた後、カスタムデータ設定はどうなりますか。

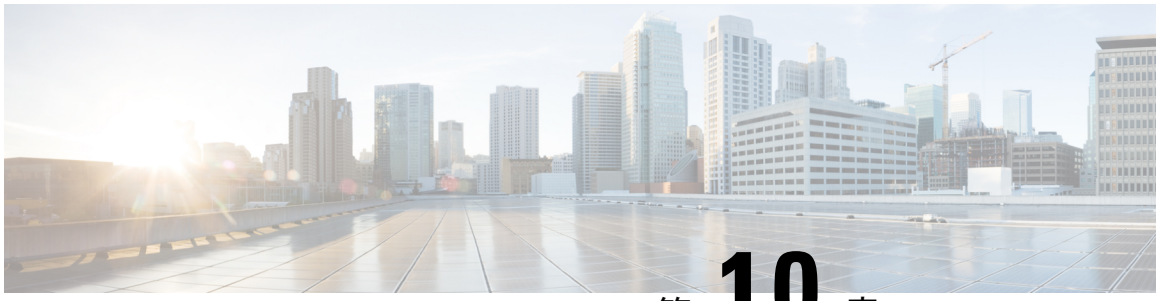
A. 既存の設定データが削除されます。新規インストールの場合と同様に、ブートストラップまたはカスタムデータ設定を実行する必要があります。

Q. 初期設定へのリセット後、カスタムデータはどうなりますか。

A. 初期設定へのリセットを実行すると、ディスク上の設定とファイルが消去されます。ルータは新規インストールのように起動し、適切な場所で構成ファイルを探します。このアクションによって、モードおよび関連する設定が決定されます。

Q. PayG ライセンスを使用して Cisco Catalyst 8000V インスタンスを任意のモードで展開できますか。

A. PayG ライセンスモデルを使用する場合、Cisco Catalyst 8000V インスタンスをコントローラモードで展開したり、コントローラモードに切り替えたりすることはできません。このモードは、PayG ライセンスモデルをサポートしていません。



第 10 章

Security-Enhanced Linux のサポート

この章では SELinux の機能について説明します。具体的な内容は次のとおりです。

概要

Security-Enhanced Linux（SELinux）は、Linux カーネル セキュリティ モジュールとシステム ユーティリティで構成されるソリューションで、強力で柔軟な Mandatory Access Control（MAC）アーキテクチャを Cisco IOS-XE プラットフォームに組み込みます。

SELinux には機密性と整合性の要件に基づいて情報を分離するための拡張メカニズムが備わっています。これにより、アプリケーションのセキュリティメカニズムの改ざんやバイパスの脅威に対処し、悪意のあるアプリケーションや欠陥のあるアプリケーションによって引き起こされる可能性のある障害を封じ込めることができます。

SELinux の前提条件

この機能に関する固有の要件はありません。

SELinux の制限事項

この機能に関する特定の制限はありません。

SELinux に関する情報

SELinux はユーザープログラムやシステムサービスを、割り当てられた機能を実行するために必要になる最小限の権限に制限する強制アクセス制御ポリシーを適用します。これにより、（バッファのオーバーフローや設定ミスなどによって）侵害された場合、害を生じさせるこれらのプログラムやデーモンの能力が削減または排除されます。これは、Cisco IOS-XE プラットフォームで MAC を適用することによる最小権限の原則の実用的な実装です。この制限メカニズムは、従来の Linux アクセス制御メカニズムとは独立して機能します。SELinux は、アプリケーションプロセスからリソースオブジェクトへのアクセスを制御するポリシーを定義する機能を提供します。これにより、プロセス動作の明確な定義と制限を明確にできます。

SELinux は、システムで有効になっている場合、**Permissive モード**または **Enforcing モード**のいずれかで動作します。

- Permissive モードでは、SELinux はポリシーを適用せず、リソースアクセスポリシーの違反によって発生した拒否のシステムログのみを生成します。操作は拒否されず、リソースアクセスポリシー違反についてのみログに記録されます。
- Enforcing モードでは、SELinux ポリシーが有効になり、適用されます。アクセスポリシールールに基づいてリソースアクセスを拒否し、システムログを生成します。

Cisco IOS XE 17.13.1a 以降、サポートされている Cisco IOS XE プラットフォームでは、SELinux はデフォルトで Enforcing モードで有効になっています。Enforcing モードでは、必要な許可ポリシーを持たないシステムリソースアクセスは違反として扱われ、操作は拒否されます。拒否が発生すると、違反操作は失敗し、システムログが生成されます。Enforcing モードでは、ソリューションはアクセス違反防止モードで機能します。

サポートされるプラットフォーム

Cisco IOS XE 17.13.1a 以降、SELinux は次のプラットフォームで有効になっています。

- Cisco 1000 シリーズ アグリゲーション サービス ルータ
- Cisco 1000 シリーズ サービス統合型ルータ
- Cisco 4000 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 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
- Cisco Catalyst 8500 および 8500L シリーズ エッジ プラットフォーム
- Cisco VG シリーズ ゲートウェイ：VG400、VG410、VG420、および VG450
- Cisco 1100 ターミナル サービス ゲートウェイ

SELinux の設定

Enforcing モードで SELinux 機能を有効化または操作するために必要な追加の要件や設定手順はありません。

SELinux の機能の一部として、次のコマンドが導入されています。

```
set platform software selinux {default | enforcing | permissive}
platform security selinux {enforcing | permissive}
show platform software selinux
```

（注） これらの新しいコマンドは、**サービス内部**コマンドとして実装されます。

SELinux の設定（EXEC モード）

set platform software selinux コマンドを使用して、EXEC モードで SELinux を設定します。

次に、EXEC モードでの SELinux 設定の例を示します。

```
Device# set platform software selinux ?

default  Set SELinux mode to default
enforcing  Set SELinux mode to enforcing
permissive  Set SELinux mode to permissive
```

SELinux の設定（CONFIG モード）

platform security selinux コマンドを使用して、コンフィギュレーション モードで SELinux を設定します。

次の例は、CONFIG モードでの SELinux 設定を示しています。

```
Device(config)# platform security selinux

enforcing  Set SELinux policy to Enforcing mode
permissive  Set SELinux policy to Permissive mode

Device(config)# platform security selinux permissive

Device(config)#
*Oct 20 21:52:45.155: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!

Device(config)#
```

SELinux の例

次に、モードを Enforcing から Permissive に変更した場合の出力例を示します。

```
"*Oct 20 21:44:03.609: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!"
```

次に、モードを Permissive から Enforcing に変更した場合の出力例を示します。

```
"*Oct 20 21:44:34.160: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode upgraded to enforcing!"
```

（注） SELinux モードが変更されると、この変更はシステム セキュリティ イベントと見なされ、システムログメッセージが生成されます。

Syslog メッセージリファレンス

機能重大度ニーモニック	%SELINUX-1-VIOLATION
重大度の意味	アラートレベルログ
メッセージ	該当なし
メッセージの説明	リソースのアクセスポリシーが存在しないプロセスによって、リソースアクセスが実行されました。操作にフラグが設定され、リソースアクセスが拒否されました。プロセスリソースアクセスが拒否されたという情報を含むシステムログが生成されました。
コンポーネント	SELINUX
推奨処置	次の関連情報を添付ファイルとしてCisco TACにご連絡ください。 • コンソールまたはシステムに出力されるとおりのメッセージ • **show tech-support** コマンドの出力（テキストファイル） • ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）： **request platform software trace archive target <URL>** • **show platform software selinux** コマンドの出力

次に、syslog メッセージの例を示します。

例 1：

```
*Nov 14 00:09:04.943: %SELINUX-1-VIOLATION: R0/0: audispd: type=AVC
msg=audit(1699927057.934:129): avc: denied { getattr } for pid=5899 comm="ls"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

例 2：

```
*Nov 14 00:09:04.947: %SELINUX-1-VIOLATION: R0/0: audispd: t type=AVC
msg=audit(1699927198.486:130): avc: denied { write } for pid=6012 comm="echo"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive= 0
```

SELinux の有効化の確認

show platform software selinux コマンドを使用して、SELinux 設定モードを表示します。

```
Device# show platform software selinux
========================================
IOS-XE SELINUX STATUS
========================================
SElinux Status :    Enabled
Current Mode :      Enforcing
Config file Mode :  Enforcing
```

SELinux のトラブルシューティング

デバイスまたはネットワークで SELinux 違反のインスタンスがある場合は、次の詳細を Cisco TAC に連絡してください。

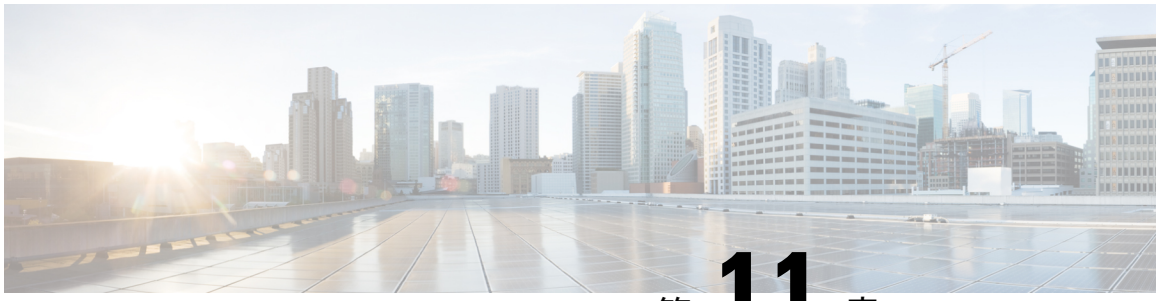
- コンソールまたはシステムログに出力されるとおりのメッセージ。次に例を示します。

  ```
  device#request platform software trace archive target
      flash:selinux_btrace_logs
  ```

- **show tech-support** コマンドの出力（テキストファイル）
- ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）：

  request platform software trace archive target <URL>

- **show platform software selinux** コマンドの出力



第 11 章

Cisco Catalyst 8000V ネットワーク インターフェイスの VM ネットワーク インターフェイスへのマッピング

ルータ ネットワーク インターフェイスの vNIC へのマッピング

Cisco Catalyst 8000V では、GigabitEthernet ネットワーク インターフェイスを、VM によって割り当てられた論理的な仮想ネットワーク インターフェイス カード（vNIC）名にマッピングします。次に、VM は物理 MAC アドレスに対して論理 vNIC 名をマッピングします。

Cisco Catalyst 8000V インスタンスを初めて起動したときに、VM の作成時に追加された論理 vNIC インターフェイスに、ルータインターフェイスがマッピングされます。次のイメージは、vNIC と Cisco Catalyst 8000V ルータインターフェイスの関係を示しています。

Cisco Catalyst 8000V インスタンスを起動した後、**show platform software vnic-if interface-mapping** コマンドを使用して、vNIC を持つルータ上の論理インターフェイスと vNIC MAC アドレスの間のマッピングを表示する必要があります。このコマンドの出力は、Cisco IOS XE のリリースバージョンによって異なります。

（注） GigabitEthernet0 インターフェイスはサポートされなくなりました。

```
Router# show platform software vnic-if interface-mapping
------------------------------------------------------------------------
Interface Name         Short Name     vNIC Name                 Mac Addr
------------------------------------------------------------------------
GigabitEthernet2        Gi2         eth2 (vmxnet3)           0050.5689.0034
GigabitEthernet1        Gi1         eth1 (vmxnet3)           0050.5689.000b
------------------------------------------------------------------------
```

ディスプレイに表示される vNIC 名は、Cisco Catalyst 8000V インスタンスがハイパーバイザ上のインターフェイスにマッピングするために使用する論理インターフェイスです。VM のインストール中に追加された対応する NIC 名に常にマッピングされるわけではありません。たとえば、表示されている論理「eth1」vNIC 名は、VM インストールプロセスで追加された「NIC1」に必ずしもマッピングされない場合があります。

注意 Cisco Catalyst 8000V でギガビット イーサネット ネットワーク インターフェイスの設定を開始する前に、インターフェイスのマッピングを確認することが重要です。これにより、ネットワーク インターフェイス構成が VM ホスト上の正しい物理 MAC アドレスインターフェイスに適用されます。

ルータを再起動し、vNIC を追加または削除しない場合、インターフェイスマッピングは以前と同じままになります。ルータを再起動して vNIC を削除する場合は、残りのインターフェイスの設定がそのまま残っていることを確認します。詳細については、「Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除」 を参照してください。

Cisco Catalyst 8000V でのネットワーク インターフェイスの追加と削除

Cisco Catalyst 8000V は、ルータの GigabitEthernet インターフェイスを、VM によって割り当てられた論理 vNIC 名にマッピングします。この論理 vNIC 名は、VM ホストの MAC アドレスにマッピングされます。Cisco Catalyst 8000V で GigabitEthernet インターフェイスを追加または削除するには、VM の vNIC を追加または削除します。ルータがアクティブな間に vNIC を追加できます。

VM から vNIC を削除するには、最初に VM の電源をオフにする必要があります。vNIC を削除した場合は、ルータを再起動する必要があります。vNIC を追加および削除する方法の詳細は、VMware のマニュアルを参照してください。

（注） インターフェイスのホット追加/削除は、コントローラモードで動作する Cisco Catalyst 8000V ではサポートされていません。インターフェイスのホット追加/削除を実行する必要がある場合は、CLI を使用して、コントローラモードでリセット操作を設定（**request platform software sdwan config reset**）します。

⚠

注意 Cisco Catalyst 8000V ネットワーク インターフェイス設定を更新せずに vNIC を削除すると、ルータの再起動時に設定の不一致が発生するリスクがあります。ルータを再起動して vNIC を削除すると、残りの論理 vNIC 名が別の MAC アドレスに再割り当てされる可能性があります。その結果、Cisco Catalyst 8000V インスタンスの GigabitEthernet ネットワーク インターフェイスは、ハイパーバイザ上の異なる物理インターフェイスに再割り当てされる可能性があります。

ネットワーク インターフェイスを追加または削除する前に、まず **show platform software vnic-if interface-mapping** コマンドを使用して、インターフェイスと vNIC のマッピングを確認します。

```
Router# show platform software vnic-if interface-mapping
------------------------------------------------------------------------------
Interface Name             Driver Name               Mac Addr
------------------------------------------------------------------------------
GigabitEthernet3            vmxnet3                 000c.2946.3f4d
GigabitEthernet2            vmxnet3                 0050.5689.0034
GigabitEthernet1            vmxnet3                 0050.5689.000b
------------------------------------------------------------------------------
```

VM のネットワーク インターフェイスを追加または削除した後、ネットワーク インターフェイスの設定を変更する前に、新しいインターフェイスと vNIC のマッピングを確認します。次の例は、新しい vNIC が追加された後のインターフェイスマッピングを示しています。新しい vNIC は、Cisco Catalyst 8000V インスタンスの GigabitEthernet4 ネットワーク インターフェイスにマッピングされます。

```
Router# show platform software vnic-if interface-mapping
------------------------------------------------------------------------------
Interface Name             Driver Name               Mac Addr
------------------------------------------------------------------------------
GigabitEthernet4            vmxnet3                 0010.0d40.37ff
GigabitEthernet3            vmxnet3                 000c.2946.3f4d
GigabitEthernet2            vmxnet3                 0050.5689.0034
GigabitEthernet1            vmxnet3                 0050.5689.000b
------------------------------------------------------------------------------
```

実行中の VM からの vNIC の削除

実行中の VM から vNIC を削除するには、`clear platform software` コマンドを使用します（後述）。ハイパーバイザ設定から vNIC を削除する前に、このコマンドを実行します。これは、「2 段階ホットリムーブ」の一部です。

2 段階ホットリムーブをサポートするハイパーバイザを確認するには、「vNIC Two-Step Hot Remove Support = Yes」のハイパーバイザを探します

clear platform software vnic-if interface GigabitEthernet*interface-number*

interface-number：0 ～ 32 の値。

例：

```
Router# clear platform software vnic-if interface GigabitEthernet4
```

次に、ハイパーバイザ設定から vNIC を削除します。

（注） ハイパーバイザから vNIC 設定を削除する前に、`clear platform software vnic-int interface` コマンドを実行する必要がなくなりました。このコマンドは、将来のリリースでは廃止される予定です。

Cisco Catalyst 8000V ネットワーク インターフェイスと VM の複製

Cisco Catalyst 8000V インスタンスを初めてインストールすると、vNIC 名を MAC アドレスにマッピングするデータベースが作成されます。このデータベースは、vNIC を追加または削除する場合に、ルータインターフェイス間の永続的なマッピングと vNIC から MAC アドレスへのマッピングを維持するために使用されます。インターフェイスは、VMware が保持する保存済みの汎用一意識別子（UUID）にマッピングされます。

ルータ ネットワーク インターフェイスと vNIC 間のマッピングは、Cisco Catalyst 8000V がインストールされている現在の VM にのみ適用されます。VM が複製された場合、保存されている UUID は現在の UUID と一致せず、インターフェイスマッピングはルータ設定と一致しません。

インターフェイスマッピングの不一致を防ぐには、複製前に元の VM で次の手順を実行します。

（注） 複製プロセスを開始する前に、複製された VM で必要な数の設定済み vNIC が元の VM に含まれていることを確認します。

ステップ 1 元の VM で **clear platform software vnic-if nvtable** コマンドを入力します。

このコマンドは、元の VM の永続的なインターフェイス データベースをクリアし、ハイパーバイザへのインターフェイスマッピングを更新します。

ステップ 2 Cisco Catalyst 8000V をリブートします。

ステップ 3 複製された VM で、**show platform software vnic-if interface-mapping** コマンドを使用してインターフェイスのマッピングを確認します。

ステップ 4 複製された VM のルータインターフェイスを適宜設定します。

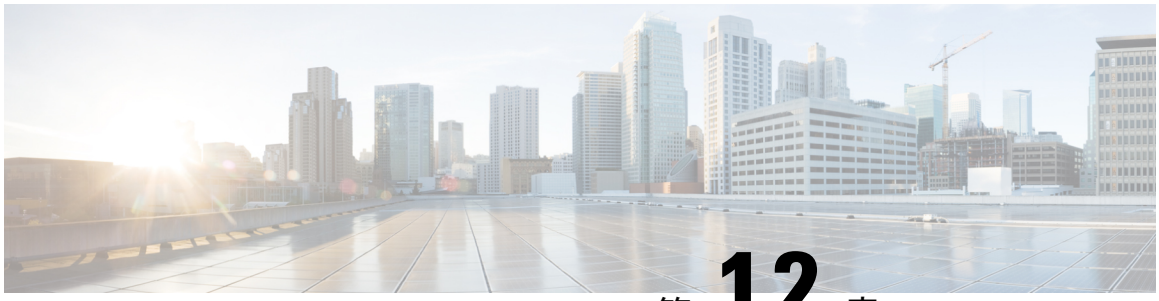
複製された VM のルータ設定は、元の VM の設定と一致する必要があります。

Cisco Catalyst 8000V ネットワーク インターフェイスと vSwitch インターフェイスのマッピング

Cisco Catalyst 8000V インターフェイスに対応するために、さまざまな方法で ESXi のネットワーク インターフェイスを設定できます。各 Cisco Catalyst 8000V ルータインターフェイスが 1 つのホスト イーサネット インターフェイスにマッピングされるように、ネットワーク インターフェイスを設定できます。

または、複数の Cisco Catalyst 8000V インターフェイスが 1 つのホスト ESXi イーサネット インターフェイスを共有するようにネットワーク インターフェイスを設定することもできます。

3 番目の方法は、Cisco Catalyst 8000V インターフェイスを vSwitch のトランクインターフェイスに直接マッピングすることです。



第 12 章

SD ルーティングデバイスでのソフトウェアアップグレード

この章では、SD ルーティングデバイスのソフトウェアをアップグレードする方法について説明します。ここで説明する内容は、次のとおりです。

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 Cisco SD ルーティング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。このワークフローでは、ソフトウェアの**ダウンロードとアップグレード**を実行できます。

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。指定した日時にワークフローをスケジュールできます。

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 SD ルーティングデバイスで実行されていることを確認します。

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

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 SD-WAN Manager のツールバーから [Task-list] アイコンをクリックします。Cisco SD-WAN Manager には、実行中のすべてのタスクのリストが、成功と失敗の合計数とともに表示されます。

1. Cisco SD-WAN Manager のメニューで**[Workflows]** > **[Workflow Library]**の順に選択します。

（注） Cisco SD-WAN Manager 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。
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、SD ルーティングデバイスのアップグレード中に制御接続が Cisco SD-WAN Manager 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、SD ルーティング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 SD-WAN Manager のツールバーから [Task-list] アイコンをクリックします。

   Cisco SD-WAN Manager には、実行中のすべてのタスクのリストが、成功と失敗の合計数とともに表示されます。

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 SD-WAN Manager 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 SD ルーティングデバイスの詳細が表示されます。

SDルーティングデバイスの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

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。

始める前に

ステップ 1 Cisco SD-WAN Manager のメニューから**[Workflows]** > **[Workflow Library]**の順に選択します。

または

[Workflows] > **[Popular Workflows]** > **[Software Upgrade]** の順に選択します。.

ステップ 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。

ステップ 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。

ステップ 4 [Start Date]、[Start Time]、[Select Timezone] を選択します。

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

ステップ 5 [Next] をクリックします。

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。

SDルーティングで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 SD-WAN Manager のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
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 SD ルーティング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 SD ルーティングデバイスのソフトウェアイメージの削除

SD ルーティングデバイスで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 SD-WAN Manager 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。

SDルーティングデバイスでのソフトウェアアップグレードのスケジュールに関する機能情報

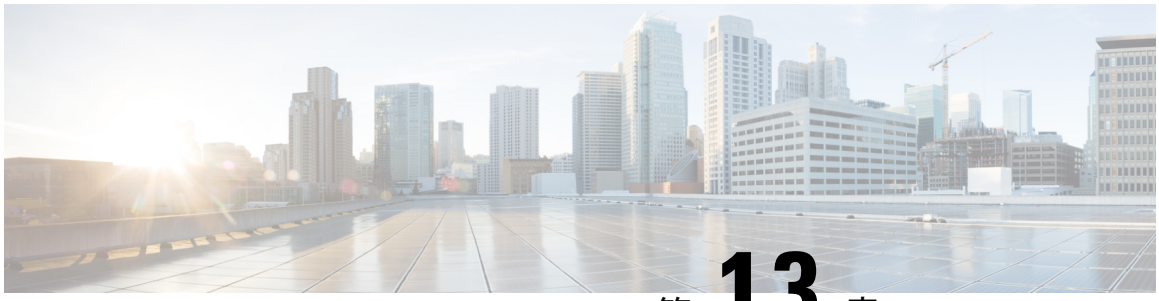
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

表 *14 : SD* ルーティングデバイスでのソフトウェアアップグレードのスケジュールに関する機能情報

機能名	リリース	機能情報
SD ルーティングデバイスでのソフトウェアアップグレードのスケジュール	Cisco IOS XE リリース 17.13.1a	この機能を使用すると、Cisco SD-Routing デバイスでソフトウェアイメージのアップグレードをスケジュールできます。これにより、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。



第 13 章

SD ルーティング設定グループ

この章では、SD ルーティング設定グループの設定方法について説明します。ここで説明する内容は、次のとおりです。

設定グループに関する情報

設定グループ機能は、Cisco Catalyst SD-WAN Manager を使用して SD ルーティングデバイスを設定するためのシンプルで再利用可能な構造化された方法を提供します。

- **設定グループ**：設定グループは、Cisco Catalyst SD-WAN Manager によって管理されるネットワーク内の 1 つ以上のデバイスに適用できる機能または設定の論理グループです。このグループ化は、ビジネスニーズに基づいて定義およびカスタマイズできます。
- **機能プロファイル**：機能プロファイルは、さまざまな設定グループ間で再利用できる設定の柔軟な構成要素です。必要な機能、推奨される機能、または独自に使用される機能に基づいてプロファイルを作成し、プロファイルを組み合わせてデバイス設定を完成させることができます。
- **機能パーセル**：機能は、さまざまな設定グループ間で共有する個々の機能です。

設定グループワークフロー

設定グループ機能を使用すると、次のことができます。

- 設定グループの作成

- 設定グループとデバイスの関連付け
- 設定グループでのデバイスの展開

設定グループの前提条件

- Cisco IOS XE Catalyst SD-Routing デバイスの最小ソフトウェアバージョン：Cisco IOS XE リリース 17.13.1。

設定グループの作成

設定グループを作成するには、次の手順を実行します。

ステップ 1 [Cisco IOS XE Catalyst SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] > [Add CLI based Configuration Group] の順に選択します。

ステップ 2 [Add CLI Group] ポップアップ ダイアログ ボックスで、設定グループ名を入力します。

ステップ 3 [Solution Type] ドロップダウンリストをクリックし、SD ルーティングデバイスのソリューションタイプとして [sd-routing] を選択します。

ステップ 4 [Description] フィールドに機能の説明を入力します。

ステップ 5 [Create] をクリックします。

[Feature Profiles] タブと [Associated Device] タブを含む新しい設定グループページが表示されます。

ステップ 6 [Feature Profiles] タブで、次の手順を実行します。

a) ドロップダウンリストから [Load Running Config from Reachable Device] をクリックし、設定を作成するデバイスのシステム IP を選択します。[Preview] テキストボックスの要件に基づいて設定を編集できます。

または

b) 右上隅の [Import Config Files] をクリックし、デバイスに適用する設定ファイルを選択します。

または

c) [Config Preview] テキストボックスに設定を入力します。

ステップ 7 [Save] をクリックして、コンフィギュレーションを保存します。

SD ルーティングデバイスと設定グループの関連付け

設定グループを作成した後、デバイスを設定グループに関連付けることができます。デバイスを設定グループに関連付けるには、次の手順を実行します。

ステップ 1 [Cisco SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] を選択します。
ステップ 2 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します。
ステップ 3 [Associated Devices] をクリックし、関連付けるデバイスを選択します。
ステップ 4 [Save] をクリックします。

SD ルーティングデバイスの展開

設定グループをデバイスに関連付けると、デバイスを展開できます。設定グループを使用して SD ルーティングデバイスを展開するには、次の手順を実行します。

ステップ 1 [Cisco SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] を選択します。
ステップ 2 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します。
ステップ 3 [Associated Devices] をクリックします。
ステップ 4 1 つ以上のデバイスを選択し、[Deploy] をクリックします。
ステップ 5 [Add and Review Configuration] ページで、変数を編集できます。
ステップ 6 [Apply] をクリックします。
ステップ 7 [Summary] ページで、[Preview CLI] をクリックして設定をプレビューします。
ステップ 8 [Save] をクリックします。

設定グループからの SD ルーティングデバイスの削除

設定グループから SD ルーティングデバイスを削除するには、次の手順を実行します。

ステップ 1 [Cisco SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] を選択します。
ステップ 2 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します。
ステップ 3 [Associated Devices] をクリックします。
ステップ 4 [Devices] テーブルで、設定グループから削除するデバイスを選択します。
ステップ 5 [Remove Device] をクリックします。

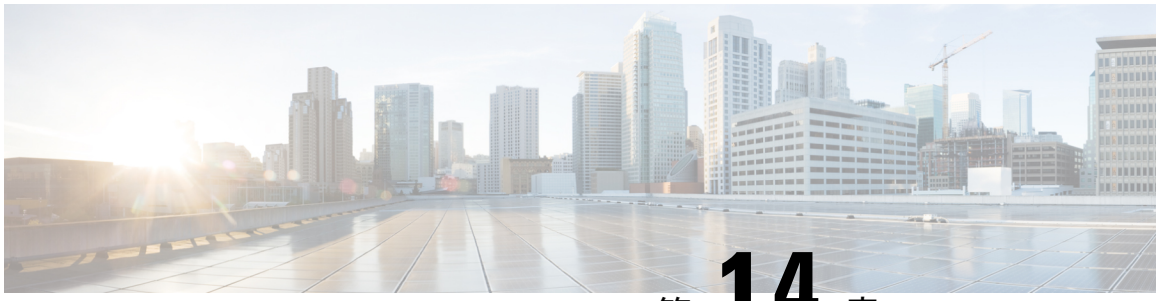
SD ルーティング設定グループの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

表 *15 : SD* ルーティング設定グループの機能情報

機能名	リリース	機能情報
SDルーティング設定グループ	Cisco IOS XE リリース 17.13.1a	SD ルーティング設定グループ機能は、Cisco Catalyst SD-WAN Manager を使用して SD ルーティングデバイスを設定するためのシンプルで再利用可能な構造化された方法を提供します。



第 14 章

Cisco SD-Routing Cloud OnRamp for Multicloud

この章では、SD ルーティングデバイスで Cloud OnRamp for Multicloud を設定する方法について説明します。ここで説明する内容は、次のとおりです。

概要

Cisco Catalyst SD-Routing Cloud OnRamp for Multicloud は、エンタープライズ WAN をパブリッククラウドに拡張します。このマルチクラウド ソリューションは、パブリック クラウド インフラストラクチャを Cisco Catalyst SD ルーティングデバイスに統合するのに役立ちます。AWS Transit Gateway（TGW）を使用して、SD ルーティングブランチサイトをサポートします。これらの機能により、ブランチデバイスは、クラウドネットワークとインターフェイスするアプリケーションにアクセスできます。この機能は、Cisco IOS XE 17.13.1 リリース以降でサポートされます。

（注） Cisco IOS XE 17.12.1a 以降、**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** へ、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** へのコンポーネントのブランド変更が行われました。

AWS 統合に関する情報

トランジットゲートウェイは、VPC とオンプレミスネットワークを相互接続するために使用できるネットワーク トランジット ハブです。VPC または VPN 接続をトランジットゲートウェイに接続できます。VPC と VPN 接続の間を流れるトラフィックの仮想ルータとして機能します。

Cisco SD-WAN Manager コントローラを使用して、マルチクラウド環境の Cloud OnRamp を設定および管理できます。Cisco SD-WAN Manager の設定ウィザードは、パブリック クラウド ア

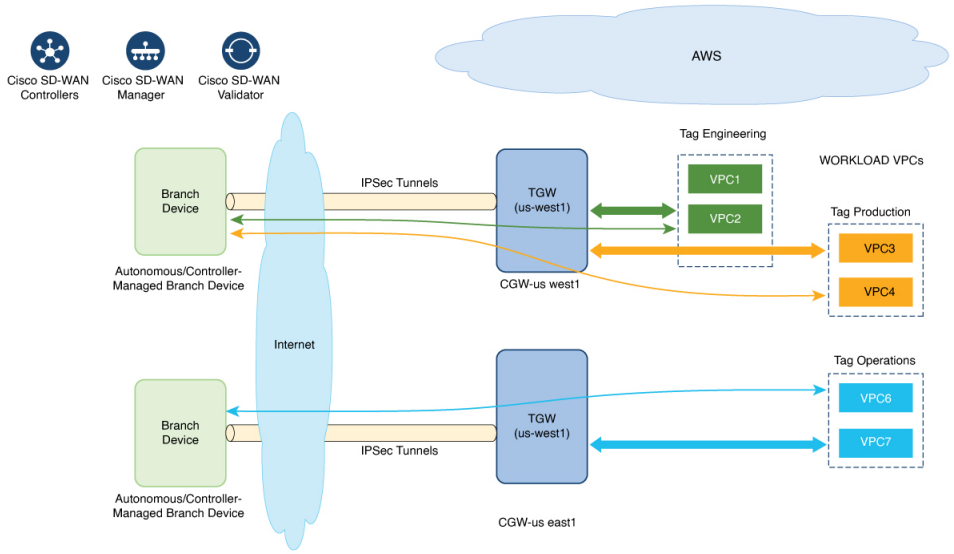
カウントへのトランジットゲートウェイの起動を自動化し、オーバーレイネットワーク内のブランチで、パブリック クラウド アプリケーションとそれらのアプリケーションのユーザーとの間の接続を自動化します。この機能は、Cisco クラウドルータ上の AWS 仮想プライベートクラウド（VPC）で動作します。

Cloud OnRamp for Multicloud は、複数の AWS アカウントとの統合をサポートしています。

SD ルーティングデバイスを使用した AWS Branch Connect

SD ルーティングベースのブランチを介して SD-Routing Cloud OnRamp を展開する場合は、SD ルーティングベースの設定グループを介して展開する必要があります。また、Cloud OnRamp 接続中にトンネルベースの設定が機能するように、それぞれの CG デバイス CLI テンプレートを使用してブートアップ ライセンス レベルを手動で設定する必要があります。

エッジ/ブランチデバイスは、セキュアなポイントツーポイントトンネルを介してクラウド内のホスト VPC に接続します。エッジデバイスと AWS Transit Gateway（TGW）の間に IPSec トンネルが設定されます。これらのトンネルは、ブランチ VPN または VRF トラフィックと BGP ルーティングトラフィックを伝送します。BGP を使用して、デバイスとトランジットゲートウェイがルーティング情報を交換し、ルーティングテーブルを構築します。



SD ルーティングブランチデバイスには、デフォルトの VRF のみを設定できます。このデフォルト VRF を使用して、SD-Routing Cloud OnRamp ブランチ接続を介してマッピングできます。マッピングに他の VPN/VRF を使用することはできません。SD ルーティングソリューションとともに、SD-WAN ソリューションに複数の VPN マッピングを設定できます。Cisco SD-WAN と Cisco SD-Routing の両方の接続を共存させることができます。

（注） ブランチサイトには、クラウドに接続する複数のブランチエンドポイントを設定できます。

SD ルーティングデバイス向け Cloud OnRamp の利点

SD-Routing Cloud OnRamp は、マルチクラウドワークフローを通じて SD ルーティングデバイスを使用して AWS または Azure に展開されたクラウドワークロードのセキュアなクラウド接続をサポートします。

Cloud onRamp の前提条件

Cloud onRamp の前提条件は次のとおりです。

- ブランチサイトは到達可能な状態であり、ステータスは同期中（In-Sync）である必要があります。
- ブランチサイトには、次のいずれかのブートレベルライセンスが必要です。
  - network-advantage
  - network-essentials
  - network-premier

  ライセンスがないと、サイトを接続するときに、IPSec トンネル設定が適用されません。
- インターフェイスには、AWS TGW または Azure vHub、あるいはブランチデバイスの NAT から到達可能なパブリック IP アドレスが割り当てられている必要があります。割り当てられていないと、ブランチサイトと AWS TGW または Azure vHub の間にトンネルが形成されません。
- SD ルーティングブランチは、設定グループを使用して展開するか、設定グループに移植する必要があります。
  - Cloud onRamp 機能を使用するための導入準備または互換性のある SD ルーティングデバイスを取得するには、既存のデバイスの導入準備 （122 ページ）および設定グループの自動化されたワークフローを使用した新しい SD ルーティングデバイスの導入準備 （123 ページ）のセクションを参照してください。

制限事項

- Cloud OnRamp は、異なるリージョンの TGW 間のピアリングをサポートしていません。

SD ルーティングデバイスでの AWS 統合の設定

ここでは、SD ルーティングデバイスの機能を導入準備するためのワークフローについて説明します。

- 既存のデバイスの導入準備：
  - 既存の自律型デバイスの SD ルーティングデバイスへの変換、および Cloud onRamp 機能の使用

- Cloud onRamp 機能を使用するための既存の非設定グループベースの SD ルーティングデバイスの変換
- 設定グループの自動化されたワークフローを使用した新しい SD ルーティングデバイスの導入準備

既存のデバイスの導入準備

既存のデバイスを導入準備するには、次の手順を実行します。

ステップ 1 既存の自律デバイスを SD ルーティングデバイスに手動で展開または変換するには、「Onboarding the Devices Manually」のセクションに記載されている手順に従います。

または

ステップ 2 クイック接続ワークフローを使用して SD ルーティングデバイスを展開するには、「Onboarding the SD-Routing Devices Using Bootstrap」のセクションに記載されている手順に従います。

前提条件：

ステップ 3 SD ルーティングデバイスを設定グループに移植するには、次の手順を実行します。

（注） 手順 1 と 2 のデバイスでは、次に進む前に次の前提条件を満たしている必要があります。

- ユーザー名とパスワード（admin/admin）を使用してデバイスにログインします。
- コマンドプロンプトで、**license boot level network-advantage addon dna-advantage** コマンドを設定します。
- 設定を保存し、デバイスをリブートします。Cisco SD-WAN Manager の [Configuration Devices] で、デバイスが同期していることを確認します。

a) [Cisco IOS XE Catalyst SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] > [Add CLI based Configuration Group] の順に選択します
b) [Add CLI Group] ポップアップ ダイアログ ボックスで、設定グループ名を入力します。
c) [Solution Type] ドロップダウンリストをクリックし、SD ルーティングデバイスのソリューションタイプとして [sd-routing] を選択します。
d) [Description] フィールドに、説明を入力します。
e) [Create] をクリックします。

[Feature Profiles] タブと [Associated Device] タブを含む新しい設定グループページが表示されます。

f) ドロップダウンリストから [Load Running Config from Reachable Device] をクリックし、設定を作成するデバイスのシステム IP を選択します。[Preview] テキストボックスの要件に基づいて設定を編集できます。
g) [Configuration Preview] テキストボックスにロードされた設定をコピーし、テキストファイルとしてシステムに保存します。

ステップ 4 SD ルーティングデバイスに設定グループを追加するには、次の手順を実行します。

a) [Cisco SD-WAN Manager] の メニューから、[Configuration] > [Configuration Groups] > [Add Configuration Group] > [Create SD-Routing Config] を選択します。
b) [Name] フィールドに、設定グループの名前を入力します。
c) [Description] フィールドに、説明を入力します。
d) [Create SD-Routing Config] をクリックします。
e) [Configuration Group Created] ポップアップ ダイアログ ボックスで、[No, I will Do It Later] オプションをクリックします。
f) [What's Next?] セクションで、[Go to Configuration Group] をクリックします。
g) 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します。
h) [Feature Profiles] で CLI プロファイルをクリックし、[Unconfigured] を選択します。
i) [Create New] をクリックします。
j) 一意の名前を入力します。テキストファイルとして保存されている設定をコピーして貼り付けます。
k) [Save] をクリックします。

ステップ 5 [Associate Devices] をクリックし、SD ルーティングデバイスのサイト ID を選択して、関連付けを続行します。

ステップ 6 展開ステータスのリンクをクリックし、展開が成功したことを確認します。

ステップ 7 [Configuration] > [Devices] ページで、次の詳細を確認します。

- [Device Status]：デバイスのステータスは [In Sync] である必要があります
- [Managed By]：ステップ 4a で作成したそれぞれの SD ルーティング設定グループ。

ステップ 8 ステータスを確認するには、**show sd-routing connections summary** コマンドを使用します。

設定グループの自動化されたワークフローを使用した新しい SD ルーティングデバイスの導入準備

設定グループの自動化されたワークフローを使用して新しい SD ルーティングデバイスを導入準備するには、次の手順を実行します。

ステップ 1 [Cisco SD-WAN Manager] の メニューから、[Configuration] > [Configuration Groups] > [Add Configuration Group] > [Create SD-Routing Config] を選択します。
ステップ 2 [Name] フィールドに、設定グループの名前を入力します。
ステップ 3 [Description] フィールドに、説明を入力します。
ステップ 4 [Create SD-Routing Config] をクリックします。
ステップ 5 [Configuration Group Created] ポップアップ ダイアログ ボックスで、[No, I will Do It Later] オプションをクリックします。
ステップ 6 [What's Next?] セクションで、[Go to Configuration Group] をクリックします。
ステップ 7 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します。
ステップ 8 [Feature Profiles] で CLI プロファイルをクリックし、[Unconfigured] を選択します。
ステップ 9 [Create New] をクリックします。
ステップ 10 基本設定グループを設定します。

この例は、設定グループの最小 CLI を示しています。

```
Configurations:
==============
sd-routing
organization-name CSRQA20231024
site-id 1
system-ip 4.7.8.9
vbond ip 44.226.182.48
vbond port 12346
wan-interface GigabitEthernet1
!
interface GigabitEthernet1
no shutdown
negotiation auto
ip address dhcp
exit
interface GigabitEthernet2
no shutdown
negotiation auto
ip address dhcp
exit

ip domain lookup

license boot level network-advantage addon dna-advantage
no logging console
```

ステップ 11 [Save] をクリックします。

ステップ 12 [Associate Devices] > [Associate Devices] の順にクリックします。

ステップ 13 [Unassigned] を選択し、UUID を 1 つ選択します。

ステップ 14 [Save] をクリックします。

ステップ 15 それぞれのシステム IP、サイト ID、およびホスト名を使用してデバイスをプロビジョニングできます。

ステップ 16 [Next] をクリックします。

ステップ 17 [Deploy] をクリックし、

ステップ 18 展開ステータスのリンクをクリックし、展開が成功したことを確認します。

ステップ 19 [Configuration] > [Devices] に移動し、uuid の 3 つのドットに対して [generate bootstrap] をクリックし、WAN インターフェイス名（例：GigabitEthernet1）を入力してブートストラップを生成します

ステップ 20 UUID 名の横にある [(…)] をクリックし、[Generate bootstrap] をクリックします。

ステップ 21 [WAN Interface] フィールドに、インターフェイス名 GigabitEthernet1 を入力し、ブートストラップを生成します。

ステップ 22 ブートストラップを使用して、AWS コンソールのそれぞれの AMI に対して Cisco 8000v インスタンスを展開し、WAN インターフェイスにパブリック IP を割り当てます。

ステップ 23 展開ステータスのリンクをクリックし、展開が成功したことを確認します。

ステップ 24 [Configuration] > [Devices] ページで、次の詳細を確認します。

- [Device Status]：デバイスのステータスは [In Sync] である必要があります
- [Managed By]：ステップ 1 で作成したそれぞれの SD ルーティング設定グループ。

ステップ 25 ステータスを確認するには、**show sd-routing connections summary** コマンドを使用します。

AWS クラウドアカウントの作成

AWS クラウドアカウントを作成するには、次の手順に従ってください。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。Cloud OnRamp for Multicloud ダッシュボードが表示されます。

ステップ 2 [Setup] ペインで [Associate Cloud Account] をクリックします。[Associate Cloud Account] ページの外部 ID をメモします。

ステップ 3 [Cloud Provider] フィールドで、ドロップダウンリストから [Amazon Web Services] を選択します。

ステップ 4 [Cloud Account Name] フィールドにアカウント名を入力します。

ステップ 5 （任意）[Description] フィールドに説明を入力します。

ステップ 6 [Use for Cloud Gateway] で、アカウントにクラウドゲートウェイを作成する場合は [Yes] を選択し、しない場合は [No] を選択します。

ステップ 7 [Login in to AWS With] フィールドで、使用する認証モデルを選択します。

- **Key**
- **IAM Role**

[Key] モデルを選択した場合は、[API Key] および [Secret Key] フィールドで、それぞれのキーを指定します。

または

[IAM Role] モデルを選択した場合は、Cisco SD-WAN Manager が提供する [External ID] を使用して IAM ロールを作成します。ウィンドウに表示された外部 ID をメモして、IAM ロールの作成時に使用できる [Role ARN] 値を指定します。

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降、IAM ロールを作成するには、AWS 管理コンソールを使用して、Cisco SD-WAN Manager が提供する外部 ID をポリシーに入力する必要があります。次の手順を実行します。

1. 既存の Cisco SD-WAN Manager EC2 インスタンスに IAM ロールをアタッチします。
    1. ポリシーを作成するには、AWS ドキュメントの IAM ロールの作成（コンソール）のトピックを参照してください。AWS の [Create policy] ウィザードで、[JSON] をクリックし、次の JSON ポリシードキュメントを入力します。

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",
```

```
    "Action": "sts:AssumeRole",
"Resource": "*"
    }
]
}
```

2. IAM ロールを作成し、手順 1 で作成したポリシーに基づいて Cisco SD-WAN Manager EC2 インスタンスにアタッチする方法については、AWS Security Blog の「Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console」ブログを参照してください。

   （注） [Attach permissions policy] ウィンドウで、手順 1 で作成した AWS 管理ポリシーを選択します。

   （注） 次の権限セットが許可されます。

   - AmazonEC2FullAccess
   - IAMReadOnlyAccess
   - AWSNetworkManagerFullAccess
   - AWSResourceAccessManagerFullAccess

   AWS IAM ロールの作成の詳細については、「Creating an AWS IAM Role」を参照してください。

2. マルチクラウド環境に使用する AWS アカウントで IAM ロールを作成します。

   1. AWS ドキュメントの IAM ロールの作成（コンソール）のトピックを参照して、[Require external ID] をオンにし、手順 2 でメモした外部 ID を貼り付けて、IAM ロールを作成します。
   2. ロールを担当できるユーザーを変更するには、AWS ドキュメント のロール信頼ポリシーの変更（コンソール）のトピックを参照してください。

      [IAM Roles] ウィンドウで、下にスクロールして、前の手順で作成したロールをクリックします。

      [Summary] ウィンドウで、上部に表示される [Role ARN] をメモします。

      （注） 手順 7 で IAM ロールとして認証モデルを選択した場合は、このロール ARN 値を入力できます。

   3. 信頼関係を変更したら、[JSON] をクリックし、次の JSON ドキュメントを入力します。変更内容を保存します。

      （注） 次の JSON ドキュメントのアカウント ID は、Cisco SD-WAN Manager EC2 インスタンスに属しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
        "Principal": {
          "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
          "StringEquals": {
            "sts:ExternalId": "[vManage provided External ID]"
         }
        }
      }
    ]
}
```

ステップ 8 [Add] をクリックします。クラウドアカウントの詳細を表示または更新するには、[Cloud Account Management] ページで [...] をクリックします。また、関連付けられたホスト VPC タグまたはクラウドゲートウェイがない場合は、クラウドアカウントを削除することもできます。

クラウドグローバル設定の構成

AWS のクラウドグローバル設定を構成するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]**を選択します。[Setup] ペインで [Cloud Global Settings] をクリックします。[Cloud Global Settings] ウィンドウが表示されます。

ステップ 2 [Cloud Provider] フィールドで、[Amazon Web Services] を選択します。

ステップ 3 [Cloud Gateway Solution] ドロップダウンリストをクリックして、[Transit Gateway – Branch-connect] を選択します。

- [Transit Gateway–Branch-connect]：AWS クラウドでインスタンス化されたトランジットゲートウェイを介して、さまざまな SD ルーティングデバイスをクラウド内の VPC に接続できるようにします。このオプションでは、AWS VPN 接続（IPSec）アプローチを使用します。

ステップ 4 [Cloud Gateway BGP ASN Offset] フィールドに、値を入力します。

ステップ 5 [Intra Tag Communication] を選択します。オプションは、[Enabled] または [Disabled] です

ステップ 6 [Program Default Route in VPCs into TGW/Core] を選択します。オプションは、[Enabled] または [Disabled] です。

ステップ 7 [Enabled] または [Disabled] をクリックして、[Enable Periodic Audit] フィールドを有効または無効にします。

定期監査を有効にすると、Cisco SD-WAN Manager は 2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、不一致レポートが生成されます。

ステップ 8 [Enabled] または [Disabled] をクリックして、[Enable Auto Correct] フィールドを有効または無効にします。自動修正オプションを有効にすると、定期的な監査がトリガーされるたびに、検出されたすべての回復可能な問題が自動修正されます。

ステップ 9 [Add] または [Update] をクリックします。

ホスト プライベート ネットワークの検出

利用可能なアカウントの各リージョンすべてにわたって、すべてのアカウントのホスト VPC を検出できます。ホスト VPC 検出が呼び出されると、VPC の検出はキャッシュなしで実行されます。

ホスト プライベート ネットワークを検出するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]**を選択します。[Discover] の下の [Host Private Networks] をクリックします。[Discover Host Private Networks] ウィンドウに、使用可能な VPC のリストが表示されます。

[host VPC] テーブルには次の列があります。

- クラウド リージョン
- アカウント名
- ホスト VPC 名
- ホスト VPC タグ
- アカウント ID
- ホスト VPC ID

必要に応じて、列をクリックして VPC を並べ替えます。

ステップ 2 [Region] ドロップダウンリストをクリックして、特定のリージョンに基づいて VPC を選択します。

ステップ 3 [Tag Actions] をクリックして、次のアクションを実行します。

- [Add Tag]：選択した VPC をグループ化し、これらの VPC に同時にタグ付けします。
- [Edit Tag]：選択した VPC をあるタグから別のタグに移行します。
- [Delete Tag]：選択した VPC のタグを削除します。

複数のホスト VPC をタグの下にグループ化できます。同じタグの下のすべての VPC は、単一のユニットと見なされます。

クラウドゲートウェイの作成

クラウドゲートウェイは、クラウド内のトランジットVPC（TVPC）とトランジットゲートウェイをインスタンス化したものです。クラウドゲートウェイを作成するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。[Manage] の下にある [Create Cloud Gateway] をクリックします。[Manage Cloud Gateway - Create] ウィンドウが表示されます。

ステップ 2 [Cloud Provider] フィールドで、ドロップダウンリストから [Amazon Web Services] を選択します。

ステップ 3 [Cloud Gateway Name] フィールドに、クラウドゲートウェイ名を入力します。

ステップ 4 （任意）[Description] に説明を入力します。

ステップ 5 [Account Name] ドロップダウンリストからアカウント名を選択します。

ステップ 6 [Region] ドロップダウンリストからリージョンを選択します。

ステップ 7 [Add] をクリックして、新しいクラウドゲートウェイを作成します。

サイトの接続

クラウドゲートウェイにサイトを接続するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択し、[Manage] の下の [Gateway Management] を選択します。[Cloud Gateway] ウィンドウが表示されます。テーブルには、クラウドアカウント名、ID、クラウドタイプ、トランジットゲートウェイとともにクラウドゲートウェイのリストが表示されます。

クラウドゲートウェイごとに、サイトを表示、削除、またはさらに接続できます。

ステップ 2 目的のクラウドゲートウェイで、[(…)] をクリックし、[Cloud Gateway] を選択します。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Attach Sites] をクリックします。

ステップ 5 [Next] をクリックします。[Attach Sites - Select Sites] ウィンドウが表示されます。テーブルには、選択した WAN インターフェイスを持つサイトが表示されます。

ステップ 6 [Available Sites] からサイトを 1 つ以上選択し、それらを [Selected Sites] に移します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Attach Sites - Site Configuration] ウィンドウで、[Tunnel Count] を入力します。トンネル数の範囲は 1 ～ 8 で、各トンネルは 2.5 Gbps の帯域幅を提供します。

ステップ 9 [Attach Sites - Select Interface] ウィンドウで、インターフェイスの詳細を入力します。このインターフェイスは、TGW へのトンネルを形成するために使用されます。

シスコが提供する

ステップ 10 [Accelerated VPN] オプションで、[Enabled] または [Disabled] を選択します。AWS Global Accelerator は、クラウドへの接続を最適化するのに役立ちます。

ステップ 11 [Use selected interface as Preferred Path] オプションで、[Enabled] または [Disabled] を選択します。マルチクラウドワークフローは、選択した WAN インターフェイスをデフォルトパスとして設定します。

ステップ 12 [Next] をクリックします。

ステップ 13 [Save and Exit] をクリックします。設定が成功すると、ブランチデバイスが正常に接続されたことを示すメッセージが表示されます。

ステップ 14 デバイスのステータスを確認するには、**show running cofig** コマンドを使用します。

ステップ 15 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

サイトの切断

クラウドゲートウェイからサイトを切り離すには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] > [Cloud Gateways] を選択します。テーブルには、クラウドアカウント名、ID、クラウドタイプ、トランジットゲートウェイとともにクラウドゲートウェイのリストが表示されます。

ステップ 2 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Gateway] を選択します。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Available Sites] から 1 つ以上のサイトを選択し、[Detach Sites] をクリックします。

[Are you sure you want to detach sites from cloud gateway?] というメッセージがウィンドウに表示されます。

ステップ 5 [OK] をクリックします。

クラウドゲートウェイに接続されているサイトは切り離されます。

ステップ 6 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

サイトの編集

サイトを編集するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] > [Cloud Gateways] を選択します。テーブルには、クラウドアカウント名、ID、クラウドタイプ、トランジットゲートウェイとともにクラウドゲートウェイのリストが表示されます。

ステップ 2 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Gateway] を選択します。

ステップ 3 [Edit Site Details] をクリックします。

ステップ 4 [Edit Sife Details] ダイアログボックスで、トンネル数を入力します。

ステップ 5 [Accelerated VPN] フィールドを有効または無効にします。デフォルトでは、このフィールドは [Enabled] になっています。

ステップ 6 [Use Select Interface as Preferred path] フィールドを有効または無効にします。デフォルトでは、このフィールドは [Enabled] になっています。

ステップ 7 [Submit] をクリックします。

インテント管理 - 接続

Cisco SD-WAN Manager のマッピングワークフローにより、Cisco Catalyst SD-Routing VPN（セグメント）と VPC 間の接続、および VPC から VPC への接続が可能になります。VPC はタグに基づいて表されます。

（注） SDルーティングブランチデバイスには、デフォルトのVRFのみを設定できます。このデフォルト VRF を使用して、SD-Routing Cloud OnRamp ブランチ接続を介してマッピングできます。マッピングに他のVPN/VRFを使用することはできません。SDルーティングソリューションとともに、SD-WAN ソリューションに複数の VPN マッピングを設定できます。Cisco SD-WAN と Cisco SD-Routing の両方の接続を共存させることができます。

システムが接続のインテントを記録すると、クラウドゲートウェイが存在するリージョンのクラウドでマッピングが実現されます。クラウドゲートウェイが異なるリージョンに存在しなくても、マッピングインテントを入力できます。ユーザー マッピング インテントは保持され、新しいクラウドゲートウェイまたはマッピングの変更が検出されたときに実現されます。クラウドゲートウェイが異なるリージョンでインスタンス化されると、マッピングインテントがそれらのリージョンで実現されます。同様に、タグ付け操作はさまざまなリージョンのマッピングにも影響を与える可能性があり、タグごとのマッピングはクラウドで実現されます。

Cloud OnRamp for Multicloud ダッシュボードで、[Management] の下の [Connectivity] をクリックします。[Intent Management - Connectivity] ウィンドウが表示されます。ウィンドウには、接続ステータスと次の凡例が表示されます。

- 空白：編集可能
- グレー：システム定義済み
- 青：インテント定義済み
- 緑：インテント実現済み
- 赤：インテント実現済み（エラーあり）

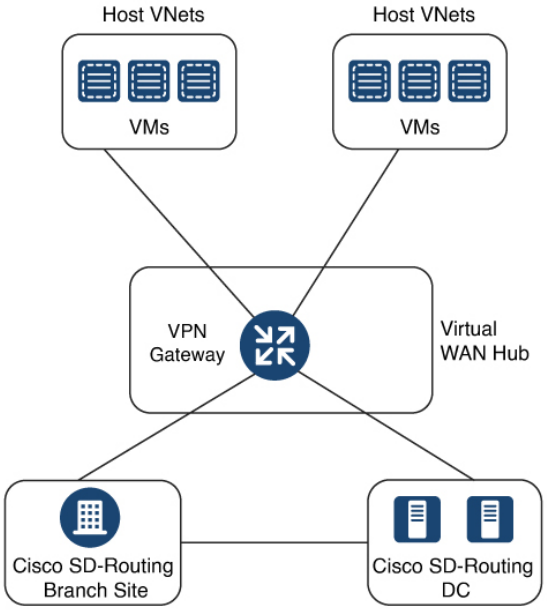
[Connectivity] ウィンドウでは、次のことができます。

- 必要に応じて、接続の変更を表示します。
- フィルタ処理とソート。
- さまざまなリージョンのクラウドゲートウェイに依存しない接続を定義します。
- クラウドゲートウェイが存在するすべてのリージョンで接続を実現します。

Azure 仮想 WAN ハブと Cisco SD ルーティングの統合

Cisco Catalyst SD-Routing ソリューションと Azure 仮想 WAN の統合により、マルチクラウド展開の Cloud OnRamp が強化され、Cisco VPN ゲートウェイを Azure 仮想 WAN ハブのネットワーク仮想アプライアンスとして設定できます。

この統合により、トランジット仮想ネットワーク（VNet）を作成する必要がなくなり、Azure 仮想 WAN ハブを介してホスト VNet 接続を直接制御できるため、クラウドサービスの消費モデルが簡素化されます。Azure 仮想 WAN は、Microsoft Azure を介して最適化および自動化されたブランチからクラウドへの接続を提供するネットワーキングサービスです。Azure と通信できる SD ルーティング ブランチ デバイスを接続して設定できます。Azure 仮想ハブ内に VPN ゲートウェイを構成すると、より高速で広い帯域幅が提供され、トランジット VNet を使用する場合の速度と帯域幅の制限が克服されます。



仮想 WAN ハブ統合の仕組み

SD ルーティングブランチとパブリック クラウド アプリケーション間の接続は、Azure のマルチクラウド SD ルーティングワークフローの Cloud OnRamp の一部として Azure 仮想 WAN ハブ内で設定された Azure VPN ゲートウェイによって提供されます。

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud フローは、地理的なクラウドリージョン内の既存の VNet を検出し、選択した VNet をオーバーレイネットワークに接続できるようにします。このようなシナリオでは、Cloud OnRamp for Multicloud を使用すると、レガシーパブリッククラウド接続と Cisco Catalyst SD ルーティングネットワークを簡単に統合できます。

Cisco SD-WAN Manager の設定ウィザードは、パブリック クラウド アカウントに接続するための Azure 仮想 WAN ハブの起動を自動化します。また、このウィザードは、パブリック クラウ

ドアプリケーションと、オーバーレイ ネットワーク内のブランチにいるそれらのアプリケーションのユーザーとの間の接続を自動化します。Cisco SD-Routing Manager では、タグを使用して、ブランチ内のサービスのデフォルト VRF をパブリック クラウド インフラストラクチャ内の特定の VNet にマッピングできます。

VNet から VPN へのマッピング

Cisco SD-WAN Manager のインテント管理ワークフローは、Cisco SD ルーティングのデフォルト VRF（ブランチネットワーク）と VNet 間の接続、および VNet から VNet への接続を可能にします。SD ルーティングと SD-WAN 接続マッピングの両方を有効にできます。SD-WAN VPN を有効にすると、SD ルーティング VRF がデフォルトで有効になります。VNet は、Cloud OnRamp for Multicloud の Discover ワークフローで作成されたタグで表されます。Azure リージョン内で VNet タグを作成すると、同じタグを共有する他の VNet および VPN に基づいてマッピングが自動的に作成されます。

Cisco SD-WAN Manager が接続のインテントを記録すると、クラウドゲートウェイが存在するリージョンのクラウドでマッピングが実現されます。クラウドゲートウェイが異なるリージョンに存在しなくても、マッピングインテントを入力できます。マッピングインテントは、新しいクラウドゲートウェイまたはマッピングの変更が検出されたときに保持され、実現されます。クラウドゲートウェイが異なるリージョンでインスタンス化または検出されると、マッピングインテントがそれらのリージョンで実現されます。同様に、タグ付け操作はさまざまなリージョンのマッピングにも影響を与える可能性があり、タグごとのマッピングはクラウドで実現されます。

Azure 仮想 WAN 統合ワークフローのコンポーネント

ブランチとデータセンターをパブリック クラウド インフラストラクチャに接続するためのクラウドゲートウェイは、Azure 仮想ハブ VPN ゲートウェイをホストする論理オブジェクトです。Azure リソースグループ、Azure 仮想 WAN、Azure VPN ゲートウェイ、および Azure 仮想 WAN ハブで構成されます。

リソースグループ

すべての Azure ネットワーキングリソースはリソースグループに属し、リソースグループは Azure サブスクリプションの下に作成されます。Azure クラウドゲートウェイの場合、Azure 仮想 WAN と Azure 仮想 WAN ハブはリソースグループの下に作成されます。

したがって、Azure クラウドゲートウェイを作成する最初の手順は、リソースグループを作成することです。

リソースグループを作成したら、Azure 仮想 WAN を構成できます。

Azure 仮想 WAN

Azure 仮想 WAN は、Azure ネットワーキングサービスのバックボーンです。既存の Azure リソースグループの下に作成されます。Azure 仮想 WAN には、各仮想ハブが異なる Azure リージョンに属している限り、複数の Azure 仮想ハブを含めることができます。Azure リージョンごとに 1 つの仮想ハブのみがサポートされます。

リージョン内のリソースグループで仮想 WAN を定義したら、次のステップは Azure 仮想 WAN ハブを作成することです。

Azure 仮想 WAN ハブ

Azure 仮想 WAN ハブは、デフォルトの VRF サイトと VPN ゲートウェイおよび VNet 間のコア接続を管理します。仮想ハブが作成されると、VPN ゲートウェイを Azure ネットワーキングサービスに統合できます。

Azure の前提条件

- サポートされる最小リリース：Cisco IOS XE Catalyst SD-Routing リリース 17.13.1。
- Azure クラウドアカウントの詳細。
- Azure マーケットプレイスへのサブスクリプション。
- Cisco SD-WAN Manager はインターネットに接続されている必要があり、Azure アカウントを認証するために Microsoft Azure と通信できる必要があります。

Azure SD ルーティング Cloud OnRamp の制限事項

- リージョンごとに作成できる VPN ゲートウェイは 1 つだけです。ただし、1 つのリージョンに複数の NVA ベースのクラウドゲートウェイを作成できます。
- Cisco SD-WAN Manager では、1 つのリソースグループのみが許可されます。
- 同じリージョンに VPN ゲートウェイと NVA ベースのクラウドゲートウェイを組み合わせることはできません。
- VPN ゲートウェイしかない場合は、監査を実行できません。監査は、少なくとも 1 つの NVA ベースのクラウドゲートウェイがある場合にのみ実行できます。

SD ルーティング用の Azure 仮想 WAN ハブの構成

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローを使用して、Azure 仮想 WAN ハブを作成し、Cisco Catalyst SD-Routing ブランチサイトをプライベートネットワークまたはホスト VNet のアプリケーションに接続します。Azure 仮想 WAN ハブを設定するには、次のタスクを実行します。

アカウントと Cisco SD-WAN Manager の関連付け

アカウントを Cisco SD-WAN Manager に関連付けるには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。

ステップ 2 [Setup] で、[Associate Cloud Account] をクリックします。

ステップ 3 [Cloud Provider] フィールドで、ドロップダウンリストから [Microsoft Azure] を選択します。

ステップ 4 必要な情報を入力します。

フィールド	説明
クラウドアカウント名	Azure サブスクリプションの名前を入力します。
説明（任意）	アカウントの説明を入力します。このフィールドは任意です。
クラウドゲートウェイで使用	[Yes] を選択して、アカウントにクラウドゲートウェイを作成します。デフォルトでは [No] が選択されています。
テナント ID	Azure Active Directory（AD）の ID を入力します。テナント ID を見つけるには、Azure Active Directory に移動し、[Properties] をクリックします。
サブスクリプション ID	このワークフローの一部として使用する Azure サブスクリプションの ID を入力します。
Client ID	既存の Azure アプリケーション ID を入力します。Azure AD にアプリケーションを登録する方法、クライアント ID と秘密キーを取得する方法などの詳細については、Azure のドキュメントを参照してください。
秘密キー（Secret Key）	クライアント ID に関連付けられたパスワードを入力します。

ステップ 5 [Add] をクリックします。

グローバルクラウド設定の追加と管理

グローバルクラウド設定を追加および管理するには、次の手順を実行します。

ステップ 1 [Cloud OnRamp for Multicloud] ウィンドウで、[Setup] エリアの [Cloud Global Settings] をクリックします。

ステップ 2 [Cloud Provider] フィールドで、ドロップダウンリストから [Microsoft Azure] を選択します。

ステップ 3 グローバル設定を編集するには、[Edit] をクリックします。

ステップ 4 グローバル設定を追加するには、[Add] をクリックします。

ステップ 5 [Software Image] フィールドで、Azure Virtual Hub で使用する WAN エッジデバイスのソフトウェアイメージを選択します。

ステップ 6 [SKU Scale] フィールドで、容量要件に基づいて、ドロップダウンリストからスケールを選択します。

ステップ 7 [IP Subnet Pool] フィールドで、Azure Virtual WAN ハブに使用する IP サブネットプールを指定します。サブネットプールには、/16 ～ /24 の範囲内のプレフィックスが必要です。

ステップ 8 [Autonomous System Number] フィールドで、仮想ハブとの eBGP ピアリングのためにクラウドゲートウェイが使用する ASN を指定します。

ステップ 9 [Push Monitoring Metrics to Azure] フィールドで、[Enabled] または [Disabled] を選択します。[Enabled] を選択すると、Azure サブスクリプションに関連付けられたクラウド ゲートウェイ メトリックが Microsoft Azure Monitoring Service ポータルに定期的に送信されます。これらのメトリックは、すべての NVA ベンダーに対して Microsoft Azure によって規定された形式で送信されます。

ステップ 10 [Advertise Default route to Azure Virtual Hub] フィールドを有効または無効にします。デフォルトでは、このフィールドは [Disabled] になっています。[Enabled] をクリックすると、仮想ネットワークからのインターネットトラフィックが Cisco Catalyst SD-WAN ブランチ経由でリダイレクトされます。

ステップ 11 [Enabled] または [Disabled] をクリックして、[Enable Periodic Audit] フィールドを有効または無効にします。

定期監査を有効にすると、Cisco SD-WAN Manager は 2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、不一致レポートが生成されます。

ステップ 12 [Enabled] または [Disabled] をクリックして、[Enable Auto Correct] フィールドを有効または無効にします。自動修正オプションを有効にすると、定期的な監査がトリガーされるたびに、検出されたすべての回復可能な問題が自動修正されます。

ステップ 13 [Add] または [Update] をクリックします。

クラウドゲートウェイの作成と管理

クラウドゲートウェイの作成には、Azure 仮想 WAN ハブとハブ内の 2 つの Cisco VPN ゲートウェイのインスタンス化または検出が含まれます。

クラウドゲートウェイを作成および管理するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。

ステップ 2 [Manage] で、[Create Cloud Gateway] をクリックします

ステップ 3 [Cloud Provider] フィールドで、ドロップダウンリストから [Microsoft Azure] を選択します。

ステップ 4 [Cloud Gateway Name] フィールドに、クラウドゲートウェイの名前を入力します。

ステップ 5 （任意）[Description] フィールドに、クラウドゲートウェイの説明を入力します。

ステップ 6 [Account Name] フィールドで、ドロップダウンリストから Azure アカウント名を選択します。

（注） 保持できる Azure アカウントは 1 つだけです。

ステップ 7 [Region] フィールドで、ドロップダウンリストから [Azure] リージョンを選択します。

（注） リージョン内の VPN ゲートウェイは 1 つだけです。リージョンに VPN ゲートウェイがある場合、同じリージョンに NVA ゲートウェイを配置することはできません。

ステップ 8 [Resource Group] フィールドで、ドロップダウンリストからリソースグループを選択するか、[Create New] を選択します。

（注） 新しいリソースグループを作成する場合は、既存のすべてのクラウドゲートウェイを削除する必要があります。また、次の 2 つのフィールドで新しい Azure 仮想 WAN と Azure 仮想 WAN ハブを作成する必要があります。

ステップ 9 [Virtual WAN] フィールドで、ドロップダウンリストから Azure 仮想 WAN を選択します。または、[Create New] をクリックして、新しい Azure 仮想 WAN を作成します。

ステップ 10 [Virtual HUB] フィールドで、ドロップダウンリストから Azure 仮想 WAN ハブを選択します。または、[Create New] をクリックして、新しい Azure 仮想 WAN ハブを作成します。

ステップ 11 [Solution Type] フィールドで、ドロップダウンリストから Cisco vHub と VPN を選択します。

ステップ 12 [SKU Scale Unit Size] フィールドで、ドロップダウンリストから SKU スケールユニットサイズを選択します。

ステップ 13 [Add] をクリックして VPN ゲートウェイを展開します。

サイトの接続

クラウドゲートウェイにサイトを接続するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] > [Cloud Gateways] を選択します。テーブルには、クラウドアカウント名、ID、クラウドタイプ、トランジットゲートウェイとともにクラウドゲートウェイのリストが表示されます。

クラウドゲートウェイごとに、サイトを表示、削除、またはさらに接続できます。

ステップ 2 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Gateway] を選択します。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Attach Sites] をクリックします。

ステップ 5 [Next] をクリックします。[Attach Sites - Select Sites] ウィンドウが表示されます。テーブルには、選択した WAN インターフェイスを持つサイトが表示されます。

ステップ 6 [Available Sites] からサイトを 1 つ以上選択し、それらを [Selected Sites] に移します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Attach Sites - Site Configuration] ウィンドウで、[Tunnel Count] を入力します。トンネル数は 1 で、帯域幅は 2.5 Gbps です。

ステップ 9 [Use selected interface as Preferred Path] オプションで、[Enabled] または [Disabled] を選択します。マルチクラウドワークフローは、選択した WAN インターフェイスをデフォルトパスとして設定します。

ステップ 10 [Next] をクリックします。

ステップ 11 [Save and Exit] をクリックします。設定が成功すると、ブランチデバイスが正常に接続されたことを示すメッセージが表示されます。

ステップ 12 デバイスのステータスを確認するには、**show running cofig** コマンドを使用します。

ステップ 13 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

サイトの切断

クラウドゲートウェイからサイトを切り離すには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] > [Cloud Gateways] を選択します。テーブルには、クラウドアカウント名、ID、クラウドタイプ、トランジットゲートウェイとともにクラウドゲートウェイのリストが表示されます。

ステップ 2 目的のクラウドゲートウェイで、[…] をクリックし、[Cloud Gateway] を選択します。

ステップ 3 [Attach SD-Routing] をクリックします。

ステップ 4 [Available Sites] から 1 つ以上のサイトを選択し、[Detach Sites] をクリックします。

[Are you sure you want to detach sites from cloud gateway?] というメッセージがウィンドウに表示されます。

ステップ 5 [OK] をクリックします。

クラウドゲートウェイに接続されているサイトは切り離されます。

ステップ 6 設定のステータスを表示するには、Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] > [Feature Profile] を選択し、[View Details] をクリックします。

ホスト VNet の検出とタグの作成

Azure 仮想ハブを作成したら、仮想ハブのリージョンでホスト VNet を検出できます。ホスト VNet を検出してタグを作成するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。

ステップ 2 [Discover] ワークフローで、[Host Private Networks] をクリックします。

ステップ 3 [Cloud Provider] フィールドで、[Microsoft Azure] を選択します。

ステップ 4 [Tag Actions] ドロップダウンリストをクリックして、次のいずれかを選択します。

ul

- [Add Tag]：VNet または VNet のグループのタグを作成します。
- [Edit Tag]：選択した VNet の既存のタグを変更します。
- [Delete Tag]：選択した VNet のタグを削除します。

VNet タグとブランチネットワーク VRF のマッピング

Cisco Catalyst SD-Routing ネットワークの VNet-VRF マッピングを編集するには、次の手順を実行します。

始める前に

VNet から VRF へのマッピングを有効にするには、1 つまたは複数の Azure リージョンで VNet のセットを選択し、タグを定義します。次に、同じタグを使用して VNet をマッピングするデフォルトの VRF を選択します。1 セットのブランチオフィスには 1 セットの VNet のみをマッピングできます。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。

ステップ 2 [Intent Management] で、[Connectivity] をクリックします。

ステップ 3 インテントを定義するには、[Edit] をクリックします。

ステップ 4 VRF、およびそれに関連付けられている VNet タグに対応するセルを選択し、[Save] をクリックします。

[Intent Management - Connectivity] ウィンドウには、ブランチ VRF とそれらがマッピングされている VNet タグ間の接続ステータスが表示されます。画面の上部には、さまざまなステータスを理解するのに役立つ凡例が表示されます。表示されたマトリックス内のセルのいずれかをクリックすると、[Mapped]、[Unmapped]、[Outstanding] マッピングなど、詳細なステータス情報が表示されます。

VNet の再調整

VNet を再配布して、特定のタグのリージョン内のすべてのクラウドゲートウェイ間で既存の VNet をいつでもロードバランスすることができます。クラウドゲートウェイ全体で [Auto] オプションが選択されている VNet のみを再割り当てできます。VNet の割り当ては、ロード バランシング アルゴリズムに基づいています。再調整にはクラウドゲートウェイへの VNET のデタッチと再アタッチが含まれるため、トラフィックの中断が発生する可能性があります。VNet の再調整後、[tagging] ページで、VNET からクラウドゲートウェイへの修正済みマッピングを表示できます。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。

ステップ 2 [Intent Management] ワークフローで、[Rebalance VNETS (Azure)] をクリックします。

ステップ 3 [Cloud Provider] フィールドで、[Microsoft Azure] を選択します。

ステップ 4 [Region] フィールドで、ドロップダウンリストから [Azure] リージョンを選択します。

（注） Cisco 17.13.1 リリースでは、1 つのリージョンに設定できる VPN ゲートウェイは 1 つだけです。

ステップ 5 [Tag Name] フィールドで、ドロップダウンリストからタグを選択します。

ステップ 6 [Rebalance] をクリックします。

Cisco SD-Routing Cloud OnRamp for Multicloud の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

表 *16 : Cisco SD-Routing Cloud OnRamp for Multicloud* の機能情報

機能名	リリース	機能情報
Cisco SD-Routing Cloud OnRamp for Multicloud	Cisco IOS XE リリース 17.13.1a	Cisco SD-Routing Cloud OnRamp for Multicloud は、エンタープライズ WAN をパブリッククラウドに拡張します。このマルチクラウドソリューションは、パブリック クラウドインフラストラクチャを Cisco Catalyst SD ルーティングデバイスに統合するのに役立ちます。これらの機能により、デバイスはクラウドでホストされているアプリケーションにアクセスできます。

第 15 章

SD ルーティングデバイスでのアプリケーション パフォーマンス モニタリング

この章では、SD ルーティングデバイスでアプリケーションのパフォーマンスをモニターする方法について説明します。ここで説明する内容は、次のとおりです。

SDルーティングデバイスでのアプリケーションパフォーマンス モニタリング

この章では、SD ルーティングデバイスでアプリケーションのパフォーマンスをモニターする方法について説明します。ここで説明する内容は、次のとおりです。

アプリケーション パフォーマンス モニターに関する情報

アプリケーション パフォーマンス モニター機能は、インテントベースのパフォーマンスモニターを設定できる、簡素化されたフレームワークです。この機能を使用すると、クライアントセグメント、ネットワークセグメント、サーバーセグメントでフィルタリングされたエンドツーエンドのアプリケーションパフォーマンスをリアルタイムで表示できます。この情報は、アプリケーションのパフォーマンスを最適化するのに役立ちます。

アプリケーション パフォーマンス モニターは、特定のトラフィックの評価指標を収集するのに使用される、事前定義された設定です。

アプリケーション パフォーマンス モニタリングの主なコンセプト

- **モニタリングプロファイル**：プロファイルは、コンテキストに対して有効または無効にすることができる、事前定義された一連のトラフィックモニターです。この機能の一部として、SD ルーティング パフォーマンス プロファイルに、Cisco Catalyst SD ルーティング インターフェイスを通過するトラフィックをモニタリングするためのアプリケーション応答時間（ART）集約モニターが含まれるようになりました。SD ルーティング パフォーマン

スプロファイルには、インテントに基づいてトラフィックをフィルタリングする専用ポリシーがあります。

- **コンテキスト**：インターフェイスの入力トラフィックと出力トラフィックの両方にアタッチされるパフォーマンス モニター ポリシー マップに相当します。コンテキストには、有効にする必要があるトラフィックモニターに関する情報が含まれます。インターフェイスにコンテキストがアタッチされると、入力トラフィックと出力トラフィックにそれぞれ1つずつ、合計2つのポリシーマップが作成されます。トラフィックモニターで指定されている方向に基づいてポリシーマップがアタッチされると、トラフィックのモニターが開始されます。

アプリケーション パフォーマンス モニターのワークフロー

パフォーマンスモニターは、ダイレクト インターネット アクセス（DIA）インターフェイスでのみ有効にできます。モニタリング対象は、DIAインターフェイスで送受信されるトラフィックのパフォーマンスです。その後、さまざまな show コマンドを使用することで、モニタリングしているアプリケーションの詳細を表示できます。

アプリケーション パフォーマンス モニタリングの前提条件

- Cisco IOS XE Catalyst SD-Routing デバイスの最小ソフトウェアバージョン：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a

制限事項

アプリケーション パフォーマンス モニターの制限事項は次のとおりです。

- アプリケーション パフォーマンス モニターは、SD ルーティングデバイスで ART のみをサポートします。
- このリリースでは、ダイレクト インターネット アクセス（DIA）シナリオのみがサポートされています
- パフォーマンスのモニタリングは、IPv4 トラフィックでのみサポートされます。IPv6 トラフィックはサポートされていません。
- アプリケーション パフォーマンス モニターは、デバイス上のマルチ アプリケーション集約モニターをサポートしていません。
- APM で使用されるクラスマップは、最大 2 つのレイヤクラスマップのみをサポートし、3 つ以上のレイヤクラスマップをサポートしません。
- Cisco SD-WAN Manager では、SD ルーティングデバイスの APM を設定するために、CLI ベースの設定グループのみがサポートされています。

アプリケーション パフォーマンス モニターの設定

DIA インターフェイスでアプリケーション パフォーマンス モニターを有効にし、ART のトラフィック メトリックをモニターできます。

DIA インターフェイスでのパフォーマンスの有効化

次の例は、SD-Routing application-aggregation プロファイルを使用してパフォーマンスモニターのコンテキストを設定する方法を示しています。この設定により、ART トラフィックメトリックのモニタリングが有効になり、特定のインターフェイスに適用されます。

```
class-map match-any APP_PERF_MONITOR_APPS_0
 match protocol attribute application-group amazon-group
 match protocol attribute application-group box-group
 match protocol attribute application-group concur-group
 match protocol attribute application-group dropbox-group
 match protocol attribute application-group google-group
 match protocol attribute application-group gotomeeting-group
 match protocol attribute application-group intuit-group
 match protocol attribute application-group ms-cloud-group
 match protocol attribute application-group oracle-group
 match protocol attribute application-group salesforce-group
 match protocol attribute application-group sugar-crm-group
 match protocol attribute application-group webex-group
 match protocol attribute application-group zendesk-group
 match protocol attribute application-group zoho-crm-group
class-map match-any APP_PERF_MONITOR_FILTERS     --- class-map max 2 layer supported, 3
 or more layer class-map not supported for APM feature
 match class-map APP_PERF_MONITOR_APPS_0
!
```

この設定例では、パフォーマンスモニターのコンテキストを設定する方法を示します。

```
performance monitor context APP_PM_POLICY profile application-aggregation
 exporter destination local-controller source Null0
 traffic-monitor art-aggregated class-and APP_PERF_MONITOR_FILTERS interval-timeout 300
 sampling-interval 100
```

この設定例では、インターフェイスでパフォーマンスモニターのコンテキストを有効にする方法を示します。

```
interface GigabitEthernet1                                                    --- DIA
interface(s)
 performance monitor context APP_PM_POLICY
```

SD ルーティングデバイスでのアプリケーション パフォーマンス モニタリングの設定

設定グループを作成するには、次の手順を実行します。

ステップ 1 [Cisco IOS XE Catalyst SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] > [Add CLI based Configuration Group] の順に選択します。

ステップ 2 [Add CLI based Configuration Group] ポップアップ ダイアログ ボックスで、設定グループ名を入力します。

ステップ 3 [Solution Type] ドロップダウンリストをクリックし、SD ルーティングデバイスのソリューションタイプとして [sd-routing] を選択します。

ステップ 4 [Description] フィールドに機能の説明を入力します

ステップ 5 [Next] をクリックします。

ステップ 6 [Load Running Config from Reachable Device] ドロップダウンリストをクリックし、実行構成を選択するか、テキストボックスに構成 CLI を追加します。

ステップ 7 [Save] をクリックします。

ステップ 8 設定グループ名の横にある [...] をクリックし、[Edit] を選択します

ステップ 9 [Associated Devices] をクリックします。

ステップ 10 1 つ以上のデバイスを選択し、[Deploy] をクリックします

（注） アプリケーション パフォーマンス モニタリングは、パフォーマンス モニター コンテキスト プロファイルおよびフローモニターがインターフェイスに接続されている場合、パフォーマンス モニター コンテキスト プロファイルおよびフローモニターの変更をサポートしません。

ステップ 11 [Configuration] > [Configuration Groups] > [Deploy] をクリックします

ステップ 12 設定グループ名の横にある [...] をクリックし、[Edit] を選択してパフォーマンス モニター コンテキスト プロファイルとフローモニターを変更し、インターフェイスに再接続します。

ステップ 13 [Deploy] をクリックします。

ステップ 14 [Save] をクリックします。

アプリケーション パフォーマンス モニターの確認

SD ルーティングデバイスのアプリケーション パフォーマンス モニターの設定を確認するには、**show performance monitor cache monitor** コマンドを使用します。

```
Device#show performance monitor cache monitor APP_PM_POLICY-art_agg detail format record
Monitor: APP_PM_POLICY-art_agg
Data Collection Monitor:
  CAT-art-aggregated CTX:0 ID:2947958679|2000002 Epoch:0
  Max number of records:             675000
  Current record count:              7
  High Watermark:                    13
  Record added:                      14
  Record aged:                       7
  Record failed to add:              0
  Synchronized timeout (secs):       300


FLOW DIRECTION:                          Output
TIMESTAMP MONITOR START:                 14:10:00.000
FLOW OBSPOINT ID:                        4294967298
INTERFACE OVERLAY SESSION ID OUTPUT:     0
IP VPN ID:                               65535
APPLICATION NAME:                        layer7 share-point
connection server resp counter:          1477
connection to server netw delay sum:     10822  < --- SND_ samples
connection to server netw delay min:     100
connection to server netw delay max:     103
connection to client netw delay sum:     3559 < --- CND_ samples
connection to client netw delay min:     20
connection to client netw delay max:     198
connection application delay sum:        936
connection application delay min:        0
connection application delay max:        122
connection responder retrans packets:    2    <---- lost_samples
connection to server netw jitter mean:   0
connection count new:                    108      < ---- SND/CND_counts
connection server packets counter:       2018     <---- total_samples

Latency(SND  ms) = SND_ samples/ SND/CND_counts
```

```
Latency(CND  ms) = CND_ samples/ SND/CND_counts
Loss ratio = lost_samples /total_samples
```

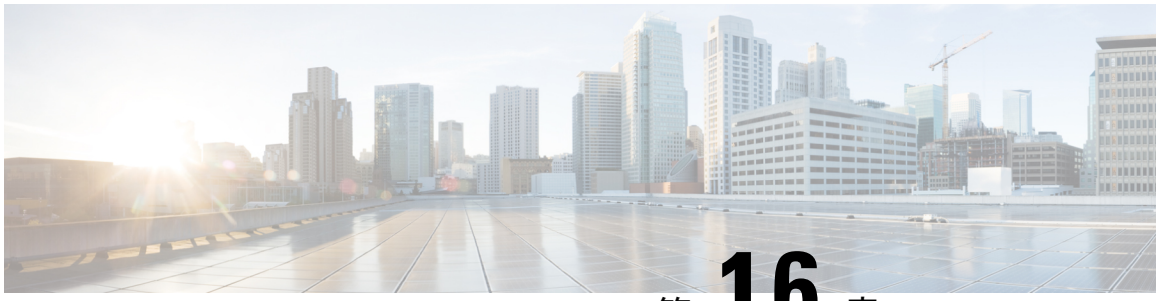
アプリケーション パフォーマンス モニターの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

表 *17*：アプリケーション パフォーマンス モニターの機能情報

機能名	リリース	機能情報
Cisco SD ルーティング アプリケーション パフォーマンス モニター	Cisco IOS XE リリース 17.13.1a	アプリケーション パフォーマンス モニター機能では、インテントベースのパフォーマンスモニターを設定できる、簡素化されたフレームワークが導入されています。このフレームワークを使用すると、クライアントセグメント、ネットワークセグメント、ネットワークセグメントでフィルタリングされたエンドツーエンドのアプリケーション パフォーマンスをリアルタイムで表示できます。



第 16 章

SD ルーティングデバイスでの Flexible NetFlow アプリケーションの可視性

この章では、SD ルーティングデバイスで Flexible NetFlow アプリケーションの可視性を設定する方法について説明します。ここで説明する内容は、次のとおりです。

SD ルーティングデバイスでの Flexible NetFlow アプリケーションの可視性

この章では、SD ルーティングデバイスで Flexible NetFlow アプリケーションの可視性を設定する方法について説明します。ここで説明する内容は、次のとおりです。

Flexible NetFlow アプリケーションの可視性に関する情報

Flexible NetFlow（FNF）は、デバイスを通過するパケットの統計情報を提供します。WAN または LAN インターフェイス上の FNF は、アプリケーション インテリジェンス エンジン（SAIE）を使用して、Cisco SD ルーティングデバイスの WAN または LAN インターフェイスに到達するすべてのトラフィック（入力と出力の両方）を可視化します。アプリケーション インテリジェンス エンジン フローは、基本ヘッダー情報を超えてパケットを調べる機能を提供します。SAIE フローは、特定のパケットの内容を判別し、その情報を統計目的で記録するか、パケットに対してアクションを実行します。

（注） FNF は、WAN または LAN インターフェイスにのみ適用できます。WAN インターフェイスと LAN インターフェイスの両方に適用しないでください。

デバイスで Flexible NetFlow アプリケーションの可視性を有効にするには、次の方法で Cisco SD-WAN Manager を使用してフローデータ集約を有効にする必要があります。

- パフォーマンス モニター コンテキスト プロファイル（推奨される方法）
- フローエクスポータをローカルコントローラへ

（注） 既存の FNF モニターがある場合は、新しいパフォーマンスモニターを追加することによるパフォーマンスへの影響を回避するために、既存の FNF モニターのフローエクスポータとしてフローエクスポータをローカルコントローラに追加します。それ以外の場合は、パフォーマンス モニター コンテキスト プロファイルを使用できます。

SAIE フローを使用した Flexible NetFlow アプリケーションの可視性の前提条件

前提条件は次のとおりです。

- デバイスが Cisco IOS XE 17.13.1a イメージを実行していることを確認します。
- Cisco SD-WAN Manager でフローデータ集約が有効になっていることを確認します。

制限事項

制限事項は次のとおりです。

- Cisco SD-WAN Application Intelligence Engine（SAIE）による集約統計のみがサポートされます。
- オンデマンドのトラブルシューティングはサポートされません。
- コンテキストプロファイルと FNF エクスポータが同じ名前を使用している場合、**show flow exporter name** コマンドはそのうちの 1 つだけを表示します。
- パフォーマンス モニター コンテキスト プロファイルおよびローカルコントローラへのフローエクスポータは、コンテキストプロファイルまたはローカルコントローラへのフローエクスポータのいずれかのみを使用できます。そうでない場合は、パケットをダブルカウントします。

• CLI ベースの設定グループのみがサポートされています。

Flexible NetFlow アプリケーションの可視性の有効化

デバイスのコンテキストプロファイルまたはフローエクスポータを使用して、FNFアプリケーションの可視性を有効にできます。

コンテキスト プロファイル オプション 1 の設定

このオプションを使用することをお勧めします。次に、デバイスでコンテキストプロファイルを使用してフローデータ集約を有効にする例を示します。

```
performance monitor context FNF profile app-visibility
 exporter destination local-controller source Null0
 traffic-monitor app-visibility-stats

interface GigabitEthernet5
 performance monitor context FNF
```

デバイスは、インターフェイスに接続されると、このプロファイルを FNF フローモニターに適用します。

フロー エクスポータ オプション 2 の設定

次に、デバイスでフローエクスポータを使用してフローデータ集約を有効にする例を示します。

```
flow exporter fnf-1
 destination local controller
 export-protocol ipfix
 template data timeout 300
 option interface-table timeout 300
 option vrf-table timeout 300
 option application-table timeout 300
 option application-attributes timeout 300

flow record fnf-app-visiblility
 match routing vrf input
 match interface input
 match interface output
 match application name
 collect counter bytes long
 collect counter packets long

flow monitor fnf-app-visiblility
 exporter fnf-1
 cache timeout inactive 10
 cache timeout active 60
 cache entries 5000
 record fnf-app-visiblility

interface GigabitEthernet5
 ip flow monitor fnf-app-visiblility input
 ip flow monitor fnf-app-visiblility output
 ipv6 flow monitor fnf-app-visiblility input
 ipv6 flow monitor fnf-app-visiblility output
```

Flexible NetFlow アプリケーションの可視性の設定

SD ルーティングデバイスで FNF アプリケーションの可視性を設定するには、次の手順を実行します。

ステップ 1 [Cisco IOS XE Catalyst SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] > [Add CLI based Configuration Group] の順に選択します。

ステップ 2 [Add CLI configuration Group] ポップアップ ダイアログ ボックスで、設定グループ名を入力します。

ステップ 3 [Solution Type] ドロップダウンリストをクリックし、SD ルーティングデバイスのソリューションタイプとして [sd-routing] を選択します。

ステップ 4 [Description] フィールドに機能の説明を入力します

ステップ 5 [Next] をクリックします。

[Feature Profiles] タブと [Associated Device] タブを含む新しい設定グループページが表示されます。

ステップ 6 [Feature Profiles] セクションで、対応する設定を追加します。

ステップ 7 [Save] をクリックして、コンフィギュレーションを保存します。

ステップ 8 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択します

ステップ 9 [Associated Devices] をクリックします。

ステップ 10 1 つ以上のデバイスを選択し、[Deploy] をクリックします

（注） Flexible Netflow は、パフォーマンス モニター コンテキスト プロファイルおよびフローモニターがインターフェイスに接続されている場合、パフォーマンス モニター コンテキスト プロファイルおよびフローモニターの変更をサポートしません。

ステップ 11 [Configuration] > [Configuration Groups] > [Deploy] をクリックします

ステップ 12 設定グループ名の横にある [(…)] をクリックし、[Edit] を選択してパフォーマンス モニター コンテキスト プロファイルとフローモニターを変更し、インターフェイスに再接続します。

ステップ 13 [Deploy] をクリックします。

ステップ 14 [Save] をクリックします。

Cisco SD-WAN Manager を使用した Flexible NetFlow アプリケーションの可視性の確認

FNF アプリケーションの可視性を確認するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択し、リストから SD ルーティングデバイスを選択します。

ステップ 2 左側のペインで、[SAIE Applications] > [Filter] の順に選択します。

ステップ 3 [Filter By] ダイアログボックスで、VPN を選択します。

ステップ 4 [Traffic Source] で、[LAN] または [Remote Access] チェックボックスをオンにします。

ステップ 5 [Search] をクリックして、選択したフィルタに基づいてフローレコードを検索します。

フローレコードが表示されます。

ステップ 6 [Export] をクリックして、フローレコードをローカルシステムにエクスポートします。

ステップ 7 [Reset All] をクリックして、すべての検索フィルタをリセットします。

Flexible NetFlow アプリケーションの可視性の確認

SD ルーティング FNF アプリケーションの可視性を計算するために使用される基本的なネットワークメトリックを確認するには、**show performance monitor context** [profile name] **configuration**、**show platform sofware td-l database content dta fnf-statistics**、および **show performance monitor context fnf traffic monitoring app-visibility-stats cache** コマンドを使用します。

```
Device #show performance monitor context fnf configuration
!================================================================================
! Equivalent Configuration of Context fnf !
!================================================================================
!Exporters
!==========
!
flow exporter fnf-1
description performance monitor context fnf exporter
destination local controller
export-protocol ipfix
template data timeout 300
option interface-table timeout 300 export-spread 0
option vrf-table timeout 300 export-spread 0
option application-table timeout 300 export-spread 0
option application-attributes timeout 300 export-spread 0
!
!Access Lists
!=============
!Class-maps
!===========
!Samplers
!=========
!Records and Monitors
!=====================
!
flow record fnf-app-visiblility-v4
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visiblility-v4
```

```
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
cache timeout active 60
cache entries 5000
record fnf-app-visiblility-v4
!
!
flow record fnf-app-visiblility-v6
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visiblility-v6
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
cache timeout active 60
cache entries 5000
record fnf-app-visiblility-v6
!
!Interface Attachments
!======================
interface GigabitEthernet5
ip flow monitor fnf-app-visiblility-v4 input
ip flow monitor fnf-app-visiblility-v4 output
ipv6 flow monitor fnf-app-visiblility-v6 input
ipv6 flow monitor fnf-app-visiblility-v6 output
```

```
Device# show performance context fnf traffic-monitor app-visibility stats cache
Monitor fnf-app-visibility-v4

Cache  type:                              Normal (platform cache)
Cache  size :                                   10000
Current entries:                                 2
High Watermark:                                  4

Flows added:                                     6
Flows aged:                                      4
 - Inactive timeout           (10sec)            4

IP VRF  ID INPUT  INFE INPUT  INTF OUTPUT  APP Name           bytese long   pkts long
======  ========  ==========  ===========  ================   ============  ==========
1         (1)       Gi3         Gi5        layer7 share-point  1517476       3277
1         (1)       Gi5         Gi3       layer7 share-point  1306568       3463
```

SD ルーティングデバイスでの Flexible NetFlow アプリケーションの可視性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

表 *18 : SD* ルーティングデバイスでの *Flexible NetFlow* アプリケーションの可視性の機能情報

機能名	リリース	機能情報
SD ルーティングデバイスでの Flexible NetFlow アプリケーションの可視性	Cisco IOS XE リリース 17.13.1a	Flexible NetFlow（FNF）の機能は、デバイスを通過するパケットの統計情報を提供し、トンネルまたはサービス VPN の識別に役立ちます。また、SD-Routing Application Intelligence Engine（SAIE）を使用して、Cisco SD ルーティングデバイスの VPN0 を通過するすべてのトラフィックを可視化します。

第 17 章

SDルーティングデバイスでのパケットキャプチャ

この章では、SD ルーティングデバイスでパケットキャプチャを設定する方法について説明します。ここで説明する内容は、次のとおりです。

SD ルーティングデバイスでのパケットキャプチャ

この章では、SD ルーティングデバイスでパケットキャプチャを設定する方法について説明します。ここで説明する内容は、次のとおりです。

パケットキャプチャについて

パケットキャプチャ機能を使用すると、SDルーティングデバイスのトラフィックをキャプチャして分析できます。選択した VRF でターゲットインターフェイスを選択することで、パケットキャプチャを開始できます。また、送信元 IP アドレス、宛先 IP アドレス、レイヤ 4 プロトコル番号などを指定することで、単純なトラフィックフィルタを設定できます。

パケットキャプチャの設定

前提条件

- Cisco IOS XE Catalyst SD-Routing デバイスの最小ソフトウェアバージョン：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1。
- [Administration] > [Settings] ページでデータストリームが有効になっていることを確認します。

制限事項

制限事項は次のとおりです。

- xDSL（ATM/イーサネット インターフェイス）はサポートされていません。
- ダイナミック仮想アクセスインターフェイスは、FlexVPN でのみサポートされます。
- ループバック インターフェイスはサポートされていません
- BDI およびレイヤ 2 EFP/サービス インスタンス インターフェイスはサポートされていません。

パケットキャプチャの設定

パケットキャプチャを設定するには、次の手順を実行します。

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

ステップ 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。

ステップ 3 左ペインで [Troubleshooting] をクリックし、[Packet Capture] をクリックします。

ステップ 4 [VPN] フィールドで、インターフェイスをフィルタリングするための VPN を選択します。

ステップ 5 [Interface corresponding to the VPN] フィールドで、パケットをキャプチャするターゲットインターフェイスを選択します。

ステップ 6 （任意）[Traffic Filters] をクリックして、関連するトラフィックのみをキャプチャするようにフィルタを設定します。これにより、ネットワークの負荷が軽減され、特定のパケットの分析が容易になります。

a) [Source IP] フィールドに、パケットをキャプチャするデバイスの送信元 IP アドレスを入力します。
b) [Destination IP] フィールドに、パケットをキャプチャするデバイスの宛先 IP アドレスを入力します。
c) [Source Port] フィールドに送信元ポート番号を入力します。
d) [Destination Port] フィールドに宛先ポート番号を入力します。

（注） 送信元ポートと宛先ポートは、プロトコルが 6（TCP）または 17（UDP）の場合にのみ適用されます。

e) **トグル**ボタンを使用して**双方向**フィルタを有効にし、送信元 IP トラフィックと宛先 IP トラフィックの両方をフィルタリングします。

ステップ 7 [Start] をクリックします。

Cisco SD-WAN Manager は、指定されたフィルタを使用してパケットのキャプチャを開始します。

ステップ 8 [Force Stop] またはタイムアウトオプションを使用して、パケットキャプチャを停止できます。また、5MB のパケットをキャプチャすると、パケットキャプチャは自動的に停止します。

ステップ 9 [Download] アイコンをクリックして、パケットキャプチャファイルをシステムにダウンロードします。

（注） パケットキャプチャプロセスの実行中は、[Packet Capture] ページを更新したり、ページから移動したりしないでください。

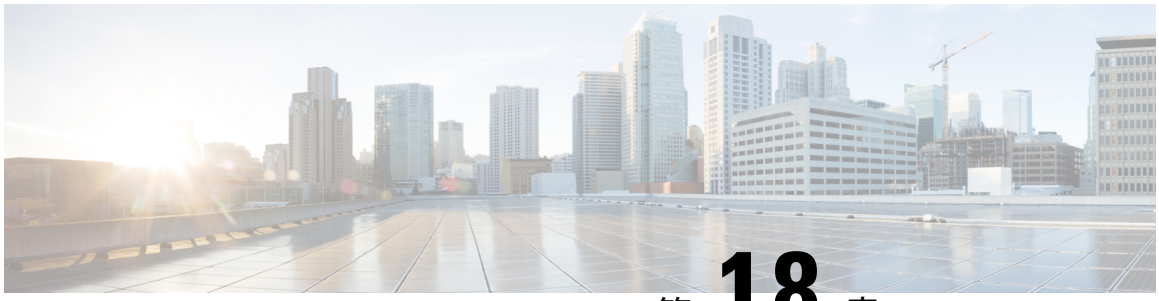
SD ルーティングのパケットキャプチャの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

表 *19 : SD* ルーティングのパケットキャプチャの機能情報

機能名	リリース	機能情報
SD ルーティングのパケットキャプチャ	Cisco IOS XE リリース 17.13.1a	この機能を使用すると、双方向 IPv6 トラフィックデータをキャプチャして SD ルーティングデバイスの接続をトラブルシューティングするオプションを設定できます。



第 18 章

SD ルーティングデバイスでの速度テスト

この章では、SD ルーティングデバイスで速度テストを設定する方法について説明します。ここで説明する内容は、次のとおりです。

SD ルーティングデバイスでの速度テスト

この章では、SD ルーティングデバイスで速度テストを設定する方法について説明します。ここで説明する内容は、次のとおりです。

速度テストに関する情報

インターネット速度テスト：Cisco SD-WAN Manager はネットワーク速度をテストします。Cisco SD-WAN Manager は、デバイスをクライアントサイトとして指定し、iperf3 サーバーをリモートサイトとして指定します。iperf3 サーバーの IP アドレス（またはドメイン名）とポート番号を指定できます。

速度テストでは、送信元デバイスから選択または指定した iperf3 サーバーへのアップロード速度と、iperf3 サーバーから送信元デバイスへのダウンロード速度を測定します。

速度テストの前提条件

速度テストには、ターゲットデバイスのデバイスホスト名が必要です。また、データストリームを有効にする必要があります。データストリームを有効にするには、[Settings] ページに移動し、[Settings] > [Data Stream] を選択します。

インターネット速度テストの実行

速度テストを実行するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから **[Monitor]** > **[Devices]** 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. 次を指定します。
   - [Source Interface]：ドロップダウンリストから、ローカルデバイスの送信元インターフェイスを選択します。
   - [Destination Device]：ドロップダウンリストから [Internet] を選択します。
   - [iPerf3 Server]：（オプション）ドメイン名または iPerf3 サーバーの IP アドレスを IPv4 形式で入力します。
   - [Server Port Range]：（オプション）サーバーポートまたはポート範囲を入力します。たとえば、5201、5210、または 5201 ～ 5205 などです。
6. [Start Test] をクリックします。

   速度テストの結果が表示されます。

速度テストの確認

速度テストが正常に実行されると、[Speed Test] ページに次の詳細が表示されます。

- 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、最近取得した回線速度の結果を報告します。
- アップロード速度を測定する場合、パケットは送信元デバイスから iPerf3 サーバーに送信され、送信元デバイスは宛先から確認応答を受信します。

  ダウンロード速度を測定する場合、パケットは iPerf3 サーバーから送信元デバイスに送信され、宛先デバイスは送信元から確認応答を受信します。

速度テストの問題のトラブルシューティング

次の表に、速度テストのトラブルシューティング情報を示します。

表 *20*: トラブルシューティング シナリオ

エラー情報	考えられる根本的な原因
iperf サーバーアドレスの解決に失敗しました	DNS サーバーがエッジデバイスで設定されていないか、エッジデバイスで設定された DNS サーバーから iperf サーバーを解決できません。
速度テストのサーバーに到達できません	速度テストサーバーの ping に失敗しました。エッジデバイスがサーバー IP に到達できません。
iPerf クライアント：ストリームに接続できません：リソースが一時的に使用できません	速度テストサーバーに接続できません。アクセスは、アクセス制御リスト（ACL）の権限によってブロックされている可能性があります。
iPerf クライアント：サーバーに接続できません	iPerf3 サーバーは、ユーザー指定のポートまたはデフォルトポート 5201 でテストサービスを提供していません。
デバイスエラー：速度テストが進行中です	選択した送信元または宛先デバイスが速度テストを実行しているため、新しいテストを開始できません。
デバイスエラー：サーバー設定の読み取りに失敗しました	データストリーム設定がありません。 回避策：SD ルーティングデバイスで CLI コマンドを実行し、SD ルーティング制御接続をクリアすると、問題を解決できます。
速度テストセッションがタイムアウトになりました	速度テストが 180 秒以内に正常に完了しませんでした。これは、速度テスト中に SD ルーティングデバイスが Cisco SD-WAN Manager への制御接続を失ったためである可能性があります。

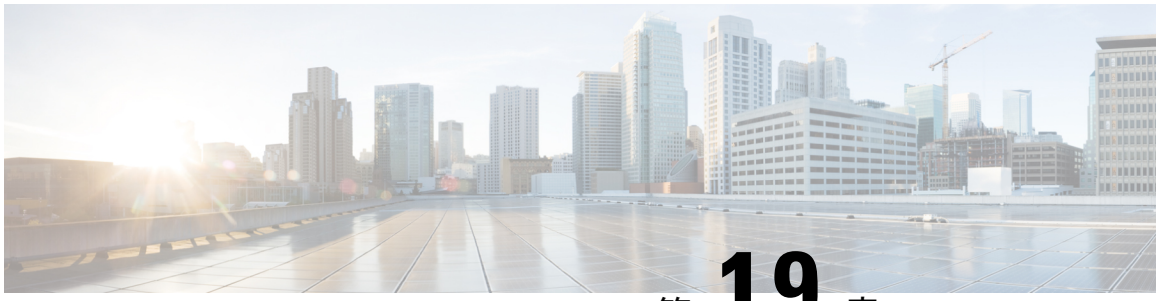
Cisco SD-WAN Manager を使用した SD ルーティングデバイスでの速度テストに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

表 *21 : Cisco SD-WAN Manager* を使用した *SD* ルーティングデバイスでの速度テストに関する機能情報

機能名	リリース情報	説明
速度テスト	Cisco IOS XE 17.13.1	Cisco SD-WAN Manager を使用すると、デバイスと iPerf3 サーバー間のネットワーク速度と使用可能な帯域幅を測定できます。速度テストでは、送信元デバイスから宛先デバイスへのアップロードおよびダウンロードの速度を測定します。



第 19 章

VNF セキュアブートの有効化

セキュアブートは、Unified Extensible Firmware Interface（**UEFI**）標準の一部であり、OEM（Original Equipment Manufacturer）によって信頼されているソフトウェアのみを使用してデバイスを起動します。UEFI（Unified Extensible Firmware Interface）仕様は、受け入れ可能なデジタル署名を持たないソフトウェアのロードを防ぐセキュアブート方法を定義しています。デバイスが起動すると、ファームウェアはブートソフトウェアとオペレーティングシステムの署名をチェックします。署名が有効な場合、デバイスが起動し、ファームウェアがオペレーティングシステムに制御を渡します。

セキュアブート機能は、システムの起動プロセス中に悪意のあるソフトウェアアプリケーションと不正なオペレーティングシステムがシステムにロードされないようにします。セキュアブート機能を有効にすると、許可されたソフトウェアアプリケーションのみがデバイスから起動します。この機能により、デバイス上で起動するソフトウェアアプリケーションがシスコによって認定されていることを確認できます。セキュアなコンピューティングシステムによって、システム上の意図したソフトウェアがマルウェアや改ざんされたソフトウェアを使用せずに実行されるようにします。

システムブートモードとブートローダーのバージョンを表示するには、**show platform software system boot** コマンドを実行します。

```
Router#show platform software system boot
Boot mode: EFI
Bootloader version: 2.0
```

機能制限

- 次のセキュアブート環境がサポートされています。
  - ESXi バージョン 6.5 以上
  - オープンスタックライセンスを使用した KVM RHEL 7.5
  - NFVIS リリース 3.11 以降
- EFI ファームウェアモードのみがセキュアブートをサポートします
- GRUB2 および新しいディスク パーティション レイアウトが使用可能です

（注） 各ハイパーバイザには、ゲスト VM のセキュアブートを可能にする固有のプロセスがあります。セキュアブートを有効にするには、ハイパーバイザ固有のマニュアルを参照してください。

セキュアブートを有効にするためのハイパーバイザ固有の一連の手順を以下におおまかに示します。

ESXi セキュアブートの設定

- VM バージョン 13 以上を使用する ESXi 6. 5 以降のバージョンを使用して VM を作成します。EFI ファームウェアモードを選択するには、[VM Options] > [Boot Options] > [Firmware] > [EFI] の順に移動します。
- 初回起動後、IOS プロンプトが完了したら、VM の電源をオフにします。
- [Edit Settings] > [VM Options] > [Boot Options] > [Secure Boot] で EFI セキュアブートを有効にします。
- VM の電源をオンにすると、VNF が安全に起動します。

重要 VMの作成後にファームウェアモードを（BIOSからEFI、またはその逆に）変更することはできません。

KVM セキュアブートの設定

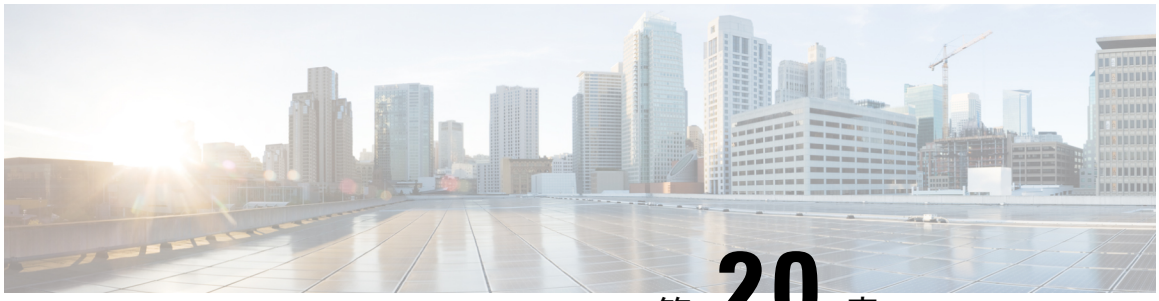
- VM を作成します。
- VM が作成され、VNF IOS プロンプトが完了したら、VM の電源をオフにします。
- [EFI Firmware] メニューから PK、KEK、および db 証明書をインストールし、リセットします。

  カスタムキーを作成するには、セキュアブートのカスタムキーに関する説明を参照してください。db 証明書については、 MicCorUEFCA2011_2011-06-27.crt および MicWinProPCA2011_2011-10-19.crt を参照してください。
- VM をセキュアブートします。

NFVIS セキュアブートの設定

- NFVIS 3.11 リリース以降にアップグレードします。
- Cisco Catalyst 8000V EFI tarball を NFVIS リポジトリに登録します。
- 登録された EFI イメージを使用して VM を作成します。

• VM をセキュアブートします。



第 20 章

コンソールアクセスの設定

Cisco Catalyst 8000V を VM として起動

VM の電源がオンになると Cisco Catalyst 8000V が起動します。設定に応じて、仮想 VGA コンソールまたは仮想シリアルポート上のコンソールでインストールプロセスをモニターできます。

（注） 仮想 VGA コンソールの代わりにハイパーバイザのシリアルポートから Cisco Catalyst 8000V にアクセスして設定する場合は、VM の電源をオンにしてルータを起動する前に、この設定を使用するよう VM をプロビジョニングする必要があります。

ステップ 1 VM の電源を入れます。VM の電源投入後 5 秒以内に、次の 2 つのステップ（ステップ 2 または 3）のいずれかで説明したコンソールを選択し、ルータのブートアップを表示して Cisco Catalyst 8000V CLI にアクセスします。

ステップ 2 （オプション）**Virtual Console** を選択します

仮想コンソールの使用を選択した場合、この手順の残りのステップは適用されません。Cisco Catalyst 8000V は、5 秒以内に他のオプションを選択しない場合、仮想コンソールを使用して起動します。Cisco Catalyst 8000V インスタンスがブートプロセスを開始します。

ステップ 3 （オプション）**Serial Console** を選択します

VM で仮想シリアルポートコンソールを使用するには、このオプションを選択します。

このオプションを機能させるには、仮想シリアルポートが VM にすでに存在している必要があります。

（注） ブートプロセス中にコンソールポートを選択するオプションは、Cisco Catalyst 8000V の初回起動時にのみ使用できます。Cisco Catalyst 8000V の初回起動後にコンソールポートアクセスを変更するには、インストール後のコンソールポートアクセスの変更 （172 ページ）を参照してください。

Cisco Catalyst 8000V がブートプロセスを開始します。

ステップ 4 **telnet://***host-ipaddress***:***portnumber* または **telnet** *host-ipaddress portnumber*（UNIX xTerm 端末から）2 つのコマンドのいずれかを使用して、VM に Telnet 接続します。次の例は、VM での Cisco Catalyst 8000V 初期ブート出力を示しています。

システムは最初に SHA-1 を計算します。これには数分かかる場合があります。SHA-1 が計算されると、カーネルが起動します。初期インストールプロセスが完了すると、.iso パッケージファイルが仮想 CD-ROM から削除され、VM がリブートされます。これにより、Cisco Catalyst 8000V が仮想ハードドライブから正常に起動できるようになります。

（注） システムは、初回インストール時にのみ再起動します。

Cisco Catalyst 8000V の起動に必要な時間は、使用するリリースとハイパーバイザによって異なる場合があります。

ステップ 5 起動後、メインのソフトウェアイメージおよびゴールデンイメージと、強調表示されたエントリを 3 秒以内に自動的に起動する手順を示す画面が表示されます。ゴールデンイメージのオプションを選択せず、メインのソフトウェアイメージを起動させます。

（注） Cisco Catalyst 8000V には、シスコの多くのハードウェアベースのルータに含まれている ROMMON イメージは含まれていません。インストール中、インストールされたバージョンのバックアップコピーがバックアップパーティションに保存されます。このコピーは、ブートイメージをアップグレードした場合、元のブートイメージを削除した場合、または何らかの理由でディスクが破損した場合に、起動元として選択できます。バックアップコピーからの起動は、ROMMON から別のイメージを起動することと同じです。GRUB モードにアクセスするための構成レジスタの設定変更の詳細については、GRUB モードへのアクセス （284 ページ）を参照してください。

これで、標準コマンド **enable**、**configure terminal** の順に入力して、ルータ設定環境を開始できます。

Cisco Catalyst 8000V インスタンスを初めて起動するとき、ルータが起動するモードはリリースバージョンによって異なります。

サポートされているスループットと機能を取得するには、ソフトウェアライセンスをインストールするか、評価ライセンスを有効にする必要があります。リリースバージョンに応じて、ブートレベルを有効にするか、最大スループットレベルを変更して、Cisco Catalyst 8000V を再起動する必要があります。

インストールされているライセンス テクノロジー パッケージは、**license boot level** コマンドで設定されたパッケージレベルと一致している必要があります。ライセンスパッケージが設定と一致しない場合、スループットは 100 Kbps に制限されます。

（VMware ESXi のみ）.iso ファイルを使用して VM を手動で作成した場合は、基本的なルータプロパティを設定する必要があります。Cisco IOS XE CLI コマンドを使用するか、vSphere GUI でプロパティを手動で設定できます。

Cisco Catalyst 8000V コンソールへのアクセス

仮想 VGA コンソールからの Cisco Catalyst 8000V へのアクセス

Cisco Catalyst 8000V ソフトウェアイメージをインストールする場合、使用する設定は仮想 VGA コンソールです。次の場合、仮想 VGA コンソールから Cisco Catalyst 8000V CLI にアクセスするために他の設定を変更する必要はありません。

- 起動プロセス中にコンソール設定を変更しないでください
- VM 設定に 2 つの仮想シリアルポートを追加しないでください。これは、自動コンソール検出を使用している場合に適用されます。

仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセス

仮想シリアルポートを介した Cisco Catalyst 8000V へのアクセスの概要

デフォルトでは、仮想 VGA コンソールを使用して Cisco Catalyst 8000V インスタンスにアクセスできます。自動コンソール検出を使用して、2 つの仮想シリアルポートが検出された場合、Cisco Catalyst 8000V CLI は最初の仮想シリアルポートで使用できます。

シリアルコンソールを使用するように VM を設定することもできます。シリアルコンソールは常に Cisco Catalyst 8000V CLI の最初の仮想シリアルポートの使用を試みます。ハイパーバイザ上に仮想シリアルポートを設定するには、次の項を参照してください。

（注） Citrix XenServer は、シリアルコンソールを介したアクセスをサポートしていません。

VMware ESXi でのシリアルコンソールアクセスの作成

VMware vSphere を使用して次の手順を実行します。詳細については、VMware vSphere のマニュアルを参照してください。

ステップ 1 VM の電源をオフにします。

ステップ 2 VM を選択し、仮想シリアルポートを設定します。

a) [Edit Settings] > [Add] の順に選択します。
b) [Device Type] > [Serial port] の順に選択します。[Next] をクリックします。
c) [Select Port Type] を選択します。
[Connect via Network] を選択し、[Next] をクリックします。

ステップ 3 [Select Network Backing] > [Server (VM listens for connection)] を選択します。

次の構文を使用して [Port URI] を入力します。

telnet://:*portnumber*

ここで、*portnumber* は仮想シリアルポートのポート番号です。

[I/O mode] で、[Yield CPU on poll] オプションを選択し、[Next] をクリックします。

ステップ 4 VM の電源を投入します。

ステップ 5 VM の電源がオンになったら、仮想シリアルポート コンソールにアクセスします。

ステップ 6 仮想シリアルポートのセキュリティ設定を行います。

a) 仮想シリアル ポートの [ESXi host] を選択します。

b) [Configuration] タブをクリックし、[Security Profile] をクリックします。

c) [Firewall] セクションで、[Properties] をクリックし、次に [VM serial port connected over Network] の値を選択します。

これで、Telnet ポート URI を使用して Cisco IOS XE コンソールにアクセスできるようになります。仮想シリアルポートを設定すると、VM の仮想コンソールから Cisco Catalyst 8000V にアクセスすることはできなくなります。

（注） これらの設定を使用するには、Cisco Catalyst 8000V のブートアップ中に GRUB メニューの **Auto Console** オプションまたは **Serial Console** オプションを選択する必要があります。仮想 VGA コンソールを使用して Cisco Catalyst 8000V ソフトウェアをすでにインストールしている場合は、Cisco IOS XE **platform console auto** コマンドまたは Cisco IOS XE **platform console serial command** のいずれかを設定し、仮想シリアルポートを介したコンソールアクセスが機能するように VM をリロードする必要があります。

KVM でのシリアルコンソールアクセスの作成

サーバーの KVM コンソールを使用して、次の手順を実行します。詳細については、KVM のマニュアルを参照してください。

ステップ 1 VM の電源をオフにします。

ステップ 2 デフォルトの [Serial 1] デバイス（存在する場合）をクリックし、[Remove] をクリックします。これにより、最初の仮想シリアルポートとしてカウントされるデフォルトの pty ベースの仮想シリアルポートが削除されます。

ステップ 3 [Add Hardware] をクリックします。

ステップ 4 [Serial] を選択して、シリアルデバイスを追加します。

ステップ 5 [Character Device] で、ドロップダウンメニューから [TCP Net Console (tcp)] デバイスタイプを選択します。

ステップ 6 [Device Parameters] で、ドロップダウンメニューからモードを選択します。

ステップ 7 [Host] で、**0.0.0.0** と入力します。サーバーは、任意のインターフェイスで Telnet 接続を受け入れます。

ステップ 8 ドロップダウンメニューからポートを選択します。

ステップ 9 [Use Telnet] オプションを選択します。

ステップ 10 [Finish] をクリックします。

これで、Telnet ポート URI を使用して Cisco IOS XE コンソールにアクセスできるようになります。詳細については、仮想シリアルポートでの Cisco Catalyst 8000V コンソールへの Telnet セッションの開始（171 ページ）を参照してください。

（注） これらの設定を使用するには、Cisco Catalyst 8000V の起動中に GRUB メニューの **Auto Console** オプションまたは **Serial Console** オプションを選択する必要があります。仮想 VGA コンソールを使用して Cisco Catalyst 8000V ソフトウェアをすでにインストールしている場合は、仮想シリアルポートを介したコンソールアクセスを機能させるために、Cisco IOS XE **platform console auto** コマンドまたは **platform console serial** コマンドを設定し、VM をリロードする必要があります。

仮想シリアルポートでの Cisco Catalyst 8000V コンソールへの Telnet セッションの開始

Cisco IOS XE CLI コマンドを使用して、次の手順を実行します。

ステップ 1 VM に Telnet 接続します。

- 次のコマンドを使用します。**telnet://***host-ipaddress***:***portnumber*
- または、UNIX 端末から次のコマンドを使用します。

  telnet *host-ipaddress portnumber*

ステップ 2 Cisco Catalyst 8000V IOS XE パスワードプロンプトで、ログイン情報を入力します。次に、*mypass* というパスワードを入力する例を示します。

例：

```
User Access Verification
Password: mypass
```

（注） パスワードが設定されていない場合は、**Return** を押します。

ステップ 3 ユーザー EXEC モードで、次のように **enable** コマンドを入力します。

例：

```
Router> enable
```

ステップ 4 パスワード プロンプトに、システム パスワードを入力します。次に、*enablepass* というパスワードを入力する例を示します。

例：

```
Password: enablepass
```

ステップ 5 イネーブルパスワードが許可されると、特権 EXEC モードプロンプトが次のように表示されます。

例：

```
Router#
```

ステップ 6 これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

ステップ 7 Telnet セッションを終了するには、次の例のように **exit** または **logout** コマンドを使用します。

例：

```
Router# logout
```

インストール後のコンソールポートアクセスの変更

Cisco Catalyst 8000V インスタンスが正常に起動したら、Cisco IOS XE コマンドを使用して、ルータへのコンソールポートアクセスを変更できます。コンソールポートアクセスを変更した後は、ルータをリロードするか、電源を再投入する必要があります。

ステップ 1 **enable**

例：

```
Router> enable
```

特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。

ステップ 2 **configure terminal**

例：

```
Router# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 次のいずれかを実行します。

- **platform console virtual**
- **platform console serial**

例：

```
Router(config)# platform console virtual
```

例：

```
Router(config)# platform console serial
```

platform console *x* のオプション：

- **virtual**：ハイパーバイザの仮想 VGA コンソールを介して Cisco Catalyst 8000V にアクセスすることを指定します。

- **serial**：VM のシリアルポートを介して Cisco Catalyst 8000V にアクセスすることを指定します。

Note：このオプションは、ハイパーバイザがシリアル ポート コンソール アクセスをサポートしている場合にのみ使用してください。

ステップ 4 end

例：

```
Router(config)# end
```

コンフィギュレーション モードを終了します。

ステップ 5 copy system:running-config nvram:startup-config

例：

```
Router# copy system:running-config nvram:startup-config
```

実行設定を、NVRAM スタートアップ設定にコピーします。

ステップ 6 reload

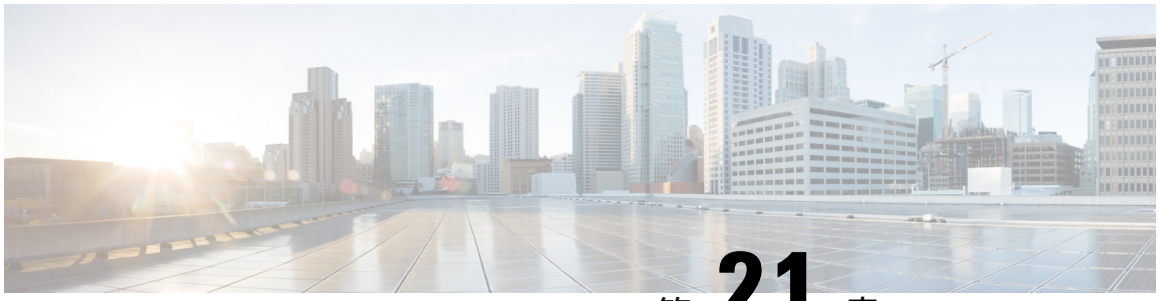
例：

```
Router# reload
```

オペレーティング システムをリロードします。

次のタスク

コンソールアクセスを設定したら、Cisco Catalyst 8000V ライセンスをインストールします。ライセンスをインストールして使用する方法については、このガイドの「ライセンス」の章を参照してください。



第 21 章

ライセンスとライセンスモデル

この章では、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なライセンス、サポートされているスループットのオプション、および使用可能なライセンスとスループットを設定する方法について説明します。また、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なライセンスモデルについても説明します。

（注） この章の情報は、主に自律モードで動作するデバイスに適用されます。比較と完全性を期すために、特定のセクションにはコントローラモードへの参照が含まれています。情報がコントローラモードに適用される場合、その旨が明確に示されています。

シスコのライセンスの詳細については、https://cisco.com/go/licensingguide を参照してください。

この章の主な内容は、次のとおりです。

使用可能なライセンスとライセンスモデルの機能情報

次の表に、Cisco Catalyst 8000 エッジ プラットフォーム ファミリに適用されるライセンス関連の変更の概要を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

表 *22*：使用可能なライセンスとライセンスモデルの機能情報

機能名	リリース	機能情報
自律モードでの Tier 1 および 250 Mbps スループット設定の 500 Mbps 集約	Cisco IOS XE 17.14.1a	仮想プラットフォームでは、250 Mbps または T1 のスループットを設定すると、HSECK9 ライセンスがデバイスで使用可能な場合、スループットは 500 Mbps の送信（Tx）データのみに制限されます。以前のリリースでは、スループットは 200 Mbps Tx に制限されていました。 物理プラットフォームでは、250 Mbps または T1 のスループットを設定すると、HSECK9 ライセンスがデバイスで使用可能な場合、総スループットのスロットリングが有効になります。スループットは 500 Mbps に制限され、アップストリームおよびダウンストリーム方向のトラフィックの分散が許可されます。以前のリリースでは、双方向スループットスロットリングは T1 および 250 Mbps に適用され、スループットは各方向で 250 Mbps に制限されていました。 スロットリング動作のリリースごとの変更（188 ページ）を参照してください。
総スループットのスロットリング - 仮想プラットフォーム	Cisco IOS XE Cupertino 17.9.1a	Cisco Catalyst 8000 エッジ プラットフォーム ファミリの仮想プラットフォームでは、すべてのスループットレベルで、デバイスに双方向スループット値を設定すると、総スループットのスロットリングが有効になります。 この機能拡張は、仮想プラットフォームに常に適用されていたスロットリング動作を変更しません。スロットリングは、送信されるデータ（Tx）にのみ適用されます。受信したデータ（Rx）はスロットリングされません。 スループット （185 ページ）および数値および階層ベースのスループット（185 ページ）を参照してください。

機能名	リリース	機能情報
総スループットのスロットリング - 物理プラットフォーム	Cisco IOS XE Cupertino 17.8.1a	Cisco Catalyst 8000 エッジ プラットフォーム ファミリの物理プラットフォームでは、スループットレベルが 250 Mbps を超え、階層 2 以上の階層で、デバイスに双方向スループット値を設定すると、総スループットのスロットリングが有効になります。これは、アップストリームおよびダウンストリーム方向のトラフィックの分布に関係なく、トラフィックが集約的にスロットルされることを意味します。 双方向スループットは、ライセンス PID で表されます（たとえば、Cisco DNA-C-**500M**-E-3Y および Cisco DNA-C-**T2**-E-3Y）。総スループットは双方向スループットの 2 倍です。 スロットリング動作のリリースごとの変更（188 ページ）を参照してください。
階層ベース ライセンス	Cisco IOS XE Cupertino 17.7.1a	既存の帯域幅ベースの（数値）スループットの設定に加えて、階層ベースのスループット設定のサポートが導入されました。 最も低いスループットレベルから始めて、使用可能な階層は階層 0（T0）、階層 1（T1）、階層 2（T2）、階層 3（T3）です。それぞれの階層はスループットレベルを表します。 製品のライセンス PID が階層ベースの場合、ライセンスは CSSM Web UI の階層値とともに表示されます。 階層ベースのライセンスを持つ製品の場合、階層ベースのスループット値を設定でき、階層ベースのスループット値に変換することもできます。 スループット （185 ページ）および数値および階層ベースのスループット（185 ページ）を参照してください。

機能名	リリース	機能情報
Cisco Digital Network Architecture（Cisco DNA）ライセンス	Cisco IOS XE Amsterdam 17.3.2	Cisco DNA ライセンスのサポートは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで導入されました。 Cisco DNA ライセンスは、ネットワーク スタック ライセンスと DNA スタックアドオンライセンスに分類されます。 Cisco DNA ライセンス （179 ページ）を参照してください。
高セキュリティライセンス（HSECK9）	Cisco IOS XE Amsterdam 17.3.2	HSECK9 ライセンスのサポートは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで導入されました。 高セキュリティライセンス （181 ページ）を参照してください。
Cisco Unified Border Element ライセンス（Cisco UBE ライセンス） Cisco Unified Communications Manager Express ライセンス（Cisco Unified CME ライセンス） Cisco Unified Survivable Remote Site Telephony ライセンス（Cisco Unified SRST ライセンス）	Cisco IOS XE Amsterdam 17.3.2	Cisco UBE、Cisco Unified CME、Cisco Unified SRST ライセンスのサポートは Cisco Catalyst 8000 エッジプラットフォーム ファミリで導入されました Cisco CUBE ライセンス （184 ページ）、Cisco Unified CME ライセンス （184 ページ）、および Cisco Unified SRST ライセンス （184 ページ）を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

入手可能なライセンス

このセクションでは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なすべてのライセンス、使用ガイドライン、および注文に関する考慮事項について説明します。

Cisco DNA ライセンス

Cisco Digital Network Architecture（Cisco DNA）ソフトウェアライセンスは、いくつかの機能固有のライセンスを組み合わせたものです。

（注） Cisco DNA ライセンスには、次を除くすべての機能ライセンスが含まれています。高セキュリティ（HSECK9）、Cisco Unified Border Element（Cisco UBE）、Cisco Unified Communications Manager Express（Cisco Unified CME）、および Cisco Unified Survivable Remote Site Telephony（Cisco Unified SRST）。『Cisco DNA ライセンスの発注時の考慮事項 （180 ページ）』を参照してください。

Cisco DNA ライセンスは、ネットワーク スタック ライセンスと DNA スタックアドオンライセンスに分類されます。

Catalyst 8000V エッジソフトウェア、Catalyst 8200、および 8300 シリーズ エッジ プラットフォームで使用可能な Cisco DNA ライセンス：

ネットワークスタック ライセンス：

- Network Essentials
- Network Advantage：Network Essentials で使用可能な機能などが含まれます。
- Network Premier：Network Essentials、Network Advantage で使用可能な機能などが含まれます。

Cisco DNA スタックアドオンライセンス：

- Cisco DNA Essentials：Network Essentials でのみ使用可能なアドオンライセンス。
- Cisco DNA Advantage：Network Advantage でのみ使用可能なアドオンライセンス。Cisco DNA Essentials で使用可能な機能などが含まれます。
- Cisco DNA Premier：Network Premier でのみ使用可能なアドオンライセンス。Cisco DNA Essentials、Cisco DNA Advantage で使用可能な機能などが含まれます。

Catalyst 8500 シリーズ エッジ プラットフォームで使用可能な Cisco DNA ライセンス：

ネットワークスタック ライセンス：

- Network Advantage
- Network Premier：Network Advantage で使用可能な機能などが含まれます。

Cisco DNA スタックアドオンライセンス：

- Cisco DNA Advantage
- Cisco DNA Premier：Network Premier でのみ使用可能なアドオンライセンス。Cisco DNA Advantage で使用可能な機能などが含まれます。

Cisco DNA ライセンスの使用に関するガイドライン

- Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべてのプラットフォームに適用されるガイドライン：
  - ネットワークスタック ライセンスは恒久的つまり永久ライセンスであり、有効期限はありません。
  - Cisco DNA スタックアドオンライセンスは、サブスクリプションつまり期限付きライセンスであり、特定の日付までのみ有効です。3 年間および 5 年間のオプションは、すべての Cisco DNA スタックアドオンライセンスで使用できます。特定の Cisco DNA スタックアドオンライセンスでは、7 年間のサブスクリプションのオプションを使用できます。
  - Tier 3（T3）以上の階層は、Network Essentials および Cisco DNA Essentials ライセンスではサポートされていません。

    これは、T3 以上の階層をスループットとして設定している場合、ブートレベルライセンスを Network Essentials および Cisco DNA Essentials に変更できないことも意味します。

    Cisco DNA ライセンスで使用可能なさまざまな階層の詳細については、階層および数値のスループットのマッピング （189 ページ）を参照してください。

- Catalyst 8000V エッジソフトウェアにのみ適用されるガイドライン：

  Catalyst 8000V エッジソフトウェアでは、ネットワークスタック ライセンスを設定するときに、対応する Cisco DNA スタックアドオンライセンスも設定する必要があります。

- Catalyst 8200、8300、8500 シリーズ エッジプラットフォームにのみ適用されるガイドライン：
  - 各 ネットワークスタック ライセンスで使用できる Cisco DNA スタックアドオンライセンスはオプションです。Cisco DNA スタックアドオンライセンスなしでネットワークスタック ライセンスを設定できますが、対応するネットワークスタック ライセンスなしで Cisco DNA スタックアドオンライセンスを設定することはできません。
  - Cisco DNA スタックアドオンライセンスを使用する場合は、有効期限が切れる前にライセンスを更新して引き続き使用するか、Cisco DNA スタックアドオンライセンスを非アクティブ化してからデバイスをリロードしてネットワークスタック ライセンス機能での運用を継続します。

Cisco DNA ライセンスの発注時の考慮事項

Cisco DNA ライセンスには、すべてのパフォーマンス、ブースト、およびテクノロジー パッケージ ライセンス（securityk9、uck9、および appxk9）が含まれます。つまり、Cisco DNA ネットワーク スタック ライセンスまたは Cisco DNA スタックアドオンライセンスを注文する際に、パフォーマンス、ブースト、およびテクノロジーパッケージのライセンスが必要であるか適用される場合、注文に自動的に追加されます。

購入するライセンス製品 ID（PID）は、Cisco DNA スタックアドオンライセンス PID のみです。

新しいハードウェアと一緒にCisco DNAライセンスを注文した場合でも、ライセンスはデバイスに事前設定されていません。デバイスでブートレベルライセンスを設定してからスループットを設定する必要があります。

Cisco DNA ライセンスを注文する場合は、スループット値も指定します。注文するスループットが 250 Mbps を超える場合は、Catalyst 8500 および 8500L シリーズ エッジ プラットフォームを除く、Cisco Catalyst 8000 エッジプラットフォーム ファミリのすべてのバリアントでHSECK9ライセンスが必要です。詳細については、高セキュリティライセンス （181 ページ）を参照してください。

階層ベースのスループット値が T1 のライセンス PID を注文すると、HSECK9 ライセンスが自動的に注文に追加されます。

高セキュリティライセンス

高セキュリティライセンス（HSECK9 ライセンス）は輸出規制ライセンスであり、米国の輸出管理法によって制限されています。このライセンスは、完全な暗号化機能、つまり 250 Mbps を超えるスループット、および一定数以上のトンネル数を使用するために必要です（次の表を参照）。この要件は、Catalyst 8500 および 8500L シリーズ エッジ プラットフォームを除く Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべてのデバイスに適用されます。

Catalyst 8500 および 8500L シリーズ エッジ プラットフォームでのみ、スループットとトンネルの規模は、HSECK9 ライセンスが利用できないことによる影響を受けません。これらのプラットフォームでは、HSECK9 ライセンスはコンプライアンスの目的でのみ必要です。Cisco Catalyst 8000 エッジ プラットフォーム ファミリの残りのすべてのモデルでは、HSECK9 ライセンスがない場合、サポートされるトンネル数とスループットが制限されます。次の表に、HSECK9 ライセンスなしでサポートされるトンネル数とサポートされるスループットを示します。

PID	HSECK9 ライセンスなしのトンネルの数	HSECK9 ライセンスなしでサポートされるスループット
C8000V	150	T0、T1
C8200-1N-4T	1000	T0、T1
C8200L-1N-4T	1000	T0、T1
C8300-1N1S-4T2X	1000	T0、T1
C8300-1N1S-6T	1000	T0、T1
C8300-2N2S-4T2X	1000	T0、T1

PID	HSECK9 ライセンスなしのトンネルの数	HSECK9 ライセンスなしでサポートされるスループット
C8300-2N2S-6T	1000	T0、T1
C8500-12X4QC	該当なし	該当なし
C8500-12X	該当なし	該当なし
C8500-20X6C	該当なし	該当なし
C8500L-8S4X	該当なし	該当なし

（注） 「スループット」という用語は、物理プラットフォームで暗号化されたスループットを指します。仮想プラットフォームでは、暗号化されたスループットと非暗号化スループットを組み合わせたものを指します。

HSECK9 ライセンスを使用すると、トンネル数の制限が解除され、250 Mbps を超えるスループットを設定することもできます。使用可能なスループットオプションの詳細については階層および数値のスループットのマッピング （189 ページ）を参照してください。

HSECK9 ライセンスがデバイスで使用されているかどうかを確認するには、特権 EXEC モードで **show license summary** コマンドを入力します。Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべてのデバイスで、HSECK9 ライセンスは次のように表示されます。Router US Export Lic. for DNA (DNA_HSEC)。次に例を示します。

```
Device# show license summary

Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage_T2    (NWSTACK_T2_A)                    1 IN USE
  dna-advantage_T2        (DSTACK_T2_A)                     1 IN USE
  Router US Export Lic... (DNA_HSEC)                        1 IN USE
```

HSECK9 ライセンスの使用に関するガイドライン

HSECK9 ライセンスはシャーシに関連付けられています。そのため、暗号化機能を使用するシャーシ UDI ごとに 1 つの HSECK9 ライセンスが必要です。

HSECK9 ライセンスは、使用前に承認が必要です。この承認は、Smart Licensing Authorization Code（SLAC）によって提供されます。使用する HSECK9 ライセンスごとに SLAC をインストールする必要があります。SLAC は CSSM で生成され、CSSM から取得されます。CSSM か

らSLACを取得する方法は、実装したトポロジによって異なります。詳細については、HSECK9 ライセンス用の SLAC のインストール （203 ページ）を参照してください。

SLAC がインストールされているかどうかを確認するには、特権 EXEC モードで **show license authorization** コマンドを入力します。SLACがインストールされている場合、ステータスフィールドに「SMART AUTHORIZATION INSTALLED on <timestamp>」と表示されます。次に例を示します。

```
Device# show license authorization
Overall status:
  Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
       Status: SMART AUTHORIZATION INSTALLED on Dec 03 08:24:35 2021 UTC
       Last Confirmation code: 418b11b3

Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for DNA based Routers
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

HSECK9 ライセンスの発注時の考慮事項

Catalyst 8000 ハードウェア プラットフォームと同じ注文で Cisco DNA ライセンスを注文した場合、HSECK9 ライセンスを注文するオプションが使用可能であるか、該当する場合は選択されています。たとえば、Catalyst 8500 シリーズ エッジ プラットフォームの場合、ハードウェアを注文すると、HSECK9 ライセンスが自動的に注文に追加されます。これは、これらのプラットフォームでは 250 Mbps を超えるスループットのサポートが開始されるためです。さらに、HSECK9 ライセンスに必要な SLAC もデバイスに工場出荷時にインストールされています。

Catalyst 8000 ハードウェア プラットフォームとは別の注文で Cisco DNA ライセンスを注文する場合、必要に応じて、Catalyst 8000 ハードウェア プラットフォームの注文で HSECK9 ライセンスを別に注文する必要があります。

注文する新しいハードウェアで HSECK9 ライセンスを使用する予定の場合は、スマートアカウントとバーチャルアカウントの情報を注文時に提供します。これにより、シスコは工場出荷時に HSECK9 ライセンスの SLAC をハードウェアにインストールできます。デバイスの使用を開始する前に、デバイスのスループットを設定する必要があります。

（注） HSECK9 ライセンスを（ハードウェアの注文ではなく）個別に注文した場合、SLAC を工場でインストールすることはできません。

Cisco CUBE ライセンス

Cisco Unified Border Element ライセンス（Cisco UBE ライセンス）では、有効にする前にブートレベルを設定する必要はありません。購入後、設定ガイドを参照して、使用可能な Cisco UBE 機能を設定できます。

Cisco UBE ライセンスで使用できる機能については、次の場所にある必要なリリースの『Cisco Unified Border Element Configuration Guide』を参照してください。https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html

サポートされているプラットフォームおよび Cisco UBE ライセンスの購入については、https://www.cisco.com/c/ja_jp/products/collateral/unified-communications/unified-border-element/data-sheet-c78-729692.html のデータシートを参照してください。必要に応じて、Cisco UBE ライセンスを個別に注文する必要があります。他のライセンスには自動的には含まれません。

Cisco UBE ライセンスの使用状況をレポートする方法については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。このライセンスモデルのコンテキストでは、Cisco UBE ライセンスは非強制ライセンスです。

Cisco Unified CME ライセンス

Cisco Unified Communications Manager Express ライセンス（Cisco Unified CME ライセンス）では、有効にする前にブートレベルを設定する必要はありません。購入後、設定ガイドを参照して、使用可能な機能を設定できます。

Cisco Unified CME ライセンスで使用可能な機能については、『Cisco Unified Communications Manager Express System Administrator Guide』を参照してください。

サポートされているプラットフォームおよび Cisco Unified CME ライセンスの購入については、https://www.cisco.com/c/ja_jp/products/collateral/unified-communications/unified-communications-manager-express/datasheet-c78-744069.html のデータシートを参照してください。必要に応じて、Cisco Unified CME ライセンスを個別に注文する必要があります。他のライセンスには自動的には含まれません。

Cisco Unified CME ライセンスの使用状況をレポートする方法については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。このライセンスモデルのコンテキストでは、Cisco Unified CME ライセンスは非強制ライセンスです。

Cisco Unified SRST ライセンス

Cisco Unified Survivable Remote Site Telephony ライセンス（Cisco Unified SRST ライセンス）では、有効にする前にブートレベルを設定する必要はありません。購入後、設定ガイドを参照して、使用可能な Unified SRST 機能を設定できます。

Cisco Unified SRST ライセンスで使用可能な機能については、『Cisco Unified SCCP and SIP SRST System Administrator Guide (All Versions)』を参照してください。

サポートされているプラットフォームおよび Cisco Unified SRST ライセンスの購入については、https://www.cisco.com/c/ja_jp/products/collateral/unified-communications/unified-communications-manager-express/datasheet-c78-744069.html

のデータシートを参照してください。必要に応じて、Cisco Unified SRST ライセンスを個別に注文する必要があります。他のライセンスには自動的には含まれません。

Unified SRST ライセンスの使用状況をレポートする方法については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。このライセンスモデルのコンテキストでは、Unified SRST ライセンスは非強制ライセンスです。

スループット

スループットは、デバイスを介して転送できるデータの量を示します。この値は、自律モードで設定します。その後、設定されたレートでデータが送信（Tx）および受信（Rx）されます。

スループットを明示的に設定しない場合、デフォルトのスループットが有効になります。

デバイスの設定されたスループットを確認するには、該当するコマンドを入力します。

- 物理プラットフォームの場合、**show platform hardware throughput crypto** コマンドを特権 EXEC モードで入力します。
- 仮想プラットフォームの場合、**show platform hardware throughput level** コマンドを特権 EXEC モードで入力します。

次のセクションでは、スループット値の表示方法、デバイスのスループットが暗号化されたスループットと暗号化されていないスループットのどちらを指しているかとその意味、デバイスのスループットに制限を適用するかどうかとその方法について説明します。

数値および階層ベースのスループット

使用できるスループットは、デバイスの Cisco DNA ライセンス製品 ID（PID）で指定されます。これは、数値または階層で表すことができる値です。デバイスにも設定されているのと同じ値です。

数値スループット値

スループットが数値で表される場合、数値スループット値と呼ばれます。たとえば、Cisco DNA-C-**10M**-E-3Y は、10M（= 10 Mbps）の数値スループット値を持つライセンス PID です。

デバイスに応じて、他の使用可能な数値スループット値の例は、15M、25M、50M、100M、250M、500M、1G、2.5G、5G、10G などです。250 Mbps を超えるスループットには、HSECK9 ライセンスが必要です。

階層ベースのスループット値

スループットが階層によって表される場合、階層ベースのスループット値と呼ばれます。階層はスループットレベルを表し、数値スループット値にマッピングされます。たとえば、DNA-C-**T0**-E-3Y は、階層ベースのスループット値 T0 を持つライセンス PID です。これに相当するマッピングされる数値は、最大 25 Mbps のスループットです。

（注） 階層ベースのスループットの設定は、Cisco IOS XE Cupertino 17.7.1a 以降でサポートされます。このリリース以降、階層ベースのスループット設定は、デバイスでスループットを設定する方法としても推奨されます。

最も低いスループットレベルから始めて、使用可能な階層は階層 0（T0）、階層 1（T1）、階層 2（T2）、階層 3（T3）、階層 4（T4）、階層 5（T5）です。T2 以上の階層は、HSECK9 ライセンスが必要です。

階層については、次の点に注意してください。

- すべての階層が、すべての Cisco DNA ライセンスで利用できるわけではありません。

  たとえば、T3 以上の階層は Network Essentials および Cisco DNA-Essentials ライセンスでは使用できません。これは、設定されたスループットとして T3 がある場合、ブートレベルライセンスを Network Essentials および Cisco DNA Essentials に変更できないことも意味します。

- 各階層は、プラットフォームごとに異なる数値にマッピングされるか、異なる数値を意味します。

  Cisco Catalyst 8000 エッジ プラットフォーム ファミリの異なるプラットフォームは、異なる最大スループットレベルをサポートします。たとえば、T2 は、C8300-2N2S-4T2X の場合は 1G スループット、C8200-1N-4T の場合は 500M、C8200L-1N-4T の場合は 250M になります。

特定の Cisco DNA ライセンスで使用可能な階層を確認し、特定のプラットフォームの各階層に相当する数値を調べるには、この章の階層および数値のスループットのマッピング（189 ページ）のセクションを参照してください。

デバイス上で数値スループット値を設定するタイミングと、階層ベースのスループットを設定するタイミングについては、この章の数値と階層ベースのスループットの設定（197 ページ）セクションを参照してください。

暗号化および非暗号化スループット

暗号化スループットは、暗号スループットとも呼ばれ、暗号化アルゴリズムによって保護されるスループットです。

一方、非暗号化スループットはプレーンテキストです。非暗号化スループットは、Cisco Express Forwarding（CEF）トラフィックとも呼ばれます。

重要　物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズエッジプラットフォーム）の場合、このドキュメントでの「スループット」とはすべて、暗号スループットを指します。

仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、このドキュメントでの「スループット」とはすべて、暗号スループットと非暗号化スループットを組み合わせたものを指します。

スロットルされたスループットとスロットルされていないスループット

スロットルされたスループットは、制限が適用されているスループットです（スループット値を設定すると、設定された範囲までデバイスのスループットがスロットルされます）。

スロットルされていないスループットは、制限が適用されないことを意味し、デバイスのスループットはデバイスの最大能力になります。

（注）　仮想プラットフォームでは、スループットがスロットルされている場合、スロットルは送信データにのみ適用されます。受信データは常にスロットルされません。物理プラットフォームでは、スループットがスロットルされている場合、スロットルは送信および受信データに適用されます。

物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズエッジプラットフォーム）では、暗号化されていないスループット（送信および受信）はデフォルトでスロットルされません。

スロットリング動作のタイプ：集約および双方向

システムは、双方向の方法または集約的な方法でスロットリングを適用できます。

双方向スループットスロットリング

ここで、システムは各方向のデータをスロットルします。双方向スロットリングが有効な場合、送信データは双方向スループット値で制限され、受信データは双方向スループット値で個別に制限されます（仮想プラットフォームに常に適用される例外に注意してください。受信データはスロットリングされません）。

たとえば、双方向スループット値が 25 Mbps または T0 で、双方向スループット スロットリングが有効である場合は、次のようになります。

- 仮想プラットフォームでは、送信データの上限は 25 Mbps です。受信データはスロットリングされません。
- 物理プラットフォームでは、Tx データの上限は 25 Mbps、Rx データの上限は 25 Mbps です。

（注） ライセンスPIDに表示される値（数値または階層ベース）は、双方向スループット値を表します。

総スループットのスロットリング

ここで、システムは設定された値を2倍にし、この集約制限でスループットをスロットリングします。総スループットのスロットリングが有効な場合、トラフィックは各方向で個別にスロットリングされません。

たとえば、設定されている双方向スループット値が 500 Mbps で、総スループットのスロットリングが有効である場合は、次のようになります。

- 仮想プラットフォームでは、送信データの上限は 1 Gbps です。受信データはスロットリングされません。
- 物理プラットフォームでは、アップストリームおよびダウンストリーム方向のトラフィックは、1 Gbps の集約制限内の任意の比率にすることができます（たとえば、800 Mbps 送信と 200 Mbps 受信、または 300 Mbps 送信と 700 Mbps 受信）。

スロットリング動作のリリースごとの変更

デバイスのスループットが双方向の方法でスロットリングされるか、集約的な方法でスロットリングされるかを確認するには、デバイスで実行されているソフトウェアバージョンを確認し、以下で説明するスロットリング動作のリリースごとの変更点を参照してください。

- **Cisco IOS XE Cupertino 17.7.x 以前**：双方向のスループットスロットリングのみが有効です。これは、物理プラットフォームと仮想プラットフォームに適用されます。
- **Cisco IOS XE Cupertino 17.8.1a 以降**：
  - 物理プラットフォームでのみ、250 Mbps を超えるスループット値または T2 以上の階層を設定すると、総スループットのトスロットリングが有効になります。

    C8200L-1N-4T では、250 Mbps の数値を設定すると、双方向のスループットスロットリングが有効になり、各方向で最大 250 Mbps を使用できます。ただし、階層 T2 を設定すると、集約スロットリングが有効になり、任意の送信および受信データ比率で 500 Mbps を使用できます。
  - 仮想プラットフォームでは、送信データのスロットリングは引き続き適用され、受信データは引き続きスロットリングされません。
- **Cisco IOS XE Cupertino 17.9.1a 以降**：仮想プラットフォームでは、すべてのスループットレベルとすべての階層で、集約スループットスロットリングが有効です。

（注） 仮想プラットフォームで設定したスループットレベルの集約が 250 Mbps を超える場合、HSECK9 ライセンスがデバイスで使用可能でない限り（つまり、SLAC がインストールされている場合）、総スループットスロットリングは有効になりません。

- **Cisco IOS XE 17.14.1a 以降**：物理および仮想プラットフォームでは、250 Mbps または T1 のスループットを設定すると、HSECK9 ライセンスがデバイスで使用可能である限り、総スループットスロットリングが有効になります。仮想プラットフォームでは、これは送信データのスループットが 500 Mbps に制限されることを意味します。物理プラットフォームでは、これは 500 Mbps の集約制限が任意の送信および受信データの比率で使用できることを意味します。

  HSECK9 ライセンスがデバイスで使用できず、250 Mbps または T1 のスループット値を設定すると、双方向スループットスロットリングが有効になります。仮想プラットフォームでは、これは送信データのスループットが 250 Mbps でスロットリングされることを意味します。物理プラットフォームでは、スループットは各方向で 250 Mbps でスロットリングされます。

階層および数値のスループットのマッピング

次の表に、各階層に相当する数値と、各階層で使用可能な Cisco DNA ライセンスに関する情報を示します。

ヒント マッピング表では、階層に相当する数値のみを明示します。このマッピングは、ユーザーが利用できる最終的なスループットを反映するものではありません。利用できるスループットは、デバイスの機能、デバイスで実行されているソフトウェアバージョン、およびそのバージョンのスロットリング動作によって異なります。

（注） 階層ベースのスループット値が T1 のライセンス PID を購入すると、HSECK9 ライセンスが自動的に提供されます。

Y：Network Premium および Cisco DNA Premium

Y：Network Advantage および Cisco DNA Advantage

Y：Network Essentials および Cisco DNA Essentials

* は HSECK9 ライセンスが必要です。C8500 および C8500L では、HSECK9 ライセンスはコンプライアンス目的でのみ必要です。

表 *23* : 仮想プラットフォームの階層および数値スループットマッピング（*C8000v*）

17.9.1a 以降の階層：	**T0**		**T1**		**T2***			**T3***			**T4***
17.7.x、17.8.x の階層：	**T0**	**T1**			**T2***			**T3***			**T4***
数値マッピング：	**15 M**	**25M**	**50M**	**100M**	**250M**	**500M**	**1G**	**2.5G**	**5G**	**10G**	スロットルなし
使用可能な **Cisco DNA** ライセンス：	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y	Y Y	Y Y	Y Y

表 *24* : 物理プラットフォームの階層および数値スループットマッピング（*C8200*、*C8300*、*C8500*）

17.8.1a 以降の階層：	T0		T1			T2*			T3*			T4*	T5*
17.7.x の階層：	T0		T1			T2*			T3*			該当なし	該当なし
設定された数値：	**10M**	**15 M**	**25M**	**50M**	**100M**	**250M**	**500M**	**1G**	**2.5G**	**5G**	**10G**	**50G**	スロットルなし
C8200-1N-4T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y						
C8200L-1N-4T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y							
C8300-1N1S-4T2X	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y				
C8300-1N1S-6T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y					
C8300-2N2S-4T2X	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y				
C8300-2N2S-6T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y					
C8500-12X									Y Y	Y Y	Y Y		
C8500-12X4QC									Y Y	Y Y	Y Y		
C8500-20X6C												Y Y	Y Y
C8500L-8S4X								Y Y	Y Y	Y Y	Y Y		

自律モードで使用可能なスループットとスロットリングの仕様

これらの表は、利用資格があるスループットを示します。これは、デバイス、スループット値（集約または数値）、およびスロットリングが集約または双方向のどちらで適用されるかを決定するリリースに基づいています。

表 *25 : C8000v*

スループット＝暗号化および非暗号化スループット
受信データはスロットリングされません
* HSECK9 ライセンスが必要です。

サポートされるスループット値（デフォルトは **10M**）	**17.4.1a** 以上で使用可能なスループットとスロットリング	**17.7.1a** 以上で使用可能なスループットとスロットリング	**17.9.1a** 以上で使用可能なスループットとスロットリング	**17.14.1a** 以上で使用可能なスループットとスロットリング
10M	10M Tx のみ	10M Tx のみ	20M Tx のみ	20M Tx のみ
15 M	15M Tx のみ	15M Tx のみ	30M Tx のみ	30M Tx のみ
25M	25M Tx のみ	25M Tx のみ	50M Tx のみ	50M Tx のみ
50M	50M Tx のみ	50M Tx のみ	100M Tx のみ	100M Tx のみ
100M	100M Tx のみ	100M Tx のみ	200M Tx のみ	200M Tx のみ
250M	250M Tx のみ	250M Tx のみ	250M Tx のみ	HSECK9 あり：500M Tx HSECK9 なし：250M Tx
500M*	500M Tx のみ	500M Tx のみ	1G Tx のみ	1G Tx のみ
1G*	1G Tx のみ	1G Tx のみ	2G Tx のみ	2G Tx のみ
2.5G*	2.5G Tx のみ	2.5G Tx のみ	5G Tx のみ	5G Tx のみ
5G*	5G Tx のみ	5G Tx のみ	10G Tx のみ	10G Tx のみ
10G*	10G Tx のみ	10G Tx のみ	20G Tx のみ	20G Tx のみ
T0	-	15M Tx のみ	50M Tx のみ	50M Tx のみ
T1	-	100M Tx のみ	200M Tx のみ	HSECK9 あり：500M Tx HSECK9 なし：250M Tx
T2*	-	1G Tx のみ	2G Tx のみ	2G Tx のみ
T3*	-	10 Tx のみ	20G Tx のみ	20G Tx のみ

T4*	-	スロットルなし	スロットルなし	スロットルなし

表 *26 : C8200-1N-4T*

スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。				
サポートされるスループット値（デフォルトは 10M）	**17.4.1a 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向
15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向
250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
500M*	500M 双方向	500M 双方向	1G 集約	1G 集約
T0	-	15M 双方向	25M 双方向	25M 双方向
T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2	-	500M 双方向	1G 集約	1G 集約

表 *27 : C8200L-1N-4T*

スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。				
サポートされるスループット値（デフォルトは 10M）	**17.5.1a 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向

15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向
250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T0	-	15M 双方向	25M 双方向	25M 双方向
T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2*	-	250M 双方向	500M 集約	500M 集約
-			（注） 17.8.1a 以降、C8200-1N-4T-L では、250 Mbps の数値を設定すると、各方向で最大 250 Mbps を使用できます。ただし、階層ベースの値 T2 を設定する場合（HSECK9 ライセンスが必要）、500 Mbps を任意の送信および受信データ比率で使用できます。	

表 *28 : C8300-1N1S-4T2X、C8300-2N2S-4T2X*

スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。				
サポートされるスループット値 （デフォルトは **10M**）	**17.3.2 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向
15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向

250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
500M*	500M 双方向	500M 双方向	1G 集約	1G 集約
1G*	1G 双方向	1G 双方向	2G 集約	2G 集約
2.5G*	2.5G 双方向	2.5G 双方向	5G 集約	5G 集約
T0	-	15M 双方向	25M 双方向	25M 双方向
T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2*	-	1G 双方向	2G 集約	2G 集約
T3*	-	10G 双方向	20G 集約	20G 集約

表 *29 : C8300-1N1S-6T、C8300-2N2S-6T*

				スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。
サポートされるスループット値（デフォルトは 10M）	**17.3.2 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向
15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向
250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
500M*	500M 双方向	500M 双方向	1G 集約	1G 集約
1G*	1G 双方向	1G 双方向	2G 集約	2G 集約
T0	-	15M 双方向	25M 双方向	25M 双方向

T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2*	-	1G 双方向	2G 集約	2G 集約

表 *30 : C8500-12X、C8500-12X4QC*

スループット = 暗号化されたスループット *HSECK9 ライセンスは、コンプライアンス目的でのみ必要です。			
サポートされるスループット値 **（デフォルトは 10M）**	**17.3.2 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**
2.5G*	2.5G 双方向	2.5G 双方向	5G 集約
5G*	5G 双方向	5G 双方向	10G 集約
10G*	10G 双方向	10G 双方向	20G 集約
T3*	-	10G 双方向	20G 集約

表 *31 : C8500L-8S4X*

スループット = 暗号化されたスループット *HSECK9 ライセンスは、コンプライアンス目的でのみ必要です。			
サポートされるスループット値 **（デフォルトは 10M）**	**17.4.1a 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**
1G*	1G 双方向	1G 双方向	2G 集約
2.5G*	2G 双方向	2G 双方向	5G 集約
5G*	5G 双方向	5G 双方向	10G 集約
10G*	10G 双方向	10G 双方向	20G 集約
T2*	-	1G 双方向	2G 集約
T3*	-	10G 双方向	20G 集約

表 *32 : C8500-20X6C*

スループット = 暗号化されたスループット *HSECK9 ライセンスは、コンプライアンス目的でのみ必要です。	
サポートされるスループット値 （デフォルトは T4）	**17.10.1a 以上で使用可能なスループットとスロットリング**
T4*	50G 集約
T5*	スロットルなし

SD-WAN コントローラモードで使用可能なスループットとスロットリングの仕様

PID	**PID** の導入リリース	**HSECK9** なしのスループット（双方向）	**HSECK9** ありのスループット（**17.3.2** 以上 **17.8.1a** 未満、双方向）	**HSECK9** ありのスループット（**17.8.1a** より後、集約）
C8300-1N1S-4T2X （デフォルトは 250M）	17.3.2	250M	スロットルなし	スロットルなし
C8300-2N2S-6T （デフォルトは 250M）	17.3.2	250M	1G	2G
C8300-1N1S-6T （デフォルトは 250M）	17.3.2	250M	1G	2G
C8300-2N2S-4T2X （デフォルトは 250M）	17.3.2	250M	スロットルなし	スロットルなし
C8200-1N-4T （デフォルトは 250M）	17.4.1a	250M	500M	1G
C8200L-1N-4T （デフォルトは 250M）	17.5.1a	250M	250M	500M
C8500-12X4QC （デフォルトはスロットルなし）	17.3.2	スロットルなし	スロットルなし	スロットルなし

PID	PID の導入リリース	HSECK9 なしのスループット（双方向）	HSECK9 ありのスループット（17.3.2 以上 17.8.1a 未満、双方向）	HSECK9 ありのスループット（17.8.1a より後、集約）
C8500-12X （デフォルトはスロットルなし）	17.3.2	スロットルなし	スロットルなし	スロットルなし
C8500L-8S4X （デフォルトはスロットルなし）	17.4.1a	スロットルなし led	スロットルなし	スロットルなし
C8500-20X6C （デフォルトは T4）	17.10.1a	スロットルなし	-	スロットルなし
C8000v （デフォルトは 250M）	17.4.1a	250M	スロットルなし	スロットルなし

数値と階層ベースのスループットの設定

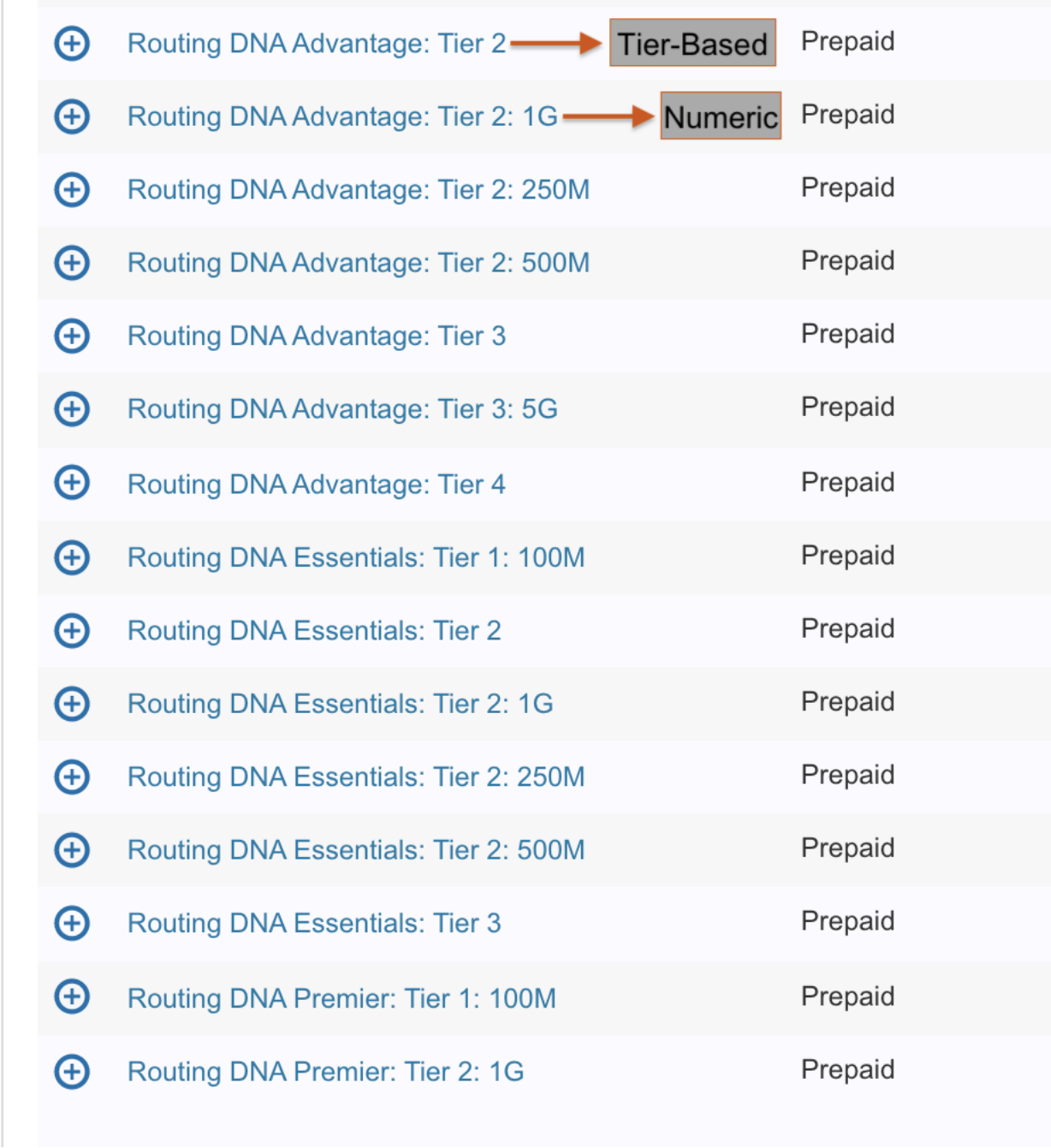
Cisco IOS XE Cupertino 17.7.1a での階層ベースのスループットの設定の導入により、デバイスでスループットを設定する際に、数値と階層ベースの両方のオプションを使用できます。このセクションでは、数値のスループット値を設定するタイミングと、階層ベースのスループットを設定するタイミングについて説明します。

階層ベースまたは数値ライセンスのいずれがあるかの識別

Cisco Smart Software Manager（CSSM）は、すべてのシスコ ソフトウェア ライセンスを管理できるポータルです。購入したすべてのライセンス PID は、CSSM Web UI の https://software.cisco.com → [Manage licenses] に一覧表示されます。階層ベースのライセンスと数値ライセンスのどちらがあるかを識別する方法の 1 つは、CSSM でライセンスがどのように表示されるかを確認することです。

これを行うには、ポータルにログインし、対応するスマートアカウントとバーチャルアカウントで、[Inventory] > [Licences] に移動して、アカウントのライセンスを表示します。次のスクリーンショットは、両方がどのように表示されるかを示しています。

図 *1 : CSSM Web UI* に表示される数値と階層の値



数値または階層ベースのスループット値を設定するかどうかに関する推奨事項

- 数値のライセンス PID を購入した場合、ライセンスは CSSM Web UI に数値のスループット値と階層ベースの値とともに表示されます。このようなライセンスでは、数値のスループット値のみを設定することをお勧めします。

  『数値のスループットの設定 （203 ページ）』を参照してください。

- 階層ベースのライセンス PID を購入した場合、ライセンスは CSSM Web UI に階層の値のみで表示されます。このようなライセンスの場合、CSSM Web UI の表示と一致するように階層ベースのスループット値を設定するか、数値のスループット値を設定できます。

  階層ベースのスループットの設定 （207 ページ）または数値のスループットの設定 （203 ページ）を参照してください。

（注） CSSM に階層ベースのライセンス PID があり、デバイスで数値のスループット値を設定する場合、機能への影響はありません。

設定された値を数値または階層ベースの値に変換するタイミング

次のシナリオでは、数値から階層ベースのスループットの設定に、または階層ベースのスループットの設定から数値に変換できるタイミング、変換が必要なタイミング、および変換がオプションであるタイミングをさらに明確にします。

- デバイスに数値のスループット値を設定し、ライセンス PID が数値のライセンスの場合：階層ベースのスループット値に変換してはなりません。
- デバイスに数値のスループット値を設定し、ライセンス PID が階層ベースのライセンスの場合：スループットの設定を階層ベースの値に変換できますが、これはオプションです。階層ベースのスループット値に変換しない場合、機能への影響はありません。

  階層ベースの値に変換する場合は、数値のスループット値から階層への変換 （212 ページ）を参照してください。
- 階層ベースのスループット値がサポートされているリリースにアップグレードし、ライセンス PID が階層ベースの場合：アップグレード後にスループットを階層ベースの値に変換できますが、これはオプションです。階層ベースのスループット値に変換しない場合、機能への影響はありません。

  『数値のスループットをサポートするリリースから階層をサポートするリリースへのアップグレード （214 ページ）』を参照してください。
- 階層ベースのスループット値がサポートされているリリースにアップグレードし、ライセンス PID が数値である場合：階層ベースのスループット値に変換してはなりません。
- 数値のスループット値のみがサポートされているリリースにダウングレードし、ライセンス PID とスループットの設定が階層ベースである場合：ダウングレードする前に、設定を数値のスループット値に変更する必要があります。

  階層をサポートするリリースから数値のスループットのみをサポートするリリースへのダウングレード （215 ページ）を参照してください。

使用可能なライセンスとスループットの設定方法

このセクションでは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なさまざまなライセンスについて、使用を開始する前にタスクを完了する必要のあるシーケンスについて説明します。

Cisco DNA ライセンスの場合：[Configure a Boot Level License] → [Configure Numeric or Tier-Based Throughput] → [Implement a Smart Licensing Using Policy Topology] → [Report License Usage (If Applicable)]。

HSECK9 ライセンスの場合：[Configure a Boot Level License] → [Implement a Smart Licensing Using Policy Topology] → [Install SLAC] [1] → [Enable HSECK9 on applicable platforms] [2] → [Configure Numeric or Tier-Based Throughput] → [Report License Usage (If Applicable)]。

Cisco UBE、Cisco Unified CME、または Cisco Unified SRST ライセンスの場合：[Implement a Smart Licensing Using Policy Topology] → [Report License Usage (If Applicable)]。

ブートレベルライセンスの設定

新しいデバイス用にCisco DNAライセンスを購入した場合、または既存のデバイスがあり、デバイスに現在設定されているライセンスを変更（アップグレードまたはダウングレード、追加または削除）する場合は、次のタスクを実行します。

これによりライセンスレベルが設定されます。設定された変更を有効にする前にリロードが必要です。

ステップ 1 show version

現在設定されているブートレベルライセンスを表示します。

添付の例では、Network Advantage と Cisco DNA Advantage のライセンスがデバイスに設定されています。

例：

```
Device# show version
<output truncated>
Technology Package License Information:

------------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
------------------------------------------------------------------
Smart License  Perpetual    network-advantage  network-advantage
Smart License  Subscription dna-advantage      dna-advantage

<output truncated>
```

ステップ 2 configure terminal

[1] SLAC がシスコ出荷時にインストールされている場合（新しいハードウェアの場合）、このステップはスキップします

[2] Catalyst 8200 および 8300 シリーズ エッジ プラットフォームだけのグローバル コンフィギュレーション モードで **license feature hseck9** コマンドを入力します。

グローバル コンフィギュレーション モードを開始します。

例：

```
Device# configure terminal
```

ステップ 3 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを設定します。

- 物理プラットフォームの場合：[**no**] **license boot level** {**network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] | **network-premier** [**addon dna-premier**] }
- 仮想プラットフォームの場合：[**no**] **license boot level** {**network-advantage** {**addon dna-advantage**} | **network-essentials** {**addon dna-essentials**} | **network-premier** {**addon dna-premier**} }

ブートレベルライセンスを設定します。

すべてのプラットフォームで、最初にネットワーク スタック ライセンスを設定します。この後にのみ、対応するアドオンライセンスを設定できます。

コマンド構文では、Cisco DNA スタックアドオンライセンスの設定が物理プラットフォームではオプションであり、仮想プラットフォームでは必須であることに注意してください。

添付の例は、物理プラットフォームである C8300-1N1S-4T2X ルータの設定を示しています。ネットワーク スタック ライセンスである Network Premier と、対応するアドオンライセンスである Cisco DNA-Premier が設定されています。

例：

```
Device(config)# license boot level network-premier addon dna-premier
% use 'write' command to make license boot config take effect on next boot
```

ステップ 4 **exit**

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Device# exit
```

ステップ 5 **copy running-config startup-config**

コンフィギュレーション ファイルに設定を保存します。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
<output truncated>
```

ステップ 6 **reload**

デバイスがリロードされます。ステップ 3 で設定されたライセンスレベルは、このリロード後にのみ有効になり、表示されます。

例：

```
Device# reload
Proceed with reload? [confirm]

*Dec  8 01:04:12.287: %SYS-5-RELOAD: Reload requested by console.
```

```
Reload Reason: Reload Command.
<output truncated>
```

ステップ 7 **show version**

現在設定されているブートレベルライセンスを表示します。

添付の例では、出力により、Network Premier および Cisco DNA-Premier ライセンスが設定されていることが確認されます。

例：

```
Device# show version
<output truncated>
Technology Package License Information:

------------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
------------------------------------------------------------------
Smart License  Perpetual    network-premier    network-premier
Smart License  Subscription dna-premier        dna-premier
<output truncated>
```

ステップ 8 **show license summary**

使用されているライセンス、カウント、およびステータスに関する情報を含む、ライセンス使用状況の概要を表示します。

例：

```
Device# show license summary

Account Information:
  Smart Account: Eg-SA As of Dec 08 08:10:33 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-premier_T2      (NWSTACK_T2_P)                    1 IN USE
  dna-premier_T2          (DSTACK_T2_P)                     1 IN USE
```

ステップ 9 完全な使用状況レポート（必要な場合）

ライセンスレベルを設定した後、ライセンス使用情報を報告するために、RUM レポート（リソース使用率測定レポート）を CSSM に送信する必要がある場合があります。レポートが必要かどうかを確認するには、システムメッセージを待つか、show コマンドを使用してポリシーを参照します。

- レポートが必要であることを示すシステムメッセージ：%SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will be required in [dec] days. [dec] は、レポート要件を満たすために残された時間（日数）です。
- show コマンドを使用する場合は、**show license status** 特権 EXEC コマンドの出力を参照し、[Next ACK deadline] フィールドを確認します。これは、この日付までに RUM レポートを送信して CSSM から acknowledgement（ACK）をインストールする必要があることを意味します。

RUM レポートの送信方法は、ポリシーを使用したスマートライセンシング環境で実装したトポロジによって異なります。詳細については、『How to Configure Smart Licensing Using Policy: Workflows by Topology』を参照してください。

HSECK9 ライセンス用の SLAC のインストール

Smart Licensing Authorization Code（SLAC）は、Cisco Smart Software Manager（CSSM）ポータルで生成、取得されます。

製品を CSSM に接続して SLAC を取得する方法はいくつかあります。CSSM に接続する各方法がトポロジと呼ばれます。サポートされているトポロジの 1 つを実装して、対応するメソッドで SLAC をインストールできるようにする必要があります。

すべてのメソッドの詳細については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』ドキュメントの「Supported Topologies」を参照してください。

（注） デバイスにブートレベルライセンスがすでに設定されていることを確認します。ブートレベルライセンスの設定 （200 ページ）を参照してください。show version 特権 EXEC コマンドの出力で、ライセンスが [License Level] フィールドに指定されていることを確認します。

SLAC のインストール後に必要なタスク

SLAC をインストールした後、プラットフォームに該当する場合のみ、次の必要なタスクを完了します。

プラットフォーム	SLAC のインストール後に必要なタスク
Catalyst 8200 および 8300 シリーズエッジプラットフォームの場合	グローバル コンフィギュレーション モードで **license feature hseck9** コマンドを入力します。これにより、これらのプラットフォームで HSECK9 ライセンスが有効になります。
Catalyst 8500 シリーズ エッジ プラットフォームの C8500L モデルの場合	SLAC のインストール後にデバイスをリロードします。

数値のスループットの設定

このタスクでは、物理プラットフォームおよび仮想プラットフォームで数値のスループットレベルを変更する方法を示します。スループットレベルを設定しない場合、プラットフォームのデフォルトのスループットレベルが有効になります。

スループットレベルを設定するには、物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズ エッジ プラットフォーム）でリロードが必要です。仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、リロードは必要ありません。

始める前に

- 数値および階層ベースのスループット（185 ページ）および数値と階層ベースのスループットの設定 （197 ページ）のセクションを参照してください。
- デバイスにブートレベルライセンスがすでに設定されていることを確認します。ライセンスが設定されていないと、スループット値を設定できなくなります。ブートレベルライセンスの設定 （200 ページ）を参照してください。**show version** 特権 EXEC コマンドの出力で、ライセンスが [License Level] フィールドに指定されていることを確認します。
- 250 Mbps を超えるスループットを設定する場合は、このタスクを開始する前に Smart Licensing Authorization Code（SLAC）をインストールする必要があります。HSECK9 ライセンス用の SLAC のインストール （203 ページ）を参照してください。
- `250M`の値は、HSECK9 ライセンスの有無にかかわらず設定できます。システムでは両方が許可されます。違いは、HSECK9 がデバイスで使用可能な場合には集約スロットリングが有効になることです。スロットリング動作のリリースごとの変更 （188 ページ）を参照してください。
- 使用できるスループットに注意してください。これは、購入した Cisco DNA ライセンス PID に示されています。

ステップ 1 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

添付の例：

- **show platform hardware throughput crypto** の出力例は、物理プラットフォーム（C8300-2N2S-4T2X）のものです。ここでは、スループットレベルが 250M にスロットルされています。
- **show platform hardware throughput level** の出力例は、仮想プラットフォーム（C8000V）のものです。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 250M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 250M
Crypto Throughput is throttled at 250M
Default Crypto throughput level: 10M
Current boot level is network-advantage

OR
```

```
Device# show platform hardware throughput level
The current throughput level is 1000000 kb/s
```

ステップ 2 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

例：

```
Device# configure terminal
```

ステップ 3 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを設定します。

- 物理プラットフォームの場合：**platform hardware throughput crypto** {**100M** | **10M** | **15M** | **1G** | **2.5G** | **250M** | **25M** | **500M** | **50M**}
- 仮想プラットフォームの場合：**platform hardware throughput level MB** {**100** | **1000** | **10000** | **15** | **25** | **250** | **2500** | **50** | **500** | **5000**}

スループットレベルを設定します。表示されるスループットオプションは、デバイスによって異なります。

（注） 物理プラットフォームおよび仮想プラットフォームでは、ブートレベルライセンスが設定されていることを確認します。そうしないと、コマンドがコマンドラインインターフェイスで有効なものとして認識されません。

添付の例：

- 物理プラットフォームで 1 Gbps が設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは集約スループットスロットリングが適用されることを意味します。リロード後は、アップストリームとダウンストリームのスループットの合計が 2 Gbps の制限を超えることはありません。
- 仮想プラットフォームで 5000 Mbps が設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは送信データが 5000 Mbps でスロットリングされることを意味します。受信データはスロットリングされません。

例：

```
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
Device(config)# platform hardware throughput crypto 1G
% These values don't take effect until the next reboot.
Please save the configuration.

OR

Device(config)# platform hardware throughput level MB 5000
%Throughput has been set to 5000 Mbps.
```

ステップ 4 **exit**

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Device# exit
```

ステップ 5 **copy running-config startup-config**

コンフィギュレーション ファイルに設定を保存します。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

ステップ 6 **reload**

デバイスがリロードされます。

（注） スループットを設定しているデバイスが物理プラットフォーム上にある場合にのみ、この手順を実行します。

仮想プラットフォームでスループットを設定している場合は、この手順をスキップしてください。

例：

```
Device# reload
```

ステップ 7 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- **物理プラットフォームの場合**：**show platform hardware throughput crypto**
- **仮想プラットフォームの場合**：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

ヒント 物理プラットフォームでは、**show platform hardware qfp active feature ipsec state** 特権 EXEC コマンドを入力して、設定されているスループットレベルを表示することもできます。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 1G
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 2G(Aggregate)
Default Crypto throughput level: 10M

OR

Device# show platform hardware throughput level
The current throughput level is 5000000 kb/s
```

階層ベースのスループットの設定

このタスクでは、物理および仮想プラットフォームで階層ベースのスループットレベルを設定する方法を示します。スループットレベルを設定しない場合、プラットフォームのデフォルトのスループットレベルが有効になります。

階層ベースのスループットレベルは、Cisco IOS XE Cupertino 17.7.1a 以降でのみサポートされます。

スループットレベルを設定するには、物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズ エッジ プラットフォーム）でリロードが必要です。仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、リロードは必要ありません。

始める前に

- 数値および階層ベースのスループット（185ページ）および数値と階層ベースのスループットの設定 （197 ページ）のセクションを参照してください。
- デバイスにブートレベルライセンスがすでに設定されていることを確認します。ライセンスが設定されていないと、スループット値を設定できなくなります。ブートレベルライセンスの設定 （200 ページ）を参照してください。**show version** 特権 EXEC コマンドの出力で、ライセンスが [License Level] フィールドに指定されていることを確認します。
- Tier 2（T2）以上の階層を設定する場合は、このタスクを開始する前に Smart Licensing Authorization Code（SLAC）をインストールする必要があります。HSECK9 ライセンス用の SLAC のインストール （203 ページ）を参照してください。
  - 物理プラットフォームでは、SLACがインストールされていない場合、T2以上の階層は表示されません。
  - 仮想プラットフォームでは、SLAC がインストールされていない場合でも、すべての階層オプションが表示されます。ただし、T2 以上の階層を設定する場合は SLAC が必要です。
- 階層 3（T3）を設定する場合は、ブートレベルライセンスが Network Advantage/Cisco DNA Advantage、または Network Premier/Cisco DNA Premier であることを確認してください。T3 以上の階層は、Network Essentials および Cisco DNA Essentials ではサポートされていません。
- `T1` 値は、HSECK9 ライセンスの有無にかかわらず設定できます。システムでは両方が許可されます。違いは、HSECK9 がデバイスで使用可能な場合には集約スロットリングが有効になることです。スロットリング動作のリリースごとの変更 （188 ページ）を参照してください。
- 使用できるスループットに注意してください。これは、購入した Cisco DNA ライセンス PID に示されています。

ステップ 1 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

添付の例：

- **show platform hardware throughput crypto** の出力例は、物理プラットフォーム（C8300-2N2S-4T2X）のものです。この例ではスループットは現在 250 Mbps にスロットルされています。
- **show platform hardware throughput level** の出力例は、仮想プラットフォーム（C8000V）のものです。この例では現在のスループットレベルは 10 Mbps です。

例：

```
Device# show platform hardware throughput crypto
show platform hardware throughput crypto
Current configured crypto throughput level: 250M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 250M
Crypto Throughput is throttled at 250M
Default Crypto throughput level: 10M
Current boot level is network-premier

OR

Device# show platform hardware throughput level
The current throughput level is 10000 kb/s
```

ステップ 2 show license authorization

（オプション）製品インスタンスの SLAC 情報を表示します。

添付の例：

- SLAC は物理プラットフォームにインストールされています。これは、T2 を設定できるようにするためです。
- SLAC は仮想プラットフォームでは使用できません。これが後続の手順でスループットの設定にどのように影響するかに注意してください。

例：

```
Device# show license authorization
Overall status:
  Active: PID:C8300-2N2S-4T2X,SN:FDO2250A0J5
      Status: SMART AUTHORIZATION INSTALLED on Mar 02 05:05:19 2022 UTC
      Last Confirmation code: 418b11b3

Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for
    DNA based Routers
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
```

```
Purchased Licenses:
  No Purchase Information Available

OR

Device# show license authorization
Overall status:
  Active: PID:C8000V,SN:9I8GRCH8CMN
      Status: NOT INSTALLED
```

ステップ 3 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

例：

```
Device# configure terminal
```

ステップ 4 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを設定します。

- 物理プラットフォームの場合：**platform hardware throughput crypto** {**T0** | **T1** | **T2** | **T3** | **T4** | **T5**}
- 仮想プラットフォームの場合：**platform hardware throughput level MB** {**T0** | **T1** | **T2** | **T3** | **T4** }

階層ベースのスループットを設定します。表示されるスループットオプションは、デバイスによって異なります。

（注） わかりやすくするために、階層のみがコマンドで指定されています。CLI でコマンドを入力すると、添付の例に示すように、数値と階層の値が表示されます。

以下は、物理プラットフォームと仮想プラットフォームの両方に適用されます。

- ブートレベルライセンスはすでに設定されていることを確認します。そうでなければ、スループットの設定のコマンドはコマンド ライン インターフェイスで有効なものとして認識されません。
- T2 以上の階層を設定している場合は、SLAC がインストールされています。

  物理プラットフォームでは、SLAC がインストールされていない場合、T2 以上の階層を設定することはできません。

  仮想プラットフォームで、SLAC なしで T2 以上の階層を設定すると、製品インスタンスは自動的に CSSM にアクセスして SLAC を要求してインストールしようとします。成功した場合、スループットは設定された階層に設定されます。成功しなかった場合、システムはスループットを 250 Mbps に設定します。SLAC がインストールされている場合、スループットは自動的に最後に設定された値に設定されます。

添付の例：

- 物理プラットフォームで 1 Gbps が設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは集約スループットスロットリングが適用されることを意味します。リロード後は、アップストリームとダウンストリームのスループットの合計が 2 Gbps の制限を超えることはありません。
- 仮想プラットフォームで 5000 Mbps が設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは送信データが 5000 Mbps でスロットリングされることを意味します。受信データはスロットリングされません。

- 物理プラットフォーム（**platform hardware throughput crypto**）では、SLAC がインストールされているため、T2 以上の階層が表示されます。SLAC が使用できない場合、表示される最上位の階層は T1 です。

  デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは集約スループットスロットリングが適用されることを意味します。リロード後は、アップストリームとダウンストリームのスループットの合計が 2 Gbps の制限を超えることはありません。

- 仮想プラットフォーム（**platform hardware throughput level MB**）では、すべての階層が表示されます。T2 が設定された後、SLAC がインストールされていないために設定が行われていないことを警告するシステムメッセージが表示されます。

例：

```
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
  T0    T0(up to 15 mbps) bidirectional thput
  T1    T1(up to 100 mbps) bidirectional thput
  T2    T2(up to 2 gbps) aggregate thput
  T3    T3(up to 5 gbps) aggregate thput

Device(config)# platform hardware throughput crypto T2
% These values don't take effect until the next reboot.
Please save the configuration.
*Mar 02 05:06:19.042: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD:
New throughput level not applied until reload; please save config

OR
Device(config)# platform hardware throughput level MB ?
  100    Mbps
  1000   Mbps
  10000  Mbps
  15     Mbps
  25     Mbps
  250    Mbps
  2500   Mbps
  50     Mbps
  500    Mbps
  5000   Mbps
  T0     Tier0(up to 15M throughput)
  T1     Tier1(up to 100M throughput)
  T2     Tier2(up to 1G throughput)
  T3     Tier3(up to 10G throughput)
  T4     Tier4(unthrottled)

Device(config)# platform hardware throughput level MB T2
%Requested throughput will be set once HSEC authorization
code is installed
```

ステップ 5 exit

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Device# exit
```

ステップ 6 **copy running-config startup-config**

コンフィギュレーション ファイルに設定を保存します。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

ステップ 7 **reload**

デバイスがリロードされます。

（注） スループットを設定しているデバイスが物理プラットフォーム上にある場合にのみ、この手順を実行します。

仮想プラットフォームでスループットを設定している場合は、この手順をスキップしてください。

例：

```
Device# reload
```

ステップ 8 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- **物理プラットフォームの場合**：**show platform hardware throughput crypto**
- **仮想プラットフォームの場合**：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

添付の例：

- 物理プラットフォームでは、階層の値は T2 に設定されています。

  ヒント 物理プラットフォームでは、**show platform hardware qfp active feature ipsec state** 特権 EXEC コマンドを入力して、設定されているスループットレベルを表示することもできます。

- 仮想プラットフォームでは、スループットは 250 Mbps に設定されています。SLAC がインストールされている場合、スループットは自動的に最後に設定された値である T2 に設定されます。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: T2
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 2G(Aggregate)
Default Crypto throughput level: 10M
Current boot level is network-premier

OR
```

```
Device# show platform hardware throughput level
The current throughput level is 250000 kb/s
```

数値のスループット値から階層への変換

このタスクでは、数値のスループット値を階層ベースのスループット値に変換する方法を示します。数値のスループット値が階層の値にどのようにマッピングされるかを知るには、階層および数値のスループットのマッピング （189 ページ）の表を参照してください。

スループットレベルを変換するには、物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズ エッジ プラットフォーム）でリロードが必要です。仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、リロードは必要ありません。

始める前に

- 数値と階層ベースのスループットの設定（197ページ）のセクションを参照してください。
- 250 Mbps 以上の数値のスループットを変換する場合は、デバイスに SLAC がインストールされていることを確認してください。HSECK9 ライセンス用の SLAC のインストール（203 ページ）を参照してください。
- このデバイスで実行されているソフトウェアバージョンは、Cisco IOS XE Cupertino 17.7.1 以降のリリースです。

ステップ 1 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスで現在実行されているスループットを表示します。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 500M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 500M
Crypto Throughput is throttled at 500M
Default Crypto throughput level: 10M
Current boot level is network-premier

OR

Device# show platform hardware throughput level
The current throughput level is 100000 kb/s
```

ステップ 2 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**license throughput crypto auto-convert**
- 仮想プラットフォームの場合：**license throughput level auto-convert**

数値のスループットを階層ベースのスループット値に変換します。変換された階層の値は CLI に表示されます。

例：

```
Device# license throughput crypto auto-convert
Crypto throughput auto-convert from level 500M to T2

% These values don't take effect until the next reboot.
Please save the configuration.
*Dec  8 03:21:01.401: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD:
New throughput level
not applied until reload; please save config

OR

Device# license throughput level auto-convert
%Throughput tier set to T1 (100 Mbps)
% Tier conversion is successful.
Please write memory to save the tier config
```

ステップ 3 **copy running-config startup-config**

コンフィギュレーション ファイルに設定を保存します。

（注） 数値から階層ベースのスループットへの変換に使用するコマンドは特権 EXEC コマンドですが、このコマンドは実行コンフィギュレーションを数値から階層ベースの値に変更します。したがって、次のリロードが階層の値とともに表示されるように設定を保存する必要があります。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

ステップ 4 **reload**

デバイスがリロードされます。

（注） リロードは、物理プラットフォームでのみ必要です。

例：

```
Device# reload
Proceed with reload? [confirm]
*Dec  8 03:24:09.534: %SYS-5-RELOAD: Reload requested by console.
Reload Reason:
Reload Command
```

ステップ 5 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスで現在実行されているスループットを表示します。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: T2
```

```
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 1G
Default Crypto throughput level: 10M
Current boot level is network-premier


OR

Device# show platform hardware throughput level
The current throughput level is 100000 kb/s
```

ステップ 6 変換が完了したことを確認します。

- 物理プラットフォームの場合：**license throughput crypto auto-convert**
- 仮想プラットフォームの場合：**license throughput level auto-convert**

ヒント 変換が完了したことをクロスチェックするために、変換コマンドを再度入力することもできます。数値のスループット値がすでに変換されている場合は、変換されていることを確認するメッセージが表示されます。

例：

```
Device# license throughput crypto auto-convert
Crypto throughput is already tier based, no need to convert.

OR

Device# license throughput level auto-convert
% Tier conversion not possible since the device is already
in tier licensing
```

数値のスループットをサポートするリリースから階層をサポートするリリースへのアップグレード

Cisco IOS XE Cupertino 17.7.1 以降のリリースにアップグレードし、さらにライセンス PID が階層ベースの場合、スループットの設定を階層ベースの値に変換するか、数値のスループットの設定を保持できます。

（注） CSSM に階層ベースのライセンス PID があり、デバイスで数値のスループット値が設定されている場合、機能への影響はありません。

階層ベースの値に変換する場合は、設定されているスループットレベルに応じて必要なアクションに注意してください。

アップグレード前のスループットの設定	アップグレード前のアクション	17.7.1 以降へのアップグレード後のアクション
250 Mbps 未満	処置は不要です。	数値のスループット値から階層への変換 （212 ページ）
250 Mbps と等しい	T2 に変換する場合は、HSECK9 ライセンスを取得して SLAC をインストールします。	数値のスループット値から階層への変換 （212 ページ）
250 Mbps より大きい	処置は不要です。	数値のスループット値から階層への変換 （212 ページ）

階層をサポートするリリースから数値のスループットのみをサポートするリリースへのダウングレード

数値のスループットの設定のみがサポートされているリリースにダウングレードする場合は、ダウングレードする前に、階層ベースのスループットの設定を数値のスループット値に変換する必要があります。これは、ライセンス PID が階層ベースのライセンス PID である場合でも適用されます。

⚠

注意 階層ベースのスループット値がダウングレード前に設定されていて、数値に変更せずにダウングレードした場合、階層の設定は 17.7.1 より前のイメージでは認識されず、設定は失敗します。さらに、スループットがダウングレード前のレベルに復元されない場合があり、ダウングレード後に数値のスループットレベルを設定する必要があります。

ダウングレード前のスループットの設定	ダウングレード前のアクション	17.7.1 より前のバージョンにダウングレードした後のアクション
数値	処置は不要です。	処置は不要です。
階層	数値のスループットの設定 （203 ページ）	処置は不要です。

使用可能なライセンスモデル

ライセンスモデルは、使用するライセンスをシスコへどのように説明するか、または報告するかを定義します。Cisco Catalyst 8000 エッジ プラットフォーム ファミリでは、次のライセンスモデルを使用できます。

ポリシーを使用したスマートライセンス

このライセンスモデルでは、使用するライセンスを購入し、デバイスで設定してから、必要に応じてライセンスの使用状況を報告します。輸出規制ライセンスおよび適用ライセンスを使用している場合を除き、ソフトウェアとそれに関連付けられているライセンスの使用を開始する前に、キーの登録や生成などのライセンス固有の操作を完了する必要はありません。

このライセンスモデルは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべての製品でサポートされています。

詳細については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。

ペイアズユーゴー（PAYG）ライセンス

（注） このライセンスモデルは、Catalyst 8000V エッジソフトウェアでのみ使用できます。

Cisco Catalyst 8000V は、自律モードとコントローラモードの両方で、Amazon Web Services（AWS）および Microsoft Azure Marketplace での PAYG ライセンスモデルをサポートします。Cisco Catalyst 8000V 時間課金 Amazon マシンイメージ（AMI）またはペイアズユーゴー ライセンスモデルでは、指定された期間インスタンスを使用できます。

- 自律モードでは、AWS または Azure Marketplace から直接インスタンスを起動して使用を開始できます。ライセンスはイメージに埋め込まれ、インスタンスを起動すると、選択したライセンスパッケージと設定されたスループットレベルが有効になります。
- Cisco IOS-XE Bengaluru 17.5.1 からサポートされるコントローラモードでは、『Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing』に従って、最初にデバイスを Cisco SD-WAN にオンボードする必要があります。この後、AWS からインスタンスを起動すると、無制限のスループットのためにライセンスがすでにインストールされたデバイスが表示されます。

マネージド サービス ライセンス契約

マネージド サービス ライセンス契約（MSLA）は、サービスプロバイダー向けの購入プログラム契約です。

- **Cisco SD-WAN コントローラモードの MSLA**

  Cisco SD-WAN コントローラモードでは、MSLA は Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべての製品でサポートされます。詳細については、以下を参照してください。

  『Managed Service Licensing Agreement (MSLA) for Cisco SD-WAN At-a-Glance』

  『Cisco SD-WAN Getting Started Guide』→「Manage Licenses for Smart Licensing Using Policy」

  『Cisco vManage How-Tos for Cisco IOS XE SD-WAN Devices』→「Manage Licenses for Smart Licensing Using Policy」

- **自律のモードの MSLA**

  自律モードでは、MSLA は Cisco IOS XE Cupertino 17.9.1a 以降の Catalyst 8000V エッジソフトウェアでのみ使用できます。

  詳細については、「MSLA」を参照してください。

第 22 章

Cisco Catalyst 8000V ハードウェアと VM の要件の確認

Cisco Catalyst 8000V の問題をトラブルシューティングしやすくするために、サポートされているハードウェアにルータがインストールされ、次の VM の要件が満たされていることを確認します。

- サーバハードウェアがハイパーバイザベンダーでサポートされていることを確認します。

  VMware を使用している場合、サーバーが VMware ハードウェア互換性リストに含まれていることを確認します。詳細については、VMware のマニュアルを参照してください。

- 使用されている I/O デバイス（FC、iSCSI、SAS など）が VM ベンダーによってサポートされていることを確認します。

- 十分な RAM が VM とハイパーバイザ ホスト用のサーバに割り当てられていることを確認します。

  VMware を使用している場合、サーバーに VM と VMware ESXi の両方をサポートするのに十分な RAM があることを確認します。

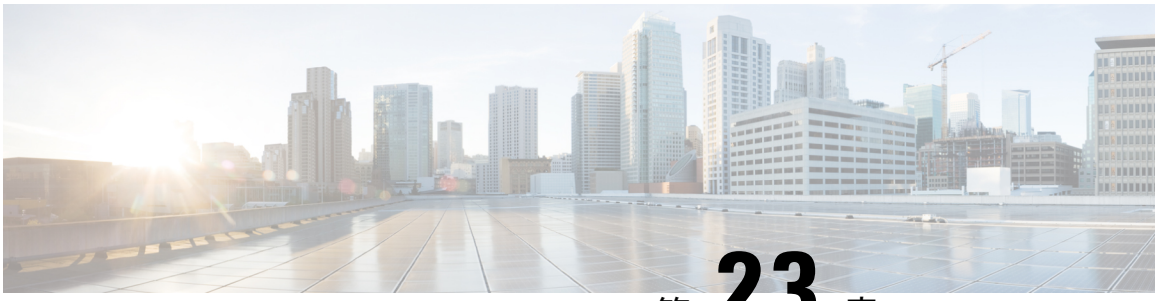
- Cisco Catalyst 8000V でハイパーバイザのバージョンがサポートされていることを確認します。

- メモリの量、CPU の数、およびディスクサイズについて適切に VM が設定されていることを確認します。

- サポートされているネットワーク ドライバを使用して vNIC が設定されていることを確認します。

- Cisco IOS XE 17.6.1 以降、ホストと VM が RDRAND または RDSEED、あるいはその両方の命令をサポートしている場合は、FIPS モードを有効にできます。それ以外の場合は、エラーメッセージが表示されます。

（注） 一部のハイパーバイザには、VM での RDSEED または RDRAND、あるいはその両方の使用をブロックする設定オプションまたはランタイムオプションがあります。これらのオプションは有効にしないでください。つまり、FIPS モードを有効にする場合は、RDSEED または RDRAND、あるいはその両方がハイパーバイザによってブロックされないようにする必要があります。



第 23 章

Cisco IOS XE ソフトウェアのアップグレード

Cisco Catalyst 8000V 仮想ルータは、Cisco CSR1000V または Cisco ISRv と同じプラットフォームである Cisco IOS XE プラットフォームで動作します。Cisco Catalyst 8000V ルータを使用するには、まず Cisco Software Download ページからソフトウェアイメージを取得します。インストールファイルを取得し、インストールまたはアップグレードを開始します。インストールファイルの詳細については、インストール ファイル （9 ページ）を参照してください。

既存の Cisco CSR1000V または Cisco ISRv を使用している場合は、[Cisco Software Download] ページから最新のインストールファイルをダウンロードし、この章で説明する手順に従ってアップグレードプロセスを開始する必要があります。

Cisco Catalyst 8000V のソフトウェアパッケージ

Cisco Catalyst 8000V のソフトウェアイメージは、統合パッケージおよびオプションのサブパッケージとして使用できます。各統合パッケージには、ソフトウェアサブパッケージのコレクションが含まれています。各ソフトウェアサブパッケージは、仮想ルータのさまざまな要素を制御する個別のソフトウェアファイルです。統合パッケージを使用すると、個々のサブパッケージすべてを 1 度のソフトウェアイメージのダウンロードでアップグレードすることができます。

個々のソフトウェアサブパッケージは別々にアップグレードすることができます。あるいは、特定の統合パッケージのソフトウェアサブパッケージすべてを、統合パッケージ全体のアップグレードの一環としてアップグレードすることも可能です。統合パッケージに含まれる個々のサブパッケージを使用してルータを実行する場合は、Cisco.com からイメージをダウンロードし、そのイメージから個々のサブパッケージを抽出します。

サブパッケージを使用したアップグレードは、統合パッケージを使用したアップグレードよりもメモリ消費が少なくなります。このため、特にフットプリントが小さい展開状況では、サブパッケージを使用したアップグレード方法を推奨します。

（注） Cisco ISRv または Cisco CSR1000V を Cisco Catalyst 8000V にアップグレードしても、ファイルシステムのレイアウトは変更されず、ファイルシステムに依存するセキュアオブジェクトストアなどの新機能も一切提供されません。これらの機能を利用するには、新規インストールを実行する必要があります。

重要 既存の Cisco CSR1000V または Cisco ISRV を使用するユーザーが Cisco Catalyst 8000V にアップグレードする場合、ライセンスは現状のまま機能します。ただし、250 Mbps を超えるスループットレベルを実行するには、HSECK9 ライセンスが必須です。アップグレード前に 250 Mbps を超えるスループットレベルを実行していた場合は、アップグレード後にサービスを継続するために HSECK9 ライセンスを購入する必要があります。アップグレード後に HSECK9 ライセンスが使用できない場合、スループットは 250 Mbps に制限されます。Cisco DNA サブスクリプションベースのライセンスモデルに切り替える場合は、新しい Catalyst 8000V 展開を実行する必要があります。

Cisco Catalyst 8000V のアップグレードのための前提条件

- シスコのソフトウェア ダウンロード ページから Cisco Catalyst 8000V ソフトウェアイメージを取得します。インストールファイルの入手方法については、「インストールファイルのダウンロード」を参照してください。
- アップグレードを実行する前に、ハイパーバイザのバージョンを確認します。Cisco Catalyst 8000V で現在使用中の Cisco IOS XE バージョンでハイパーバイザのバージョンがサポートされていない場合、アップグレードは成功しません。
- Cisco Catalyst 8000V ソフトウェアイメージに関する VM のメモリ要件が満たされていることを確認します。アップグレード後のバージョンに以前のバージョンよりも大きなメモリ

が必要になる場合は、アップグレードプロセスを開始する前に、VM に対するメモリの割り当てを引き上げます。

Cisco CSR1000V および Cisco ISRV アップグレードの HSECK9 ライセンス要件

スループットが 250 Mbps を超える Cisco CSR1000V または Cisco ISRV ルータを Cisco Catalyst 8000V（Cisco IOS XE Bengaluru 17.4.1 以降）にアップグレードする場合は、高セキュリティ（HSECK9）ライセンスが必要です。

アップグレード前の構成に応じて、アップグレードする前に、対応する HSECK9 ライセンス要件を満たしていることを確認します。

- Cisco CSR1000V または Cisco ISRV が CSSM に接続されている場合は、次のことを確認する必要があります。
  - 250 Mbps を超えるスループットは、スタートアップ構成の一部です。

    スタートアップ構成を確認するには、特権 EXEC モードで **show running-config** コマンドを入力します。次に例を示します。

    ```
    Device# show running-config | include throughput
    platform hardware throughput level MB 500
    ```

  - CSSM 内の対応するスマートアカウントとバーチャルアカウントで、必要な数の HSECK9 ライセンス（DNA_HSECK9）の残高がプラスになっています。

  アップグレード前のアクションは必要ありません。デバイスが CSSM に接続されている限り、アップグレード時にデバイスは HSECK9 要求を自動的にトリガーし、必要なスマートライセンス認証コード（SLAC）をインストールします。

- Cisco CSR1000V または Cisco ISRV が特定のライセンス予約（SLR）を使用している場合は、SLR 承認コードを更新して HSECK9 ライセンス（DNA_HSECK9）を含めてから、デバイスをアップグレードする必要があります。これにより、アップグレード後もスループットが中断されなくなります。

  この例では、SLR 承認コードを更新する方法を示します。Example: Smart Licensing (SLR With Throughput >250 Mbps, Without Export-Controlled License) to Smart Licensing Using Policy。

スループットが 250 Mbps 以下の場合、HSECK9 ライセンスのインストールは必要ありません。

Cisco Catalyst 8000V のアップグレードの制約事項

- 新しいソフトウェアバージョンへのアップグレードは、同じ VM 上でのみ実行できます。この手順では、別の VM で同じまたはアップグレードされたソフトウェアバージョンを実

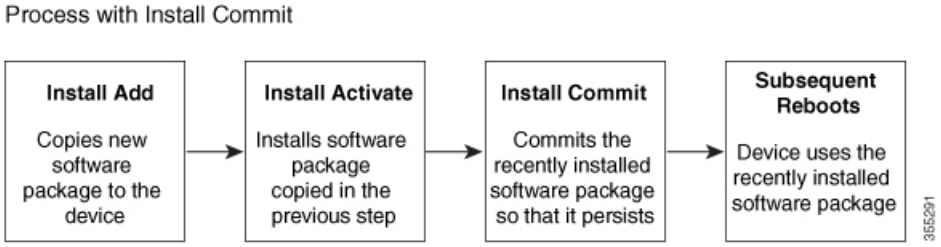
行している既存のルータをインストールまたは再ホストする方法については説明していません。

- .binファイルは、ソフトウェアのアップグレードまたはダウングレードに適用されます。.isoファイル、qcow2 ファイル、および .ova ファイルは、初回インストールのみに使用します。
- Cisco Catalyst 8000V にアップグレードする場合、ライセンスは現状のまま機能します。ただし、CDNA ライセンスモデルに切り替える場合は、新規インストールを実行する必要があります。
- Cisco Catalyst 8000V ルータは、In-Service Software Upgrade（ISSU）をサポートしていません。
- x86 ハードウェアのシステム要件は、ルータで現在実行されているハードウェアの要件と異なる場合があります。
- Cisco CSR1000V または Cisco ISRv からのアップグレードの場合、ディスクパーティション構造は以前のバージョンと同じままであり、セキュア オブジェクト ストレージ機能は使用できません。
- 16.12.x より前の Cisco CSR1000V または Cisco ISRv から Cisco Catalyst 8000V にアップグレードする場合は、まず現在のバージョンから 16.12.x にアップグレードします。その後、Cisco Catalyst 8000V の最新バージョンにアップグレードしてください。
- Cisco Catalyst 8000V は PCI パススルーをサポートしていないため、PCI パススルーを実行している Cisco CSR1000V を Cisco Catalyst 8000V にアップグレードすることはできません。
- Cisco Catalyst 8000V を新しくインストールした場合、Cisco ISRv または Cisco CSR1000V にダウングレードすることはできません。以前に保有していた Cisco CSR1000V を Cisco Catalyst 8000V にアップグレードした場合、Cisco CSR1000V にダウングレードできますが、Cisco ISRv にダウングレードすることはできません。
- Cisco CSR1000V から Cisco Catalyst 8000V にアップグレードする場合、または Cisco Catalyst 8000V の下位バージョンから上位バージョンにアップグレードする場合は、N-2 または N-1 から N へのリリースアップグレードパスのみがサポートされます。ここで、N-1 および N-2 は拡張メンテナンスリリースを指します。たとえば、CSR1000V 17.3.x インスタンスを Cisco Catalyst 8000V 17.11.1a リリースにアップグレードする場合、17.6.x は更新する必要がある最も低い N-x バージョンです。
- Cisco Catalyst 8000V は、L2TP クライアントや L2TP ネットワークサーバー（LNS）を含む L2TP 機能をサポートしていません。

インストールモードのプロセスフロー

インストールモードのプロセスフローは、Cisco Catalyst 8000V のインストールとアップグレードを実行するための 3 つのコマンド（**install add**、**install activate**、**install commit**）で構成されています。

次のフローチャートは、インストールコマンドを使用したインストールプロセスを説明しています。



install add コマンドは、ソフトウェアパッケージをローカルまたはリモートの場所からプラットフォームにコピーします。FTP、HTTP、HTTPs、または TFTP を使用できます。このコマンドは、.package ファイルの個々のコンポーネントをサブパッケージと packages.conf ファイルに展開します。またファイルを検証して、イメージファイルが Cisco Catalyst 8000V に固有であることを確認します。

install activate コマンドは、必要な検証を実行し、**install add** コマンドを使用して以前に追加されたパッケージをプロビジョニングします。また、システムのリロードをトリガーします。

install commit コマンドは、**install activate** コマンドを使用して以前にアクティブ化されたパッケージを確認し、リロード後も更新が持続されるようにします。

（注） 更新をインストールすると、以前にインストールしたソフトウェアイメージが置換されます。インスタンスには、常に 1 つのイメージのみをインストールできます。

次の表に、Cisco IOS XE プラットフォームをインストールまたはアップグレードするときに使用するコマンドのリストを示します。

表 *33 :* インストールコマンド一覧

コマンド	構文	目的
install add	**install add file** *location:filename.bin*	イメージおよびパッケージの内容をソフトウェアリポジトリにコピーします。ファイルの場所はローカルでもリモートでもかまいません。このコマンドは次のことを行います。 • ファイルのチェックサム、プラットフォームの互換性チェックなどを検証します。 • パッケージの個々のコンポーネントをサブパッケージと packages.conf に展開します。 • イメージをローカルインベントリにコピーし、次の手順で使用できるようにします。
install activate	**install activate**	**install add** コマンドを使用して追加されたパッケージをアクティブ化します。 • **show install summary** コマンドを使用して、非アクティブなイメージを確認します。 • このコマンドを実行すると、システムがリロードされます。アクティベーションを続行するかどうかを確認します。確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。

コマンド	構文	目的
(install activate) auto abort-timer	**install activate auto-abort timer** *<30-1200>*	**auto-abort timer** は自動的に開始され、デフォルト値は 120 分です。指定された時間内に **install commit** コマンドが実行されない場合、アクティベーションプロセスは中止され、システムは最後にコミットされた状態に戻ります。 • **install activate** コマンドを実行しながらタイマーの値を変更できます。 • **install commit** コマンドはタイマーを停止し、インストールプロセスを続行します。 • **install activate auto-abort timer stop** コマンドは、パッケージをコミットせずにタイマーを停止します。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。 • このコマンドは、3 ステップインストールのバリアントでのみ有効です。
install commit	**install commit**	**install activate** コマンドを使用してアクティブ化されたパッケージをコミットし、リロード後も持続するようにします。 • **show install summary** コマンドを使用して、コミットされていないイメージを確認します。

コマンド	構文	目的
install abort	**install abort**	インストールを中止し、システムを最後にコミットされた状態に戻します。 • このコマンドは、パッケージがアクティブ化された状態（コミットされていない状態）の場合にのみ適用されます。 • **install commit** コマンドを使用してイメージをすでにコミットしている場合は、**install rollback to** コマンドを使用して望みのバージョンに戻ります。
install remove	**install remove {file** <*filename*> **| inactive}**	プラットフォームリポジトリから非アクティブなパッケージを削除します。このコマンドを使用して、スペースを解放します。 • **file**：指定されたファイルを削除します。 • **inactive**：非アクティブなファイルをすべて削除します。

コマンド	構文	目的
install rollback to	**install rollback to {base | label | committed | id}**	保存されているインストールポイントか、最後にコミットされたインストールポイントに、ソフトウェアセットをロールバックします。このコマンドには次のような特長があります。 • リロードが必要です。 • パッケージがコミットされた状態の場合にのみ適用されます。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。 （注） 以前のイメージへのインストールのロールバックを実行する場合は、以前のイメージはインストールモードでインストールされている必要があります。

上記のコマンドとは別に、次の show コマンドを使用してインストールまたはアップグレードを確認することもできます。

表 *34 : show* コマンドの一覧

コマンド	構文	目的
show install log	**show install log**	プラットフォームがブートされた後に実行されたすべてのインストール操作の履歴と詳細を提供します。
show install package	**show install package** <*filename*>	指定された .pkg/.bin ファイルに関する詳細を提供します。
show install summary	**show install summary**	イメージバージョンとそれに対応するインストール状態の概要を提供します。

コマンド	構文	目的
show install active	**show install active**	アクティブなパッケージに関する情報を提供します。
show install inactive	**show install inactive**	非アクティブなパッケージがある場合は、そのパッケージに関する情報を提供します。
show install committed	**show install committed**	コミットされたパッケージに関する情報を提供します。
show install uncommitted	**show install uncommitted**	コミットされていないパッケージがある場合は、そのパッケージに関する情報を提供します。
show install rollback	**show install rollback {point-id | label}**	保存されているインストールポイントに関連付けられたパッケージを表示します。
show version	**show version [rp-slot] [installed [user-interface] | provisioned | running]**	プラットフォームの情報とともに、現在のパッケージに関する情報を表示します。

Cisco Catalyst 8000V をインストールモードで起動する場合

単一のコマンド（1 ステップインストール手順）または複数の個別のコマンド（3 ステップインストール手順）を使用してソフトウェアパッケージをインストールして、アクティブ化し、コミットできます。

Cisco Catalyst 8000V デバイスがバンドルモードで動作している場合、1 ステップインストールの手順を使用して、最初にバンドルモードからインストールモードに変換する必要があります。その後、1 ステップまたは 3 ステップのインストール方法を使用して、後続のインストールとアップグレードを実行できます。

1 ステップインストールまたはバンドルモードからインストールモードへの変換

この手順では、特権 EXEC モードで **install add file activate commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

1 ステップインストールの手順は、バンドルブートモードで実行されているプラットフォームをインストールモードに変換します。コマンドの実行後、プラットフォームはインストールブートモードでリブートします。

（注）
- すべての CLI アクション（追加、アクティブ化など）が実行されます。
- 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
- このワークフローの 2 番目のステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。
- プロンプトレベルが [None] に設定されていて、保存されていない設定がある場合、インストールは失敗します。コマンドを再発行する前に、設定を保存する必要があります。

手順の概要

1. **enable**
2. **install add file location:** *filename* [**activate commit**]
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**install add file location:** *filename* [**activate commit**] 例： `Device# install add file bootflash:c8000v-universalk9.BLD_POLARIS_DEV_LATEST_20220227_153436.SSA.bin activate commit`	ソフトウェア インストール パッケージをローカルまたはリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよびpackages.confファイルに展開します。プラットフォームおよびイメージバージョンの検証および互換性チェックを実行し、パッケージをアクティブ化し、そのパッケージをコミットして複数回リロードしても維持されるようにします。 このコマンドを実行すると、プラットフォームがリロードされます。
ステップ 3	**exit** 例： `Device# exit`	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

3 ステップインストール

3 ステップインストールの手順では、個別の **install add**、**install activate**、および **install commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

（注）
- この手順は、プラットフォームがインストールモードになった後にのみ実行できます。
- すべての CLI アクション（追加、アクティブ化など）が実行されます。
- 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
- このワークフローの install activate ステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。

手順の概要

1. **enable**
2. **install add file location:** *filename*
3. **show install summary**
4. **install activate** [**auto-abort-timer** <*time*>]
5. **install abort**
6. **install commit**
7. **install rollback to committed**
8. **install remove** {**file** *filesystem: filename* | **inactive**}
9. **show install summary**
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**install add file location:** *filename* 例： `Device# install add file bootflash:c8000v-universalk9.BLD_POLARIS_DEV_LATEST_20220227_153436.SSA.bin`	ソフトウェア インストール パッケージをリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに展開します。
ステップ 3	**show install summary** 例： `Device# show install summary`	（オプション）イメージバージョンとそれに対応するインストール状態の概要を提供します。

	コマンドまたはアクション	目的
ステップ 4	**install activate** [**auto-abort-timer** <*time*>] 例： `Device# install activate auto-abort-timer 120`	以前に追加されたパッケージをアクティブ化し、プラットフォームをリロードします。 • ソフトウェアの完全インストールを実行する場合は、パッケージファイル名を指定しないでください。 • **install activate** コマンドで **auto-abort-timer** が自動的に開始されます。タイマーのデフォルトは 120 分です。タイマーの期限が切れる前に **install commit** コマンドが実行されない場合、インストールプロセスは自動的に終了します。プラットフォームがリロードされ、最後にコミットされたバージョンで起動します。
ステップ 5	**install abort** 例： `Device# install abort`	（オプション）ソフトウェアインストールのアクティブ化を中止し、プラットフォームを最後にコミットされたバージョンに戻します。 このコマンドは、イメージがアクティブ化されている状態でのみ使用できます。イメージがコミットされた状態の場合は使用できません。
ステップ 6	**install commit** 例： `Device# install commit`	新しいパッケージのインストールをコミットし、リロード後も変更が持続されるようにします。
ステップ 7	**install rollback to committed** 例： `Device# install rollback to committed`	（オプション）最後にコミットした状態にプラットフォームをロールバックします。
ステップ 8	**install remove** {**file** *filesystem: filename* | **inactive**} 例： `Device# install remove inactive`	（オプション）ソフトウェア インストール ファイルを削除します。 • **file**：特定のファイルを削除します。 • **inactive**：未使用および非アクティブ状態のインストールファイルを削除します。
ステップ 9	**show install summary** 例： `Device# show install summary`	（オプション）現在のシステムの状態に関する情報を表示します。このコマンドの出力は、このコマンドよりも先に実行された **install** コマンドに応じて変化します。
ステップ 10	**exit** 例：	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device# exit	

リリース 17.06.02 からリリース 17.07.01 へのアップグレード出力の例

```
====================================
Upgrade steps
install add file bootflash:/ c8000v-universalk9.17.07.01a.SPA.bin
install activate
install commit
====================================

Router#show version | inc IOS XE
Cisco IOS XE Software, Version 17.06.02
Router#show version | inc mode
Router operating mode: Autonomous

Router# dir bootflash:*bin*
Directory of bootflash:/*bin*

Directory of bootflash:/

   31  -rw-   832807301   Mar 7 2022 02:07:28 +00:00  c8000v-universalk9.17.07.01a.SPA.bin
5183766528 bytes total (2348220416 bytes free)

Router#install add file bootflash:/c8000v-universalk9.17.07.01a.SPA.bin
install_add: START Mon Mar 7 02:16:30 UTC 2022
install_add: Adding PACKAGE
install_add: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
  [1] Add package(s) on R0
  [1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.07.01a.0.1883
SUCCESS: install_add  Mon Mar  7 02:20:07 UTC 2022
VK5-C8K-8G-1762-1#

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.06.02.0.2786
IMG   I    17.07.01a.0.1883

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------

=====================
install activate
=====================

Router# show install summary
```

```
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.06.02.0.2786
IMG   I    17.07.01a.0.1883

Router# install activate
install_activate: START Mon Mar  7 02:50:00 UTC 2022
install_activate: Activating PACKAGE
Following packages shall be activated:
/bootflash/c8000v-rpboot.17.07.01a.SPA.pkg
/bootflash/c8000v-mono-universalk9.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_nim_xdsl.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_nim_shdsl.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_nim_ge.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_nim_cwan.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_nim_async.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_ngwic_t1e1.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_dsp_sp2700.17.07.01a.SPA.pkg
/bootflash/c8000v-firmware_dreamliner.17.07.01a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby

  [1] Activate package(s) on R0
    --- Starting list of software package changes ---
    Old files list:
      Modified c8000v-firmware_dreamliner.17.06.02.SPA.pkg
      Modified c8000v-firmware_dsp_sp2700.17.06.02.SPA.pkg
      Modified c8000v-firmware_ngwic_t1e1.17.06.02.SPA.pkg
      Modified c8000v-firmware_nim_async.17.06.02.SPA.pkg
      Modified c8000v-firmware_nim_cwan.17.06.02.SPA.pkg
      Modified c8000v-firmware_nim_ge.17.06.02.SPA.pkg
      Modified c8000v-firmware_nim_shdsl.17.06.02.SPA.pkg
      Modified c8000v-firmware_nim_xdsl.17.06.02.SPA.pkg
      Modified c8000v-mono-universalk9.17.06.02.SPA.pkg
      Modified c8000v-rpboot.17.06.02.SPA.pkg
    New files list:
      Added c8000v-firmware_dreamliner.17.07.01a.SPA.pkg
      Added c8000v-firmware_dsp_sp2700.17.07.01a.SPA.pkg
      Added c8000v-firmware_ngwic_t1e1.17.07.01a.SPA.pkg
      Added c8000v-firmware_nim_async.17.07.01a.SPA.pkg
      Added c8000v-firmware_nim_cwan.17.07.01a.SPA.pkg
      Added c8000v-firmware_nim_ge.17.07.01a.SPA.pkg
      Added c8000v-firmware_nim_shdsl.17.07.01a.SPA.pkg
      Added c8000v-firmware_nim_xdsl.17.07.01a.SPA.pkg
      Added c8000v-mono-universalk9.17.07.01a.SPA.pkg
      Added c8000v-rpboot.17.07.01a.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

Send model notification for install_activate before reload
Install will reload the system now!
SUCCESS: install_activate  Mon Mar  7 02:57:34 UTC 2022


==================================
```

```
install commit
==================================

Router# show version | inc IOS XE
Cisco IOS XE Software, Version 17.07.01a
Router# show version | inc mode
Router operating mode: Autonomous
Router# show license udi
UDI: PID:C8000V,SN:9JM01Z7G2JH
```

インストール モードでのアップグレード

この章に記載されている 1 ステップインストールまたは 3 ステップインストールの手順を使用して、インストールモードで Cisco Catalyst 8000V をアップグレードします。

インストールモードでのダウングレード

ダウングレード先のイメージがインストールモードでインストールされている場合、**install rollback** コマンドを使用して、プラットフォームを適切なイメージにポイントすることにより、プラットフォームを以前のバージョンにダウングレードします。

この **install rollback** コマンドはプラットフォームをリロードし、前のイメージで起動します。

（注） **install remove inactive** コマンドを使用して前のファイルを削除していない場合にのみ、**install rollback** コマンドは成功します。

（注） このコマンドを使用できない場合は、**install** コマンドを使用して古いイメージをインストールすることでダウングレードすることもできます。

ダウングレードの設定例

```
==========================
install rollback
==========================

Router# install rollback to base
install_rollback: START Tue Mar 01 03:25:46 UTC 2022
install_rollback: Rolling back to base
This operation may require a reload of the system. Do you want to proceed? [y/n]
*Mar 29 21:17:36.496: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
 rollback
--- Starting Rollback ---
Performing Rollback on all members
 [1] Rollback package(s) on  R0
 [1] Finished Rollback package(s) on  R0
Checking status of Rollback on [R0]
Rollback: Passed on [R0]
Finished Rollback operation
```

```
SUCCESS: install_rollback Tue Mar 01 03:30:16 UTC UTC 2022
```

ソフトウェアインストールの中止

ソフトウェアパッケージのアクティブ化は次の方法で中止できます。

- **install commit** コマンドを発行する前に auto-abort-timer が期限切れになるようにします。新しいイメージをアクティブ化した後にプラットフォームをリロードすると、（3 ステップインストールの方法で）auto-abort-timer がトリガーされます。タイマーが期限切れになるとインストールプロセスが終了します。プラットフォームはリロードし、最後にコミットしたバージョンのソフトウェアイメージで起動します。

  install commit コマンドを使用せずに、**install auto-abort-timer stop** コマンドを使用してこのタイマーを停止します。このプロセスでは、新しいイメージはコミットされていないままです。

- **install abort** コマンドを使用して、新しいソフトウェアのインストール前に実行していたバージョンにプラットフォームを戻します。このコマンドは、**install commit** コマンドを発行する前に使用します。

中止の設定例

```
============================
install abort
============================
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   U    17.09.01.0.154628

--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 01:56:56
--------------------------------------------------------------------------------

Router# show version | inc IOS XE
Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20220227_153436
Router# show version | inc mode
Router operating mode: Autonomous
Router# install abort
install_abort: START Tue Mar 01 04:03:52 UTC 2022

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Abort ---
Performing Abort on all members
 [1] Abort packages(s) on  R0
 [1] Finished Abort packages(s) on  R0
Checking status of Abort on [R0]
Abort: Passed on [R0]
```

```
Finished Abort operation

SUCCESS: install_abort Tue Mar 01 04:04:45 UTC 2022

Router# Mar  1 04:04:50.161: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
 reload action requested
```

インストールコマンドを使用したソフトウェアインストールのトラブルシューティング

問題 ソフトウェアインストールのトラブルシューティング

解決法 インストールの概要、ログ、およびソフトウェアバージョンを表示するには、次のshowコマンドを使用します。

- **show install summary**
- **show install log**
- **show version**
- **show version running**

問題 インストールに関するその他の問題

解決法 インストールに関する問題を解決するには、次のコマンドを使用します。

- **dir** <*install directory*>
- **more location:***packages.conf*
- **show tech-support install**：このコマンドはインストール情報に固有の情報を表示する**show**コマンドを自動的に実行します。
- **request platform software trace archive target bootflash** <*location*>：このコマンドは、最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、この情報を指定された場所に保存します。

よく寄せられる質問

Q. Cisco Catalyst 8000V を Cisco CSR1000V や Cisco ISRv にダウングレードできますか。

A. Cisco CSR1000V または Cisco ISRv 17.3.x 以降のバージョンから Cisco Catalyst 8000V にアップグレードした場合にのみ、Cisco Catalyst 8000V からダウングレードできます。

（注） Cisco Catalyst 8000V を新しくインストールした場合、Cisco CSR1000V や Cisco ISRv にダウングレードすることはできません。

Q. Cisco CSR1000V 16.12.x 以前のバージョンからアップグレードする場合、Secure Object Storage はサポートされますか。

A. いいえ。Secure Object Storage はアップグレードでは引き継がれません。Secure Object Storage のサポートを有効にするには、新規インストールを実行するか、VM を再インストールする必要があります。

Q. Cisco CSR1000V または Cisco ISRv から Cisco Catalyst 8000V にアップグレードする場合、ライセンスを変更する必要がありますか。

A. Cisco Catalyst 8000V にアップグレードしても、ライセンスは同じままです。ただし、ライセンスはアップグレード後に SL から SLE に移行します。アップグレード前のスループットが 250M 以下の場合、アップグレード後もそのまま保持されます。

スループットが 250M を超え、デバイスが CSSM に登録されていた場合、接続はそのまま維持され、スループットによってデバイスへの SLAC のインストールが自動的にトリガーされます。対応するスループットは、SLAC がインストールされると設定されます。

デバイスが CSSM に接続されておらず、スループットが 250M を超えていた場合は、オフラインモードで SLAC を手動でインストールするか、CSSM との信頼を確立するために SLE コマンドを設定する必要があります。次に、SLAC のインストールをトリガーするようにスループットを設定します。

（注） SLAC がインストールされていない場合、スループットは 250M のままです。

Q. アップグレードプロセスの自動化は可能ですか。

A. いいえ。移行の自動化は現在サポートされていません。

Q. ダウングレードの実行時、障害モードではどんな処理が実行されますか。

A. ダウングレードの結果として Cisco CSR1000V イメージが起動すると、システムはパーティションの形式をチェックしますパーティションの形式が要件に一致しない場合、起動は停止されます。アップグレードまたはダウングレードの結果として Cisco Catalyst 8000V イメージが起動する場合、既存のパーティション形式を使用して起動を続行します。

Q. アップグレード後のメモリとパフォーマンスにはどのような影響がありますか。

A. Cisco Catalyst 8000V イメージのサイズが若干大きくなる場合があり、全体的なメモリフットプリントに影響が及ぶ可能性があります。とはいえ、その結果として全体的なメモリ要件が変更されることはありません。このイメージに必要な最小 RAM は 4 GB で、この機能によるパフォーマンスへの影響はありません。

第 24 章

vCPU 分散の設定

この章では、テンプレートを使用したコントロールプレーン（CP）、データプレーン（DP）、およびサービスプレーン（SP）のvCPUの割り当てと分散を指定します。サービスプレーンには、SNORT を実行しているコンテナが含まれていることに注意してください。

vCPU 分散には、次のいずれかのテンプレートを使用します。

vCPU 分散：コントロールプレーン超高

次の表に、コントロールプレーン超高テンプレートの vCPU 分散を示します。

表 *35*：コントロールプレーン超高：*vCPU* 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1 1/2	1 1/2	0 ～ 5
サービスプレーン	1/3	1/2	1 1/2	1 1/2	0 ～ 5
データ プレーン	1/3	1	1	5	6 ～ 15

（注） コントロールプレーン超高テンプレートを使用すると、サービス プレーン アプリケーションは、その動作のために 1.5 のフルコアを取得できます。たとえば、Wide Area Application Services（WAAS）の場合です。

vCPU 分散：コントロールプレーン高

次の表に、コントロールプレーン高テンプレートの vCPU 分散を示します。

表 *36 :* コントロールプレーン高：*vCPU* 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1	1	0 ～ 3
サービスプレーン	1/3	1/2	1	1	0 ～ 3
データ プレーン	1/3	1	2	6	4 ～ 15

（注） コントロールプレーン高テンプレートは、データプレーン高テンプレートと比較して、コントロールプレーン/サービスプレーンのサービスに追加のコアを割り当てます（コントロールプレーン用に 1 つのコア、サービスプレーン用に別のコアがあります）。サービス プレーン アプリケーションがない場合、コントロールプレーンはすべてのリソース（両方のコア）を使用します。

vCPU 分散：データプレーン高

（注） データプレーン高テンプレートは、デフォルトの vCPU 分散テンプレートです。[Template] オプションの設定出力に [None] と表示されている場合でも、データプレーン高テンプレートがデフォルトで適用されます。

上記のステートメントは、コントローラモードで実行されている Cisco Catalyst 8000V インスタンスには適用されません。

次の表に、データプレーン高テンプレートの vCPU 分散を示します。

表 *37 :* データプレーン高：*vCPU* 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1/2	1/2	0 ～ 1
サービスプレーン	1/3	1/2	1/2	1/2	0 ～ 1
データ プレーン	1/3	1	3	7	2 ～ 15

（注） デフォルトでは、Cisco Catalyst 8000V コアの割り当ては、パフォーマンスのためにより大きなデータプレーンを優先します。サービス プレーン アプリケーションがない場合、コントロールプレーンはサービスプレーンのリソースも使用します。

vCPU 分散：データプレーン並

データプレーン並テンプレートの vCPU 分散を使用して、vCPU 分散のテンプレートを使用する前と同じように Cisco Catalyst 8000V を強制的に動作させることができます。

つまり、ovf-env.xml ファイルで指定されているように、vCPU 分散用のデータプレーン高テンプレートを使用して Cisco Catalyst 8000V VM を作成するとします。後でデータプレーン並テンプレートで CLI コマンドを使用して、データプレーン高テンプレートによって以前に適用された XML ファイル設定を上書きできます。

vCPU 分散：サービスプレーン高

次の表に、サービスプレーン高テンプレートの vCPU 分散を示します。

表 *38 :* サービスプレーン高：*vCPU* 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1	2	0 ～ 7
サービスプレーン	1/3	1/2	1	2	0 ～ 7
データ プレーン	1/3	1	2	4	8 ～ 15

（注） サービスプレーン高テンプレートを使用すると、サービス プレーン アプリケーション（Snort IPS など）は、その動作に最大 2 つのフルコアを使用できます。

vCPU 分散：サービスプレーン中

次の表に、サービスプレーン中テンプレートの vCPU 分散を示します。

表 *39：*サービスプレーン中：*vCPU* 分散

vCPU の数	1	2	4	8	16
コントロールプレーン	1/3	1/2	1	1	0 ～ 3
サービスプレーン	1/3	1/2	1	1	0 ～ 3
データ プレーン	1/3	1	2	6	4 ～ 15

データプレーン、コントロールプレーン、サービスプレーン全般にわたる vCPU 分散の設定

Cisco Catalyst 8000V CLI で `platform resource` コマンドを入力して、vCPU 分散用のテンプレートを選択します。

configure template

platform resource *template*

例：

```
Router# configure template
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# platform resource ?
  control-plane-extra-heavy Use Control Plane Extra Heavy template
  control-plane-heavy   Use Control Plane Heavy template
  data-plane-heavy      Use Data Plane Heavy template
  data-plane-normal     Use Data Plane Normal template
  service-plane-heavy   Use Service Plane Heavy template
  service-plane-medium  Use Service Plane Medium template
Router(config)# platform resource service-plane-heavy
```

（注） `platform resource` コマンドを入力した後、Cisco Catalyst 8000V インスタンスを再起動してテンプレートをアクティブにする必要があります。

アクティブ vCPU 分散テンプレートの決定

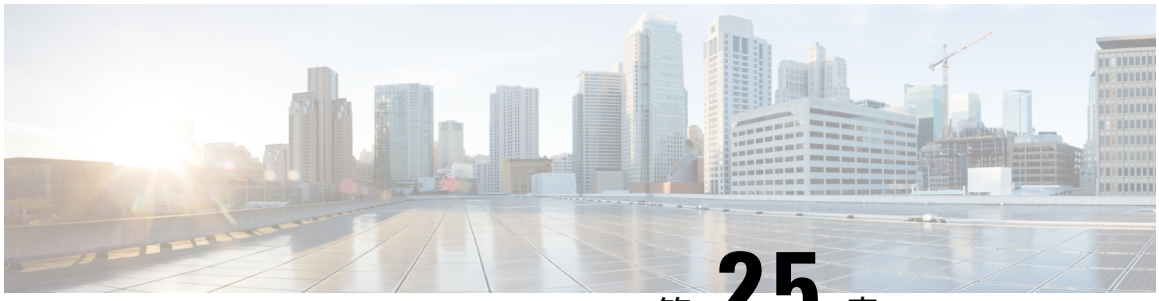
vCPU 分散に使用されているテンプレートを確認するには、次のコマンドを使用します。

show platform software cpu alloc

例：

```
Router# show platform software cpu alloc
CPU alloc information:
Control plane cpu alloc: 0-1
Data plane cpu alloc: 2-3
Service plane cpu alloc: 0-1
Template used: CLI-service_plane_heavy
```

（注） コントロールプレーンとサービスプレーンは、コア 0 と 1 を共有します。



第 25 章

Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理

この章では、Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理とモニタリングについて説明します。ここで説明する内容は、次のとおりです。

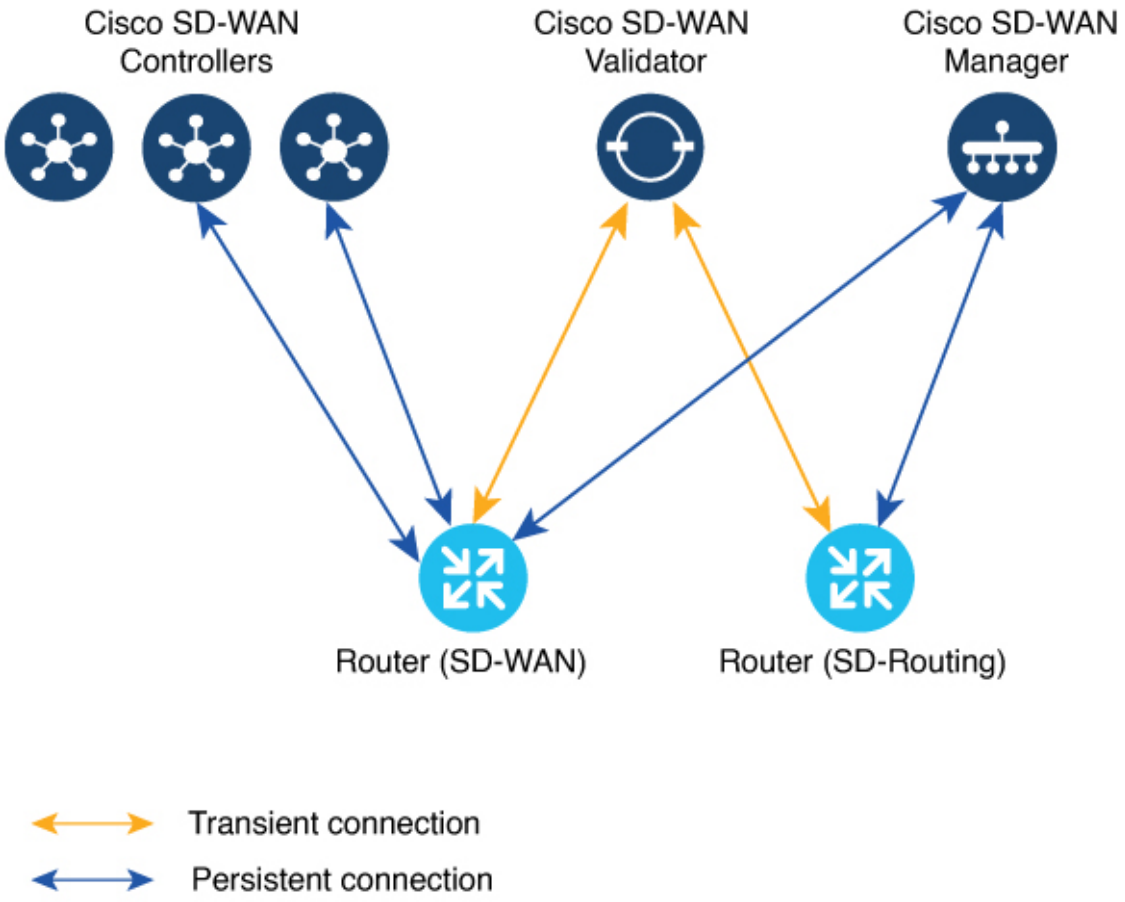
Cisco SD-WAN Manager を使用した SD ルーティングデバイスのモニタリングについて

この機能を使用すると、非 SD-WAN モードで動作している Cisco IOS XE デバイスで Cisco SD-WAN Manager を使用して基本的な管理機能を実行できます。Cisco IOS XE 17.12.1a 以降、このようなデバイスは SD ルーティングデバイスと呼ばれます。単一のネットワーク管理システム（NSM）（Cisco SD-WAN Manager）を使用して、すべての Cisco IOS XE ルータを管理およびモニタリングすることで、ソリューションの導入を簡素化できます。

（注） Cisco IOS-XE ソフトウェアの No Payload Encryption（NPE）または No Lawful Intercept and No Payload Encryption（NOLI/NPE）イメージは、Cisco SD-WAN Manager 機能を使用した SD ルーティングデバイスの管理をサポートしていません。

（注） この機能に必要な最小ソフトウェアバージョンは、Cisco IOS XE 17.12.1a および Cisco SD-WAN リリース 20.12.1 です。

図 *2 : SD* ルーティングデバイスの管理



Cisco SD-WAN Manager を使用して SD ルーティングデバイスを管理するメリット

1. エンタープライズ ネットワークでは、1 つの NMS（Cisco SD-WAN Manager）で Cisco Catalyst SD-WAN 環境と SD ルーティング環境に対応できます。
2. 同じ Cisco SD-WAN Manager 上で Cisco SD-WAN デバイスと SD ルーティングデバイスが共存できます。

前提条件

SD ルーティングデバイスをオンボードするための前提条件は次のとおりです。

- デバイスがインストールモードで Cisco IOS XE 17.12.1a イメージを実行していることを確認します。これらのモードの詳細については、「Switch Modes Using Cisco CLI」[英語] を参照してください。
- Cisco SD-WAN Manager インスタンスがオンプレミスまたはクラウドでホストされていること。
- デバイスから Cisco SD-WAN Manager への接続が確立されていること。
- Cisco SD-WAN Manager からの管理に必要な DMI を有効にするために、netconf-yang モデルを有効にします。
- 自律モードで動作するデバイスは、コントローラ（Cisco SD-WAN Validator および Cisco SD-WAN Manager）とのセキュアな制御接続を確立するために、次の基本設定を手動で行う必要があります。
  - システムのプロパティ：
    - システム IP
    - サイト ID
    - 組織名
    - Cisco SD-WAN Validator 情報（Cisco SD-WAN Validator サーバーの IP アドレスまたは FQDN ）
  - インターフェイス設定
    - 静的または動的 IP アドレスとサブネットマスクを持つ物理インターフェイス
    - Cisco SD-WAN Validator または Cisco SD-WAN Manager への到達可能性を提供するダイナミックルーティングまたはデフォルトルート

制限事項

- Cisco SD-WAN Manager への Cisco SD ルーティングデバイスのオンボーディングは、universalk9 イメージでのみサポートされます。ペイロード暗号化機能のない（NPE）イメージはサポートされていません。
- Cisco IOS XE 17.12.1a リリースでは、基本的なモニタリングがサポートされており、後続のリリースで追加機能をサポート予定です。サポートされている機能の詳細については、プラットフォーム固有のリリースノートを参照してください。
- Cisco SD ルーティングデバイスは、コントローラに到達可能なインターフェイスから Cisco SD-WAN Manager への制御接続を 1 つだけ確立できます。
- Cicso SD ルーティングデバイスでは、Cisco SD-WAN コントローラとのアクティブな接続が確立されません。
- Cisco SD-WAN Manager への接続では、専用の管理インターフェイスはサポートされていません。

サポートされる WAN エッジデバイス

サポートされている WAN エッジプラットフォームとオンボーディングオプションを次の表に示します。

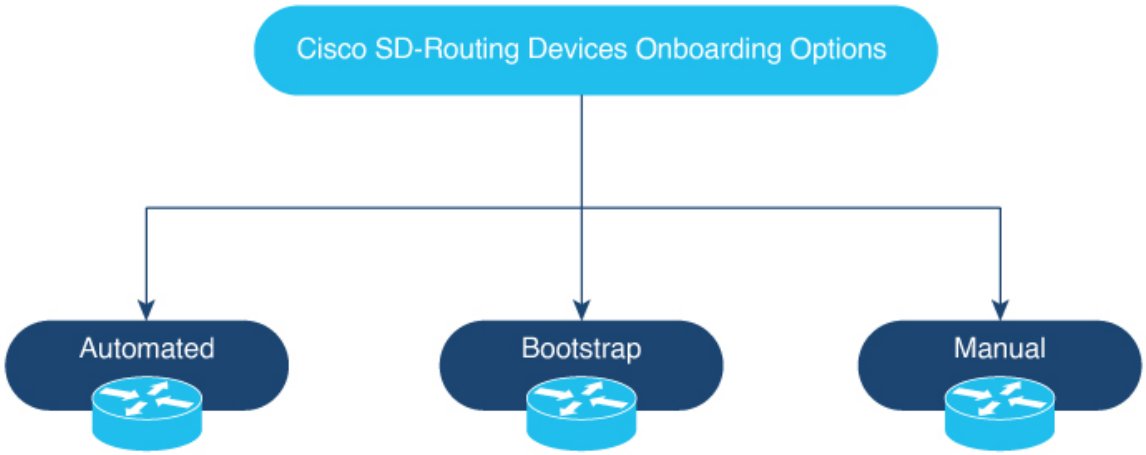
表 *40*：サポートされている *WAN* エッジプラットフォームとオンボーディングオプション

プラットフォーム	Automated	Bootstrap	手動
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ			
ASR1001-HX	対応	対応	対応
ASR1002-HX	対応	対応	対応
Cisco 4400 シリーズ サービス統合型ルータ			
Cisco 4431 ISR	対応	対応	対応
Cisco 4451 ISR	対応	対応	対応
Cisco 4461 ISR	対応	対応	対応
Cisco 4300 シリーズ サービス統合型ルータ			
Cisco 4321 ISR	対応	対応	対応
Cisco 4331 ISR	対応	対応	対応
Cisco 4351 ISR	対応	対応	対応

プラットフォーム	Automated	Bootstrap	手動
Cisco 4200 シリーズ サービス統合型ルータ			
Cisco 4221 ISR	対応	対応	対応
Cisco 100 シリーズ サービス統合型ルータ			
Cisco 1000 ISR	対応	対応	対応
Cisco Catalyst 8000V シリーズ エッジ プラットフォーム			
Cisco Catalyst 8000V	該当なし （注） 自動オンボーディングは、ハードウェアデバイスのみが対象です。	対応	対応
Cisco Catalyst 8200 シリーズ エッジ プラットフォーム			
C8200-1N-4T	対応	対応	対応
C8200L-1N-4T	対応	対応	対応
Cisco Catalyst 8300 シリーズ エッジ プラットフォーム			
C8300-1N1S-4T2X|6T	対応	対応	対応
C8300-2N2S-4T2X|6T	対応	対応	対応
Cisco Catalyst 8500 シリーズ エッジプラットフォーム			
C8500-12X4QC	対応	対応	対応
C8500-12X	対応	対応	対応
C8500L-8S4X	対応	対応	対応
C8500-20X6C	対応	対応	対応

SD ルーティングデバイスのオンボーディング

ここでは、SD ルーティングデバイスをオンボードするためのワークフローについて説明します。



- SD ルーティングデバイスのオンボーディング
  - 自動オンボーディング：Dynamic Host Configuration Protocol（DHCP）および Cisco Plug and Play（PNP）を使用して、デバイスを Cisco SD-WAN Manager に自動的にオンボードします。
  - ブートストラップ オンボーディング：ブートフラッシュまたは USB 上のブートストラップファイルを使用し、Cisco SD-WAN Manager に到達するために必要な最小構成でデバイスを設定します。
  - 手動オンボーディング：IOS-XE コマンドを使用してデバイスを手動で設定し、Cisco SD-WAN Manager にデバイスをオンボードします。

SD ルーティングデバイスをオンボードするための前提条件は次のとおりです。

- システム IP

手動オンボーディングの前提条件は次のとおりです。

- サイト ID
- 組織名
- Cisco SD-WAN Validator 情報（Cisco SD-WAN Validator サーバーの IP アドレスまたは FQDN）
- Cisco SD-WAN Manager に接続するためのインターフェイス（物理、サブインターフェイス、ループバック）

自動化されたワークフローを使用した SD ルーティングデバイスのオンボーディング

自動化されたワークフローを使用して SD ルーティングデバイスをオンボードするには、次の手順を実行します。

- プラグアンドプレイ接続ポータルを設定します
- Quick Connect ワークフローを使用して Cisco SD-WAN Manager を設定します
- Day-0 モードでデバイスを起動します

プラグアンドプレイ接続ポータルの設定

PnP 接続ポータルを設定するには、次の手順を実行します。

始める前に

シスコユーザー ID を使用して、PnP 接続ポータル、アクティブなスマートアカウントおよびバーチャルアカウントにアクセスできることを確認します。また、PnP Connect ポータルで、アカウントのスマートアカウントまたはバーチャルアカウント管理者として関連付けられている CCO ID を使用する必要があります。

（注） [Cisco SD-WAN Managerの設定（Cisco SD-WAN Manager Settings）] ページでスマートアカウントのログイン情報を入力した後にのみ、プラグアンドプレイ接続の同期を有効にできます。

ステップ 1 sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。

ステップ 2 コントローラプロファイルを作成し、エンタープライズ ネットワークの場合は**ルート CA** をアップロードします。

（注） オーバーレイネットワークが **Cisco PKI** の場合、証明書をアップロードする必要はありません。

ステップ 3 コントローラプロファイルとコントローラタイプを入力し、[Next] をクリックします。

ステップ 4 [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。

ステップ 5 デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

Quick Connect ワークフローを使用した Cisco SD-WAN Manager の設定

Quick Connect ワークフローを使用して Cisco SD-WAN Manager を設定するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Workflows] > [Quick Connect] の順に選択します。

ステップ 2 [Get Started] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 プロビジョニングファイル（.csv または .viptela）を PnP から Cisco SD-WAN Manager にアップロードしていない場合は、**.csv upload**、**.viptela upload**、[Sync Smart Account] オプションのいずれかを使用して、デバイスを Cisco SD-WAN Manager に追加できます。デバイスがすでに Cisco SD-WAN Manager に追加されている場合は、[skip for now] オプションを選択します。

（注） .csv ファイルは、ハードウェアデバイスにのみ適用できます。.viptela ファイルは、ハードウェアデバイスとソフトウェアデバイスの両方に適用できます。

ステップ 5 まだ同期していない場合は、[Sync Smart Account] をクリックします。デバイスの表にデバイスがリストされているはずです。

[Sync Smart Account]をクリックします。

ステップ 6 **[Next]** をクリックします。

ステップ 7 [Add and Review Device Configuration] ダイアログボックスで、サイト ID、システム IP、ホスト名を入力し、[Apply] をクリックします。

ステップ 8 **[Next]** をクリックします。

ステップ 9 オプションタグを追加し、[Next] をクリックします。

ステップ 10 追加されたデバイスを確認するには、[Configuration] > [Devices] の順に選択し、[Table Settings] で [enable Device Model] をクリックします。

ステップ 11 ネットワーク内のルータのリストが表示され、各ルータに関する詳細情報が表示されます。デバイスが追加されたことを確認するには、**[Configuration]** > **[Certificates]** の順に選択します。

SD ルーティングデバイスの起動

SD ルーティングデバイスを起動するには、次の手順を実行します。

ステップ 1 Day-0 状態でデバイスを起動しますデバイスが Day-0 状態でない場合は、**reload** オプションとともに **controller-mode reset** または **writer erase** コマンドを使用して、Day-0 状態にします。

ステップ 2 デバイスが Gigabit Etherner0 インターフェイス以外のいずれかのインターフェイスで DHCP を介して IP アドレスを取得していることを確認します。また、デバイスが devicehelper.cisco.com および Cisco SD-WAN Validator に到達可能であることを確認します。

（注） Cisco SD-WAN Manager への接続では、専用の管理インターフェイスはサポートされていません。

ステップ 3 デバイス制御接続が Cisco SD-WAN Manager で稼働します。

ステップ 4 **show sd-routing connections summary** コマンドを使用して、エッジデバイスの制御接続ステータスを確認します。

例：

```
Router#show sd-routing connections summary

PEER                                          PEER
PEER     PEER  PEER             SITE        PEER                                  PRIV
PEER                                  PUB
TYPE     PROT  SYSTEM IP        ID           PRIVATE IP                            PORT   PUBLIC
 IP                               PORT   STATE   UPTIME
------------------------------------------------------------------------------------------------
Cisco SD-WAN Manager  dtls  172.16.255.22    200         10.0.12.22
12446  10.0.12.22                              12446  up      12:05:29:3
```

ステップ 5 Cisco SD-WAN Manager で制御接続ステータスを確認します。

ブートストラップを使用したSDルーティングデバイスのオンボーディング

ブートストラップを使用して SD ルーティングデバイスをオンボードするには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Workflows] > [Quick Connect] の順に選択します。

ステップ 2 [Get Started] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 プロビジョニングファイル（*.csv* または *.viptela*）を PnP から Cisco SD-WAN Manager にアップロードしていない場合は、**.csv upload**、**.viptela upload**、[Sync Smart Account] オプションのいずれかを使用して、デバイスを Cisco SD-WAN Manager に追加できます。デバイスがすでに Cisco SD-WAN Manager に追加されている場合は、[skip for now] オプションを選択します。

（注） .csv ファイルは、ハードウェアデバイスにのみ適用できます。.viptela ファイルは、ハードウェアデバイスとソフトウェアデバイスの両方に適用できます。

ステップ 5 導入準備するデバイスを選択し、[Next] をクリックします。

ステップ 6 [Add and Review Configuration] ダイアログボックスで、サイト ID、システム IP、ホスト名を入力し、[Apply] をクリックします。

ステップ 7 追加されたデバイスを確認するには、[Configuration] > [Devices] の順に選択し、[Table Settings] で [enable Device Model] をクリックします。

ステップ 8 [Configuration] > [Certificate] ページで、デバイスが有効な状態であることを確認します。

ステップ 9 Cisco SD-WAN Manager のメニューから、[Configuration] > [Devices] の順に選択します。

ステップ 10 Cisco SD ルーティング ソフトウェア デバイス（Cisco c8000V）の場合は、次の手順を実行してブートストラップを生成し、デバイスをオンボードします。

（注） ハードウェアデバイスの場合は、ステップ 11 の手順に従います。

a) ウィンドウの右側のペインで [...] をクリックし、[Generate Bootstrap Configuration] を選択します。

b) [Cloud-init] オプションを選択し、WAN インターフェイス名の名前を入力して、[OK] をクリックします。

（注） 選択したインターフェイスで DHCP が有効になっており、Cisco SD-WAN Validator と Cisco SD-WAN Manager に到達可能であることを確認します。また、ソフトウェアデバイスの場合は、VPN0 インターフェイスとしてギガビットイーサネット 1 インターフェイスのみを使用します。

c) [Download] をクリックして、デバイスにイメージをダウンロードします。

例：

サンプルイメージ：*ciscosdwan_cloud_init.cfg*

証明書付きのサンプルイメージ：*ciscosdwan_cloud_init_with_ent_cert.cfg*

d) クラウドベースのコントローラの場合、ダウンロードしたブートストラップファイルは、デバイスの導入時にユーザーデータフィールドとして追加できます。コントローラを SD ルーティングモードで起動し、Cisco SD-WAN Validator および Cisco SD-WAN Manager との接続を確立します。

ステップ 11 ハードウェアデバイスの場合は、次の手順を実行してブートストラップを生成し、デバイスをオンボードします。

a) デバイスページの Cisco SD-WAN Manager のメニューから、[Export Bootstrap Configuration] をクリックします。

b) [SD-Routing] のチェックボックスをオンにします。[Export Bootstrap Configuration] ダイアログボックスで、[WAN Interface name] を入力します。

（注） 管理インターフェイス名は、Cisco IOS XE デバイスのモデルによって異なる場合があります。オンボードするモデルに基づいて、Cisco SD-WAN Validator および Cisco SD-WAN Controller に到達できるインターフェイス名を指定します。

c) [Generate Generic Configuration] をクリックして、ハードウェアデバイスに適用可能な .cfg 形式の汎用ブートストラップをダウンロードします。ファイルを解凍し、ファイル名を *ciscosdawn.cfg* に変更します。

（注） 選択したインターフェイスで DHCP が有効になっており、Cisco SD-WAN ValidatorとCisco SD-WAN Managerに到達可能であることを確認します。

ブートストラップファイルには、組織名、Cisco SD-WAN 検証 IP、およびルート CA 証明書が含まれます。エンタープライズ ネットワークの場合は、エンタープライズルート CA 証明書が含まれます。

d) ブートストラップファイルを *ciscosdwan.cfg* というファイル名でデバイスのブートフラッシュにコピーします。

e) **sd-routing bootstrap load bootflash:ciscosdwan.cfg** コマンドを実行します。

例：

```
Router# sd-routing bootstrap load bootflash:ciscosdwan.cfg
Located the file. Beginning to extract the data
Extraction summary
-Organization name - "aniltb2"
```

```
-Interface - GigabitEthernet0/0/0
-vbond  - 99.99.1.51
Successfully extracted root-cert info

Do you want to proceed and apply extracted
parameters to enable sd-routing feature?? (yes/[no]): yes
Successfully configured bootstrap extracted parameters
Router#
*May 10 08:56:11.159: %SYS-5-CONFIG_P: Configured programmatically by process Exec from console as console
*May 10 09:05:11.751: %DMI-5-AUTH_PASSED: R0/0: dmiauthd: User 'vmanage-admin' authenticated successfully from
 201.201.201.1:41902  for netconf over ssh. External groups
```

f) **show sd-routing system status**、**show sd-routing system status**、および **show sd-routing local-properties summary** コマンドを使用して、制御接続を確認します。

デバイスの手動でのオンボーディング

SD ルーティングデバイスを手動でオンボードするには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Workflows] > [Quick Connect] の順に選択します。

ステップ 2 [Get Started] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 プロビジョニングファイル（.csv または .viptela）を PnP から Cisco SD-WAN Manager にアップロードしていない場合は、**.csv upload**、**.viptela upload**、[Sync Smart Account] オプションのいずれかを使用して、デバイスを Cisco SD-WAN Manager に追加できます。デバイスがすでに Cisco SD-WAN Manager に追加されている場合は、[skip for now] オプションを選択します。

（注） .csv ファイルは、ハードウェアデバイスにのみ適用できます。.viptela ファイルは、ハードウェアデバイスとソフトウェアデバイスの両方に適用できます。

ステップ 5 導入準備するデバイスを選択し、[Next] をクリックします。

ステップ 6 [Add and Review Configuration] ダイアログボックスで、サイト ID、システム IP、ホスト名を入力し、[Apply] をクリックします。

ステップ 7 追加されたデバイスを確認するには、[Configuration] > [Devices] の順に選択し、[Table Settings] で [enable Device Model] をクリックします。

ステップ 8 ネットワーク内のルータのリストが表示され、各ルータに関する詳細情報が表示されます。デバイスが追加されたことを確認するには、**[Configuration]** > **[Certificates]** の順に選択します。

ステップ 9 手動でオンボードするデバイスに応じて、次の手順のいずれかを実行します。

a) ハードウェアデバイスの場合は、システムの起動後に IOS コマンドを使用して、最初の Day-0 設定を入力します。

b) Cisco SD ルーティング ソフトウェア デバイスの場合は、ブートストラップなしで Amazon Web Services（AWS）または Azure に Cisco c8000v を導入します。

ステップ 10 Cisco SD-WAN Manager で制御接続を有効にするための最小限のパラメータを設定します。

例：

```
netconf-yang

sd-routing
  no ipv6-strict-control
  organization-name "%Your Org. Name%"
  site-id %id%
  system-ip %system ip%
  vbond name %vbond name or vbond ip%
  vbond port 12346
  wan-interface %uplink interface%

ip route 0.0.0.0 0.0.0.0 %next hop ip%

interface %uplink interface%
   ip address  %dhcp or static%
   no shutdown
```

ステップ 11 SD ルーティングモードを有効にするために必要なパラメータを設定します。

a) インターフェイスが静的 IP アドレスまたは DHCP を使用して設定されていることを確認します。また、インターフェイスは **no shut** 状態である必要があります。

b) Validator の IP または Validator の名前を設定します。

c) システム IP、サイト ID、組織名、および WAN インターフェイスを設定します。

ステップ 12 vdaemon のステータスをチェックして、この機能が有効になっていることを確認します。

例：

```
Router# show platform software yang-management process state
Confd Status: Started


Process               Status              State
------------------------------------------------------
nesd                  Running             Active
syncfd                Running             Active
ncsshd                Running             Not Applicable
dmiauthd              Running             Active
nginx                 Running             Not Applicable
ndbmand               Running             Active
pubd                  Running             Active
```

```
Router#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id         : 29075
  Status           : S
  Session id       : 8829
  User time        : 263002
  Kernel time      : 347183
  Priority         : 20
  Virtual bytes    : 405110784
  Resident pages   : 12195
  Resident limit   : 18446744073709551615
  Minor page faults: 716496
  Major page faults: 9130
```

ステップ 13 企業向けのオーバーレイネットワークの場合は、**request platform software sd-routing root-cert-chain install bootflash:cacert.pem** コマンドを使用してルート証明書をインストールします。Cisco SD-WAN Manager

が **Cisco PKI** ではなくエンタープライズ証明書で設定されている場合は、デバイスにルート証明書をインストールする必要があります。

ステップ 14 デバイスに応じて、次のいずれかの手順を実行します。

a) Cisco 8000v デバイスの場合は、CA から Cisco 8000v にルート証明書をコピーします。

b) Cisco デバイスは、デフォルトで PKI および Symantec ルート証明書とともにロードされます。エンタープライズルート証明書をインストールする必要がある場合は、**request platform software sd-routing root-cert-chain install** <*path-to-root-cert*> コマンドを使用します。

例：

```
Device# request platform software sd-routing root-cert-chain install
bootflash:ctrl_mng/cacert.pem
```

ステップ 15 クライアントのエンタープライズルート証明書をインストールします。

（注） デフォルトでは、証明書はハードウェアデバイスにロードされます。この手順は、ソフトウェアデバイスを手動でオンボードする場合を対象としています。

ステップ 16 **request platform software sd-routing csr upload** <*bootflash:ctrl_mng/test*> コマンドを使用して、デバイスの証明書署名付き要求（CSR）を生成します。*bootflash:ctrl_mng/* ディレクトリ内に作成されたフォルダには、任意の名前を指定できます。

ステップ 17 生成された CSR ファイルを、エンタープライズ CA があるディレクトリにコピーします。ルートキーとルート CA 証明書を使用して証明書を署名し、pem 形式の証明書ファイルを生成できます。

ステップ 18 生成された *certificate.pem* ファイルをデバイスにコピーし、**request platform software sd-routing certificate install** <*path-to-certificate-file*> コマンドを使用して、デバイスに証明書をインストールします。

ステップ 19 証明書のインストールステータスを確認します。

例：

```
SJC_Primary# show sd-routing local-properties summary
….....
certificate-status               Installed
certificate-validity             Valid
certificate-not-valid-before     Apr 25 00:55:28 2023 GMT
certificate-not-valid-after      Apr 24 00:55:28 2024 GMT
….........
dns-name                         Validator
site-id                          100
tls-port                         0
system-ip                        172.16.255.11
chassis-num/unique-id            C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                       12345707
```

ステップ 20 Cisco SD-WAN Manager でデバイスをオンボードします。クライアント証明書をインストールする場合は、Cisco SD-WAN Manager に以下を追加します。

a) シャーシ番号とシリアル番号を取得します。シャーシ番号とシリアル番号を取得するには、**how sd-routing local-properties** または **show sd-routing certificate serial** コマンドを使用します。

```
Router# show sd-routing local-properties summary
chassis-num/unique-id            C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                       12345707
```

b) **request vedge add chassis-num** <*Chassis id*> **org-name** <*Org Name*> **serial-num** <*Serial number from c8kv*> コマンドを使用してシャーシ ID をアップロードします。

または

c) シャーシ番号とシリアル番号を使用して *.viptela* ファイルを作成し、そのファイルを Cisco SD-WAN Manager にアップロードしてコントローラに送信します。

ステップ 21 Cisco SD-WAN Manager で制御接続ステータスを確認します。

例：

```
Router#show sd-routing connections summary

PEER                                          PEER
PEER     PEER  PEER             SITE        PEER                                  PRIV
PEER                                    PUB
TYPE     PROT  SYSTEM IP        ID          PRIVATE IP                            PORT   PUBLIC
 IP                                 PORT   STATE   UPTIME
------------------------------------------------------------------------------------------------
vmanage  dtls  172.16.255.22    200         10.0.12.22                            12446
10.0.12.22                              12446  up      12:05:29:3
```

トークンを使用したシャーシのアクティブ化によるデバイスのオンボーディング

シャーシ番号をアクティブ化にするには、次の手順を実行します。

（注） この方法は、Cisco SD-WAN ソフトウェアデバイス（Cisco c8000v）でのみ使用できます。

ステップ 1 PnP スマート同期方式を使用して Cisco SD-WAN Manager にデバイスを追加します。

ステップ 2 sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。

ステップ 3 コントローラプロファイルを作成し、エンタープライズ ネットワークの場合は**ルート CA** をアップロードします。

ステップ 4 コントローラタイプに vBond と入力し、[Next] をクリックします。

ステップ 5 [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。

ステップ 6 デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

ステップ 7 Cisco SD-WAN Manager のメニューから **[Administration]** > **[Settings]** の順に選択します。

ステップ 8 [Smart Account Credentials] に移動し、[Edit] をクリックします。

ステップ 9 ユーザー名とパスワードを入力し、[Save] をクリックします。

ステップ 10 次の方法を使用して、PnP Connect ポータルからデバイスリストをインポートできます。

a) [Configuration] > [Devices] の順に選択し、[Sync Smart Account] をクリックします。

または

a) PnP Connect からダウンロードした *.viptela* をアップロードします。[Controller profiles] に移動し、[Download the Provisioning file] をクリックします。
b) Cisco SD-WAN Manager のメニューから、[Configuration] > [Devices] > [Upload WAN Edge List] の順に選択します。

ステップ 11 デバイスは、スタートアップ コンフィギュレーションで自律モードになります。デバイスは Day-0 モードになりません。

ステップ 12 デバイスに最小設定を適用します。

例：

```
netconf-yang
!
sd-routing
 no ipv6-strict-control
 organization-name "vIptela Inc Regression"
 site-id 500
 system-ip 172.16.255.15
 vbond ip 10.0.12.26
 vbond port 12346
 wan-interface GigabitEthernet2
!
ip route 0.0.0.0 0.0.0.0 10.0.5.13
!
ip interface GigabitEthernet2
 ip address 10.0.5.11 255.255.255.0
 no shutdown
!
```

ステップ 13 Cisco SD-WAN Manager のメニューから、[Configuration] > [Certificates] の順に選択し、オンボードするデバイスの UUID とワンタイムパスワード（OTP）を取得します。

ステップ 14 ソフトウェアデバイスによって生成されたシャーシ番号を上書きするには、**request platform soft sd-routing activate chassis** <新たにアップロードされたシャーシ ID> **token** <Cisco SD-WAN Manager によって生成されたトークン> コマンドを使用します。

ステップ 15 企業向けのオーバーレイネットワークの場合は、**request platform software sd-routing root-cert-chain install bootflash:cacert.pem** コマンドを使用してエンタープライズルート証明書をインストールします。オーバーレイネットワークが **Cisco PKI** の場合、ルート証明書をインストールする必要はありません。

（注） 証明書署名要求（CSR）を生成して署名する必要はありません。CSR は、ステップ 14 の実行中に生成されます。

ステップ 16 次のコマンドを使用して、エッジデバイスの制御接続ステータスを確認します。

例：

```
show sd-routing local-properties summary
show sd-routing local-properties wan ipv4
show sd-routing connections summary
show sd-routing connections history
```

マルチテナント SD ルーティングデバイスのオンボーディング

ここでは、マルチテナント SD ルーティングデバイスをオンボードするためのワークフローについて説明します。

- 自動オンボーディング
- 手動オンボーディング

自動化されたワークフローを使用したマルチテナント SD ルーティングデバイスのオンボーディング

マルチテナント SD ルーティングデバイスをオンボードするには、次の手順を実行します。

ステップ 1 sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。

a) 仮想アカウントを作成します。
b) コントローラプロファイルを作成し、エンタープライズ ネットワークの場合はルート CA をアップロードします。
c) コントローラタイプに vBond と入力し、[Next] をクリックします。
d) [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。
e) デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

または

ステップ 2 Cisco SD-WAN Manager のメニューから、[Workflows] > [Quick Connect] の順に選択します。

ステップ 3 [Get Started] をクリックします。

ステップ 4 [Next] をクリックします。

ステップ 5 .csv ファイルを Cisco SD-WAN Manager にアップロードしていない場合は、いずれかのアップロードオプションを使用してファイルをアップロードします。ファイルをアップロード済みの場合は、[skip for now] オプションを選択します。

ステップ 6 [Sync Smart account]、[csv upload]、[.viptela upload] のいずれかをクリックします。デバイスの表にデバイスがリストされているはずです。

ステップ 7 ソフトウェアデバイスの場合は、前の項で説明したようにブートストラップファイルを生成し、c8000v ユーザー設定ファイルとして追加します。

（注） マルチテナント設定の場合は、システム IP を設定する際に、Quick Connect ワークフローを使用する必要があります。CLI オプションを使用してシステム IP を設定しないでください。

ステップ 8 デバイスタイプに基づいて、次のいずれかの手順を実行します。

a) ソフトウェアデバイスの場合は、Azure または AWS に Cisco c8000v を展開し、カスタムデータまたはユーザーデータ入力としてブートストラップファイルを入力します。

b) ハードウェアデバイスの場合は、デバイスを Day-0 状態で起動します。デバイスが Day-0 状態でない場合は、**reload** オプションとともに **controller-mode reset** または **writer erase** コマンドを使用して、Day-0 状態にします。

ステップ 9 デバイスで Cisco SD-WAN Manager が起動します。

ステップ 10 デバイスのステータスを確認するには、**show sd-routing connection summary status** および **show sd-routing local-properties summary** コマンドを使用します。

マルチテナント SD ルーティングデバイスの手動によるオンボーディング

マルチテナント SD ルーティングデバイスを手動でオンボードするには、次の手順を実行します。

ステップ 1 Cisco Catalyst 8000v を自律モードで Azure または AWS に展開します。

a) sotware.cisco.com > [Network Plug and Play] > [Manage Devices] に移動し、スマートアカウントとバーチャルアカウントにアクセスできることを確認します。
b) 仮想アカウントを作成します。
c) コントローラプロファイルを作成し、エンタープライズ ネットワークの場合はルート CA をアップロードします。
d) コントローラタイプに vBond と入力し、[Next] をクリックします。
e) [Add Controller Profile] に必要なパラメータを入力し、[Next] をクリックします。
f) デバイスを PnP 接続に追加します。デバイスを追加する場合は、[Device Mode] フィールドで、ドロップダウンリストから SD ルーティングモードのデバイスに対して [AUTONOMOUS] を選択します。

ステップ 2 Netconf-Yang を有効にするための最小パラメータを設定します。

例：

```
config terminal
 netconf-yang
end
```

ステップ 3 **show platform software yang-management process state** コマンドを使用して、Netconf-Yang のステータスを確認します。

ステップ 4 Cisco SD ルーティングモードを有効にするために必要なパラメータを設定します。

a) インターフェイスが静的 IP アドレスまたは DHCP を使用して設定されていることを確認します。また、インターフェイスは **no shut** 状態である必要があります。
b) Cisco SD-WAN Validator の IP または Cisco SD-WAN Validator の名前を設定します。
c) Cisco SD-WAN Validator、サイト ID、組織名、および WAN インターフェイスを設定します。

（注） マルチテナント設定の場合は、システム IP を設定する際に、Quick Connect ワークフローを使用する必要があります。CLI オプションを使用してシステム IP を設定しないでください。ただし、マルチテナント展開では、SD ルーティングデバイスの SP 組織名を設定するために CLI オプションを使用できます。この組織名は、マルチテナント展開のテナントの組織名を指します。デバイスがオンボードされた後、**show sd-routing local-properties summary** コマンドでのみ表示されます。

ステップ 5 vdaemon のステータスをチェックして、この機能が有効になっていることを確認します。

例：

```
Router#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id         : 29075
  Status           : S
  Session id       : 8829
  User time        : 263002
  Kernel time      : 347183
  Priority         : 20
  Virtual bytes    : 405110784
  Resident pages   : 12195
  Resident limit   : 18446744073709551615
  Minor page faults: 716496
  Major page faults: 9130
```

ステップ 6 エッジデバイスの SD ルーティング設定を確認します。また、署名用のシャーシ番号を取得し、Cisco SD-WAN Manager WAN エッジリストにアップロードします。

ステップ 7 デバイスのステータスを確認するには、**show sd-routing local-properties summary** コマンドを使用します。

ステップ 8 root-ca-chain.crt 証明書を Cisco SD-WAN Manager から SD ルーティングデバイスにコピーします。

（注） この手順は、エンタープライズ証明書方式を使用している場合にのみ必要です。**Cisco PKI** 方式を使用している場合は、この手順をスキップできます。

ステップ 9 SD ルーティングデバイスに *root-ca-chain.crt* をインストールします。

ステップ 10 プロビジョニングファイル（*.Viptela*）を PnP から Cisco SD-WAN Manager WAN エッジリストにアップロードし、コントローラに送信します。

ステップ 11 シャーシ番号、シリアル番号を使用して *.viptela* ファイルを作成し、署名します。ファイルを Cisco SD-WAN Manager にアップロードし、コントローラに送信します。

ステップ 12 Cisco SD-WAN Manager からトークンを取得します。Cisco SD-WAN Validator および Cisco SD-WAN Manager との制御接続を確立してデバイスをオンボードするには、**request platform software sd-routing activate chassis-number** <*chassis-num*> **token** <*token*> コマンドを使用します。

ステップ 13 デバイスのステータスを確認するには、**show sd-routing connection summary status** および **show sd-routing local-properties summary** コマンドを使用します。

ワンタッチプロビジョニングを使用した Cisco SD-WAN Manager へのデバイスのオンボーディング

デバイスのワンタッチプロビジョニングを実行するには、次の手順に従います。

始める前に

ワンタッチプロビジョニングを使用してデバイスを設定する場合は、プロセスが次の要件を満たしていることを確認します。

- デバイスが自律モードになっている必要があります。PnP ディスカバリを停止し、デバイスにスタートアップコンフィギュレーションまたは任意のコンフィギュレーションが必要です。デバイスが Day-0 状態であってはなりません。
- デバイスは、WAN インターフェイスを介して Cisco SD-WAN Validator および Cisco SD-WAN に到達するように設定する必要があります。

  デバイスには、SD ルーティング機能がコントローラと通信するために必要な最小限の設定が必要です。

また、ワンタッチプロビジョニング方式を使用してデバイスを Cisco SD-WAN Manager にオンボーディングすると、デバイスを追加するための次の手順が不要になります。

- **.csv** 、**.viptela**、または **sync smart account** を使用した Cisco SD-WAN Manager への WAN エッジデバイスの追加。
- シスコデバイスは SD ルーティングモードで設定する必要があります。Cisco SD-WAN Manager にデバイスを追加せずにデバイスを設定するには、手動またはブートストラップ方式を使用する必要があります。

ステップ 1 Cisco SD-WAN Manager のメニューから、[Administration] > [Settings] の順に選択し、[One Touch Provisioning] を有効にします。

ステップ 2 [One Touch Provisioning] が [Enabled] になっているか確認します。[Enabled] の場合は、ステップ 5 に進みます。

ステップ 3 [One Touch Provisioning] が [Disabled] になっている場合は、[Edit] をクリックします。

ステップ 4 [Enable Claim WAN Edges] 設定で、[Enabled] を選択して [Save] をクリックします。

ステップ 5 [Configuration] > [Devices] > [Unclaimed Devices] に移動します。

a) 要求するデバイスを選択し、[Claim Device(s)] をクリックします。

b) デバイスは、[Unclaimed WAN Edges] から削除され、[WAN Edge List] に表示されます。

ステップ 6 デバイスのステータスを確認するには、**show sd-routing system status** および **show sd-routing local-properties summary** コマンドを使用します。

機能のプロビジョニング解除

機能のプロビジョニングを解除するには、次の手順を実行します。

ステップ 1 デバイスから SD ルーティング機能の設定を削除します。

例：

（注） これにより、すべての証明書が削除されます。すべての証明書を再インストールする必要があります。

例：

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no sd-routing
Warning! Disabling this feature will result in deleting client certificates. Please backup the
certificates and use the CLIs to reinstall them on enabling this feature again.
Do you want to continue? (y/n)[n]: y
```

ステップ 2 デバイスを無効にします。手順については、「デバイスの手動でのオンボーディング （257 ページ）」の項にある手順 4 を参照してください。

ステップ 3 デバイスを削除する手順は、次のとおりです。

a) Cisco SD-WAN Manager のメニューから、[Configuration] > [Devices] の順に選択します。
b) [WAN Edge List] をクリックし、無効にするデバイスを選択します。
c) [Delete WAN Edge] をクリックします。
d) メッセージを読んで、[Yes] をクリックします。

ソフトウェアイメージの管理

ここでは、ソフトウェアイメージをアップグレードするプロセスについて説明します。Cisco SD-WAN Manager は、事前にパッケージ化された tar.gz 形式のシスコ仮想マシンイメージ、または qcow2 形式のイメージのアップロードをサポートします。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。同様に、サービスチェーンの作成中に仮想ネットワーク機能（VNF）を設定するときに、イメージパッケージファイル、またはスキャフォールドファイルを含む qcow2 イメージファイルを選択できるようになりました。Cisco SD-WAN Manager は NETCONF と通信し、自律モードデバイスが Cisco SD-WAN Manager にオンボーディングされたときに、シンプルなリモートプロシージャコールを使用して運用データを取得します。NETCONF は、ネットワークデバイスと通信する標準的なトランスポートプロトコルであり、設定データを編集するためのメカニズムを提供します。SD ルーティングデバイスの Cisco SD-WAN Manager アップグレードワークフローは、コントローラモードのワークフローに似ています。

（注） この機能を動作させるために必要な最小限のソフトウェアバージョンは、Cisco IOS XE 17.12.1a です。

CLI を使用したソフトウェアアップグレード

ソフトウェアをアップグレードするには、次の手順を実行します。

始める前に

- ディスク容量の確認：イメージのダウンロードと展開に使用可能なブートフラッシュ容量を確認します。
- イメージリポジトリの確認：リモートサーバーの到達可能性を確認します。
- 自動ブートの有効化：デバイスで自動ブートが有効になっているかどうかを確認します。

ステップ 1 ソフトウェアページの https://software.cisco.com から Cisco IOS XE リリース 17.12 イメージをダウンロードします。

ステップ 2 イメージをデバイスにアップロードします。

ステップ 3 **install add file <bootflash:/file name> activate commit** コマンドを使用して新規ソフトウェアをインストールし、アクティブ化します。

例：

```
Device# install add file <bootflash:/c8000v-universalk9.17.12.01.0.166070.SSA.bin activate commit
```

アクティベーションが完了すると、デバイスがリロードされます。

（注） これはインタラクティブなコマンドであり、確認して同意するように求められます。デバイスに保存されていない設定がある場合、このコマンドの実行に失敗します。**write memory** コマンドを実行して、ソフトウェアを再インストールする必要があります。

ステップ 4 **install commit** コマンドを使用してアップグレードを確認します。

リポジトリへのソフトウェアイメージの追加

SD ルーティングデバイスまたは Cisco SD-WAN Manager 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 SD-WAN Manager ソフトウェアリポジトリに追加する必要があります。Cisco SD-WAN Manger とリモートサーバーを使用して Cisco SD-WAN コントローラに Cisco Catalyst 8000v エッジソフトウェアをアップロードする方法の詳細については、『Cisco SD-WAN Monitor and Maintain Configuration Guide』[英語] の「Manage Software Repository」の項を参照してください。

Cisco SD-WAN Manager を使用したソフトウェアのアップグレード

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。

始める前に

- 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。

- Cisco SD-WAN Manager 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。
- 自動ブートの有効化：デバイスで自動ブートが有効になっているかどうかを確認します。

ステップ 1 Cisco SD-WAN Manager のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。

ステップ 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]、[Control Components]、[Manager] のいずれかをクリックします。

ステップ 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 SD-WAN Manager クラスタのアップグレード時に、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。

ステップ 4 [Upgrade] をクリックします。

ステップ 5 [Software Upgrade] スライドイン ペインで、次の手順を実行します。

a) 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。[Manager]、[Remote Server]、[Remote Server – Manager] のいずれかです。

（注）
- [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。
- 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、_、*、.、+、=、%、-、:、/、@、?、~

b) [SD-WAN Manager] 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。

c) [Remote Server – SD-WAN Manager] 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。

d) [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。

（注） Cisco SD-WAN Manager ソフトウェアのアップグレード中は、[Activate and Reboot] オプションは使用できません。アップグレードタスクが完了して Cisco SD-WAN Manager が再起動したら、イメージをアクティブ化する必要があります。

e) [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。

ステップ 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。

ステップ 7 Cisco SD-WAN Manager 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。

ステップ 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]、[Control Components]、[Manager] のいずれかをクリックします。

ステップ 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 SD-WAN Manager への制御接続が、設定された時間制限内に確立されない場合、Cisco SD-WAN Manager は自動的に、デバイスを以前実行されていたソフトウェアイメージに戻します。
- 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 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 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。

ソフトウェアイメージの削除

SD ルーティング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 SD-WAN Manager 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。

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 SD-WAN Manager のツールバーからタスクアイコンをクリックします。

   Cisco SD-WAN Manager には、実行中のすべてのタスクのリストが、成功と失敗の合計数とともに表示されます。

2. 矢印アイコンをクリックして、タスクの詳細を表示します。Cisco SD-WAN Manager 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 Manager を使用したデバイスのモニタリング

[Monitor] ウィンドウは、 Cisco SD ルーティングデバイス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。次のオプションを使用して接続を確立し、デバイスをモニタリングできます。

- SSH ターミナル
- ping
- traceroute

また、圧縮された .tar ファイルでシステムステータス情報を収集できます。Cisco SD-WAN Manager は、デバイスから ,tar ファイルを取得してダウンロードできます。ファイルを取得した後、デバイス上のファイルのコピーを削除して、ディスク領域を解放できます。

SD ルーティングモードを有効にすると、この機能はデバイスと Cisco SD-WAN Manager でデフォルトで有効になります。

SSH を使用したデバイスのモニタリング

SSH オプションを使用して接続を確立し、デバイスをモニタリングするには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択します。
ステップ 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。
ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[SSH Terminal] を選択します。

（または）

ステップ 4 Cisco SD-WAN Manage のメニューから、[Tools] > [SSH Terminal] の順に選択します。
ステップ 5 端末でパスワードを 2 回入力し（SD ルーティングと同じ）、デバイスとの接続を確立します。
ステップ 6 端末から **show** コマンドを実行して、デバイスをモニタリングします。

デバイスに対する ping の実行

デバイスに対して ping を実行するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択します。
ステップ 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。
ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[Ping] を選択します。
ステップ 4 [Monitor] ページで宛先 IP アドレスを入力します。
ステップ 5 [Ping] をクリックします。

ping の結果が下のウィンドウに出力されます。

ルートのトレース

トレースルートオプションを使用して、接続を確立した後にデバイスをモニタリングするには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択します。
ステップ 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。
ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[Trace Route] を選択します。
ステップ 4 [Trace Route] ページで、宛先 IP アドレスを入力します。
ステップ 5 [Start] ボタンをクリックして、トレースを開始します。

アラームおよびイベント

オーバーレイネットワーク内の個々のデバイスでイベントが発生すると、デバイスは Cisco SD-WAN Manager に通知を送信してそれを報告します。Cisco SD-WAN Manager は、イベント通知をフィルタリングし、関連するイベントを関連付け、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。

[Alarms] 画面では、オーバーレイネットワーク内の SD ルーティングデバイス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。

アラームとイベントのモニタリング

上部のバーにあるベルアイコンをクリックすると、Cisco SD-WAN Manager ダッシュボードからアラームを表示できます。アラームは、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。デフォルトでは、過去 24 時間のアラームが表示されます。または、次の手順に従って、Cisco SD-WAN Manager の [Alarms] 画面からアラームを表示します。

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

ステップ 2 Cisco SD-WAN Manager 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。

ステップ 3 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。

admin-techファイル

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、SD ルーティングデバイスから Cisco SD-WAN Manager 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 SD-WAN Manager、デバイス、またはその両方から削除できます。

Cisco SD-WAN Manager を使用した admin-tech ファイルの要求

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。admin-tech ファイルを要求するには、次の手順を実行します。

ステップ 1 Cisco SD-WAN Manager のメニューから [Tools] > [Operational Commands] の順に選択します。

ステップ 2 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。

ステップ 3 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。

a) 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。

b) 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 *bootflash:/core* または *harddisk:/core* ディレクトリに保存されます。

c) 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。

ステップ 4 [Generate] をクリックします。

Cisco SD-WAN Manager が admin-tech ファイルを作成します。ファイル名の形式は、*hostname-date-time-admin-tech.tar.gz* です。

ステップ 5 生成された admin-tech ファイルを表示するには、Cisco SD-WAN Manager のメニューから [Tools] > [Operational Commands] > [Show Admin Tech List] の順に選択します。

CLI を使用した admin-tech ファイルの要求

CLI を使用して admin-tech ファイルを要求するには、次の手順を実行します。

admin-tech ファイルを生成するには、**request tech-support** コマンドを使用します。

```
Device#request tech-support
21:03:46.447 UTC Thu Aug 10 2023 : Collecting 'show tech-support'...
21:04:51.880 UTC Thu Aug 10 2023 : 'show tech-support' collected successfully!
21:04:55.091 UTC Thu Aug 10 2023 : Collecting binary traces...
21:04:55.216 UTC Thu Aug 10 2023 : Binary traces collected successfully!
21:04:55.219 UTC Thu Aug 10 2023 : Collecting platform-dependent files...
21:05:43.467 UTC Thu Aug 10 2023 : Platform-dependent files collected successfully!
21:05:43.475 UTC Thu Aug 10 2023 : Generating tech-support bundle...
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle file
bootflash:core/1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz [size: 8648 KB]
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle generated successfully!

1HX-2017#
1HX-2017#dir bootflash:core
Directory of bootflash:/core/

1471682  -rw-                1  Aug 11 2023 04:26:51 +00:00  .callhome
45       -rw-            25429  Aug 10 2023 21:05:56 +00:00
1HX-2017_RP_0-debug_bundle_20230810-210346-UTC-info.txt
49       -rw-          8854997  Aug 10 2023 21:05:54 +00:00
1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz
1471685  drwx             4096  Mar 22 2021 20:03:54 +00:00  modules

29633794048 bytes total (16795193344 bytes free)
1HX-2017#
```

リアルタイムデータのモニタリング

デバイスに対して ping を実行するには、次の手順を実行します。

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

ステップ 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。

ステップ 3 単一デバイスの場合は、目的のデバイスで **[. .]** をクリックして、[Real Time] を選択します。

ステップ 4 [Device Options] ドロップダウンリストからデータのカテゴリを選択します。

結果が表示されます。

設定例

ここでは、設定例を紹介します。

例：Cisco SD-WAN Manager での制御接続の有効化

Cisco SD-WAN Manager で制御接続を有効にする例を以下に示します。

```
(config) sd-routing
(config-sd-routing) system-ip  172.16.255.15
(config-sd-routing) organization-name viptela
(config-sd-routing) vbond ip 10.0.12.26
(config-sd-routing) site-id 500
(config-sd-routing) wan-interface GigabitEthernet2
```

例：制御接続の有効化の確認

接続ステータスを確認するには、**show platform software yang-management process state** コマンドを使用します。

```
Device#show platform software yang-management process state
Confd Status: Started


Process              Status              State
------------------------------------------------------
nesd                 Running             Active
syncfd               Running             Active
ncsshd               Running             Not Applicable
dmiauthd             Running             Active
nginx                Running             Not Applicable
ndbmand              Running             Active
pubd                 Running             Active
```

vdaemon のステータスを確認するには、**show platform software yang-management process list r0 name vdaemon** コマンドを使用します。

```
Device#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id         : 29075
  Status           : S
  Session id       : 8829
  User time        : 263002
  Kernel time      : 347183
  Priority         : 20
  Virtual bytes    : 405110784
  Resident pages   : 12195
  Resident limit   : 18446744073709551615
```

```
Minor page faults: 716496
Major page faults: 9130
```

例：ルート証明書のインストール

ルート証明書をインストールする例を以下に示します。

```
Device# request platform software sd-routing root-cert-chain install bootflash:root-ca.crt
```

例：ルート証明書のインストールの確認

ルート証明書のインストールステータスを確認するには、**show sd-routing local-properties summary** コマンドを使用します。

```
Device#show sd-routing local-properties summary
personality                     vedge
sp-organization-name            vIPtela Inc Regression
organization-name               vIPtela Inc Regression
root-ca-chain-status            Installed
root-ca-crl-status              Not-Installed

Device#show sd-routing local-properties summary
certificate-status              Installed
certificate-validity            Valid
certificate-not-valid-before    Apr 25 00:55:28 2023 GMT
certificate-not-valid-after     Apr 24 00:55:28 2024 GMT
….......
dns-name                        vbond
site-id                         100
tls-port                        0
system-ip                       172.16.255.11
chassis-num/unique-id           C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                      12345707
```

トラブルシューティング

ここでは、Cisco SD-WAN Manager を使用して SD ルーティングデバイスを管理およびモニタリングする際に発生する一般的な問題のトラブルシューティングに使用できるコマンドについて説明します。

- **Show version**

（注） 動作モードは **show version** コマンドに含まれています。

```
When sd-routing feature is enabled:
Device#show version | include mode
Router operating mode: Autonomous (SD-Routing)
Device#

When sd-routing feature is not enabled:
Device#show version | include mode
Router operating mode: Autonomous
Device#
```

- **show platform software yang-management process state**
- **show sd-routing system status**
- **show sd-routing connections summary**
- **show platform software process list r0 name vdaemon**
- **show sd-routing local-properties summary**
- **show sd-routing local-properties wan ipv4**
- **show sd-routing local-properties vbond**
- **show sd-routing connections history**

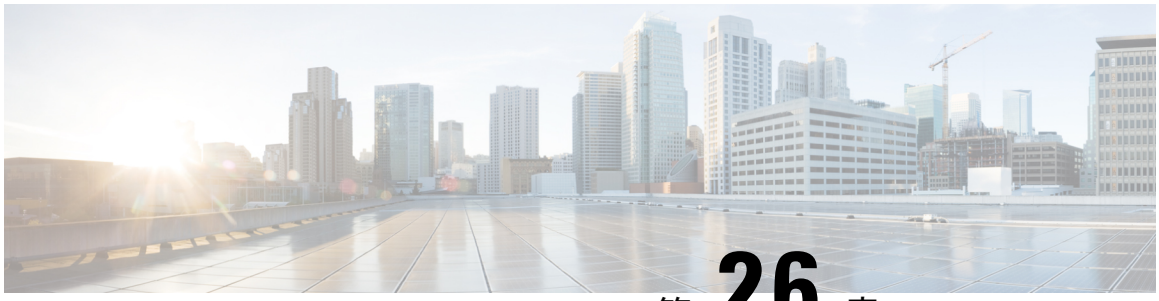
Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *41 : Cisco SD-WAN Manager* を使用した *SD* ルーティングデバイスに関する機能情報

機能名	リリース	機能情報
Cisco SD-WAN Manager を使用した SD ルーティングデバイスの管理	Cisco IOS XE リリース 17.12.1a	この機能を使用すると、Cisco SD-WAN Manager を使用して SD ルーティングデバイスの管理操作を実行できます。単一のネットワーク管理システム（Cisco SD-WAN Manager）を使用してすべての SD ルーティングデバイスをモニタリングできるため、ソリューションの導入が簡素化されます。



第 26 章

Web ユーザ インターフェイス管理

Web ユーザーインターフェイスを使用すると、わかりやすいグラフィカル インターフェイスを使用してルータのパフォーマンスを監視できます。

（注） 暗号マップトンネルを管理および設定するには、CLI を使用します。また、仮想トンネルインターフェイス（VTI）を使用してトンネルを設定し、CLI または GUI を使用してトンネルを作成することもできます。

次のいずれかのタスクの手順を実行して、ルータを設定できます。

- Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定 （277 ページ）
- 基本または詳細モード セットアップ ウィザードの使用 （278 ページ）

Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定

クイック セットアップ ウィザードを使用して、基本的なルータ設定を実行できます。ルータを設定するには、以下の手順を実行します。

始める前に

- Web UI にアクセスする前に、デバイスで基本設定を行う必要があります。

ステップ 1 シリアルケーブルの RJ-45 側をルータの RJ-45 コンソールポートに接続します。

ステップ 2 デバイスの初期設定ウィザードが表示された後、次のシステムメッセージがルータに表示されたら、「**No**」と入力してデバイスプロンプトを表示します。

Would you like to enter the initial configuration dialog? [yes/no]: no

ステップ 3 コンフィギュレーション モードで、次の設定パラメータを入力します。

```
!
ip dhcp pool WEBUIPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
username webui privilege 15 password cisco
!
interface gig 0/0/1
ip address 192.168.1.1 255.255.255.0
!
```

ステップ 4 イーサネットケーブルでデバイスとルータを接続し、gig 0/0/1 インターフェイスに接続します。

ステップ 5 システムを DHCP クライアントとして設定し、ルータの IP アドレスを自動的に取得します。

ステップ 6 ブラウザを起動し、ブラウザのアドレス行にデバイスの IP アドレスを入力します。セキュアな接続の場合は、「https://192.168.1.1/#/dayZeroRouting」と入力します。あまりセキュアではない接続の場合は、「http://192.168.1.1/#/dayZeroRouting」と入力します。

ステップ 7 デフォルトのユーザー名（webui）とデフォルトのパスワード（cisco）を入力します。

基本または詳細モード セットアップ ウィザードの使用

基本モードまたは詳細モードのセットアップを使用してルータを設定するには、次の手順を実行します。

ステップ 1 [Basic Mode] または [Advanced Mode] を選択し、[Go To Account Creation Page] をクリックします。

ステップ 2 ユーザ名とパスワードを入力します。確認のためにパスワードを再入力します。

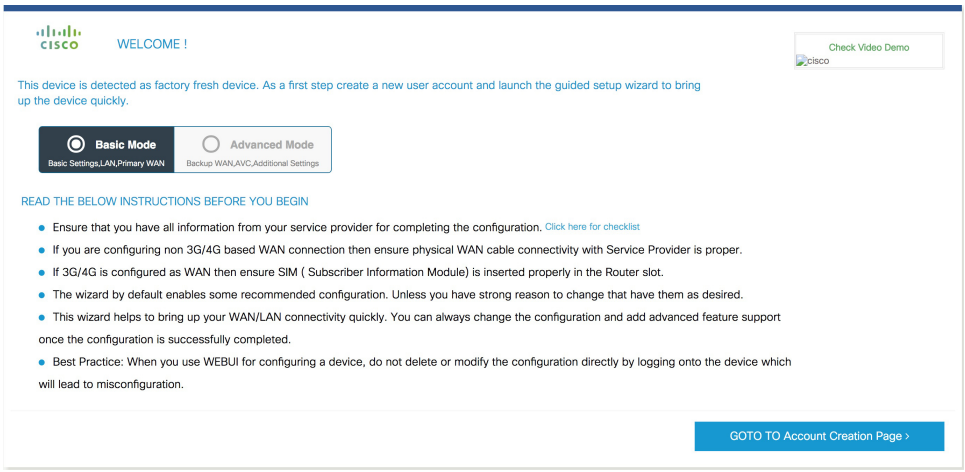
ステップ 3 [Create and Launch Wizard] をクリックします。

ステップ 4 デバイス名とドメイン名を入力します。

ステップ 5 [Time Zone] ドロップダウンリストから、適切なタイムゾーンを選択します。

ステップ 6 [Date and Time] ドロップダウンリストから、適切な日時モードを選択します。

ステップ 7 [LAN Settings] をクリックします。



LAN 設定を行います。

ステップ 1 [Web DHCP Pool/DHCP Pool] 名または [Create and Associate Access VLAN] オプションを選択します。

a) [Web DHCP Pool] を選択した場合は、次を指定します。

[Pool Name]：DGCP プール名を入力します。

[Network]：ネットワークアドレスおよびサブネットマスクを入力します。

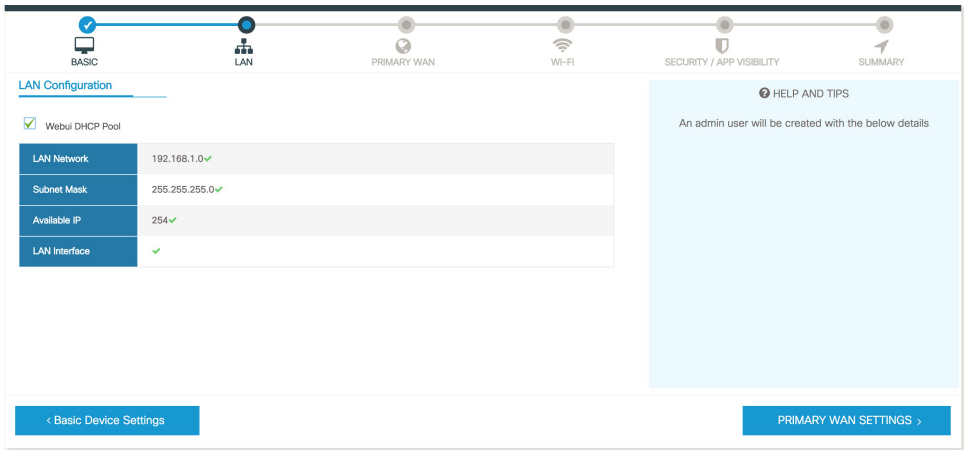
b) [Create and Associate Access VLAN] オプションを選択した場合は、次を指定します。

[Access VLAN]：アクセス VLAN の識別番号を入力します。指定できる範囲は 1 ～ 4094 です。

[Network]：VLAN の IP アドレスを入力します。

[Management Interfaces]：インターフェイスを選択し、右矢印と左矢印を使用して選択したリストボックスに移動します。ダブルクリックするかドラッグアンドドロップして、選択したリストボックスにインターフェイスを移動することもできます。

ステップ 2 [**Primary WAN Settings**] をクリックします。



プライマリ WAN 設定を行います。

ステップ 1 プライマリ WAN タイプを選択します。プライマリ WAN は、ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド（xDSL）を設定できます。

ステップ 2 ドロップダウン リストからインターフェイスを選択します。

ステップ 3 サービス プロバイダーから DNS サーバ情報を直接取得するには、[**Get DNS Server info directly from ISP**] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。

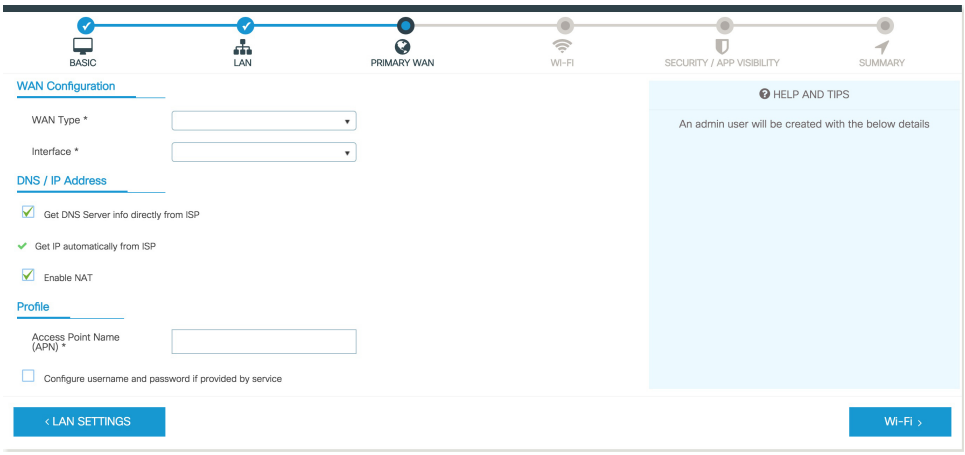
ステップ 4 [**Get IP automatically from ISP**] チェックボックスをオンにして、サービスプロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネット マスクを入力します。

ステップ 5 [**Enable NAT**] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。

ステップ 6 [Enable PPPoE] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは **PAP** と **CHAP** です。

ステップ 7 サービスプロバイダーから提供されたユーザー名とパスワードを入力します。

ステップ 8 [**Security/APP Visibility WAN Settings**] をクリックします。



セカンダリ WAN 設定を行います。

詳細設定では、セカンダリ WAN 接続を設定する必要があります。

ステップ 1 セカンダリ WAN タイプを選択します。ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド（xDSL）をセカンダリ WAN として設定できます。

ステップ 2 ドロップダウン リストからインターフェイスを選択します。

ステップ 3 サービス プロバイダーから DNS サーバ情報を直接取得するには、[**Get DNS Server info directly from ISP**] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。

ステップ 4 [**Get IP automatically from ISP**] チェックボックスをオンにして、サービスプロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネット マスクを入力します。

ステップ 5 [**Enable NAT**] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。

ステップ 6 [Enable PPPoE] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは **PAP** と **CHAP** です。

ステップ 7 サービスプロバイダーから提供されたユーザー名とパスワードを入力します。

ステップ 8 [**Security/APP Visibility WAN Settings**] をクリックします。

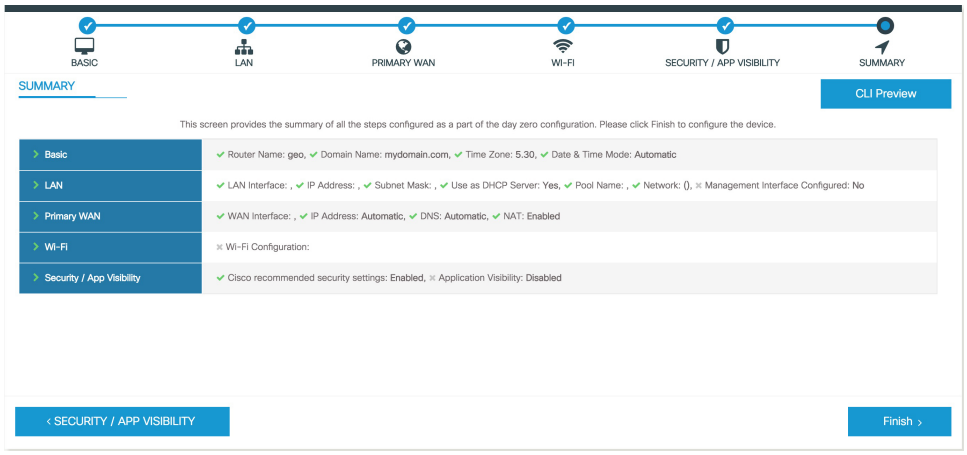
セキュリティ設定の構成

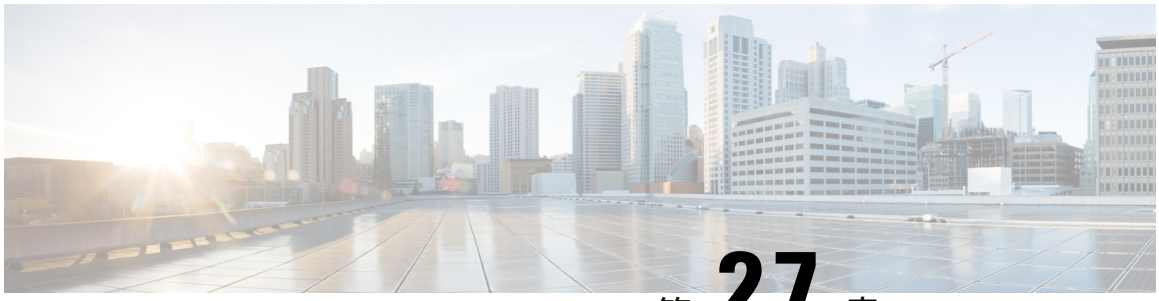
ステップ 1 すべてのパスワードがプレーンテキストで表示されないようにするには、[**Enable Recommended Settings**)] チェックボックスをオンにします。パスワードは暗号化されます。

ステップ 2 [**Day 0 Config Summary**] をクリックします。

ステップ 3 設定をプレビューするには、[CLI preview] をクリックします。

ステップ 4 [Finish] をクリックして、デイゼロセットアップを完了します。





第 27 章

GRUB モードへのアクセスと使用

Cisco Catalyst 8000V は、NVRAM 内に 16 ビットのコンフィギュレーション レジスタを搭載しています。各ビットの値は1（オン、つまり設定）または0（オフ、つまり解除）です。各ビットの設定は、次回のリロードまたはオフ/オン時のルータ動作に影響を与えます。GRUB モードでは、他のシスコ ルータの ROMMON オプションに相当するコンフィギュレーション レジスタ オプションのサブセットがサポートされます。

コンフィギュレーション レジスタを使用すると、次の作業を行うことができます。

- ルータで GRUB モード（ブートストラッププログラム）を強制的に起動させる
- 起動元およびデフォルトのブートファイル名を選択する
- 忘れたパスワードを回復する

次の表でコンフィギュレーション レジスタ ビットについて説明します。

表 *42*：コンフィギュレーション レジスタ ビットの説明

ビット番号	16 進数	意味
00 ～ 03	0x0000 ～ 0x000F	ブート フィールド。ブート フィールドの設定によって、ルータがオペレーティング システムをロードするかどうか、どこからシステム イメージを取得するかが決まります。 詳細については、表「コンフィギュレーション レジスタのブートフィールドビットの説明」を参照してください。

ビット番号	16 進数	意味
06	0x0040	システム ソフトウェアに NVRAM の内容を無視させます。これは、パスワード回復に使用できます。

（注） クラウドソリューションで実行されている Cisco Catalyst 8000V の GRUB モードの開始は、クラウドプロバイダーのコンソールアクセス機能によって異なります。クラウドプロバイダーがコンソールへの制限付きアクセスを提供している場合、パスワード回復のために GRUB モードにアクセスすることはできません。

（注） ルータの再起動時に自動的に GRUB モードになるようにルータを設定するには、0x000 設定を使用します。

- GRUB モードへのアクセス （284 ページ）
- GRUB メニューの使用 （285 ページ）
- コンフィギュレーション レジスタ（confreg）の変更 （287 ページ）
- コンフィギュレーション レジスタ設定の変更 （289 ページ）
- コンフィギュレーション レジスタの設定の表示 （290 ページ）

GRUB モードへのアクセス

GRUB モードにアクセスするには、次の手順を実行します。

ステップ 1 **enable**

例：

```
Router> enable
```

特権 EXEC モードをイネーブルにします。

- プロンプトが表示されたらパスワードを入力します。

ステップ 2 **config-register 0x0000**

例：

```
Router# config-register 0x0000
```

値「0000」（0x0）を入力して GRUB モードを開始します。

次に、GRUB モードを開始する例を示します。

```
Router(config)# config-register 0x0000

GNU GRUB  version 2.02

Minimal BASH-like line editing is supported. For the first word, TAB
lists possible command completions. Anywhere else TAB lists possible
device or file completions. ESC at any time exits.

grub> confreg 0x2102
```

grub> プロンプトで疑問符を入力すると、システムヘルプの表示と **config register** コマンドの入力の 2 つのオプションが表示されます。

GRUB メニューの使用

GRUB メニューを使用して、ルータにロードされているソフトウェアイメージを表示し、どのイメージから起動するかを選択します。GRUB メニューにアクセスするには、GRUB プロンプトで「**ESC**」と入力します。次に、GRUB メニューの表示を示します。

上下の矢印キーを使用して、どのイメージからルータを起動するかを選択します。GRUB プロンプトに戻るには、文字「**c**」を入力します。

GRUB モードの開始とイメージの選択

GR およびユニファイドブートローダー（GRUB）モードから新しいシステムイメージをロードするには、EXEC モードで次の手順を実行します。

ステップ 1　dir bootflash:

このコマンドを使用して、ブートフラッシュメモリ内のすべてのファイルおよびディレクトリを表示します。

例：

```
Router# dir bootflash:

Directory of bootflash:/
    3  -rw-     6458388   Dec 18 2020 00:00:58 c8000v.tmp
 1580  -rw-     6462268   Dec 18 2020 06:14:02 c8000v-ata
63930368 bytes total (51007488 bytes free)
```

ステップ 2　configure terminal

このコマンドを使用して、グローバル コンフィギュレーション モードを開始します。

例：

```
Router# configure terminal
Router(config)#
```

ステップ 3 **boot system bootflash:***system-image-filename*.bin

次回システム リロード後またはオフ/オン後に新しいシステム イメージをロードします。次に例を示します。

例：

```
Router(config)# boot system bootflash:
c8000v-universalk9.17.04.01a.SPA.bin
```

（注） 新しいシステムイメージが、**dir bootflash:** コマンド出力に表示される最初のファイルまたは唯一のファイルの場合は、このステップを実行する必要はありません。

ステップ 4 **do write**

または

do write memory

例：

```
Router(config)# do write memory
```

（注） **do write** コマンドまたは **do write memory** コマンドを入力すると、ブートフラッシュディスクで使用可能なイメージの GRUB メニューリストが更新されます。

ステップ 5 **config-register 0x0000**

このコマンドを使用して、GRUB モードを開始します。

次に、GRUB モードを開始する設定出力の例を示します。

例：

```
GNU GRUB  version 2.02

   Minimal BASH-like line editing is supported. For the first word, TAB
   lists possible command completions. Anywhere else TAB lists possible
   device or file completions. ESC at any time exits.


grub> confreg 0x2102
```

例：

（注） config-register を 0x0000 に設定した場合は、システムを自動起動するために、デフォルトの 0x2102 にリセットする必要があります。値が 0x0 の場合、システムは GRUB モードで停止します。

ステップ 6 **grub>** プロンプトで「ESC」と入力して、GRUB メニューにアクセスします。

起動に使用できるイメージを含む GRUB メニューが表示されます。

例：

```
Cisco IOS XE Software, Version 2020-09-17_09.24_kamitch
Cisco IOS Software [Bengaluru], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental
 Version 17.5.20200916:194029 [HEAD-/scratch/kamitch/git/polaris-work/boottime1 106]
```

```
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Wed 16-Sep-20 15:45 by kamitch


Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 18 minutes
Uptime for this control processor is 21 minutes
System returned to ROM by reload
System image file is "bootflash:packages.conf"
```

上下の矢印キーを使用して、ルータを起動するイメージを選択します。GRUB プロンプトに戻るには、文字「**c**」を入力します。

ステップ 7 ルータのソフトウェアイメージを新しいバージョンにアップグレードするには、.bin ファイルを選択します。

ステップ 8 **Enter** を押して選択したイメージを起動し、アップグレードプロセスを開始します。

コンフィギュレーション レジスタ（confreg）の変更

このセクションでは、**confreg** GRUB コマンドを使用して、コンフィギュレーション レジスタを変更する方法について説明します。このコマンドは、他のシスコ製ハードウェアルータの **confreg** ROMOM コマンドに似ています。このルータには ROMOM モードが含まれていないため、同様の機能は GRUB コマンドモードで処理されます。

グローバル コンフィギュレーション モードで **config-register** コマンドを使用して、Cisco IOS CLI からコンフィギュレーション レジスタの設定を変更することもできます。

（注） 変更したコンフィギュレーション レジスタ値は、NVRAM に自動的に書き込まれますが、新しい値が有効になるのは、ルータをリセットまたはオフ/オンしてからです。

confreg [*value*]

例：

```
grub> confreg 0x2102
```

GRUB コマンド モードでコンフィギュレーション レジスタの設定値を変更します。

- 任意で、コンフィギュレーション レジスタに対応する新しい16進値を入力します。値の範囲は0x0～0xFFFF です。
- 値を入力しなかった場合、16ビットのコンフィギュレーション レジスタの各ビットについて、入力が求められます。

次のタスク

次のコードは、GRUB モードを開始して、コンフィギュレーション レジスタを使用する例です。GRUB モードにアクセスするには、Cisco IOS XE **config-register** コマンドを入力し、値として「0000」を指定します。

```
Router(config)# config-register 0x0000

GNU GRUB  version 0.97  (638K lower / 3143616K upper memory)
 [ Minimal BASH-like line editing is supported.  For the first word, TAB
   lists possible command completions.  Anywhere else TAB lists the possible
   completions of a device/filename.  ESC at any time exits to menu. ]
grub> help
 [ Minimal BASH-like line editing is supported.  For the first word, TAB
   lists possible command completions.  Anywhere else TAB lists the possible
   completions of a device/filename.  ESC at any time exits to menu. ]
confreg [VALUE]                        help [--all] [PATTERN ...]
grub> confreg
          Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
boot: the boot loader
do you wish to change the configuration? y/n [n
]:
ignore system config info? y/n [n
]:
automatically boot default system image? y/n [n
]:
Configuration Register: 0x0
grub> confreg
          Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
boot: the boot loader
do you wish to change the configuration? y/n [n
]:
ignore system config info? y/n [n]:
automatically boot default system image? y/n [n]:
Configuration Register: 0x42
grub> confreg 0x2102
Configuration Register: 0x2102
grub> confreg
          Configuration Summary
   (Virtual Configuration Register: 0x2102)
enabled are:
boot: default image
do you wish to change the configuration? y/n [n
]:
grub>
grub>
    GNU GRUB  version 2.02  (638K lower / 3143616K upper memory)
```

```
----------------------------------------------------------------------
 0: C8000v - packages.conf
 1: C8000v - c800v-packages-universalk9
 2: C8000v - GOLDEN IMAGE
----------------------------------------------------------------------
      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, or 'c' for a command-line.
    Highlighted entry is 0:
  Booting 'C8000v - packages.conf'
root (hd0,0)
 Filesystem type is ext2fs, partition type 0x83
kernel /packages.conf rw root=/dev/ram console=ttyS1,9600 max_loop=64 HARDWARE=
virtual SR_BOOT=harddisk:packages.conf
Calculating SHA-1 hash...done
SHA-1 hash:
        calculated   817e1716:e8e62778:7dd0b806:32db2bdd:13e51407
        expected     817e1716:e8e62778:7dd0b806:32db2bdd:13e51407
package header rev 1 structure detected
Calculating SHA-1 hash...done
SHA-1 hash:
        calculated   d4eaba99:34cbda63:26151233:9d0e9aa4:9c625302
        expected     d4eaba99:34cbda63:26151233:9d0e9aa4:9c625302
Package type:0x7531, flags:0x0
   [Linux-bzImage, setup=0x2e00, size=0x2c18c00]
   [isord @ 0x7e6d0000, 0x191f000 bytes]
```

コンフィギュレーション レジスタ設定の変更

コンフィギュレーション レジスタの設定値は、GRUB からでも Cisco IOS XE CLI からでも変更できます。ここでは、Cisco IOS XE CLI からコンフィギュレーション レジスタの設定値を変更する方法について説明します。

Cisco IOS XE CLI からコンフィギュレーション レジスタの設定値を変更する手順は、次のとおりです。

ステップ 1 ルータの電源を投入します。

ステップ 2 初期ダイアログを開始するかどうか尋ねられるので、no と応答します。

例：

```
Would you like to enter the initial dialog? [yes]: no
```

数秒後にユーザー EXEC プロンプト（Router>）が表示されます。

ステップ 3 「enable」と入力して特権 EXEC モードを開始し、プロンプトが表示されたらパスワードを入力します。

例：

```
Router> enable
Password: password
Router#
```

ステップ 4 グローバル コンフィギュレーション モードを開始します。

例：

```
Router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
```

ステップ 5 コンフィギュレーション レジスタの設定値を変更するには、**config-register** *value* コマンドを入力します。*value* は **0x** を前に加えた 16 進数です。

例：

```
Router(config)# config-register 0x
value
```

ステップ 6 グローバル コンフィギュレーション モードを終了します。

例：

```
Router(config)# end
Router#
```

ステップ 7 変更した設定を NVRAM に保存します。

Router# **copy running-config startup-config**

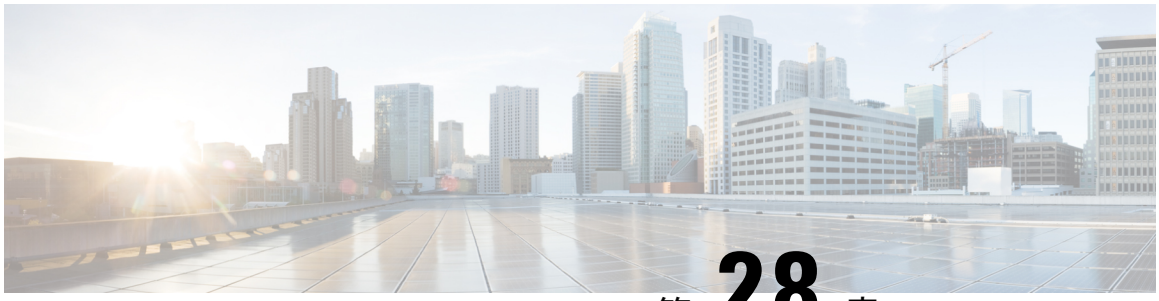
新しいコンフィギュレーション レジスタの設定値が NVRAM に保存されても、有効になるのは次回のルータ リロード時またはオフ/オン時です。

コンフィギュレーション レジスタの設定の表示

現在有効なコンフィギュレーション レジスタの設定値および次回のルータリロード時に使用される設定値を表示するには、特権 EXEC モードで **show version** コマンドを入力します。

コンフィギュレーション レジスタの設定値は、**show version** コマンド出力の最終行に示されます。

```
Configuration register is 0x142 (will be 0x142 at next reload)
```



第 28 章

工場出荷時の状態へのリセット

この章では、Cisco Catalyst 8000V の初期設定へのリセットの実行について説明します。初期設定へのリセット機能は、ルータから機密情報を削除したり、ルータを完全に機能する状態にリセットしたりするのに役立ちます。

初期設定へのリセットに関する情報

初期設定へのリセットは、ルータの現在の実行コンフィギュレーション情報およびスタートアップコンフィギュレーション情報をクリアし、ルータを以前の完全に機能する状態にリセットするプロセスです。初期設定へのリセットプロセスでは、**factory-reset all** コマンドを使用します。

（注） Cisco Catalyst 8000V インスタンスの初期設定へのリセットにかかる時間は、ストレージのタイプやルータに存在するデバイスなどの要因によって異なります。

削除される情報：

初期設定へのリセットを実行すると、次の情報が削除されます。

- ライセンス：ユーザーがインストール、製造元が提供
- 不揮発性ランダム アクセス メモリ データ
- ユーザーのログイン情報
- 起動設定
- すべての書き込み可能ファイルシステムおよび個人データ

- ROMMON 変数
- 永続ストレージデバイス
- ブートフラッシュで実行されているコンテナ

保持される情報：

ただし、次の情報は初期設定へのリセット後も保持されます。

- リセット完了後にルータへのアクセスを提供するファイルを含む重要な情報
- 初期設定へのリセットを実行する前にインストールされていたソフトウェアパッケージ
- UDI およびスマートライセンスファイル

サポートされているシナリオ：

初期設定へのリセット機能は、次のシナリオで使用できます。

- Cisco Catalyst 8000V インスタンスを安全な方法で削除する場合。
- 悪意のある攻撃によってルータのデータが侵害された場合、ルータを初期設定にリセットしてから、今後の使用のためにもう一度設定しなおす必要があります。

サポート対象プラットフォーム：

初期設定へのリセットは、Amazon Web Services、Microsoft Azure、GCP クラウド、VMware ESXi、Hyper-V を含むすべてのプラットフォームで実行されている Cisco Catalyst 8000V インスタンスでサポートされています。

初期設定へのリセット実行の前提条件

- 初期設定へのリセット操作を実行する前に、すべてのソフトウェアイメージ、設定、および個人データがバックアップされていることを確認してください。
- 初期設定へのリセットプロセスが進行中の場合は、電源の中断がないことを確認します。
- インスタンスのブートフラッシュに少なくとも 8 GB のメモリがあることを確認します。

初期設定へのリセット実行の制限事項

- ルータにインストールされているソフトウェアパッチは、初期設定へのリセット操作後に復元されません。
- 初期設定へのリセットプロセス中は、Cisco Catalyst 8000V インスタンスを再起動しないでください。

- 仮想テレタイプ（VTY）セッションを介して factory reset コマンドが発行された場合、初期設定へのリセットプロセスの完了後にセッションは復元されません。

初期設定へのリセットの実行方法

ステップ 1 Cisco Catalyst 8000V インスタンスにログインします。

ステップ 2 コマンドプロンプトで、**factory-reset all** コマンドを実行します。

次の情報が表示されます。

```
factoryreset#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
 The following will be deleted as a part of factory reset:
 1: All writable file systems and personal data
 2: Licenses
 3: Configuration
 4: User Credentials
 The system will reload to perform a factory reset.
 Note that any day0 configuration will be applied after reload
 DO NOT STOP OR INTERRUPT THE POWER DURING RESET
Are you sure you want to continue? [confirm]Connection to 172.18.25.29 closed by remote host.
Connection to 172.18.25.29 closed.
```

ステップ 3 confirm と入力して初期設定へのリセットを続行します。

（注） 初期設定へのリセットプロセスにかかる時間は、ストレージのタイプと、Cisco Catalyst 8000V インスタンスを展開するクラウドサービスによって異なります。

（注） 初期設定へのリセットプロセスを終了する場合は、**Escape** キーを押します。

次のタスク

初期設定へのリセットプロセスが完了すると、プロセスが成功したかどうかを示すログファイルがブートフラッシュに保存されます。

初期設定へのリセット後におけるスマートライセンスの復元

リセット後、スマートライセンスの設定も削除されます。トークン ID を使用して、ルータでスマートライセンスを再設定する必要があります。接続モードでは、スマートライセンス用にインスタンスを登録するときに、強制オプションを使用する必要があります。つまり、**license smart register idtoken *****token***** force** コマンドを使用する必要があります。登録プロセスが開始されます。

強制オプションを使用せず、スマートライセンスを直接設定すると、ライセンスの登録が失敗します。次に、失敗した登録の出力例を示します。

```
router#show license status
router#show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 15 22:03:29 2019 UTC
    Failure reason: The product
regid.2013-08.com.cisco.C8KV,1.0_1562da96-9176-4f99-a6cb-14b4dd0fa135 and sudi containing
 udiSerialNumber:9XIVK9PIVPK,udiPid:C8000V has already been registered.

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
```

license smart register idtoken *****token***** force コマンドを実行すると、ライセンスは登録済み（Registered）状態になります。次に、Registered 状態の設定出力の例を示します。

```
router#show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: InternalTestDemoAccount8.cisco.com
  Virtual Account: RTP-CSR-DT-Prod
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Feb 15 22:04:07 2019 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Dec 14 22:04:06 2020 UTC
  Registration Expires: Dec 15 21:59:05 2021 UTC

License Authorization:
  Status: AUTHORIZED on Dec 15 22:04:11 2020 UTC
  Last Communication Attempt: SUCCEEDED on Feb 15 22:04:11 2019 UTC
  Next Communication Attempt: Dec 17 22:04:11 2020 UTC
  Communication Deadline: Dec 16 21:58:10 2020 UTC
```

```
Export Authorization Key:
  Features Authorized:
    <none>
```

初期設定へのリセット後の動作

初期設定へのリセットが正常に完了すると、ルータが起動します。ただし、初期設定へのリセットプロセスが開始される前に、コンフィギュレーション レジスタが ROMMON から手動で起動するように設定されていた場合、ルータは ROMMON で停止します。

重要 現在のブートイメージがリモートイメージであるか USB または NIM-SSD に保存されている場合は、初期設定へのリセットプロセスを開始する前に、必ずイメージのバックアップを作成してください。

初期設定にリセットしても、Cisco Catalyst 8000V インスタンスの UDI は変更されません。初期設定へのリセット後に UDI が同じであるかどうかを確認するには、初期設定へのリセットプロセスの前後に **factoryreset#show license udi** コマンドを実行します。

スマートライセンスを設定したら、**#show license status** コマンドを実行して、インスタンスでスマートライセンスが有効になっているかどうかをチェックします。

（注） 初期設定へのリセットを実行する前に SLR を有効にしていた場合は、同じライセンスを使用し、スマートエージェントから受け取ったライセンスキーを入力します。

第 29 章

VRF ルート共有の設定

次の章では、Cisco Catalyst 8000V インスタンスで VRF ルート共有を設定する方法について説明します。VRFルート共有は、オンプレミスサイトとパブリッククラウドサイト間でトラフィックを転送する必要がある場合に必要です。クラウド全体に共有サービスを展開するには、VxLANピア間で VRF ルート共有を設定します。

VRF ルート共有に関する情報

APIC レイヤ（オンプレミス）とパブリッククラウドサイトがあるハイブリッド クラウド ソリューションでは、Cisco Catalyst 8000V インスタンスはレイヤ 3 境界を介してデータセンターを接続します。Cisco Catalyst 8000V インスタンスには、2 セットのインポートおよびエクスポートルート ターゲットで設定された VRF インスタンスがあります。インポート/エクスポート ルート ターゲットの 1 つのセットは、オンプレミス ルータの VXLAN カプセル化および L3 ルーティング情報を使用して BGP EVPN セッションに関連付けられます。インポート/エクスポートルート ターゲットの他のセットは、サービス プロバイダー ネットワークの L3VPN BGP ネイバーに関連付けられます。Cisco Catalyst 8000V インスタンスは、オンプレミスサイトとサービス プロバイダー ネットワーク間のルートをステッチすることで、EVPN 全体で L3 トラフィックの移動を可能にします。

Cisco Catalyst 8000V インスタンスは、VRF に同じ VTEP IP（VxLAN トンネルエンドポイント）と RMAC（ルータ MAC アドレス）がある場合でも、EVPN を介してトラフィックを転送します。この機能により、Cisco Catalyst 8000V インスタンスはバインディングラベルを使用してルーティングと転送チェーンを設定します。

VRF ルート共有機能を使用すると、ハイブリッドクラウド全体に共有サービスを展開できます。パブリッククラウドで実行される共有サービスは、オンプレミスサイトのエンドポイントで使用できます。Cisco Catalyst 8000V インスタンスは、オンプレミスサイト上の複数の VRF

とL3プレフィックスを共有し、その逆も同様です。APIC レイヤはアドレスをインポートし、サービスは APIC 側で使用されます。

VRF ルート共有の前提条件

VRF ルート共有機能を設定して ACI とパブリッククラウド間のトラフィックを有効にする前に、次のことを確認します。

- ACI の vPC ペアで VRF1 と VRF2 を設定します。
- VRF3 は、VGW とピアリングする Cisco Catalyst 8000V インスタンス上の VRF4 であり、VRF ごとに 2 つの RT があります。
- Cisco Catalyst 8000V インスタンスは、VRF1&2 の EVPN ルートを ACI から VRF3&4 にインポートします。
- Cisco Catalyst 8000V 側の IP BGP は、パブリッククラウドのゲートウェイにルートを再配布します。
- ACI からのルートのネクストホップは、ACI の境界リーフのスパインです。
- ルート共有 VRF 全体でプレフィックスの重複はありません。
- L3 VPN ルーティングをアドバタイズし、VRF プレフィックスを EVPN ネイバーに転送します。advertise l2vpn evpn コマンドを実行し、スティッチング RT をエクスポートして、ネイティブルートを EVPN にプッシュします。

VRF ルート共有に関する制約事項

- VRF 共有機能は、最大 32 の共通 VRF と 1000 のカスタマー VRF の組み合わせをサポートします。
- この機能は RT フィルタをサポートしていません。
- VRF ルート共有は、IPv4 アドレスでのみサポートされ、IPv6 アドレスではサポートされません。

VRF ルート共有の設定方法

サンプルトポロジと使用例

ハイブリッドクラウドでの VRF ルート共有を説明するために、サンプルトポロジについて考えてみましょう。サンプルトポロジでは、Cisco Catalyst 8000V インスタンスがパブリッククラウドの VM に展開されていると見なします。サイト A は ACI 展開サイトで、サイト B はパブ

リッククラウドです。リーフ 1 とリーフ 2 は、ACI の仮想ポートチャネル（vPC）ペアです。これらの 2 つの vPC は、異なるルート識別子（RD）で設定されます。ここでは、VRF 1 と VRF 2 が ACI の vPC ペアで設定されています。次の例を参考にしてください。

VRF1 - RT：RT-EVPN-1、プレフィックス：192.168.1.1

VRF2 - RT：RT-EVPN-2、プレフィックス：192.168.2.2

Cisco Catalyst 8000V インスタンスで VRF3 と VRF4 が設定されています。これら 2 つの VRF は音声ゲートウェイ（VGW）とペアになっており、これら 2 つの VRF には 2 つの異なるルートターゲット（RT）があります。次の例を参考にしてください。

VRF3 – EVPN 用 RT：RT-EVPN-3、IP BGP 用 RT：RT-3、プレフィックス：192.168.3.3

VRF4 – EVPN 用 RT：RT-EVPN-4、IP BGP 用 RT：RT-4、プレフィックス：192.168.4.4

このトポロジでは、BGP-EVPN ファブリックが ACI とパブリッククラウドの Cisco Catalyst 8000V インスタンスの間に存在し、Cisco Catalyst 8000V インスタンスと Azure などのクラウドサービス プロバイダーの間で IP BGP プロトコルが使用されます。BGP-EVPN ファブリックは、EVPN と IP BGP 間のスティッチングルートを再配布します。

ACI サイトとパブリッククラウド間のトラフィックフローを有効にするには、ACI と Cisco Catalyst 8000V インスタンスの両方が VRF ルート共有をサポートする必要があります。

Cisco Catalyst 8000V インスタンスは、VRF1 および VRF2 の EVPN ルートを ACI から VRF3 および VRF4 にインポートできる必要があります。Cisco Catalyst 8000V 側の IP BGP は、パブリッククラウド内の VGW へのルートを再配布します。

（注） VTEP（VxLAN トンネルエンドポイント）IP と RMAC（ルート MAC アドレス）が 2 つのリーフで同じで、VNIC だけが異なる場合、Cisco Catalyst 8000V インスタンスはトンネルを介してトラフィックを転送できます。

ユースケース

同じトポロジ例を使用して、Cisco Catalyst 8000V インスタンスで VRF ルート共有を設定する使用例を次に示します。

- VRF1 と VRF2 は VRF3 と通信できるが、VRF3 と VRF4 は相互に通信できない場合は、次の設定を実行します。

```
vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
vrf definition VRF4
rd 400:1
address-family ipv4
```

- VRF1 と VRF2 が VRF3 および 4 と通信できるが、VRF3 と VRF4 が相互に通信できない場合は、次の設定を実行します。

```
vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
vrf definition VRF4
rd 400:1
address-family ipv4
route-target export RT-EVPN-4 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
```

- VRF1 と VRF2 は VRF3 と通信できるが、VRF3 と VRF4 は相互に通信できる場合は、次の設定を実行します。

```
vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
route-target export RT-3
route-target import RT-4
vrf definition VRF4
rd 400:1
address-family ipv4
route-target import RT-3
route-target export RT-4
```

- VRF1 と VRF2 は VRF3 および 4 と通信できるが、VRF3 と VRF4 は相互に通信できる場合は、次の設定を実行します。

```
vrf definition VRF3
rd 300:1
address-family ipv4
route-target export RT-EVPN-3 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
route-target export RT-3
route-target import RT-4
vrf definition VRF4
rd 400:1
address-family ipv4
route-target export RT-EVPN-4 stitching
route-target import RT-EVPN-1 stitching
route-target import RT-EVPN-2 stitching
route-target import RT-3
route-target export RT-4
```

（注） 上記の使用例では、Cisco Catalyst 8000V インスタンスは VRF3 と VRF4 の両方で EVPN を設定する必要があります。

IP BGP はすでに VRF3 と VRF4 からすべてのルートをインポートしていますが、BGP はインポートされた VRF のルートを EVPN ピアにアドバタイズしません。

VRF ルート共有の設定

EVPN 全体で共有が行われる場合にのみ、設定で **Stitching** キーワードを使用する必要があります。

VRF ルート共有の設定

VRF 1 および VRF 2（オンプレミス）が VRF 3 および VRF 4（パブリッククラウド内）と通信できるハイブリッドクラウドで VRF ルート共有を設定するには、次の設定を実行します。このソリューション例では、VRF3 と VRF4 は相互に通信できません。

例：

```
vrf definition vrf3
rd 3:3
address-family ipv4
Route-target export 100:3
Route-target import 100:4
route-target export 3:3 stitching
route-target import 1:1 stitching
route-target import 2:2 stitching
exit-address-family
!
!
vrf definition vrf4
rd 4:4
address-family ipv4
Route-target import 100:3
Route-target export 100:4
route-target export 4:4 stitching
route-target import 1:1 stitching
route-target import 2:2 stitching
exit-address-family
!
!
interface BDI100
no shutdown
vrf forwarding vrf3
ip address 10.1.1.1 255.255.255.224
!
interface GigabitEthernet4.2
encapsulation dot1Q 2
vrf forwarding vrf3
ip address 10.4.4.1 255.255.255.224
bridge-domain 100
member vni 10100
!
interface nve1
source-interface loopback0
host-reachability protocol bgp
member vni 10100 vrf vrf3
!
router bgp 100
bgp router-id 10.11.11.11
no bgp default ipv4-unicast
neighbor 192.168.22.22 remote-as 200
neighbor 198.162.22.22 update-source loopback0
neighbor 198.162.22.22 ebgp-multihop 255
address-family ipv4 vrf vrf3
redistribute connected
neighbor 10.0.0.2 remote-as 300
```

```
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community both
advertise l2vpn evpn
exit-address-family
!
address-family l2vpn evpn
neighbor 198.162.22.22 activate
neighbor 198.162.22.22 send-community both
exit-address-family
end
```

VRF ルート共有の確認

ステップ 1 **show ip bgp l2vpn evpn summary**.

VRF デフォルトアドレスファミリ（L2VPN EVPN）の BGP サマリー情報を指定します。

例：

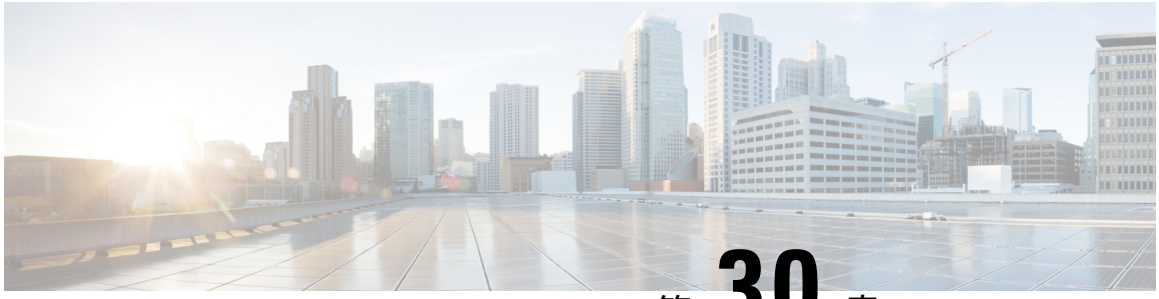
```
show ip bgp l2vpn evpn summary
BGP router identifier 10.11.11.11, local AS number 100
BGP table version is 8, main routing table version 8
7 network entries using 2408 bytes of memory
......
BGP activity 14/0 prefixes, 16/0 paths, scan interval 60 secs
7 networks peaked at 17:34:38 Aug 14 2019 CST (00:00:26.895 ago)
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
198.162.22.22     4          200       6       5        4    0    0 00:01:23        4
Device#
```

ステップ 2 **show ip route vrf vrf3 bgp | in binding**.

VRF に関連付けられた IP ルーティングテーブル情報を表示します。出力にバインディングラベルが付いている場合は、設定が成功し、BGP がバインディングラベルをネクストホップとして使用していることを示しています。

例：

```
+++ 17:35:05 Minuet(default) exec +++
show ip route vrf vrf3 bgp | in binding
B        10.2.1.0/24 [20/0] via binding label: 0x3000001, 00:00:26
B        10.2.2.0/24 [20/0] via binding label: 0x3000002, 00:00:26
B     192.168.1.0/24 [20/0] via binding label: 0x3000001, 00:00:26
B     192.168.2.0/24 [20/0] via binding label: 0x3000002, 00:00:26
Device#
```



第 30 章

ブリッジ ドメイン インターフェイスの設定

Cisco C8000V ルータは、レイヤ 3 IP アドレスにレイヤ 2 イーサネットセグメントをパッケージングするためのブリッジ ドメイン インターフェイス（BDI）機能をサポートします。

ブリッジ ドメイン インターフェイスの制約事項

ブリッジ ドメイン インターフェイスに関連する制約事項は次のとおりです。

- システムごとにサポートされるブリッジ ドメイン インターフェイスは 4096 のみです。
- ブリッジドメインインターフェイスの場合、最大伝送単位（MTU）サイズは 1500 および 9216 バイトの間で設定できます。
- ブリッジ ドメイン インターフェイスは次の機能のみをサポートします。
  - IPv4 マルチキャスト
  - QoS マーキングとポリシング。シェーピングとキューイングはサポートされません。
  - IPv4 VRF
  - IPv6 ユニキャスト転送
  - BGP、OSPF、EIGRP、RIP、IS-IS、STATIC などのダイナミックルーティング
  - IOS XE 3.8.0 以降の Hot Standby Router Protocol（HSRP）
  - IOS XE 3.8.0 以降の Virtual Router Redundancy Protocol（VRRP）
  - Flexible NetFlow

（注） Flexible NetFlow は、Cisco IOS XE 17.7.1a 以降のリリースでサポートされています。

- ブリッジ ドメイン インターフェイスは次の機能をサポートしません。
  - PPP over Ethernet（PPPoE）
  - 双方向フォワーディング検出（BFD）プロトコル
  - QoS
  - Network-Based Application Recognition（NBAR）または Advanced Video Coding（AVC）

ブリッジ ドメイン インターフェイスに関する情報

ブリッジ ドメイン インターフェイスは、レイヤ 2 ブリッジ型ネットワークとレイヤ 3 のルーテッド ネットワーク トラフィック間のトラフィックの双方向フローを許可する論理インターフェイスです。ブリッジ ドメイン インターフェイスは、ブリッジ ドメインと同じインデックスによって識別されます。各ブリッジ ドメインは、レイヤ 2 ブロードキャスト ドメインを表します。ブリッジドメインに関連付けることができるブリッジドメインインターフェイスは、1 つだけです。

ブリッジ ドメイン インターフェイスは次の機能をサポートします。

- IP 終了
- レイヤ 3 VPN の終了
- アドレス解決プロトコル（ARP）、G-ARP および P-ARP の処理
- MAC アドレスの割り当て

ブリッジ ドメイン インターフェイスを設定する前に、次の概念を理解しておく必要があります：

- イーサネット仮想回線の概要
- ブリッジ ドメイン インターフェイスのカプセル化
- MAC アドレスの割り当て
- IP プロトコルのサポート
- IP 転送のサポート
- パケット転送
- ブリッジ ドメイン インターフェイスの統計情報

イーサネット仮想回線の概要

イーサネット仮想回線（EVC）は、プロバイダーが提供しているレイヤ2サービスの単一インスタンスのエンドツーエンド表現です。さまざまなパラメータが統合されて、サービスが提供されます。シスコ EVC フレームワークでは、ブリッジ ドメインは、サービス インスタンスと呼ばれているレイヤ2インターフェイス（1つまたは複数）で構成されます。サービス インスタンスは、あるルータ上のあるポート上で EVC をインスタンス化したものです。サービス インスタンスは、設定に基づいてブリッジ ドメインに関連付けられます。

着信フレームは、次の基準に基づいてサービス インスタンスとして分類できます。

- シングル 802.1Q VLAN タグ、優先度タグ付き、または 802.1ad VLAN タグ
- 両 QinQ（内部および外部）VLAN タグ、または 802.1ad S-VLAN と C-VLAN タグの両方
- 外部 802.1p CoS ビット、内部 802.1p CoS ビット、またはその両方
- ペイロード イーサネット タイプ（5 つの選択肢をサポート：IPv4、IPv6、PPPoE-all、PPoE-discovery、PPPoE-session）

サービス インスタンスは、他のマッピング基準もサポートします。

- [Untagged]：802.1Q または 802.1ad ヘッダがないすべてのフレームにマッピングします。
- [Default]：すべてのフレームにマッピングします。

EVC アーキテクチャの詳細については、『Carrier Ethernet Configuration Guide』の「Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Router」のセクションを参照してください。

ブリッジ ドメイン インターフェイスのカプセル化

セキュリティ グループの分類には、送信先グループや宛先グループが含まれます。これは送信元の SGT と DGT で指定します。SGT ベースの PBR 機能では、SGT/DGT ベースのパケット分類のために PBR ルートマップの match 句を使用できます。SGT ベースの PBR 機能では設定できるタグの数に制限はありませんが、プラットフォームで使用できるメモリに基づいてタグを設定することをお勧めします。

EVC はブリッジ ドメインに存在する各イーサネット フロー ポイント（EFP）で様々なカプセル化を使用する機能を提供します。パケットは異なるカプセル化を設定した1つまたは複数の EFP から出力されている可能性があるため、BDI 出力ポイントは出力パケットのカプセル化を認識しないことがあります。

ブリッジ ドメインでは、すべての EFP で異なるカプセル化がある場合、BDI のタグ付けを解除する必要があります（802.1Q タグなしを使用）。EFP でブリッジ ドメインのすべてのトラフィック（ポップまたはプッシュ）をカプセル化します。ブリッジ ドメインのトラフィックのカプセル化を可能にするためには、各 EFP で rewrite を設定します。

ブリッジ ドメインでは、すべての EFP で同じカプセル化がある場合は、encapsulation コマンドを使用して BDI 上にカプセル化を設定します。BDI でのカプセル化をイネーブルにすると、タグのプッシングまたはポッピングが有効になり、それにより EFP で rewrite コマンドを設定す

る必要がなくなります。BDI でのカプセル化の設定の詳細については、「ブリッジ ドメイン インターフェイスの設定方法」を参照してください。

MAC アドレスの割り当て

Cisco C8000V ルータ上のすべての□ブリッジ ドメイン インターフェイスは、同じ MAC アドレスを共有します。最初のブリッジ ドメイン インターフェイスに MAC アドレスが割り当てられます。その後、同じ MAC アドレスが、そのブリッジ ドメインで作成されたすべてのブリッジ ドメイン インターフェイスに割り当てられます。

（注） **mac-address** コマンドを使用して、ブリッジ ドメイン インターフェイスにスタティック MAC アドレスを設定できます。

IP プロトコルのサポート

ブリッジ ドメイン インターフェイスは、Cisco C8000V ルータを有効にし、次の IP 関連プロトコルのレイヤ 2 ブリッジドメインのレイヤ 3 のエンドポイントとして機能します。

- ARP
- DHCP
- HTTP
- ICMP
- NTP
- RARP
- SNMP
- TCP
- Telnet
- TFTP
- UDP

IP 転送のサポート

ブリッジ ドメイン インターフェイスは次の IP 転送機能をサポートします。

- IPv4 の入力および出力アクセス コントロール リスト（ACL）
- IPv4 の入力および出力 QoS ポリシー。ブリッジ ドメイン インターフェイスの入力および出力サービス ポリシーでサポートされる動作は次のとおりです。
  - 分類

- マーキング
- ポリシング

- IPv4 L3 VRF

パケット転送

ブリッジ ドメイン インターフェイスはレイヤ 2 およびレイヤ 3 ネットワーク インフラ間のブリッジングおよび転送サービスを提供します。

レイヤ 2 から 3

レイヤ2ネットワークからレイヤ3ネットワークへのパケット フローの間に、着信パケットの宛先 MAC アドレスがブリッジ ドメイン インターフェイスの MAC アドレスと一致するか、宛先 MAC アドレスがマルチキャスト アドレスの場合、パケットまたはパケットのコピーがブリッジ ドメイン インターフェイスに転送されます。

（注） MAC アドレスラーニングは、ブリッジドメイン上のインターフェイスで実行できません。

レイヤ 3 からレイヤ 2

パケットがルータの物理インターフェイスのレイヤ3に到達すると、ルート検索アクションが実行されます。ルート検索がブリッジ ドメイン インターフェイスに向かうと、ブリッジ ドメイン インターフェイスはレイヤ 2 カプセル化を追加し、対応するブリッジ ドメインにフレームを転送します。バイトカウンタが更新されます。

ブリッジドメインインターフェイスが属するブリッジドメインでのレイヤ2検索中に、ブリッジ ドメインは、宛先 MAC アドレスに基づいて適切なサービス インスタンスにパケットを転送します。

ブリッジ ドメインとブリッジ ドメイン インターフェイスのステートをリンクする

ブリッジ ドメイン インターフェイスはレイヤ 3 のルーティング可能な IOS インターフェイスおよびブリッジ ドメインのポートとして機能します。ブリッジ ドメイン インターフェイスとブリッジ ドメインのいずれも、個々の管理状態で動作します。

ブリッジ ドメイン インターフェイスをシャットダウンすると、レイヤ 3 データ サービスは停止しますが、関連するブリッジ ドメインの状態は上書きされず、影響を受けません。

ブリッジ ドメインをシャットダウンすると、サービス インスタンスやブリッジ ドメイン インターフェイスを含むすべての関連メンバへのレイヤ2転送が停止します。関連するサービスインスタンスはブリッジドメインの動作状態に影響を与えます。ブリッジドメインインターフェイスは、関連するサービスインスタンスの 1 つが起動しない限り、動作することはできません。

（注） ブリッジ ドメイン インターフェイスは内部インターフェイスであるため、ブリッジ ドメイン インターフェイスの動作状態はブリッジ ドメインの動作状態には影響しません。

BDI の初期状態

BDI 最初の管理ステートは、BDI の作成方法によって異なります。スタートアップ コンフィギュレーションで起動時にBDIを作成すると、BDIのデフォルトの管理状態がアップになります。スタートアップ コンフィギュレーションに shutdown コマンドが含まれていない限り、この状態のままになります。この動作は、他のすべてのインターフェイスと一致します。コマンドプロンプトで BDI を動的に作成すると、デフォルトの管理状態はダウンになります。

BDI のリンク状態

BDI は、管理上のダウン状態、動作上のダウン状態、アップ状態の 3 種類のステートからなるリンク状態を維持します。BDIのリンク状態は、対応するユーザーによって設定されたBDI管理状態セットおよびインターフェイスステートの下位レベルの障害表示の状態の2つの独立する入力から得られます。BDI のリンク状態は、2 つの入力の状態に基づいて定義されます。

障害表示の状態	BDI 管理	
{start emdash}{end emdash}	**Shutdown**	**No Shutdown**
No faults asserted	Admin-down	Up
At least one fault asserted	Admin-down	Operationally-Down

ブリッジ ドメイン インターフェイスの統計情報

ブリッジ ドメイン インターフェイスなどの仮想インターフェイスの場合は、プロトコル カウンタは QFP から定期的に検索されます。

パケットがレイヤ 2 ブリッジ ドメイン ネットワークからドメインのインターフェイスを介してレイヤ 3 のルーティング ネットワークに流れると、パケットはブリッジ ドメイン インターフェイスの入力パケットおよびバイトとして処理されます。パケットがレイヤ3インターフェイスに到達し、ブリッジ ドメイン インターフェイスを介してレイヤ 2 ブリッジ ドメインに転送されると、パケットは出力パケットおよびバイトとして処理され、カウンタが適宜更新されます。

BDI はすべての Cisco IOS インターフェイスで、ケースとしてレイヤ 3 パケット カウンタの標準セットを維持します。レイヤ 3 のパケット カウンタを表示するには、show interface コマンドを使用します。

カウンタの表記法は、レイヤ 3 クラウドに関連しています。たとえば、input はレイヤ 2 BD からレイヤ 3 クラウドに入るトラフィックを示し、output はレイヤ 3 クラウドからレイヤ 2 BD に向かうトラフィックを示します。

BDI ステータスの統計情報を表示するには、**show interfaces accounting** コマンドを使用します。送受信されるパケットおよびバイト全体のカウントを表示するには、**show interface** <*if-name*> コマンドを使用します。

ブリッジ ドメイン インターフェイスの作成または削除

Cisco IOS ルータのインターフェイスまたはサブインターフェイスを定義する場合は、名前を付け、どのように IP アドレスに割り当てられるかを指定します。システムにブリッジドメインを追加する前にブリッジ ドメイン インターフェイスを作成できます。この新しいブリッジドメインインターフェイスは、関連するブリッジドメインの設定後にアクティブになります。

（注） ブリッジ ドメイン インターフェイスが作成されると、ブリッジ ドメインが自動的に作成されます。

ブリッジ ドメイン インターフェイスとブリッジドメインを作成すると、システムは、ブリッジドメインとブリッジ ドメイン インターフェイスのペアをマッピングするために必要なアソシエーションを保持します。

ブリッジ ドメインとブリッジ ドメイン インターフェイスのマッピングはシステムに保持されます。ブリッジドメインインターフェイスは、アソシエーションを示すために関連するブリッジ ドメインのインデックスを使用されます。

ブリッジ ドメイン インターフェイスのスケーラビリティ

次の表に、Cisco C8000V ルータのフォワーディングプロセッサ（FP）のタイプに基づいた、ブリッジ ドメイン インターフェイスのスケーラビリティの数値を示します。

表 *43 : Cisco C8000V* ルータのフォワーディングプロセッサのタイプに基づいた、ブリッジ ドメイン インターフェイスのスケーラビリティの数値

説明	0
ルータごとのブリッジ ドメイン インターフェイスの最大数	

ブリッジドメイン仮想 IP インターフェイス

仮想 IP インターフェイス（VIF）機能は、複数の BDI インターフェイスを BD インスタンスに関連付けるのに役立ちます。BD-VIF インターフェイスは、IOS 論理 IP インターフェイスの既存のすべての L3 機能を継承します。

（注） すべての BD-VIF インターフェイスに一意の MAC アドレスを設定する必要があり、異なる VRF に属している必要があります。

仮想 IP インターフェイス（VIF）機能には、次の制限事項があります。

- BD-VIF インターフェイスは IP マルチキャストをサポートしていません。
- 自動生成された MAC アドレスを持つ BD-VIF インターフェイスの数は、プラットフォームによって異なります。
- BD-VIF インターフェイスは MPLS をサポートしていません。
- ブリッジドメインごとの BD-VIF インターフェイスの最大数と、システムごとの BD-VIF インターフェイスの総数は、プラットフォームのタイプによって異なります。

サポートされる BD-VIF の最大数は、プラットフォームによって異なります。

- ASR 1000 は、ブリッジドメインに対して最大 100 の BD-VIF をサポートします。
- CSR 1000v は、ブリッジドメインに対して最大 16 の BD-VIF をサポートします。
- ISR 4000 は、ブリッジドメインに対して最大 16 の BD-VIF をサポートします。

Cisco IOS XE 17.7.1a リリースから、BD-VIF は Flexible Netflow（FnF）をサポートします。

ブリッジ ドメイン インターフェイスの設定方法

ブリッジ ドメイン インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface BDI** *{interface number}*
4. **encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]*
5. 次のいずれかを実行します。
6. **match security-group destination tag** *sgt-number*
7. **mac address** *{mac-address}*
8. **no shut**
9. **shut**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**interface BDI** *{interface number}* 例： `Router(config-if)# interface BDI3`	ブリッジ ドメイン インターフェイスを指定します。
ステップ 4	**encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]* 例： `Router(config-if)# encapsulation dot1Q 1 second-dot1q 2`	カプセル化タイプを定義します。 例では、カプセル化タイプとして dot1q を定義しています。

ステップ 5	次のいずれかを実行します。
	例：
	ip address *ip-address mask*
	例：
	例：
	ipv6 address *{X:X:X:X::X* **link-local** | *X:X:X:X::X/prefix [***anycast** | **eui-64***]* | **autoconfig** *[***default***]}*
	例：
	`Router(config-if)# ip address 10.2.2.1 255.255.255.0`
	例：
	例：
	`Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64`
		ブリッジ ドメイン インターフェイスの IPv4 または IPv6 アドレスを指定します。

ステップ 6	**match security-group destination tag** *sgt-number* 例： `Router(config-route-map)# match security-group destination tag 150`	security-group destination security tag の値を設定します。
ステップ 7	**mac address** *{mac-address}* 例： `Router(config-if)# mac-address 1.1.3`	ブリッジ ドメイン インターフェイスの MAC アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 8	**no shut** 例： `Router(config-if)# no shut`	ブリッジ ドメイン インターフェイスを有効にします。
ステップ 9	**shut** 例： `Router(config-if)# shut`	ブリッジ ドメイン インターフェイスを無効にします。

例

次に、IP アドレス 10.2.2.1 255.255.255.0 でブリッジ ドメイン インターフェイスを設定する例を示します。

```
Router# configure terminal
Router(config)# interface BDI3
Router(config-if)# encapsulation dot1Q 1 second-dot1q 2
Router(config-if)# ip address 10.2.2.1 255.255.255.0
Router(config-if)# mac-address 1.1.3
Router(config-if)# no shut
Router(config-if)# exit
```

ブリッジ ドメイン インターフェイス設定の表示と確認

手順の概要

1. **enable**
2. **show interfaces bdi**
3. **show platform software interface fp active name**
4. **show platform hardware qfp active interface if-name**
5. **debug platform hardware qfp feature**
6. **platform trace runtime process forwarding-manager module**
7. **platform trace boottime process forwarding-manager module interfaces**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**show interfaces bdi** 例： `Router# show interfaces BDI3`	対応する BDI の設定の概要を表示します。
ステップ 3	**show platform software interface fp active name** 例： `Router# show platform software interface fp active name BDI4`	フォワーディングプロセッサのブリッジ ドメイン インターフェイス設定を表示します。
ステップ 4	**show platform hardware qfp active interface if-name** 例： `Router# show platform hardware qfp active interface if-name BDI4`	データパスのブリッジ ドメイン インターフェイス設定を表示します。
ステップ 5	**debug platform hardware qfp feature** 例： `Router# debug platform hardware qfp active feature l2bd client all`	選択した CPP L2BD Client のデバッグがオンになります。
ステップ 6	**platform trace runtime process forwarding-manager module** 例： `Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module interfaces level info`	Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。
ステップ 7	**platform trace boottime process forwarding-manager module interfaces** 例： `Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager forwarding-manager level max`	ブートアップ中の、Route Processor Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。

次のタスク

各コマンドに使用できるコマンドおよびオプションの詳細については、『Cisco IOS Configuration Fundamentals Command Reference Guide』を参照してください。

ブリッジドメイン仮想 IP インターフェイスの設定

```
enable
configure terminal
[no] interface BD-VIF interface-number
  [ [no] vrf forwarding vrf-name]
  [ [no] mac address mac-address]
  [ [no] ip address ip-address mask]
  [ [no] ipv6 address {X:X:X:X::X link-local| X:X:X:X::X/prefix [anycast | eui-64] |
autoconfig [default]}]

exit
```

BD-VIF インターフェイスを削除するには、このコマンドの 'no' 形式を使用します。

VIF インターフェイスのブリッジドメインへの関連付け

```
enable
configure terminal
bridge-domain bridge-domain number
[no] member BD-VIF interface-number
exit
```

VIF インターフェイスの関連付けを解除するには、このコマンドの「no」形式を使用します。

ブリッジドメイン仮想 IP インターフェイスの確認

インターフェイスおよび IP インターフェイスの既存のすべての show コマンドは、BD-VIF インターフェイスに使用できます。

show interface bd-vif *bd-vif-id*

show ip interface bd-vif *bd-vif-id*

show bd-vif interfaces in fman-fp

show pla sof inter fp ac brief | i BD_VIF

ブリッジドメイン仮想 IP インターフェイスの設定例

```
Detail sample:

interface Port-channel1
mtu 9000
no ip address
 !Ethernet service endpoint one per neutron network
service instance 1756 ethernet
  description 4e8e5957-649f-477b-9e5b-f1f75b21c03c
  encapsulation dot1q 1756
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1756
!
interface BD-VIF5001
no shutdown
vrf forwarding vrf5001
```

```
ip address 10.0.0.1 255.255.255.0
interface BD-VIF5002
no shutdown
vrf forwarding vrf5002
ip address 10.0.0.2 255.255.255.0

bridge-domain 1756
member Port-channel1 service-instance 1756
member bd-vif5001
member bd-vif5002
```

ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. {**ip | ipv6**}**flow monitor** *monitor-name* [**sampler** *sampler-name*] {**input | output**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device (config)# interface BD-VIF 100`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。BD-VIF 番号を入力します。
ステップ 4	{**ip	ipv6**}**flow monitor** *monitor-name* [**sampler** *sampler-name*] {**input	output**} 例： `Device(config-if)# ip flow monitor FLOW-MONITOR-1 input`	ルータがインターフェイスで送受信する IP トラフィックの Flexible NetFlow フローモニターを有効にします。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow

次に、フローモニターの QFP 情報およびフロー方向を表示する **show platform hardware qfp active interface if-name** コマンドの出力例を示します。次の表に、CLI 出力のキーを示します。

設定	出力
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...

Current configuration: 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001:DB8::1/32
end

Device# show platform hardware qfp active interface if-name BD-VIF 2
General interface information
  Interface Name: BD-VIF2
  Interface state: VALID
  Platform interface handle: 20
  QFP interface handle: 17
  Rx uidb: 262138
  Tx uidb: 262127
  Channel: 0
Interface Relationships

BGPPA/QPPB interface configuration information
  Ingress: BGPPA/QPPB not configured. flags: 0000
  Egress: BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
ipv6_input enabled.
ipv6_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
2 GIC FIA state
66 PUNT INJECT DB
```

```
70 cpp_l2bd_svr
43 icmp_svr
45 ipfrag_svr
46 ipreass_svr
47 ipv6reass_svr
44 icmp6_svr
58 stile
Protocol 0 - ipv4_input
FIA handle - CP:0x55a7f59df038 DP:0x3fff1000
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  IPV4_INPUT_SRC_LOOKUP_ISSUE
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_SRC_LOOKUP_CONSUME
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_LOOKUP_PROCESS (M)
  IPV4_INPUT_FNF_FINAL
  IPV4_INPUT_IPOPTIONS_PROCESS (M)
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x55a7f59df0d8 DP:0x3ffeff00
  IPV4_VFR_REFRAG (M)
  IPV4_OUTPUT_SRC_LOOKUP_ISSUE
  IPV4_OUTPUT_L2_REWRITE (M)
  IPV4_OUTPUT_SRC_LOOKUP_CONSUME
  IPV4_OUTPUT_STILE_LEGACY
  IPV4_OUTPUT_FRAG (M)
  IPV4_BDI_OUTPUT_FNF_FINAL.
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
Protocol 6 - ipv6_input
FIA handle - CP:0x55a7f59dee58 DP:0x3fff4300
  IPV6_INPUT_SANITY_CHECK (M)
  IPV6_INPUT_DST_LOOKUP_ISSUE (M)
  IPV6_INPUT_SRC_LOOKUP_ISSUE
  IPV6_INPUT_ARL (M)
  IPV6_INPUT_DST_LOOKUP_CONT (M)
  IPV6_INPUT_SRC_LOOKUP_CONT
  IPV6_INPUT_DST_LOOKUP_CONSUME (M)
  IPV6_INPUT_SRC_LOOKUP_CONSUME
  IPV6_INPUT_STILE_LEGACY
  IPV6_INPUT_FNF_FIRST
  IPV6_INPUT_FOR_US (M)
  IPV6_INPUT_LOOKUP_PROCESS (M)
  IPV6_INPUT_FNF_FINAL
  IPV6_INPUT_LINK_LOCAL_CHECK (M)
  IPV6_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 7 - ipv6_output
FIA handle - CP:0x55a7f59dee08 DP:0x3fff4b80
  IPV6_VFR_REFRAG (M)
  IPV6_OUTPUT_SRC_LOOKUP_ISSUE
  IPV6_OUTPUT_SRC_LOOKUP_CONT
  IPV6_OUTPUT_SRC_LOOKUP_CONSUME
  IPV6_OUTPUT_L2_REWRITE (M)
  IPV6_OUTPUT_STILE_LEGACY
  IPV6_OUTPUT_FRAG (M)
  IPV6_BDI_OUTPUT_FNF_FINAL
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
```

```
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV6_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
```

次に、キャッシュ出力をレコード形式で表示する **show flow monitor** [[**name**] [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] コマンドの出力例を示します。

```
Device# show flow monitor name FLOW-MONITOR-1 cache format record

Cache type:  Normal
Cache size:  1000
Current entries:  4
High Watermark:  4
Flows added:  101
Flows aged:  97
- Active timeout (1800 secs) 3
- Inactive timeout  (15 secs) 94
- Event aged  0
- Watermark aged  0
- Emergency aged
IPV4 DESTINATION ADDRESS:
198.51.100.1 0
ipv4 source address: 10.10.11.1
trns source port: 25
trns destination port: 25
counter bytes: 72840
counter packets: 1821
IPV4 DESTINATION ADDRESS: 198.51.100.2
ipv4 source address: 10.10.10.2
trns source port: 20
trns destination port: 20
counter bytes: 3913860
counter packets: 7326
IPV4 DESTINATION ADDRESS: 198.51.100.200
ipv4 source address: 192.168.67.6
trns source port: 0
trns destination port: 3073
counter bytes: 51072
counter packets: 1824


Device# show flow monitor name FLOW-MONITOR-2 cache format record

Cache type:  Normal
Cache size: 1000
Current entries: 2
High Watermark: 3
Flows added: 95
Flows aged: 93
- Active timeout (1800 secs) 0
- Inactive timeout (15 secs) 93
- Event aged 0
- Watermark aged 0
- Emergency aged 0
IPV6 DESTINATION ADDRESS: 2001:DB8:0:ABCD::1
ipv6 source address: 2001:DB8:0:ABCD::2
trns source port: 33572
trns destination port: 23
counter bytes: 19140
counter packets: 349
IPV6 DESTINATION ADDRESS: FF02::9
ipv6 source address: 2001:DB8::A8AA:BBFF:FEBB
```

```
trns source port: 521
trns destination port: 521
counter bytes: 92
counter packets: 1
```

次に、インターフェイスのフローステータスを表示する **show flow interface** コマンドの出力例を示します。

```
Device# show flow interface BD-VIF2001

Interface GigabitEthernet0/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Input
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on

Device# show flow interface BD-VIF2002

Interface GigabitEthernet1/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Output
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on
```

次に、Flexible NetFlow 設定のフローモニターの QFP 情報およびフロー方向を表示する **show platform hardware qfp active interface if-name** | **in FNF** コマンドの出力例を示します。次の表に、CLI 出力のキーを示します。

設定	出力
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...

Current configuration : 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001::8/64
end
 Device# show platform hardware qfp active interface if-name BD-VIF 2  | in FNF
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_FNF_FINAL
  IPV4_BDI_OUTPUT_FNF_FINAL.
  IPV6_INPUT_FNF_FIRST
```

```
IPV6_INPUT_FNF_FINAL
IPV6_BDI_OUTPUT_FNF_FINAL
```

clear flow monitor name *monitor-name* [**cache** [**force-export**] | **force-export** | **statistics**] コマンドを使用すると、Flexible NetFlow フローモニター、フローモニターキャッシュ、またはフローモニター統計情報がクリアされ、フローモニターキャッシュ内のデータを強制的にエクスポートできます。

Flexible NetFlow の設定の詳細については、『Flexible NetFlow Configuration Guide, Cisco IOS XE 17』を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでのイーサネット仮想接続の設定	『Carrier Ethernet Configuration Guide』
EVC Quality of Service	http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_evc_xe.html

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	https://www.cisco.com/c/en_in/support/index.html

ブリッジ ドメイン インターフェイスの機能情報

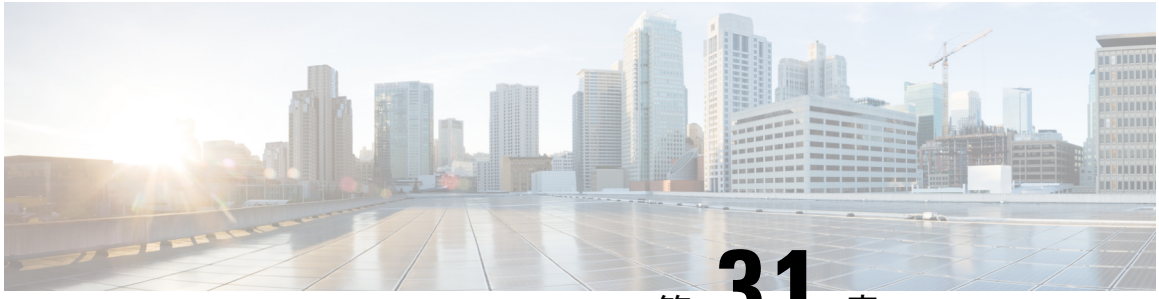
次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

表 *44*：ブリッジ ドメイン インターフェイスの機能情報

機能名	リリース	機能情報
ブリッジ ドメイン インターフェイスの設定	Cisco IOS XE Cupertino 17.7.1a	この機能は、Cisco C8000V ルータで導入されました。
ブリッジドメイン仮想 IP インターフェイス	Cisco IOS XE Cupertino 17.7.1a	この機能は、Cisco C8000V ルータで導入されました。 ブリッジドメイン仮想 IP インターフェイス（VIF）は、複数のブリッジ ドメイン インターフェイス（BDI）を単一の BD インスタンスに接続し、L2 ネットワーク内の各 IP サブネットを単一の VRF に関連付けることができるようになりました。
ブリッジドメイン仮想 IP インターフェイス（BD-VIF）上の Flexible NetFlow（FNF）	Cisco IOS XE Cupertino 17.7.1a	この機能は、Cisco C8000V ルータで導入されました。次のコマンドが導入されました。 **{ip | ipv6} flow monitor** *monitor-name* **[sampler** *sampler-name***] {input | output}**



第 31 章

MTP ソフトウェアサポートの設定

メディア ターミネーション ポイント（MTP）ソフトウェアデバイスは、Cisco Unified Communications Manager（CUCM）の大規模な導入に不可欠なコンポーネントです。これらの展開では、ソフトウェア MTP は、CUCM が Session Initiation Protocol（SIP）または H.323 エンドポイントを介してルーティングされたコールを Skinny Client Control Protocol（SCCP）コマンドでリレーできるようにすることで、2 つの接続間のメディアストリームをブリッジするようにします。SCCP コマンドにより、CUCM はコールシグナリング用の MTP を確立できます。

Cisco IOS XE 17.8.1 以降では、Cisco Catalyst 8000V デバイスでソフトウェア MTP のサポートを設定できます。Cisco Catalyst 8000V デバイスで音声機能を使用する場合は、ソフトウェア MTP を活用して、H.323 エンドポイントまたは H.323 ゲートウェイを介してルーティングされるコールパークやコール転送などの補足サービスを有効にして使用できます。

利点

Cisco Catalyst 8000V でソフトウェア MTP を設定すると、次のことが可能になります。

- Cisco Catalyst 8000V インスタンスを信頼できるリレーポイントとして Unified CM に登録します。
- エンドポイントの 1 つが DTMF シグナリングをサポートしていない場合は、SWMTP サポートを活用します。

ソフトウェア MTP のサポートを設定するための前提条件

- 着信コールレッグと発信コールレッグでコーデックとパケット化を設定します。

SRTP-DTMF インターワーキング

Cisco IOS XE 17.10.1a 以降、Secure Real-time Transport Protocol（SRTP）デュアルトーン多重周波数（DTMF）インターワーキングは、パススルーモードのソフトウェア MTP でサポートされています。SMTP は非セキュアコールの DTMF インターワーキングをサポートします。また、この機能はさらにセキュアコールの SRTP DTMF インターワーキングをサポートします。

この機能の CUCM サポートは、今後のリリースで実装される予定です。

SRTP-DTMF インターワーキングの制約事項

- SRTP-DTMF インターワーキング機能は、コーデックパススルー形式のみをサポートします。
- SRTP-DTMF インターワーキング機能は、同じ宛先 IP とポートを持つ複数の同時同期ソース（SSRC）をサポートしていません。
- SRTP-DTMF インターワーキングをサポートするコールは、非セキュア DTMF インターワーキングでサポートされるコールと比較すると、パフォーマンスにわずかな影響を与える可能性があります。

サポートされる SRTP-DTMF インターワーキングのプラットフォーム

Cisco IOS XE 17.10.1a 以降、次のプラットフォームは SMTP との SRTP DTMF インターワーキングをサポートしています。

- Cisco 4461 サービス統合型ルータ（ISR）
- Cisco Catalyst 8200 Edge シリーズ プラットフォーム
- Cisco Catalyst 8300 Edge シリーズ プラットフォーム
- Cisco Catalyst 8000V Edge ソフトウェア

ソフトウェア MTP のサポートの設定

ソフトウェア MTP のサポートを有効にして設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number* [**port** *port-number*]
4. **sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number*

5. **sccp**
6. **sccp ccm group** *group-number*
7. **associate ccm** *identifier-number* **priority** *number*
8. **associate profile** *profile-identifier* **register** *device-name*
9. **dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]
10. **trustpoint** *trustpoint-label*
11. **codec** *codec*
12. **maximum sessions** {**hardware** | **software**} *number*
13. **associate application sccp**
14. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sccp local** *interface-type interface-number* [**port** *port-number*] 例： `Router(config)# sccp local gigabitethernet0/0/0`	Cisco UCM に登録するために SCCP アプリケーション（トランスコーディングと会議）が使用する、ローカルインターフェイスを選択します。 • *interface type*：インターフェイスアドレスまたは仮想インターフェイスアドレス（イーサネットなど）。 • *interface number*：Unified CM に登録するために SCCP アプリケーションが使用するインターフェイス番号。 • （任意）**port** *port-number*：選択したインターフェイスで使用するポート番号。適用可能な範囲は 1025 ～ 65535 で、デフォルトは 2000 です。
ステップ 4	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number* 例：	使用可能なサーバーのリストに Unified CM サーバーを追加し、次のパラメータを設定します。 • *ipv4-address*：Cisco UCM サーバーの IP バージョン 4 アドレス。

	コマンドまたはアクション	目的
	`Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+`	• *ipv6-address*：Cisco UCM サーバーの IP バージョン 6 アドレス。 • *dns*：DNS 名。 • **identifier** ：Unified CM サーバーを識別する番号。適用可能な範囲は 1 ～ 65535 です。 • **port** *port-number*（任意）：TCP ポート番号。適用可能な範囲は 1025 ～ 65535 で、デフォルトは 2000 です。 • **version** *version-number*：Unified CM のバージョン。有効なバージョンは、3.0、3.1、3.2、3.3、4.0、4.1、5.0.1、6.0、および 7.0 以上です。
ステップ 5	**sccp** 例： `Router(config)# sccp`	SCCP および関連アプリケーション（トランスコーディングと会議）を有効にします。
ステップ 6	**sccp ccm group** *group-number* 例： `Router(config)# sccp ccm group 10`	Unified CM グループを作成し、SCCP Unified CM コンフィギュレーション モードを開始します。 • *group-number*：Cisco Unified CM グループを識別します。適用可能な範囲は 1 ～ 50 です。
ステップ 7	**associate ccm** *identifier-number* **priority** *number* 例： `Router(config-sccp-ccm)# associate ccm 10 priority 3`	Unified CM をグループに関連付けて、グループ内の優先順位を設定します。 • *identifier-number*：Unified CM 識別子。適用可能な範囲は 1 ～ 65535 です。 • **priority** *number*：Unified CM グループ内の Unified CM の優先順位。適用可能な範囲は 1 ～ 4 です。最も高い優先順位は 1 です。
ステップ 8	**associate profile** *profile-identifier* **register** *device-name* 例： `Router(config-sccp-ccm)# associate profile 1 register MTP0011`	デジタルシグナルプロセッサ（DSP）ファームプロファイルを Unified CM グループに関連付けます。 • *profile-identifier*：DSP ファームプロファイル。適用可能な範囲は 1 ～ 65535 です。 • **register** *device-name*：Unified CM のデバイス名。デバイス名は最大 15 文字まで入力できます。

	コマンドまたはアクション	目的
ステップ 9	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**] 例： `Router(config-sccp-ccm)# dspfarm profile 1 mtp`	DSP ファーム プロファイル コンフィギュレーション モードを開始し、DSP ファームサービスのプロファイルを定義します。 • *profile-identifier*：プロファイルを一意に識別する番号。適用可能な範囲は 1 ～ 65535 で、デフォルトはありません。 • **conference**：会議用のプロファイルを有効にします。 • **mtp**：MTP 用のプロファイルを有効にします。 • **transcode**：トランスコーディング用のプロファイルを有効にします。 • **security**（任意）：セキュア DSP ファームサービス用のプロファイルを有効にします。設定例の詳細については、ソフトウェア MTP サポートの設定例（328 ページ）の項を参照してください。
ステップ 10	**trustpoint** *trustpoint-label* 例： `Router(config-dspfarm-profile)# trustpoint dspfarm`	（任意）トラストポイントを DSP ファーム プロファイルに関連付けます。
ステップ 11	**codec** *codec* 例： `Router(config-dspfarm-profile)# codec g711ulaw`	DSP ファーム プロファイルでサポートされるコーデックを指定します。 • codec-type：優先されるコーデックを指定します。サポートされるコーデックのリストを表示するには、? を入力します。 サポートされるコーデックごとに、この手順を繰り返します。
ステップ 12	**maximum sessions** {**hardware** | **software**} *number* 例： `Router(config-dspfarm-profile)# maximum sessions software 10`	このプロファイルでサポートされる最大セッション数を指定します。 • **hardware**：MTP ハードウェアリソースがサポートするセッションの数。 • **software**：MTP ソフトウェアリソースがサポートするセッションの数。 • *number*：プロファイルでサポートされるセッションの数。適用可能な範囲は 0 ～ x で、デ

	コマンドまたはアクション	目的
		フォルトは 0 です。x の値は、リソースプロバイダーで使用可能なリソースの数に応じて、実行時に決定されます。
ステップ 13	**associate application sccp** 例： `Router(config-dspfarm-profile)# associate application sccp`	SCCP を DSP ファーム プロファイルに関連付けます。
ステップ 14	**no shutdown** 例： `Router(config-dspfarm-profile)# no shutdown`	インターフェイスのステータスを UP 状態に変更します。

ソフトウェア MTP サポートの設定例

次の出力は、Cisco Catalyst 8000V デバイスでのソフトウェア MTP サポート設定の例です。

```
sccp local GigabitEthernet1
sccp ccm 9.35.46.100 identifier 1 priority 1 version 7.0
!
sccp ccm group 1
 bind interface GigabitEthernet1
 associate ccm 1 priority 1
 associate profile 10 register SWMTP1
 associate profile 1 register c8kvsmall-mtp1
 associate profile 2 register c8kv-sec-swmtp1
!
!
!
dspfarm profile 1 mtp
 codec g711ulaw
 maximum sessions software 20000
 associate application SCCP
```

次に、セキュアな dspfarm プロファイルを使用した SRTP-DTMF インターワーキング機能の設定例を示します。

```
sccp local GigabitEthernet0/0/0
sccp ccm 172.18.151.125 identifier 1 version 7.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/0
 associate ccm 1 priority 1
 associate profile 1 register Router
!
dspfarm profile 1 mtp security
 trustpoint IOSCA
 codec g711ulaw
 codec pass-through
 tls-version v1.2
```

```
maximum sessions software 5000
associate application SCCP
```

（注） dspfarm プロファイルがコーデックパススルーでプロビジョニングされていて、TLS およびセキュリティ関連の設定がない場合、SR-TP トラフィックは SMTP リソースを通過できます。SRTP-DTMF インターワーキングのサポートを必要とするトラフィックフローの場合は、SMTP dspfarm プロファイルには **security** キーワードと TLS およびコーデックパススルー設定を含める必要があります。この dspfarm リソースプロファイルは、SRTP-DTMF インターワーキングサポートに関係なく、SRTP トラフィックを通過させることもできます。

ソフトウェア MTP サポートの確認

Cisco Catalyst 8000V デバイスで SWMTP のサポートが正常に設定されているかどうかを確認するには、**show sccp** コマンドを実行します。

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.13.40.157, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.13.40.148, Port Number: 2000
                Priority: N/A, Version: 6.0, Identifier: 1
                Trustpoint: N/A
```

dspfarm プロファイルを確認するには、**show dspfarm profile** コマンドを実行します。

```
Router# show dspfarm profile 1
Dspfarm Profile Configuration

 Profile ID = 1, Service = MTP, Resource ID = 1
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : RESOURCE ALLOCATED
 Application : SCCP   Status : NOT ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Total Number of Resources Configured : 20000
 Total Number of Resources Available : 20000
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Hardware Configured Resources : 0
 Hardware Resources Out of Service: 0
 Software Configured Resources : 20000

 Number of Hardware Resources Active : 0
 Number of Software Resources Active : 0
 Codec Configuration: num_of_codecs:1
 Codec : g711ulaw, Maximum Packetization Period : 30
```

セキュア dspfarm プロファイルのステータスに関する情報を確認するには、**show dspfarm profile** コマンドを使用して、セキュアサービスモードが設定されていることを確認します。

```
Router# show dspfarm profile 2
Dspfarm Profile Configuration
 Profile ID = 2, Service = MTP, Resource ID = 2
```

```
 Profile Service Mode : secure
 Trustpoint : IOSCA
 TLS Version  : v1.2
 TLS Cipher   : AES128-SHA
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Total Number of Resources Configured : 8000
 Total Number of Resources Available : 8000
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Hardware Configured Resources : 0
 Hardware Resources Out of Service: 0
 Software Configured Resources : 8000
 Number of Hardware Resources Active : 0
 Number of Software Resources Active : 0
 Codec Configuration: num_of_codecs:2
 Codec : pass-through, Maximum Packetization Period : 0
 Codec : g711ulaw, Maximum Packetization Period : 30
```

エンドポイント間のコール接続を確認するには、**show sccp connection details** コマンドを実行します。このコマンドは、接続が正常に確立されたことを示します。これは、設定出力の最後にあるアクティブな接続とコールレッグによって示されます。

```
Router# show sccp connection details

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)

mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id    conn_id    call-id   codec  pkt-period  dtmf_method     type    bridge-info
  mmbridge-info  srtp_cryptosuite  dscp
call_ref   spid       conn_id_tx                                          (bid, cid)
  (bid, cid)
16782237   16777254   110       g711u  20          rfc2833_pthru   rtpspi  (40,0)
   N/A            N/A              184
29751839   16777216   -
16782237   16777253   109       g711u  20          rfc2833_report  rtpspi  (40,0)
   N/A            N/A              184
29751839   16777216   -
Total number of active session(s) 1, connection(s) 2, and callegs 2
```

SMTP セキュア DTMF の場合、**show sccp connections** コマンドはコーデックタイプ（pass-th）、S タイプ（s-mtp）、および DTMF メソッド（rfc2833_pthru）に関する情報を表示します。

```
Router#sh sccp connections

sess_id    conn_id    stype   mode      codec    sport  rport   ripaddr conn_id_tx
dtmf_method

16791234   16777308   s-mtp   sendrecv  pass_th  8006   24610   172.18.153.37
rfc2833_pthru
16791234   16777306   s-mtp   sendrecv  pass_th  8004   17576   172.18.154.2
rfc2833_report

Total number of active session(s) 1, and connection(s) 2
```

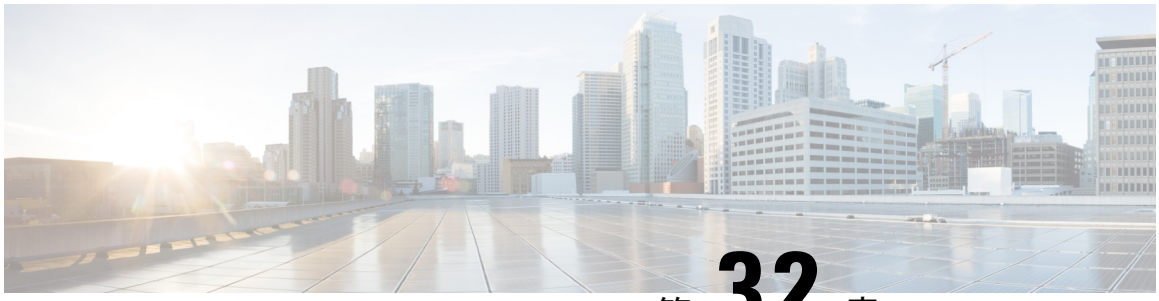
RTP 接続に関する情報を表示するには、**show rtpspi call** コマンドを使用します。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
```

```
1    22      19          Snd-Rcv   7242      17510    0x90D080F   0x90D0814    0
2    19      22          Snd-Rcv   18050     6900     0x90D080F   0x90D080F    0
```

SRTP DTMF インターワーキングがアクティブになっている場合、SRTP フィールドにはゼロ以外の値が表示されます。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
1   13      14          Snd-Rcv   8024      18270   0xA7A5355   0xAC129A02   1
2   14      13          Snd-Rcv   8026      24768   0xA7A5355   0xAC129925   1
```



第 32 章

無線対応ルーティング

無線対応ルーティング（RAR）は、無線がルーティングプロトコルOSPFv3と情報を交換し、1ホップルーティングネイバーのアピアランス、ディスアピアランス、およびリンク状態について信号で伝えるメカニズムです。

大規模なモバイルネットワークでは、ルーティングネイバーへの接続が距離と無線障害により中断されることがよくあります。該当する信号がルーティングプロトコルに到達しない場合、プロトコルタイマーを使用してネイバーのステータスが更新されます。ルーティングプロトコルには期間の長いタイマーがありますが、モバイルネットワークでは推奨されません。

RAR機能は、Cisco ISR G2およびG3シリーズ ルータ、Cisco ISR 4000シリーズ ルータでサポートされています。

PPPoE拡張は、Cisco 4000シリーズISRでサポートされるRARプロトコルです。集約によるPPPoE拡張のサポートは、Cisco IOS XE Fuji 16.7リリースから導入されています。OSPFv3およびEIGRPは、サポートされているルーティングプロトコルです。

無線対応ルーティングの利点

無線対応ルーティング機能には次のようなメリットがあります。

- 変更を即座に認識することで、ネットワーク コンバージェンスを高速化します。
- 障害の発生している、または減衰している無線リンクのルーティングを有効にします。
- ラインオブサイトパスと非ラインオブサイトパス間のルーティングを容易にします。

- 高速コンバージェンスと最適なルート選択が可能になるため、音声やビデオなど遅延の影響を受けやすいトラフィックが中断されません。
- 無線リソースと帯域幅の効率的な使用が可能になります。
- ルータで輻輳制御を実行することにより、無線リンクへの影響を軽減します。
- 無線電力の節減に基づくルート選択が可能になります。
- ルーティング機能と無線機能の分離を有効にします。
- RFC 5578、R2CP、および DLEP に準拠した無線へのシンプルなイーサネット接続を実現します。

制約事項と制限

無線対応ルーティング機能には次の制約事項と制限があります。

- DLEP および R2CP プロトコルは、Cisco 4000 シリーズ ISR ではサポートされていません。
- マルチキャストトラフィックは、集約モードではサポートされていません。
- 高可用性（HA）はサポートされていません。

パフォーマンス

無線対応ルーティング機能は、無線または VMI インターフェイスごとに最大 10 のネイバーをサポートできます。合計 30 ー 40 のネイバーに対応可能です。

システム コンポーネント

無線対応ルーティング（RAR）機能は、PPPoE、仮想マルチポイント インターフェイス（VMI）、QoS、ルーティング プロトコル インターフェイス、RAR プロトコルなどのさまざまなコンポーネントで構成される MANET（モバイル アドホック ネットワーク）インフラストラクチャを使用して導入されます。

Point-to-Point Protocol over Ethernet（PPPoE）

PPPoE は、クライアントとサーバーの間の明確に定義された通信メカニズムです。RAR の導入では、無線が PPPoE クライアントの役割を果たし、ルータが PPPoE サーバーの役割を果たします。その結果、明確に定義された予測可能な通信メカニズムを提供しながら、無線とルータを疎結合することが可能になります。

PPPoE はセッションまたは接続指向プロトコルであるため、外部無線から IOS ルータへのポイントツーポイント無線周波数（RF）リンクを拡張します。

PPPoE 拡張

PPPoE 拡張は、ルータが無線と通信するときに使用されます。PPPoE の Cisco IOS 導入では、個々のセッションは仮想アクセスインターフェイス（無線ネイバーへの接続）で表され、これらの PPPoE 拡張を使用して QoS を適用できます。

RFC5578 は、信頼ベースのフロー制御とセッションベースのリアルタイム リンク メトリックをサポートするための PPPoE の拡張を実現します。この拡張は、可変帯域幅および制限付きバッファリング機能（無線リンクなど）を使用した接続に非常に役立ちます。

仮想マルチポイント インターフェイス（VMI）

PPPoE拡張によってルータと無線間で通信するためのセットアップの大部分が実現しますが、VMIは、上位レイヤ（ルーティングプロトコルなど）が消費するイベントを管理および変換する必要に対処します。また、VMI はバイパスモードで動作します。

バイパスモードでは、無線ネイバーを表すすべての仮想アクセスインターフェイス（VAI）がルーティングプロトコル OSPFv3 および EIGRP に明示されるため、ルーティングプロトコルは、ユニキャストとマルチキャスト両方のルーティング プロトコル トラフィックに関してそれぞれの VAI と直接通信します。

集約モードでは、VMI がルーティングプロトコル（OSPF）に明示されるため、ルーティングプロトコルは VMI を活用して効率を最適化できます。ネットワークネイバーが、VMI でのブロードキャストおよびマルチキャスト機能を備えたポイントツーマルチポイント リンク上のネットワークの集合と見なされる場合、VMIは、PPPoEから作成された複数の仮想アクセスインターフェイスの集約に役立ちます。VMIは、単一のマルチアクセスレイヤ2ブロードキャスト対応インターフェイスを提供します。VMI レイヤは、ユニキャスト ルーティング プロトコル トラフィックを適切な P2P リンク（仮想アクセスインターフェイス）にリダイレクトし、フローする必要があるすべてのマルチキャスト/ブロードキャストトラフィックを複製します。ルーティングプロトコルは単一のインターフェイスと通信するため、ネットワークの完全性に影響を与えることなく、トポロジデータベースのサイズが縮小されます。

PPPoE 拡張セッションでの QoS プロビジョニング

次の例では、PPPoE 拡張セッションでの QoS プロビジョニングについて説明します。

```
policy-map rar_policer
 class class-default
  police 10000 2000 1000 conform-action transmit  exceed-action drop  violate-action
drop
policy-map rar_shaper
 class class-default
  shape average percent 1

interface Virtual-Template2
 ip address 10.92.2.1 255.255.255.0
 no peer default ip address
 no keepalive
 service-policy input rar_policer
end
```

例：バイパスモードでの RAR 機能の設定

次に、バイパスモードにおける RAR のエンドツーエンド設定の例を示します。

（注） RAR を設定する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。認証され有効になっていないと、ポイントツーポイントプロトコルはこれを RAR セッションとして認識せず、PPPoE Active Discovery Initiate（PADI）の提示の際に *manet_radio* をタグ付けしない場合があります。デフォルトでは、設定にバイパスモードが表示されません。モードがバイパスとして設定されている場合にのみ表示されます。

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

ブロードバンドの設定

```
bba-group pppoe VMI2
 virtual-template 2
service profile rar-lab
!
interface GigabitEthernet0/0/1
 description Connected to Client1
  negotiation auto
  pppoe enable group VMI2
!
```

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

バイパスモードの設定

- 仮想テンプレートで明示的に設定された IP アドレス

```
interface Virtual-Template2
ip address 192.168.90.3 255.255.255.0
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
```

```
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

- 仮想テンプレートで設定された番号なしの VMI

```
interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

バイパスモードでの仮想マルチポイント インターフェイスの設定

```
interface vmi2 //configure the virtual multi interface
ip address 192.168.2.1 255.255.0.0
physical-interface GigabitEthernet0/0/1
mode bypass

interface vmi3//configure the virtual multi interface
 ip address 192.168.3.1 255.255.0.0
 physical-interface GigabitEthernet0/0/1
mode bypass
```

OSPF ルーティングの設定

```
router ospfv3 1
 router-id 192.168.1.1
!
 address-family ipv4 unicast
  redistribute connected metric 1 metric-type 1
  log-adjacency-changes
 exit-address-family
 !
 address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
 exit-address-family
!
ip local pool PPPoEpool2 192.168.12.3 192.168.12.254
```

RAR セッションの詳細の確認

RAR セッションの詳細を取得するには、次の show コマンドを使用します。

```
Router#show pppoe session packets all
Total PPPoE sessions 2

session id: 9
local MAC address: 006b.f10e.a5e0, remote MAC address: 0050.56bc.424a
virtual access interface: Vi2.1, outgoing interface: Gi0/0/0
```

```
    1646 packets sent, 2439363 received
    176216 bytes sent, 117250290 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 32928     PADG Timer index: 0
 PADG last rcvd Seq Num: 17313
 PADG last nonzero Seq Num: 17306
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33308  rcvd: 17313
 PADC xmit: 17313  rcvd: 19709
 In-band credit pkt xmit: 7 rcvd: 2434422
 Last credit packet snapshot
  PADG xmit: seq_num = 32928, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 32928, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17313, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17313, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


session id: 10
local MAC address: 006b.f10e.a5e1, remote MAC address: 0050.56bc.7dcb
virtual access interface: Vi2.2, outgoing interface: Gi0/0/1
    1389302 packets sent, 1852 received
    77869522 bytes sent, 142156 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18787     PADG Timer index: 0
 PADG last rcvd Seq Num: 18784
 PADG last nonzero Seq Num: 18768
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18787  rcvd: 18784
 PADC xmit: 18784  rcvd: 18787
 In-band credit pkt xmit: 1387764 rcvd: 956
 Last credit packet snapshot
  PADG xmit: seq_num = 18787, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18787, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18784, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18784, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show pppoe session packets
Total PPPoE sessions 2

SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
9       2439391         1651            117252098       176714
10      1858            1389306         142580          77869914
```

```
Router#show vmi counters
Interface vmi2: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =       4280
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi3: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =       2956
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi4: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =          0
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Router#


Router#show vmi neighbor details
1 vmi2 Neighbors
      1 vmi3 Neighbors
```

```
      0 vmi4 Neighbors
      2 Total Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.168.2.2, Uptime=05:15:01
       Output pkts=89, Input pkts=0
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=9
       INTERFACE STATS:
          VMI Interface=vmi2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33038     PADG Timer index: 0
 PADG last rcvd Seq Num: 17423
 PADG last nonzero Seq Num: 17420
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33418  rcvd: 17423
 PADC xmit: 17423  rcvd: 19819
 In-band credit pkt xmit: 7 rcvd: 2434446
 Last credit packet snapshot
  PADG xmit: seq_num = 33038, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33038, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17423, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17423, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


vmi3   IPV6 Address=FE80::21E:7AFF:FE68:6100
       IPV6 Global Addr=::
       IPV4 Address=91.91.91.4, Uptime=05:14:55
       Output pkts=6, Input pkts=0
       METRIC DATA: Total rcvd=1, Avg arrival rate (ms)=0
          CURRENT: MDR=128000 bps, CDR=128000 bps
                   Lat=0 ms, Res=100, RLQ=100, load=0
          MDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          CDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          Latency  Max=0, Min=0, Avg=0 (ms)
          Resource Max=100%, Min=100%, Avg=100%
          RLQ      Max=100, Min=100, Avg=100
          Load     Max=0%, Min=0%, Avg=0%
       Transport PPPoE, Session ID=10
       INTERFACE STATS:
          VMI Interface=vmi3,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/1,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
```

```
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18896     PADG Timer index: 0
 PADG last rcvd Seq Num: 18894
 PADG last nonzero Seq Num: 18884
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18896  rcvd: 18894
 PADC xmit: 18894  rcvd: 18896
 In-band credit pkt xmit: 1387764 rcvd: 961
 Last credit packet snapshot
  PADG xmit: seq_num = 18896, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18896, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18894, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18894, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show vmi neighbor details vmi 2
              1 vmi2 Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.168.2.2, Uptime=05:16:03
       Output pkts=89, Input pkts=0
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=9
       INTERFACE STATS:
          VMI Interface=vmi2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33100     PADG Timer index: 0
 PADG last rcvd Seq Num: 17485
 PADG last nonzero Seq Num: 17449
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33480  rcvd: 17485
 PADC xmit: 17485  rcvd: 19881
 In-band credit pkt xmit: 7 rcvd: 2434460
 Last credit packet snapshot
  PADG xmit: seq_num = 33100, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33100, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17485, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17485, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


Router#show platform hardware qfp active feature ess session
Current number sessions: 2
Current number TC flow: 0
```

```
Feature Type: A=Accounting D=Policing(DRL) F=FFR M=DSCP Marking L=L4redirect P=Portbundle
 T=TC

   Session    Type      Segment1      SegType1      Segment2      SegType2 Feature Other
-------------------------------------------------------------------------------------------

        21     PPP 0x0000001500001022    PPPOE 0x0000001500002023    LTERM -------
        24     PPP 0x0000001800003026    PPPOE 0x0000001800004027    LTERM -------


Router#show platform software subscriber pppoe_fctl evsi 21
PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33215     PADG Timer index: 0
 PADG last rcvd Seq Num: 17600
 PADG last nonzero Seq Num: 17554
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33595  rcvd: 17600
 PADC xmit: 17600  rcvd: 19996
 In-band credit pkt xmit: 7 rcvd: 2434485
 Last credit packet snapshot
  PADG xmit: seq_num = 33215, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33215, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17600, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17600, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534

BQS buffer statistics
 Current packets in BQS buffer: 0
 Total en-queue packets: 0 de-queue packets: 0
 Total dropped packets: 0

Internal flags: 0x0


Router#show platform hardware qfp active feature ess session id 21
Session ID: 21

  EVSI type: PPP
  SIP Segment ID: 0x1500001022
  SIP Segment type: PPPOE
  FSP Segment ID: 0x1500002023
  FSP Segment type: LTERM
  QFP if handle: 16
  QFP interface name: EVSI21
  SIP TX Seq num: 0
  SIP RX Seq num: 0
  FSP TX Seq num: 0
  FSP RX Seq num: 0
  Condition Debug: 0x00000000
    session


Router#show ospfv3 neighbor

          OSPFv3 1 address-family ipv4 (router-id 192.168.3.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
```

```
192.168.1.1           0   FULL/  -        00:01:32    19              Virtual-Access2.1

          OSPFv3 1 address-family ipv6 (router-id 192.168.3.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.168.1.1           0   FULL/  -        00:01:52    19              Virtual-Access2.1
Router#


Router#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.0.3/8 is variably subnetted, 3 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Virtual-Access2.1
O        192.168.4.0/32 [110/1] via 192.168.4.0, 00:00:03, Virtual-Access2.1
L        192.168.5.0/32 is directly connected, Virtual-Access2.1
      192.168.0.5/32 is subnetted, 1 subnets
C        192.168.2.21 is directly connected, Virtual-Access2.1
```

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。