



Cloud OnRamp for Colocation



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

クラウドに移行するアプリケーションが増えるにつれて、トラフィックを高価な WAN 回線経由でデータセンターにバックホールする従来型のアプローチはもはや妥当ではなくなってきています。従来の WAN インフラストラクチャは、クラウド内のアプリケーションにアクセスすることを想定して設計されていませんでした。このインフラストラクチャは高額で、エクスペリエンスを低下させる不要な遅延を生みます。

ネットワークアーキテクトは、次のことを達成するために WAN の設計を再評価しています。

- クラウドへの移行をサポート。
- ネットワークコストの削減。
- クラウドトラフィックの可視性と管理性の向上。

ネットワークアーキテクトは、Software-Defined WAN (SD-WAN) ファブリックに変更して安価なブロードバンドインターネット サービスを利用し、リモートブランチから信頼性のある SaaS クラウドバウンドトラフィックをインテリジェントにルーティングします。

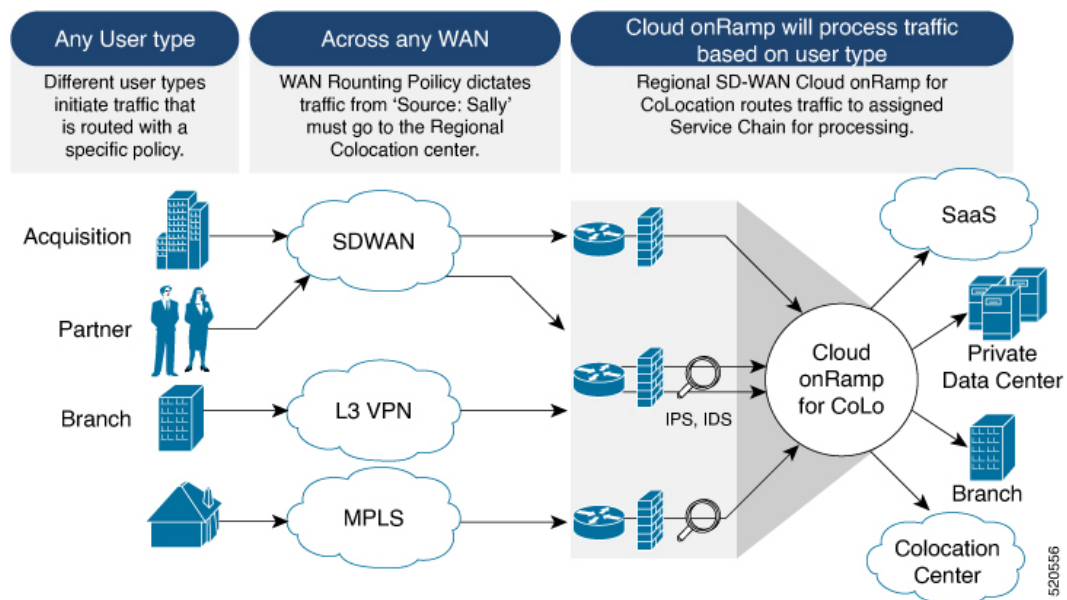
このソリューションでは、コロケーション設備向けに特別に構築された Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションにより、ブランチおよびリモートワーカーからすべてのアプリケーションがホストされている場所への最適なパスにトラフィックをルーティングします。また、このソリューションにより、分散型企業はブランチで直接インターネットア

アクセスが可能になり、Infrastructure-as-a-Service (IaaS) プロバイダーおよび Software as a Service (SaaS) プロバイダーへの接続を強化できます。

このソリューションは、大都市の周りに集まっている、または複数の国に分散している複数の分散型ブランチオフィスを持つ企業に、コロケーション設備でルーティングサービスを地域化する機能を提供します。その理由は、これらの設備がブランチに物理的に近く、企業がアクセスする必要があるクラウドリソースをホストできるためです。したがって、基本的に、仮想 Cisco Catalyst SD-WAN をコロケーションセンターの地域アーキテクチャに分散させることにより、クラウドエッジに処理能力を与えます。

次の図は、マルチクラウドアプリケーションへのアクセスを複数のブランチから地域のコロケーション設備に集約する方法を示しています。

図 1: Cisco Catalyst SD-WAN Cloud OnRamp for Colocation



このソリューションは、次の4つの特定のタイプの企業に対応できます。

- セキュリティ制限とプライバシー規制により、クラウドおよび SaaS プラットフォームへの直接インターネット接続を使用できない多国籍企業。
- Cisco Catalyst SD-WAN を使用していないが、顧客への接続が必要なパートナーおよびベンダー。これらの企業は、自社サイトに Cisco Catalyst SD-WAN ルーティングアプライアンスをインストールすることを望んでいません。
- 高帯域幅、最適なアプリケーションパフォーマンス、きめ細かいセキュリティを必要とする、地理的に分散したブランチオフィスを持つグローバルな組織。
- 安価な直接インターネットリンクを介した企業への安全な VPN 接続を必要とするリモートアクセス。

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションは、コロケーション IaaS プロバイダーによって特定のコロケーション設備内でホストできます。必要なコンポーネントを

サポートしている限り、地域ごとにニーズを満たすコロケーションプロバイダーを選択できます。

- [Cloud OnRamp for Colocation ソリューションの展開, on page 3](#)
- [Cloud OnRamp for Colocation デバイスの管理 \(4 ページ\)](#)
- [クラスタの管理, on page 7](#)
- [サービス グループの管理, on page 37](#)
- [VM カタログとリポジトリの管理, on page 57](#)
- [Cisco Catalyst SD-WAN Manager からの Cloud OnRamp for Colocation デバイスの動作ステータスのモニター \(72 ページ\)](#)
- [Cisco Catalyst SD-WAN Cloud OnRamp for Colocation マルチテナント機能 \(84 ページ\)](#)

Cloud OnRamp for Colocation ソリューションの展開

このトピックでは、colo デバイスの使用を開始し、Cisco SD-WAN Manager でクラスタを構築する手順の概要を説明します。クラスタを作成して構成したら、クラスタをアクティブ化するために必要な手順を実行できます。サービスグループまたはサービスチェーンを設計し、それらをアクティブ化されたクラスタに接続する方法を理解します。サポートされている Day-N 操作もこのトピックにリストされています。

1. ソリューションの前提条件と要件を満たします。「[Prerequisites and Requirements of Cloud OnRamp for Colocation Solution](#)」を参照してください。
 - CSP デバイス（初期 CSP アクセス用の CIMC のセットアップ）および Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチ（コンソールサーバーのセットアップ）と OOB または管理スイッチの配線を完了します。すべてのデバイスの電源をオンにします。
 - DHCP サーバーをセットアップして構成します。「[Provision DHCP Server per Colocation](#)」を参照してください。
2. インストールされている Cisco NFVIS のバージョンを確認し、必要に応じて NFVIS をインストールします。「[Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP](#)」を参照してください。
3. クラスタをセットアップまたはプロビジョニングします。クラスタは、CSP デバイスや Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチを含むすべての物理デバイスで構成されます。「[Get Started with Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution](#)」を参照してください。
 - CSP デバイスを起動します。「[Bring Up Cloud Services Platform Devices](#)」を参照してください。
 - Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチを起動します。「[Bring Up Switch Devices](#)」を参照してください。
 - クラスタをプロビジョニングして構成します。「[Provision and Configure Cluster](#)」を参照してください。

クラスタ設定でクラスタを構成します。「[Cluster Settings](#)」を参照してください。

4. クラスタをアクティブ化します。『[クラスタの作成とアクティブ化, on page 10](#)』を参照してください。
5. サービスグループまたはサービスチェーンを設計します。『[サービスグループの管理, on page 37](#)』を参照してください。



Note クラスタを作成する前、またはすべてのVMがリポジトリにアップロードされた後にクラスタをアクティブ化する前に、いつでもサービスチェーンを設計し、サービスグループを作成できます。

6. サービスグループとサービスチェーンをクラスタに接続または切り離します。『[クラスタ内のサービスグループの接続または切断, on page 56](#)』を参照してください。



Note クラスタがアクティブになった後、サービスチェーンをクラスタに接続できます。

7. (オプション) すべての Day-N 操作を実行します。
 - サービスグループを切り離して、サービスチェーンを切り離します。『[クラスタ内のサービスグループの接続または切断, on page 56](#)』を参照してください。
 - クラスタに CSP デバイスを追加および削除します。[Cloud OnRamp Colocation デバイスの追加, on page 5](#)および [Cloud OnRamp for Colocation デバイスの削除, on page 6](#)を参照してください。
 - クラスタを非アクティブ化します。『[クラスタの削除, on page 35](#)』を参照してください。
 - クラスタを再アクティブ化します。『[クラスタの再アクティブ化, on page 36](#)』を参照してください。
 - より多くのサービスグループまたはサービスチェーンを設計します。[サービスグループでのサービスチェーンの作成, on page 37](#)を参照してください。

Cloud OnRamp for Colocation デバイスの管理

Cisco SD-WAN Manager を介して、CSP デバイス、Catalyst 9500-40X デバイス、および VNF を追加できます。

Cloud OnRamp Colocation デバイスの追加

Cisco SD-WAN Manager を使用して、CSP デバイス、スイッチデバイス、および VNF を追加できます。Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューション製品識別子 (PID) を注文すると、Cisco SD-WAN Manager からアクセスできるスマートアカウントからデバイス情報を入手できます。

始める前に

セットアップの詳細が次のようになっていることを確認します。

- Cisco SD-WAN Manager IP アドレスとログイン情報、Cisco SD-WAN Validator IP アドレスとログイン情報などの Cisco Catalyst SD-WAN セットアップの詳細
- Cisco CSP デバイスの CIMC IP アドレスとログイン情報、または UCSC CIMC IP アドレスとログイン情報などの NFVIS セットアップの詳細
- 両方のスイッチコンソールにアクセス可能

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、[Tools] > [SSH Terminal] を選択して、Cisco SD-WAN Manager との SSH セッションを開始します。

ステップ 2 CSP デバイスまたはスイッチデバイスを選択します。

ステップ 3 CSP デバイスまたはスイッチデバイスのユーザー名とパスワードを入力し、[Enter] をクリックします。

ステップ 4 CSP デバイスの PID とシリアル番号 (SN) を取得します。

次の出力例は、いずれかの CSP デバイスの PID を示しています。

```
CSP# show pl
platform-detail hardware_info Manufacturer "Cisco Systems Inc"
platform-detail hardware_info PID CSP-5444
platform-detail hardware_info SN WZP224208MB
platform-detail hardware_info hardware-version 74-105773-01
platform-detail hardware_info UUID da39edec-d831-e549-b663-9e407afd5ac6
platform-detail hardware_info Version 4.6.0-15
```

出力には、CSP デバイスの PID とシリアル番号の両方が表示されます。

ステップ 5 両方の Catalyst 9500 スイッチデバイスのシリアル番号を取得します。

次のサンプルは、最初のスイッチのシリアル番号を示しています。

```
Switch1# show version
Cisco IOS XE Software, Version 17.03.03
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Fri 26-Feb-21 02:01 by mcpre
Technology Package License Information:
```

```

Technology-package
Current
-----
network-advantage    Smart License
dna-advantage        Subscription Smart License
AIR License Level:  AIR DNA Advantage
Next reload AIR license Level:  AIR DNA Advantage

Technology-package
Next reboot
-----
network-advantage
dna-advantage

```

Smart Licensing Status: Registration Not Applicable/Not Applicable

```

cisco C9500-40X (X86) processor with 1331521K/6147K bytes of memory.
Processor board ID FCW2229A0RK
1 Virtual Ethernet interface
96 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
1638400K bytes of Crash Files at crashinfo-1:.
11264000K bytes of Flash at flash:.
11264000K bytes of Flash at flash-1:.

```

```

Base Ethernet MAC Address      : 00:aa:6e:f3:02:00
Motherboard Assembly Number    : 73-18140-03
Motherboard Serial Number     : FOC22270RF8
Model Revision Number         : D0
Motherboard Revision Number   : B0
Model Number                  : C9500-40X
System Serial Number          : FCW2229A0RK
CLEI Code Number              :

```

この出力から、Catalyst 9500 スイッチ シリーズとシリアル番号を知ることができます。

ステップ 6 コロケーションクラスタ内のすべての CSP デバイスと Catalyst 9500 スイッチの PID とシリアル番号レコードを含む .CSV ファイルを作成します。

たとえば、ステップ 4 と 5 で得られた情報から、CSV 形式のファイルは次のようになります。

```
C9500-40,FCW2229A0RK CSP-5444,SN WZP224208MB
```

(注) コロケーションクラスタ内のすべてのデバイスに対して 1 つの .CSV ファイルを作成できます。

ステップ 7 Cisco SD-WAN Manager を使用して、すべての CSP とスイッチデバイスをアップロードします。詳細については、「[Uploading a device authorized serial number file](#)」を参照してください。

アップロード後、デバイスのテーブルにすべての CSP とスイッチデバイスが表示されます。

Cloud OnRamp for Colocation デバイスの削除

Cisco SD-WAN Manager から CSP デバイスを削除するには、次の手順を実行します。

始める前に

次の点を考慮してください。

- 削除するデバイスにサービスチェーンが接続されている場合は、サービスグループを切り離します。『[クラスタ内のサービスグループの接続または切断 \(56 ページ\)](#)』を参照してください。

手順

- ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Certificates]** の順に選択します。
- ステップ 2 該当するデバイスで [...] をクリックし、**[Invalid]** を選択します。
- ステップ 3 **[Configuration]** > **[Certificates]** ウィンドウで、**[Send to Controller]** をクリックします。
- ステップ 4 **[Configuration]** > **[Devices]** ウィンドウで、目的のデバイスの [...] をクリックし、**[Delete WAN Edge]** を選択します。
- ステップ 5 **[OK]** をクリックして、デバイスの削除を確認します。

デバイスを削除すると、**[WAN edge router serial number]** リストからシリアル番号とシャーシ番号が削除され、Cisco SD-WAN Manager からも設定が完全に削除されます。

クラスタの管理



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

Cloud OnRamp for Colocation 画面を使用して、クラスタで使用できるコロケーションクラスタとサービスグループを構成します。

構成する 3 つの手順は次のとおりです。

- クラスタを作成します。『[クラスタの作成とアクティブ化, on page 10](#)』を参照してください。
- サービスグループを作成します。『[サービスグループでのサービスチェーンの作成, on page 37](#)』を参照してください。

- クラスタをサービスグループに接続します。『[クラスタ内のサービスグループの接続または切断, on page 56](#)』を参照してください。

コロケーションクラスタは、2～8台のCSPデバイスと2台のスイッチの集合です。サポートされているクラスタテンプレートは次のとおりです。

- 小規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +2 CSP
- 中規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +4 CSP
- 大規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +6 CSP
- 超大規模クラスタ：2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C +8 CSP



Note 少なくとも2つのCSPデバイスを1つずつクラスタに追加してください。3つ、4つなど、最大8つのCSPデバイスを追加することができます。任意のクラスタのDay-N構成を編集し、最大8つのCSPデバイスまで各サイトにCSPデバイスのペアを追加できます。

クラスタに組み入れるすべてのデバイスのソフトウェアバージョンが同じであることを確認してください。



Note CSP-5444 および CSP-5456 デバイスを同じクラスタで使用することはできません。

クラスタの状態は次のとおりです。

- **Incomplete**：2つのCSPデバイスと2つのスイッチの最小要件を提供せずに、クラスタがCisco SD-WAN Manager インターフェイスから作成された場合。また、クラスタのアクティベーションはまだトリガーされていません。
- **Inactive**：2つのCSPデバイスと2つのスイッチの最小要件を提供した後、Cisco SD-WAN Manager インターフェイスからクラスタが作成され、クラスタのアクティベーションがまだトリガーされていない場合。
- **Init**：クラスタのアクティベーションがCisco SD-WAN Manager インターフェイスからトリガーされ、エンドデバイスへのDay-0構成プッシュが保留中の場合。
- **Inprogress**：クラスタ内のいずれかのCSPデバイスが制御接続を確立すると、クラスタはこの状態に移行します。
- **Pending**：Day-0構成のプッシュが保留中、またはVNFのインストールが保留中の場合。
- **Active**：クラスタが正常にアクティブ化され、NCSが構成をエンドデバイスにプッシュした場合。
- **Failure**：Cisco Colo Manager が起動していない場合、またはいずれかのCSPデバイスがUPイベントの受信に失敗した場合。

Active 状態または Failure 状態へのクラスタの移行は次のとおりです。

- [Inactive] > [Init] > [Inprogress] > [Pending] > [Active]— 成功
- [Inactive] > [Init] > [Inprogress] > [Pending] > [Failure]— 失敗

クラスタのプロビジョニングと構成

このトピックでは、サービスチェーンの展開を可能にするクラスタのアクティブ化について説明します。

クラスタをプロビジョニングして構成するには、次の手順を実行します。

1. 2～8 個の CSP デバイスと 2 つのスイッチを追加して、コロケーションクラスタを作成します。

起動する前に CSP デバイスをクラスタに追加し、Cisco SD-WAN Manager を使用して設定できます。AAA、デフォルトのユーザー (admin) パスワード、NTP、syslog などのグローバル機能を使用して、CSP デバイスと Catalyst 9K スイッチを設定できます。

2. サービスチェーン VLAN プール、VNF 管理 IP アドレスプール、管理ゲートウェイ、VNF データプレーン IP プール、システム IP アドレスプールなどの IP アドレスプール入力を含むコロケーションクラスタ パラメータを設定します。

3. サービス グループを設定します。

サービスグループは、1 つ以上のサービスチェーンで構成されます。



Note 定義済みまたは検証済みのサービス チェーン テンプレートのいずれかを選択するか、カスタムのサービスチェーンを作成して、サービスチェーンを追加できます。前述のように、サービスチェーンごとに、入力および出力 VLAN ハンドオフとサービスチェーンのスループットまたは帯域幅を設定します。

4. サービステンプレートから各 VNF を選択して、各サービスチェーンを構成します。VNF リポジトリにすでにアップロードされている VNF イメージを選択して、必要なリソース (CPU、メモリ、ディスク) とともに VM を起動します。サービスチェーン内の各 VNF について、次の情報を指定します。

- HA、共有 VM などの特定の VM インスタンスの動作は、サービスチェーン全体で共有できます。
- VLAN プール、管理 IP アドレス、またはデータ HA IP アドレスの一部ではなく、トークン化されたキーの Day-0 設定値。ピアリング IP や自律システム値など、最初と最後の VM ハンドオフ関連情報を指定する必要があります。サービスチェーンの内部パラメータは、指定された VLAN、管理、またはデータプレーン IP アドレスプールから Cisco SD-WAN Validator によって自動的に更新されます。

5. サービスグループごとに必要な数のサービスチェーンを追加し、クラスタに必要な数のサービスグループを作成します。
6. クラスタをサイトまたは場所に接続するには、すべての構成が完了した後にクラスタをアクティブ化します。

[Task View] ウィンドウで、クラスタのステータスが進行中からアクティブまたはエラーに変化するのを確認できます。

クラスタを編集するには、以下を行います。

1. サービスグループまたはサービスチェーンを追加または削除して、アクティブ化されたクラスタを変更します。
2. AAA、システム設定などのグローバル機能設定を変更します。

クラスタを作成する前に、サービスグループとサービスチェーンを事前に設計できます。クラスタがアクティブになった後、サービスグループをクラスタに接続できます。

クラスタの作成とアクティブ化

このトピックでは、CSP デバイス、Cisco Catalyst スイッチを1つのユニットとして使用してクラスタを形成し、クラスタ固有の構成でクラスタをプロビジョニングする方法の手順について説明します。

始める前に

- Cisco SD-WAN Manager および CSP デバイスのクロックを同期していることを確認します。CSP デバイスのクロックを同期するには、クラスタ設定に関する情報を入力するときに、CSP デバイスの NTP サーバーを構成します。
- Cisco SD-WAN Manager および Cisco SD-WAN Validator の NTP サーバーが設定されていることを確認します。NTP サーバーを設定するには、『[Cisco Catalyst SD-WAN System and Interface Configuration Guide](#)』を参照してください。
- CSP デバイスを起動するように、CSP デバイスの OTP を構成していることを確認します。『[Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide](#)』の「Bring Up Cloud Services Platform」を参照してください。
- 両方の Catalyst 9500 スイッチの電源をオンにして、それらが動作していることを確認してください。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、Cisco SD-WAN Manager を選択して、**[Configuration] > [Cloud OnRamp for Colocation]** をクリックします。

- a) **[Configure & Provision Cluster]** をクリックします。

- b) 次の情報を入力します。

表 1: クラスタ情報

フィールド	説明
Cluster Name	クラスタ名には、128 文字の英数字を含めることができます。
Description	説明には、2048 文字の英数字を含めることができます。
Site ID	オーバーレイ ネットワーク サイト識別子。サイト ID に入力する値が、他の Cisco Catalyst SD-WAN オーバーレイ要素の組織サイト ID 構造と同様であることを確認してください。
Location	場所には、128 文字の英数字を含めることができます。
Cluster Type	複数のテナント間で共有できるようにマルチテナントモードでクラスタを構成するには、[Shared] を選択します。 (注) シングルテナントモードでは、クラスタタイプはデフォルトで [Non Shared] が選択されています。

- c) スイッチを構成するには、[Switches] ボックスのスイッチアイコンをクリックします。[Edit Switch] ダイアログボックスで、スイッチ名を入力し、ドロップダウンリストからスイッチのシリアル番号を選択します。[Save] をクリックします。

スイッチ名には、128 文字の英数字を含めることができます。

ドロップダウンリストに表示されるスイッチのシリアル番号は、PnP プロセスを使用して取得され、Cisco SD-WAN Manager と統合されます。これらのシリアル番号は、CCW で Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューション PID を注文し、スイッチデバイスを調達するときに、スイッチに割り当てられます。

(注) スイッチデバイスと CSP デバイスのシリアル番号フィールドを空白のままにして、コロケーションクラスタを設計し、後でクラスタを編集して、デバイスを調達した後でシリアル番号を追加できます。ただし、シリアル番号のない CSP デバイスまたはスイッチデバイスを使用してクラスタをアクティブ化することはできません。

- d) 別のスイッチを構成するには、手順 c を繰り返します。
- e) CSP デバイスを構成するには、[Appliances] ボックスの CSP アイコンをクリックします。[Edit CSP] ダイアログボックスが表示されます。CSP デバイス名を指定し、ドロップダウンリストから CSP シリアル番号を選択します。[Save] をクリックします。

CSP デバイス名には、128 文字の英数字を含めることができます。

- f) CSP デバイスの OTP を構成して、デバイスを起動します。
- g) 残りの CSP デバイスを追加するには、手順 e を繰り返します。
- h) [Save] をクリックします。
クラスタを作成すると、クラスタ設定画面で、デバイスにシリアル番号が割り当てられていないデバイスの横に、黄色の円で囲まれた省略記号が表示されます。デバイスを編集してシリアル番号を入力できます。
- i) CSP デバイス構成を編集するには、CSP アイコンをクリックし、サブステップ e で説明されているプロセスを実行します。
- j) クラスタの必須およびオプションのグローバルパラメータを設定するには、クラスタ構成ページで、[Cluster Configuration] のパラメータを入力します。[クラスタの設定 \(12 ページ\)](#) を参照してください。
- k) [保存 (Save)] をクリックします。
作成したクラスタは、クラスタ構成ページの表に表示できます。

ステップ 2 クラスタをアクティブ化するには、次の手順を実行します。

- a) クラスタテーブルからクラスタをクリックします。
- b) 目的のクラスタの [...] をクリックし、[Activate] を選択します。

クラスタをアクティブ化すると、Cisco SD-WAN Manager はクラスタ内の CSP デバイスとの DTLS トンネルを確立し、そこで Cisco Colo Manager を介してスイッチに接続します。DTLS トンネル接続が実行されている場合、クラスタ内の CSP デバイスが Cisco Colo Manager をホストするために選択されます。Cisco Colo Manager が起動し、Cisco SD-WAN Manager がグローバルパラメータ設定を CSP デバイスと Cisco Catalyst 9500 スイッチに送信します。クラスタのアクティブ化の進行状況については、[クラスタアクティベーションの進行状況 \(23 ページ\)](#) を参照してください。



(注) Cisco vManage リリース 20.7.1 以前のリリースでは、Cisco Colo Manager (CCM) および CSP デバイス設定タスクは、タスクが作成されてから 30 分後にタイムアウトします。長時間実行されるイメージのインストール操作の場合、これらの構成タスクがタイムアウトして失敗することがありますが、クラスタのアクティブ化状態は引き続き保留中の状態のままになります。

Cisco vManage リリース 20.8.1 以降では、CCM および CSP デバイス設定タスクは、Cisco SD-WAN Manager がターゲットデバイスから受信した最後のハートビートステータスメッセージの 30 分後にタイムアウトします。この変更により、実行時間の長いイメージのインストール操作によって、タスクの作成後に事前定義された時間が経過した後に構成タスクが失敗することがなくなりました。

クラスタの設定

クラスタ設定パラメータを以下に示します。

ログインクレデンシャル

1. [Cluster Topology] ウィンドウで、[Credentials] の横にある [Add] をクリックします。
[Credentials] 設定画面で、次のように入力します。
 - (必須) [Template Name] : テンプレート名には、128 文字の英数字を含めることができます。
 - (オプション) [Description] : 説明には、2048 文字の英数字を含めることができます。
2. [New User] をクリックします。
 - [Name] フィールドに、ユーザー名を入力します。
 - [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドでパスワードを確認します。
 - [Role] ドロップダウンリストで、管理者を選択します。
3. [Add] をクリックします。
新しいユーザーとユーザー名およびパスワード、およびロールとアクションが表示されます。
4. [Save] をクリックします。
新しいユーザーのログイン情報が追加されます。
5. 構成をキャンセルするには、[Cancel] をクリックします。
6. ユーザーの既存のログイン情報を編集するには、[Edit] をクリックして構成を保存します。

リソースプール

1. [Cluster Topology] ウィンドウで、[Resource Pool] の横にある [Add] をクリックします。
[Resource Pool] 設定画面で、次のフィールドに値を入力します。
 - [Name] : IP アドレスプールの名前には、128 文字の英数字を含める必要があります。
 - [Description] : 説明には、2048 文字の英数字を含めることができます。
 2. [DTLS Tunnel IP] フィールドに、DTLS トンネルに使用する IP アドレスを入力します。複数の IP アドレスを入力するには、アドレスをカンマで区切ります。範囲を入力するには、IP アドレスをハイフンで区切ります (たとえば、172.16.0.180-172.16.255.190) 。
 3. [Service Chain VLAN Pool] フィールドに、サービスチェーンに使用する VLAN 番号を入力します。複数の番号を入力するには、カンマで区切ります。数値の範囲を入力するには、番号をハイフンで区切ります (たとえば、1021-2021) 。
- VLAN 情報を入力するときは、次の点を考慮してください。
- 1002 ~ 1005 は予約済みの VLAN 値であり、クラスタ作成 VLAN プールでは使用しないでください。



- (注) 有効な VNF VLAN プール : 1010 ~ 2000 および 1003 ~ 2000
無効 : 1002 ~ 1005 (使用しないでください)



- 注意 1002 ~ 1005 は構成に使用できません。許可される VLAN は連続している必要があります。

例 : データ VLAN プールを 1006-2006 と入力します。サービスチェーンの作成中に、この VLAN 範囲が入力/出力 VLAN で使用されないようにしてください。

4. [VNF Data Plane IP Pool] フィールドに、VNF インターフェイスでデータプレーンを自動構成するために使用する IP アドレスを入力します。複数の IP アドレスを入力するには、アドレスをカンマで区切ります。範囲を入力するには、IP アドレスをハイフンで区切ります (たとえば、10.0.0.1-10.0.0.100)。
5. [VNF Management IP Pool] フィールドで、VNF に使用する IP アドレスを入力します。複数の IP アドレスを入力するには、アドレスをカンマで区切ります。範囲を入力するには、IP アドレスをハイフンで区切ります (たとえば、192.168.30.99-192.168.30.150)。



- (注) これらのアドレスは、セキュアインターフェイスの IP アドレスです。

6. [Management Subnet Gateway] フィールドに、管理ネットワークへのゲートウェイの IP アドレスを入力します。これにより、DNS がクラスタから抜けられるようになります。
7. [Management Mask] フィールドに、フェールオーバークラスタのマスク値を入力します。たとえば、/24 です。255.255.255.0 ではありません
8. [Switch PNP Server IP] フィールドに、スイッチデバイスの IP アドレスを入力します。



- (注) スイッチの IP アドレスは、管理プールから自動的に取得され、これが最初の IP アドレスです。スイッチの DHCP サーバーで別の IP アドレスが構成されている場合、これを変更できません。

9. [Save] をクリックします。

ポート接続

表 2: 機能の履歴

機能名	リリース情報	説明
フレキシブル トポロジ	Cisco IOS XE Catalyst SD-WAN リ リース 17.3.1a Cisco vManage リリース 20.3.1 Cisco NFVIS リ リース 4.2.1	この機能により、NIC カードを柔軟に挿入し、Cloud onRamp for Colocation クラスタ内でデバイス（CSP デバイスおよび Catalyst 9500 スイッチ）を相互接続することができます。どの CSP ポートも、スイッチの任意のポートに接続できます。Stackwise Virtual Switch Link（SVL）ポートは任意のポートに接続でき、同様にアップリンクポートはスイッチの任意のポートに接続できます。
100G インター フェイスでの SVL ポート構 成のサポート	Cisco IOS XE Catalyst SD-WAN リ リース 17.8.1a Cisco vManage リリース 20.8.1 Cisco NFVIS リ リース 4.8.1	この機能を使用すると、Cisco Catalyst 9500-48Y4C スイッチの 100-G イーサネットインターフェイスに SVL ポートを構成できるため、高レベルのパフォーマンスとスループットが保証されます。

SVL およびアップリンクポートを構成するための前提条件

- SVL およびアップリンクポートを構成するときは、Cisco SD-WAN Manager で構成するポート番号が物理的にケーブル接続されたポートと一致していることを確認してください。
- 両方のスイッチにシリアル番号を割り当ててください。「[Create and Activate Clusters](#)」を参照してください。

SVL およびアップリンクポートの構成

- [Cluster Topology] ウィンドウで、[Port Connectivity] の横にある [Add] をクリックします。
[Port Connectivity] 設定画面に、構成された両方のスイッチが表示されます。スイッチポートにカーソルを合わせると、ポート番号とポートタイプが表示されます。



(注) SVL およびアップリンクポートの詳細については、『[Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide](#)』の「Wiring Requirements」を参照してください。

デフォルトの SVL およびアップリンクポートの変更

デフォルトのポート番号とポートタイプを変更する前に、Cisco Catalyst 9500-40X および Cisco Catalyst 9500-48Y4C スイッチに関する次の情報に注意してください。

- Cisco vManage リリース 20.8.1 以降では、2 つの Cisco Catalyst 9500-40X スイッチまたは 2 つの Cisco Catalyst 9500-48Y4C スイッチでコロケーションクラスタを作成するときに、2 つの SVL ポートと 1 つのデュアルアクティブ検出 (DAD) ポートを構成できます。
- SVL および DAD ポートが Cisco Catalyst 9500-48Y4C スイッチに対して正しく構成されていることを確認するには、次の情報に注意してください。
 - 同じ速度のインターフェイス、つまり 25G インターフェイスまたは 100G インターフェイスのいずれかで SVL ポートを構成します。両方のスイッチで構成が同じであることを確認します。
 - 両方のスイッチの 25G インターフェイスでのみ DAD ポートを構成します。
 - 既存のクラスタの場合、非アクティブな場合にのみ SVL ポートを変更できます。
- Cisco vManage リリース 20.8.1 以前のリリースで作成されたクラスタは、Cisco vManage リリース 20.8.1 にアップグレード後に 2 つの SVL ポートと 1 つの DAD ポートを自動的に表示します。
- Cisco Catalyst 9500-40X スイッチの場合、両方のスイッチの 10G インターフェイスで SVL および DAD ポートを構成する必要があります。
- Cisco Catalyst 9500 スイッチのデフォルトの SVL、DAD、およびアップリンクポートは次のとおりです。

Cisco Catalyst 9500-40X

- SVL ポート : Te1/0/38 ~ Te1/0/39、および Te2/0/38 ~ Te2/0/39
Cisco vManage リリース 20.7.1 以前のリリースでは、デフォルトの SVL ポートは Te1/0/38 ~ Te1/0/40 および Te2/0/38 ~ Te2/0/40 です。
- DAD ポート : Te1/0/40 および Te2/0/40
- アップリンクポート : Te1/0/36、Te2/0/36 (入力 VLAN ハンドオフ)、Te1/0/37、および Te2/0/37 (出力 VLAN ハンドオフ)

Cisco Catalyst 9500-48Y4C

- SVL ポート : Hu1/0/49 ~ Hu1/0/50 および Hu2/0/49 ~ Hu2/0/50
Cisco vManage リリース 20.7.1 以前のリリースでは、デフォルトの SVL ポートは Twe1/0/46 ~ Twe1/0/48 および Twe2/0/46 ~ Twe2/0/48 です。
- DAD ポート : Twe1/0/48 および Twe2/0/48
- アップリンクポート : 25G スループット用の Twe1/0/44、Twe2/0/44 (入力 VLAN ハンドオフ)、Twe1/0/45、および Twe2/0/45 (出力 VLAN ハンドオフ)。

- I、E、および S は、それぞれ入力、出力、および SVL ポートを表します。
- 物理的ケーブル接続がデフォルト構成と同じであることを確認し、[Save] をクリックします。

SVL ポートとアップリンクポートの接続が異なる場合にデフォルトポートを変更するには、次の手順を実行します。

1. 両方のスイッチが同じポートを使用している場合：

1. 物理的に接続されているポートに対応するスイッチのポートをクリックします。
2. ポート構成を他のスイッチに追加するには、[Apply change] チェックボックスをオンにします。

両方のスイッチが同じポートを使用していない場合：

1. [Switch1] のポートをクリックします。
 2. [Port Type] ドロップダウンリストからポートタイプを選択します。
 3. [Switch2] のポートをクリックし、ポートタイプを選択します。
2. 別のポートを追加するには、手順 1 を繰り返します。
3. [Save] をクリックします。
4. ポート接続情報を編集するには、[Cluster Topology] ウィンドウで、[Port Connectivity] の横にある [Edit] をクリックします。



(注) クラスタがアクティブ化されていない場合は、クラスタの SVL およびアップリンクポートを変更できません。

5. ポートをリセットしてデフォルト設定にするには、[Reset] をクリックします。

Cisco CSP デバイスの残りのポート（SR-IOV および OVS）とスイッチとの接続は、クラスタをアクティブ化するときに、Link Layer Discovery Protocol（LLDP）を使用して自動的に検出されます。これらのポートを設定する必要はありません。

Cisco Colo Manager は、スイッチのネイバーポートを検出し、すべての Niantic ポートと Fortville ポートが接続されているかどうかを識別します。いずれかのポートが接続されていない場合、CCM から Cisco SD-WAN Manager に通知が送信され、タスクビューウィンドウに表示できます。

NTP

必要に応じて、クラスタの NTP サーバーを構成します。

1. [Cluster Topology] ウィンドウで、[NTP] の横にある [Add] をクリックします。[NTP] 設定画面で、次のように入力します。

- [Template Name] : NTP テンプレートの名前は英数字で、最大 128 文字である必要があります。
 - [Description] : 説明は英数字で、最大 2048 文字にする必要があります。
2. [Preferred server] フィールドに、プライマリ NTP サーバーの IP アドレスを入力します。
 3. [Backup server] フィールドに、セカンダリ NTP サーバーの IP アドレスを入力します。
 4. [Save] をクリックします。
NTP サーバーが追加されます。
 5. NTP サーバーの構成をキャンセルするには、[Cancel] をクリックします。
 6. NTP サーバーの構成の詳細を編集するには、[Edit] をクリックします。

Syslog サーバ

必要に応じて、クラスターの syslog パラメータを構成します。

1. [Cluster Topology] ウィンドウで、[Syslog] の横にある [Add] をクリックします。[Syslog] 設定画面で、次のように入力します。
 - [Template Name] : システムテンプレートの名前は英数字で、最大 128 文字を含めることができます。
 - [Description] : 説明の最大長は 2048 文字で、英数字のみを使用できます。
2. [Severity] ドロップダウンリストから、ログ記録する syslog メッセージのシビラティ（重大度）を選択します。
3. 新しい syslog サーバーを追加するには、[New Server] をクリックします。
syslog サーバーの IP アドレスを入力します。
4. [Save] をクリックします。
5. 構成をキャンセルするには、[Cancel] をクリックします。
6. 既存の syslog サーバー構成を編集するには、[Edit] をクリックして構成を保存します。

TACACS 認証

表 3: 機能の履歴

機能名	リリース情報	説明
TACACS Authentication	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、Cisco CSP および Cisco Catalyst 9500 デバイスにアクセスするユーザーの TACACS 認証を構成できます。TACACS を使用してユーザーを認証すると、Cisco CSP および Cisco Catalyst 9500 デバイスへのアクセスが検証され、保護されます。

TACACS 認証は、クラスタがアクティブになった後に Cisco CSP および Cisco Catalyst 9500 デバイスにアクセスできる有効なユーザーを決定します。

考慮すべき点

- デフォルトでは、ロールベースアクセスコントロール (RBAC) を持つ管理ユーザーは、Cisco CSP および Cisco Catalyst 9500 デバイスへのアクセスを許可されています。
- TACACS と RBAC を使用して構成する場合は、同じユーザーに異なるパスワードを設定しないでください。TACACS と RBAC で同じユーザーに異なるパスワードが設定されている場合、RBAC ユーザーとパスワードの認証が使用されます。デバイスで RBAC を構成する方法については、[ログイン クレデンシャル \(13 ページ\)](#) を参照してください。

ユーザーを認証するには、次の手順を実行します。

1. TACACS サーバー構成を追加するには、[Cluster Topology] ウィンドウで、[TACACS] の横にある[Other Settings] > [Add] をクリックします。

TACACS サーバー構成を編集するには、[Cluster Topology] ウィンドウで、[TACACS] の横にある[Other Settings] > [Edit] をクリックします。

[TACACS] 設定画面で、次に関する情報を入力します。

- [Template Name] : TACACS テンプレート名には、128 文字の英数字を含めることができます。
 - (オプション) [Description] : 説明には、2048 文字の英数字を含めることができます。
2. 新しい TACACS サーバーを追加するには、[+ New TACACS SERVER] をクリックします。
 - [Server IP Address] に、IPv4 アドレスを入力します。
TACACS サーバーのホスト名には IPv4 アドレスを使用します。
 - [Secret] にパスワードを入力し、[Confirm Secret] でパスワードを確認します。

3. [Add] をクリックします。

新しい TACACS サーバーの詳細は、[TACACS] 設定画面にリストされます。



(注) 最大 4 つの TACACS サーバーを追加できます。

4. 別の TACACS サーバーを追加するには、手順 2 から手順 3 を繰り返します。
ユーザーの認証時に、最初の TACACS サーバーに到達できない場合、4 つのサーバーすべてが検証されるまで、次のサーバーが検証されます。
5. [Save] をクリックします。
6. TACACS サーバーの設定を削除するには、TACACS サーバーの詳細リストから行を選択し、[Action] の下の [Delete] をクリックします。



(注) 既存の TACACS サーバー情報を変更するには、TACACS サーバーを削除してから新しいサーバーを追加してください。

7. Cisco SD-WAN Manager で TACACS サーバーの設定を表示するには、[Configuration] > [Devices] をクリックします。
目的の Cisco CSP デバイスまたは Cisco Catalyst 9500 スイッチの[...] をクリックし、[Running Configuration] を選択します。

バックアップサーバー設定

考慮すべき点

- NFS サーバーを使用しない場合、Cisco SD-WAN Manager は、将来の RMA 要件のための CSP デバイスのバックアップコピーを正常に作成できません。
- NFS サーバーのマウント場所と構成は、クラスタ内のすべての CSP デバイスで同じです。
- クラスタ内の既存のデバイスを交換用の CSP デバイスとして考えないでください。



(注) 交換用の CSP デバイスが利用できない場合は、Cisco SD-WAN Manager にデバイスが表示されるまで待ちます。

- クラスタ内の CSP デバイ스에 障害があることを特定した後は、クラスタにそれ以上サービスチェーンを接続しないでください。
- CSP デバイスでのバックアップ操作により、NFVIS 構成と VM を含むバックアップファイルが作成されます (VM が CSP デバイスでプロビジョニングされている場合)。以下の情報を参考にしてください。
 - 自動バックアップファイルが生成され、次の形式になります。
serial_number + "_" + time_stamp + ".bkup"

次に例を示します。

```
WZP22180EW2_2020_06_24T18_07_00.bkup
```

- バックアップ操作全体のステータスと各バックアップコンポーネントの内部状態を指定する内部状態モデルが維持されます。
 - **NFVIS** : xml ファイルとしての CSP デバイスの構成バックアップ、**config.xml**。
 - **VM_Images** : 個別にリストされている **data/intdatastore/uploads** 内のすべての **VNF tar.gz** パッケージ。
 - **VM_Images_Flavors** : **img_flvr.img.bkup** などの VM イメージ。
 - **VNF** の個々の **tar** バックアップ : **vmbkp** などのファイル。
- **backup.manifest** ファイルには、バックアップパッケージ内のファイルの情報と、復元操作中に検証するためのチェックサムが含まれています。

クラスタ内のすべての CSP デバイスのバックアップコピーを作成するには、次の手順を実行します。

1. **[Cluster Topology]** ウィンドウで、**[Backup]** の横にある **[Add]** をクリックします。

バックアップサーバーの設定を編集するには、**[Cluster Topology]** ウィンドウで、**[Backup]** の横にある **[Edit]** をクリックします

[Backup] 設定画面で、次のフィールドに関する情報を入力します。

- **Mount Name** : NFS の場所をマウントした後、NFS マウントの名前を入力します。
- **Storage Space** : ディスク容量を GB 単位で入力します。
- **Server IP** : NFS サーバーの IP アドレスを入力します。
- **Server Path** : **/data/colobackup** など、NFS サーバーのフォルダパスを入力します
- **Backup** : **[Backup]** をクリックして有効にします。
- **Time** : バックアップ操作をスケジュールする時間を設定します。
- **Interval** : オプションから選択して、定期的なバックアッププロセスをスケジュールします。
 - **Daily** : 最初のバックアップは、バックアップ構成がデバイスに保存されてから 1 日後に作成され、その後は毎日作成されます。
 - **Weekly** : 最初のバックアップは、バックアップ構成がデバイスに保存されてから 7 日後に作成され、その後は毎週作成されます。
 - **Once** : バックアップコピーは選択した日に作成され、クラスタの存続期間全体にわたって有効です。未来のカレンダーの日付を選択できます。

2. **[Save]** をクリックします。

3. 過去 5 回のバックアップ操作のステータスを表示するには、**show hostaction backup status** コマンドを使用します。バックアップステータス構成コマンドについては、「[Backup and Restore NFVIS and VM Configurations](#)」を参照してください。このコマンドを使用するには、以下の手順を実行します。
 1. Cisco SD-WAN Manager で、[Tools] > [SSH Terminal] の画面をクリックして、Cisco SD-WAN Manager との SSH セッションを開始します。
 2. CSP デバイスを選択します。
 3. CSP デバイスのユーザー名とパスワードを入力し、[Enter] をクリックして CSP デバイスにログインし、**show hostaction backup status** コマンドを実行します。

CSP デバイスの復元

復元する CSP デバイスで CLI を使用する場合にはのみ、復元操作を実行できます。

1. **mount nfs-mount storage** コマンドを使用して NFS をマウントします。
詳細については、「[Network File System Support](#)」を参照してください。



(注) バックアップファイルにアクセスするには、NFS ファイルシステムをマウントするための構成が、障害のあるデバイスと一致している必要があります。NFS マウントの場所と構成はすべての CSP デバイスで同じであるため、他の正常な CSP デバイスからこの情報を表示できます。情報を表示してキャプチャするには、次のいずれかを実行します。

- [Cluster Topology] ウィンドウで、[Backup] の横にある [Add] をクリックします。
- **show running-config** コマンドを使用して、CSP デバイスで実行されているアクティブな構成を表示します。

```
mount nfs-mount storage { mount-name | server_ip server_ip | server_path server_path |
storage_space_total_gb storage_space_total_gb | storage_type storage_type }
```

```
例 : mount nfs-mount storage nfsfs/ server_ip 172.19.199.199 server_path
/data/colobackup/ storage_space_total_gb 100.0 storagetype nfs
```

2. **hostaction restore** コマンドを使用して、交換用 CSP デバイスでバックアップ情報を復元します。

次に例を示します。

```
hostaction restore except-connectivity file-path
nfs:nfsfs/WZP22180EW2_2020_06_24T18_07_00.bkup
```



(注) ステップ 2 でマウントされた NFS サーバーとの接続を維持するには、**except-connectivity** パラメータを指定します。

3. **show hostaction backup status** コマンドを使用して、過去 5 つのバックアップイメージのステータスとそれらの動作ステータスを表示します。

また、Cisco SD-WAN Manager **[Monitor]** > **[Logs]** > **[Events]** ページで利用可能な通知からバックアップイメージを表示することもできます。



- (注) Cisco vManage リリース 20.6.1 以前のリリースでは、Cisco SD-WAN Manager の **[Monitor]** > **[Events]** ページで利用可能な通知からバックアップイメージを表示できます。

4. CSP デバイスで **show hostaction restore-status** コマンドを使用して、復元プロセス全体と、システム、イメージとフレーバー、VM などの各コンポーネントのステータスを表示します。
5. ステータスを表示した後でエラーを修正するには、デバイスの工場出荷時のデフォルトへのリセットを実行します。



- (注) 工場出荷時のデフォルトにリセットすると、デバイスがデフォルト構成に設定されます。したがって、交換用デバイスで手順 1 ~ 4 の復元操作を実行する前に、復元操作のすべての前提条件が満たされていることを確認してください。

CSP デバイスで復元操作を構成する方法の詳細については、「[Backup and Restore NFVIS and VM Configurations](#)」を参照してください。

クラスタアクティベーションの進行状況

表 4: 機能の履歴

機能名	リリース情報	説明
クラスタのアクティベーションの進行状況を監視する	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能は、各ステップでクラスタのアクティブ化の進行状況を表示し、プロセス中に発生する可能性のある障害を示します。クラスタをアクティブ化するプロセスには約30分以上かかります。Cisco SD-WAN Manager タスクビューウィンドウを使用して進行状況をモニターし、 [Monitoring] ページからイベントをモニターできます。

クラスタのアクティブ化後にクラスタのアクティブ化ステータスを確認するには、タスクビューウィンドウで進行状況を表示します。



(注) Cisco vManage リリース 20.7.1 以前のリリースでは、Cisco Colo Manager が起動し、アクティブ化の進行状況が CLOUD ONRAMP タスクの一部として報告されます。このタスクは、Cisco Colo Manager の起動およびアクティブ化シーケンスの7つのステップを表示し、シーケンスが正常に完了したかどうかを示します。プッシュ機能テンプレート構成タスクは、RBAC 設定構成プッシュのステータスを表示します。

Cisco vManage リリース 20.8.1 では、Cisco SD-WAN Manager がターゲット CSP デバイスから Cisco Colo Manager Healthy を受信すると、CLOUD ONRAMP タスクが完了します。プッシュ機能テンプレート構成タスクは、Cisco Colo Manager の起動およびアクティブ化シーケンスの7つのステップを表示し、シーケンスが正常に完了したかどうか、および RBAC 設定構成プッシュのステータスを示します。

図 2: クラスタのアクティブ化 (Cisco vManage リリース 20.7.1 以前)

Status	Device IP	Message	Start Time
Success	192.168.168.241	CCM Bring up and Activation	19 Feb 2020 4:53:37 PM PST
<pre>[19-Feb-2020 16:53:38 PST] CCM : 192.168.168.241 bring up is In-Progress [19-Feb-2020 16:53:41 PST] Successfully received notification with CCM_STARTING State. Will wait for Healthy notification before sending device list [19-Feb-2020 16:54:47 PST] Successfully received notification with CCM_HEALTHY State. Will stop listening to notification [19-Feb-2020 16:54:47 PST] CCM : 192.168.168.241 bring up succeeded on CSP : 209.165.201.17 [19-Feb-2020 16:56:57 PST] CCM : 192.168.168.241 activation is In-Progress [19-Feb-2020 16:56:58 PST] Successfully received notification with INPROGRESS State from 209.165.201.17 [19-Feb-2020 16:57:09 PST] Successfully received notification with INPROGRESS State from 209.165.201.17 [19-Feb-2020 16:57:35 PST] Successfully received notification with INPROGRESS State from 209.165.201.17 [19-Feb-2020 16:58:10 PST] Successfully received notification with INPROGRESS State from 209.165.201.17 [19-Feb-2020 17:00:10 PST] Successfully received notification with INPROGRESS State from 209.165.201.17 [19-Feb-2020 17:00:15 PST] Successfully received notification with INPROGRESS State from 209.165.201.17 [19-Feb-2020 17:00:15 PST] Successfully received notification with SUCCESS State from 209.165.201.17 [19-Feb-2020 17:00:31 PST] CCM : 192.168.168.241 activation process succeeded</pre>			

図 3: CLOUD ONRAMP Cisco Colo Manager タスク (Cisco vManage リリース 20.8.1 以降)

Status	Chassis Number	Message	Start Time	System IP
Success	192.168.65.174	CCM Bring up and Activation	20 Apr 2022 2:22:56 PM PDT	192.168.65.174
<pre>[20-Apr-2022 21:22:56 UTC] CCM : 192.168.65.174 bring up is In-Progress [20-Apr-2022 21:23:18 UTC] Successfully received notification with CCM_STARTING State. Will wait for Healthy notification before sending device list [20-Apr-2022 21:24:17 UTC] Successfully received notification with CCM_HEALTHY State. Will stop listening to notification [20-Apr-2022 21:24:18 UTC] CCM : 192.168.65.174 bring up succeeded on CSP : 172.26.255.234 [20-Apr-2022 21:24:18 UTC] Post CCM 192.168.65.174 bring up, CCM Activation is in progress with PULL config</pre>				

図 4: プッシュ機能テンプレート構成タスク (Cisco vManage リリース 20.8.1 以降)

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Template successfully attache...	ccm-nExpress_cluster	CCM	ccm-nExpress_cluster	172.16.255.201	--	172.16.255.22
<pre>[2-Apr-2022 3:24:47 UTC] Device: Step 6 of 7: Both switch interfaces are up [2-Apr-2022 3:25:01 UTC] Device: Devices onboard successfully for tenant0, state: Step 7 of 7: Devices done onboarding Device list : switch1 : 10.0.5.152 (C9500-4BY-CAT2324L2G9), switch2 : 10.0.5.151 (C9500-4BY-CAT2324L2H3) [2-Apr-2022 3:25:01 UTC] Device: After devices onboard successfully, CCM will apply remaining cluster settings. [2-Apr-2022 3:25:01 UTC] Device: Loading config in CCM [2-Apr-2022 3:25:02 UTC] Device: Received configuration from vManage [2-Apr-2022 3:25:27 UTC] Device: Successfully loaded config for tenant0 [2-Apr-2022 3:25:27 UTC] Template successfully attached to device</pre>							

次の検証手順を実行します。

1. クラスタの状態を表示して状態を変更するには、以下の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Cloud OnRamp for Colocation]** を選択します。「PENDING」状態になったクラスタについては、[...] をクリックし、**[Sync]** を選択します。このアクションは、クラスタを「ACTIVE」状態に戻します。

2. クラスタが「ACTIVE」状態に戻ったかどうかを確認するには、クラスタの正常なアクティブ化を表示します。
2. CSP デバイスに存在するサービスグループを表示するには、Cisco SD-WAN Manager メニューから **[Monitor]** > **[Devices]** > **[Colocation Cluster]** を選択します。

Cisco vManage リリース 20.6.1 以前：CSP デバイスに存在するサービスグループを表示するには、Cisco SD-WAN Manager メニューから **[Monitor]** > **[Network]** > **[Colocation Clusters]** を選択します。

クラスタを選択してから、CSP デバイスを選択します。他の CSP デバイスを選択して表示できます。
3. クラスタが CSP デバイスからアクティブ化されているかどうかを確認するには、以下の手順を実行します。
 1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
 2. すべての CSP デバイスのデバイスステータスを表示し、それらが Cisco SD-WAN Manager と同期していることを確認します。
 3. CSP デバイスの状態を表示し、証明書が CSP デバイスにインストールされていることを確認します。



- (注) OTP による CSP のアクティブ化後、5 分以上 CSP デバイスの状態に「cert installed」と表示されない場合は、 を参照してください。

クラスタが CSP デバイスからアクティブ化された後、Cisco Colo Manager は、Cisco NFVIS ホストでクラスタアクティブ化タスクを実行します。

4. CSP デバイスで Cisco Colo Manager が有効になっているかどうかを表示するには、以下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。

Cisco vManage リリース 20.6.1 以前：Cisco SD-WAN Manager のメニューから **[モニター (Monitor)]** > **[ネットワーク (Network)]** の順に選択します。
 2. **[Colocation Cluster]** をクリックします。

Cisco vManage リリース 20.6.1 以前：**[Colocation Clusters]** をクリックします。

特定の CSP デバイスに対して Cisco Colo Manager が有効になっているかどうかを表示します。
5. Cisco Colo Manager の正常性をモニターするには、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。

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

2. [Colocation Cluster] をクリックします。

Cisco vManage リリース 20.6.1 以前：[Colocation Clusters] をクリックします。

目的の CSP デバイスで Cisco Colo Manager が有効になっているかどうかを表示します。

3. Cisco Colo Manager が有効な CSP デバイスの場合は、CSP デバイスをクリックします。
4. Cisco Colo Manager の正常性を表示するには、[Colo Manager] をクリックします。

Cisco Colo Manager のステータスが "STARTING" の後に "HEALTHY" に変わらない場合は、『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Troubleshoot Cisco Colo Manager Issues」のトピックを参照してください。

Cisco Colo Manager のステータスは "STARTING" の後に "HEALTHY" に変わったが、スイッチの設定がすでに完了した後、Cisco Colo Manager のステータスが 20 分以上にわたって IN-PROGRESS と表示される場合は、『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Switch devices are not calling home to PNP or Cisco Colo Manager」のトピックを参照してください。

クラスタの表示

クラスタ構成を表示するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager メニューから、[Configuration] > [Cloud OnRamp for Colocation] を選択します。

ステップ 2 目的のクラスタの [...] をクリックし、[View] を選択します。

[Cluster] ウィンドウには、クラスタ内のスイッチデバイスと CSP デバイスが表示され、構成されているクラスタ設定が表示されます。

クラスタのグローバルパラメータ、スイッチデバイスおよび CSP デバイスの構成のみを表示できます。

ステップ 3 [Cancel] をクリックし、[Cluster] ウィンドウに戻ります。

クラスタの編集

グローバルパラメータなどの既存のクラスタ構成を変更するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Colocation] を選択します

ステップ2 目的のクラスタの [...] をクリックし、[Edit] を選択します。

[Cluster] ウィンドウには、クラスタ内のスイッチデバイスと CSP デバイスが表示され、構成されているクラスタ設定が表示されます。

ステップ3 クラスタ設計ウィンドウでは、いくつかのグローバルパラメータを変更できます。クラスタがアクティブ状態か非アクティブ状態かに基づいて、クラスタで次の操作を実行できます。

1. 非アクティブ状態：

- すべてのグローバルパラメータとリソースプールパラメータを編集します。
- CSP デバイスをさらに追加します（最大 8 つ）。
- スイッチまたは CSP デバイスの名前またはシリアル番号を編集することはできません。代わりに、CSP またはスイッチを削除し、別の名前とシリアル番号を持つ別のスイッチまたは CSP を追加します。
- クラスタ構成全体を削除します。

2. アクティブ状態：

- リソースプールパラメータを除くすべてのグローバルパラメータを編集します。
(注) クラスタがアクティブなときは、リソースプールパラメータを変更できません。ただし、リソースプールパラメータを変更する唯一のオプションは、クラスタを削除し、正しいリソースプールパラメータを使用してクラスタを再作成することです。
- スイッチまたは CSP デバイスの名前またはシリアル番号を編集することはできません。
- アクティブ状態のクラスタは削除できません。
- CSP デバイスをさらに追加します（最大 8 つ）。

ステップ4 [Save Cluster] をクリックします。

CSP デバイスのクラスタへの追加

Cisco SD-WAN Manager を使用して、CSP デバイスを追加および設定できます。

始める前に

使用する Cisco NFVIS バージョンがクラスタ内のすべての CSP デバイスと同じであることを確認してください。

手順

ステップ1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Colocation] を選択します

ステップ 2 目的のクラスタの [...] をクリックし、[Add/Delete CSP] を選択します。

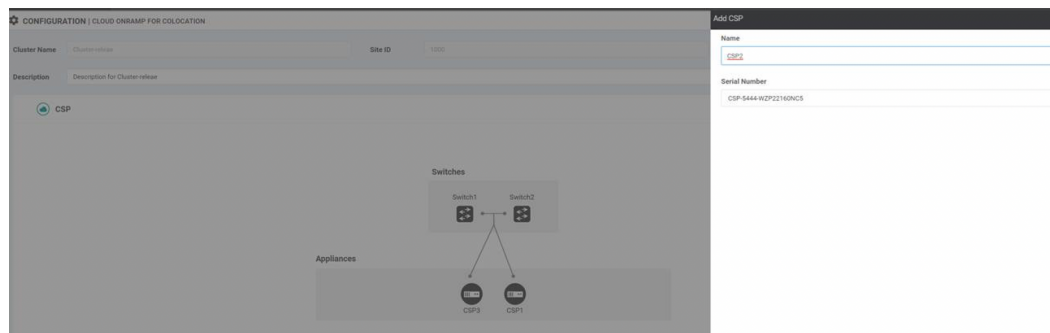
ステップ 3 CSP デバイスを追加するには、[+ Add CSP] をクリックします。[Add CSP] ダイアログボックスが表示されます。名前を入力し、CSP デバイスのシリアル番号を選択します。[Save] をクリックします。

ステップ 4 CSP デバイスを構成するには、CSP ボックスの CSP アイコンをクリックします。[Edit CSP] ダイアログボックスが表示されます。名前を入力し、CSP デバイスのシリアル番号を選択します。[Save] をクリックします。

名前には、128 文字の英数字を含めることができます。

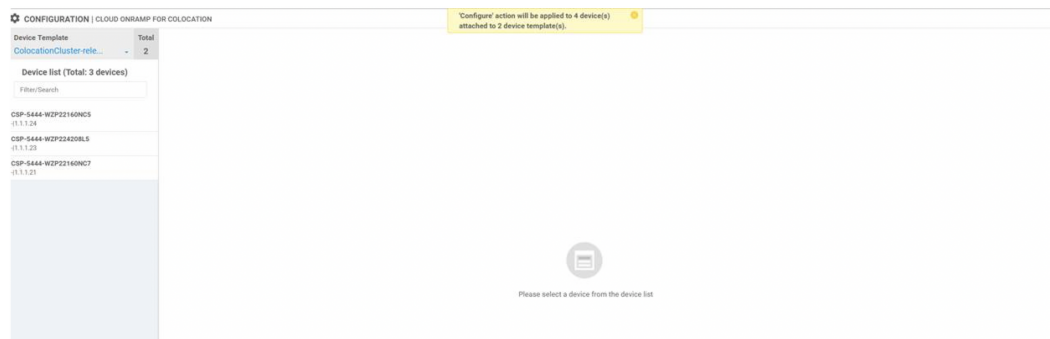
(注) CSP デバイスを起動するには、デバイスの OTP を設定してください。

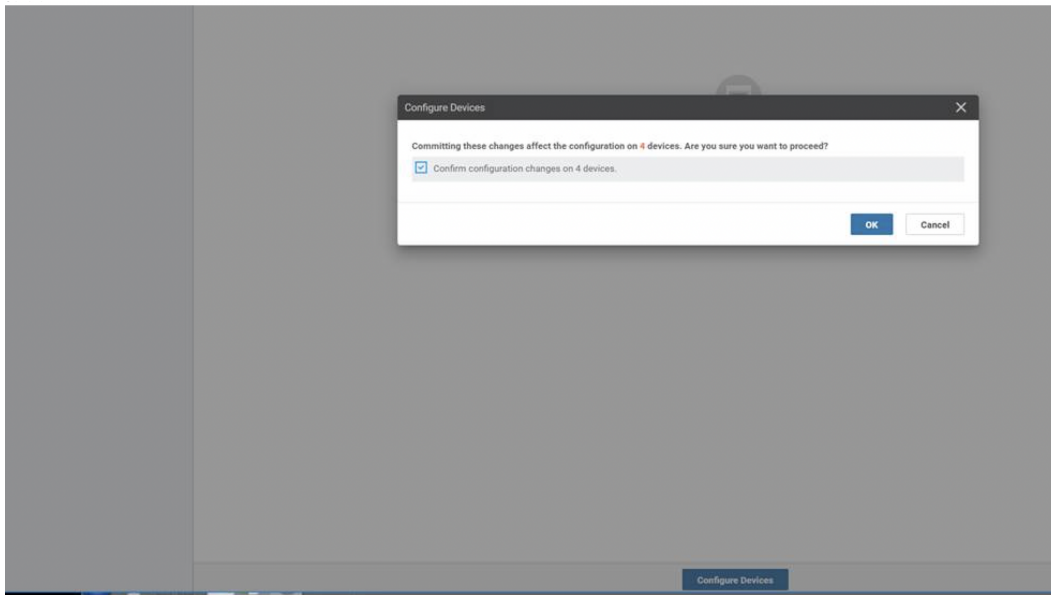
図 5: CSP デバイスの追加



ステップ 5 [Save] をクリックします。

ステップ 6 保存後、次の図に示すように、画面上の構成手順を実行します。





ステップ 7 CSP デバイスが追加されているかどうかを確認するには、実行中のすべてのタスクのリストを表示する [Task View] ウィンドウを使用します。

クラスタからの CSP デバイスの削除

Cisco SD-WAN Manager を使用して CSP デバイスを削除できます。

手順

- ステップ 1** Cisco SD-WAN Manager のメニューから、[**Configuration**] > [**Cloud OnRamp for Colocation**] を選択します
- ステップ 2** 目的のクラスタの [...] をクリックし、[**Add/Delete CSP**] を選択します。
- ステップ 3** CSP デバイスを削除するには、[**Appliances**] ボックスから [**CSP**] アイコンをクリックします。
- ステップ 4** [**Delete**] をクリックします。
- ステップ 5** [**Save**] をクリックします。
- ステップ 6** 次の図に示すように、画面上の指示に従って削除を続行します。

The screenshot shows the Cisco Colo Manager interface. At the top, there are two device entries:

- CSP-5444-WZP22160NCS (1.1.24)
- CSP-5444-WZP22420RLS (1.1.23)

Below this is a large empty area with a central icon and the text "Please select a device from the device list".

At the bottom, there is a "Push Feature Template Configuration" section with a "Validation Success" status. It shows a table of tasks:

Task	Status	Message	Cluster Number	Device Model	Hostname	System IP	Site ID	vManage IP
Done - Success	Done	Push Feature Template Config.	CSP-5444-WZP22160NCS	CSP-5444	CSP2	1.1.24	1000	1.1.1.2
Done - Scheduled	Scheduled	Device needs to install some apps. C...	CSP-5444-WZP22420RLS	CSP-5444	CSP3	1.1.23	1000	1.1.1.2
Done - Scheduled	Scheduled	Device is offline. Configuration templ...	ccm	ccm	ccm-cluster-release	1.1.20	-	1.1.1.2

Below the table, there is a log of events for the "Done - Scheduled" task, including messages like "Configuring device with Feature template: ColocationCluster-release", "Generating configuration from template", "Checking and creating device in vmanage", "Device is online", "Updating device configuration in vmanage", and "Device needs app install".

ステップ7 CSP デバイスを工場出荷時のデフォルト設定にリセットします。

ステップ8 無効な CSP デバイスをデコミッションするには、Cisco SD-WAN Manager のメニューから **[Configuration] > [Devices]** を選択します。

ステップ9 非アクティブ化されたクラスタにある CSP デバイスについては、[...] をクリックし、**[Decommission WAN Edge]** を選択します。

このアクションにより、デバイスに新しいトークンが提供されます。

削除された CSP デバイスに HA サービスチェーンが展開されている場合、対応する HA サービスチェーンは、HA インスタンスをホストする CSP デバイスから削除されます。

Cisco Colo Manager がある CSP の削除

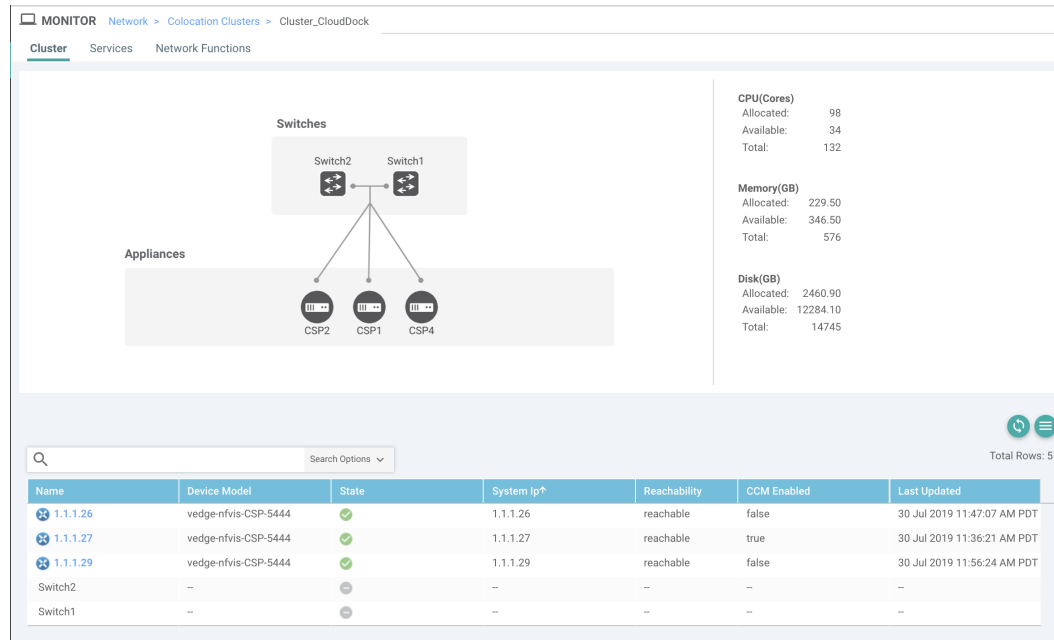
手順

ステップ1 Cisco Colo Manager をホストする CSP デバイスを特定します。

ステップ2 CSP デバイスで **[CCM Enabled]** が true であり、この CSP デバイスを削除することにした場合は、そのデバイスで [...] をクリックし、**[Add/Delete CSP]** を選択します。

[Monitor] ウィンドウから、Cisco Colo Manager が有効になっているかどうかを確認できます。次の図は、Cisco Colo Manager ステータスを表示できる場所を示しています。

図 6: Cisco Colo Manager を使用する CSP デバイス



クラスタから削除することを選択した CSP デバイスでサービスチェーンのモニタリングサービスと Cisco Colo Manager が実行されている場合は、クラスタの [Sync] をクリックしてください。同期ボタンをクリックすると、別の CSP デバイスでサービスチェーンのヘルスモニタリングサービスが開始され、既存のサービスチェーンのヘルスモニタリングが続行されます。

別の CSP デバイスで Cisco Colo Manager インスタンスを起動できるように、Cisco SD-WAN Manager にクラスタのすべての CSP デバイスへの制御接続があることを確認します。

- (注) Cisco vManage リリース 20.8.1 以前のリリースでは、Cisco Colo Manager インスタンスをホストしている CSP デバイスを削除した場合、CSP デバイスを追加して、1 つ以上の CSP デバイスで Cisco Colo Manager インスタンスを起動する必要があります。

Cisco Colo Manager がある CSP デバイスを削除すると、Cisco Colo Manager インスタンスはクラスタ上の別の CSP デバイスで開始されます。



- (注) サービスチェーンのモニタリングは、残りの CSP デバイスのいずれかで Cisco Colo Manager インスタンスが開始されなくなるまで無効になります。

RMA 後の Cisco CSP デバイスの交換

手順の概要

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Colocation] を選択します
2. 目的のクラスタの [...] をクリックし、[RMA] を選択します。
3. [RMA] ダイアログボックスで次の操作を行います。

手順の詳細

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Colocation] を選択します

ステップ 2 目的のクラスタの [...] をクリックし、[RMA] を選択します。

ステップ 3 [RMA] ダイアログボックスで次の操作を行います。

- a) アプライアンスの選択：交換する CSP デバイスを選択します。

特定のコロケーションクラスタ内のすべての CSP デバイスは、CSP Name-<Serial Number> の形式で表示されます。

- b) ドロップダウンリストから新しい CSP デバイスのシリアル番号を選択します。
c) [Save] をクリックします。

保存後、構成を表示できます。

Cisco CSP デバイスの返却

表 5: 機能の履歴

機能名	リリース情報	説明
Cisco CSP デバイスの RMA サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能を使用すると、デバイスのバックアップコピーを作成し、交換用デバイスを交換前の状態に復元することで、障害のある CSP デバイスを交換できます。HA モードで実行されている VM は、デバイスの交換中に中断されることなくトラフィックの継続的なフローで動作します。

バックアップコピーを作成し、NFVIS 構成と VM を復元できるようになりました。

考慮すべき点

- ネットワーク ファイルストレージ (NFS) サーバーを使用して、CSP デバイスの定期的なバックアップコピーを作成できます。
- バックアップ操作に外部 NFS サーバーを使用している場合は、NFS ディレクトリを定期的に保守およびクリーニングしてください。このメンテナンスにより、NFS サーバーに受信バックアップパッケージ用の十分なスペースが確保されます。
- NFS サーバーを使用しない場合は、Cisco SD-WAN Manager を使用してバックアップサーバー設定を構成しないでください。ただし、バックアップサーバー設定を構成していない場合、交換用デバイスを復元することはできません。CSP の削除を使用して、障害のあるデバイスを削除し、新しい CSP デバイスを追加してから、追加された CSP デバイスへのサービスチェーンのプロビジョニングを開始できます。

Cisco CSP デバイスの RMA プロセス

Return of Materials (RMA) プロセスは、次の順序で実行してください。

1. Cisco SD-WAN Manager を使用して、クラスタ内のすべての CSP デバイスのバックアップコピーを作成します。『[バックアップサーバー設定 \(20 ページ\)](#)』を参照してください。



(注) CSP デバイスの交換時、Cisco SD-WAN Manager を使用してクラスタを作成するときに NFS サーバーにデバイスのバックアップコピーを作成します。クラスタを起動する場合、または既存のクラスタを編集する場合は、次のいずれかを実行します。

- コロケーションクラスタの起動：クラスタの作成時およびアクティブ化時に、NFS ストレージサーバーとバックアップ間隔に関する情報を指定します。CSP デバイスでバックアップタスクが失敗した場合、デバイスはエラーを返しますが、クラスタのアクティブ化は続行されます。障害に対処した後でクラスタを更新し、クラスタが正常にアクティブ化されるまで待機してください。
 - コロケーションクラスタの編集：既存のアクティブクラスタの場合、クラスタを編集し、NFS ストレージサーバーとバックアップ間隔に関する情報を指定します。
2. シスコテクニカルサポートに連絡して、交換用の CSP デバイスを入手してください。CSP デバイスの交換の詳細については、『[Cisco Cloud Services Platform 5000 Hardware Installation Guide](#)』を参照してください。
 3. 交換用 Cisco CSP デバイスを Cisco Catalyst 9500 スイッチに再配線して、障害のあるデバイスの配線を交換用デバイスに移動します。
 4. 交換用デバイスで実行されている Cisco CSP ISO イメージが、障害のあるデバイスで実行されていたものと同じであることを確認します。
 5. CLI を使用して交換用デバイスを復元します。

CSP デバイスのバックアップと復元の前提条件と制限事項

前提条件

バックアップ操作

- Cisco SD-WAN Manager を使用してバックアップサーバー設定を構成する前に、CSP デバイスから NFS サーバーへの接続を確立する必要があります。
- NFS サーバー上のバックアップディレクトリには、書き込み権限が必要です。
- 外部 NFS サーバーは、利用可能で、到達可能であり、メンテナンスされている必要があります。外部 NFS サーバーのメンテナンスでは、利用可能なストレージスペースとネットワークの到達可能性を定期的にチェックする必要があります。
- バックアップ操作のスケジュールは、CSP デバイスのローカルの日時と同期する必要があります。

復元操作

- 交換用デバイスには、障害のあるデバイスと同じリソースが必要です。これらのリソースは、障害のある CSP デバイスとしての Cisco NFVIS イメージバージョン、CPU、メモリ、およびストレージです。
- 交換用デバイスとスイッチポート間の接続は、障害のあるデバイスおよびスイッチと同じである必要があります。
- 交換用デバイスの PNIC 配線は、Catalyst 9500 スイッチの障害のあるデバイスと一致する必要があります。

次に例を示します。

障害のあるデバイスのスロット 1/ポート 1 (eth1-1) がスイッチ 1 およびポート 1/0/1 に接続されている場合は、交換用デバイスのスロット 1/ポート 1 (eth1-1) を、スイッチ 1 およびポート 1/0/1 などの同じスイッチポートに接続します。

- 交換用デバイスのオンボーディングは、CSP デバイスの PnP プロセスを使用して完了する必要があります。
- 復元操作中にバックアップアクセスが失われるのを防ぐには、NFS サーバーをマウントしてバックアップパッケージにアクセスするための構成が、障害のあるデバイスの構成と一致している必要があります。

NFS マウントの場所と構成はすべての CSP デバイスで同じであるため、他の CSP デバイスから構成情報を表示できます。正常な CSP デバイスで実行されているアクティブな構成を表示するには、**show running-config** コマンドを使用します。復元操作中にマウントポイントを作成するときに、このアクティブな構成情報を使用します。

次に例を示します。

```
nfvis# show running-config mount
mount nfs-mount storage nfsfs/
storagetype                nfs
```

```
storage_space_total_gb 123.0
server_ip               172.19.199.199
server_path             /data/colobackup/
!
```

- 交換デバイスの復元後に、OTPプロセスを使用した Cisco SD-WAN 制御コンポーネントによる交換デバイスの認証を完了する必要があります。



(注) **request activate chassis-number chassis-serial-number token token-number** コマンドを使用して、Cisco NFVIS にログインしてデバイスを認証します。

- 交換用デバイスには、障害のあるデバイスの構成以外の構成を含めないでください。

制約事項

バックアップ操作

- CSP デバイスのアップグレード中に、定期的なバックアップ操作は開始されません。
- NFS フォルダパスが NFS サーバーで使用できない場合、バックアップ操作は開始されません。
- 特定の時間に実行できるバックアップ操作は 1 つだけです。
- NFS サーバーで使用可能なディスク容量が VM エクスポートサイズと tar.gz VM パッケージの合計サイズより小さい場合、バックアップ操作は失敗します。
- バックアップデバイス情報は、交換用の CSP デバイスでのみ復元でき、すでにクラスタの一部である既存のデバイスでは復元できません。
- NFS マウント構成は、CSP デバイス用に構成した後は更新できません。更新するには、NFS 構成を削除し、更新された構成を NFS サーバーに再適用して、バックアップスケジュールを再構成します。バックアップ操作が進行中でないときに、この更新を実行します。

復元操作

- 特定の時間に実行できる復元操作は 1 つだけです。
- バックアップファイルが NFS サーバーに存在しない場合、復元操作は開始されません。
- クラスタをシングルテナントモードからマルチテナントモードに変換する場合、およびその逆の場合、復元操作はサポートされません。

クラスタの削除

Cisco SD-WAN Manager からクラスタ全体をデコミッションするには、次の手順を実行します。

手順

-
- ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Certificates]** の順に選択します。
- ステップ 2** 削除する CSP デバイスの **[Validate]** 列を確認し、**[Invalid]** をクリックします。
- ステップ 3** 無効なデバイスについては、**[Send to Controllers]** をクリックします。
- ステップ 4** Cisco SD-WAN Manager メニューから、**[Configuration] > [Cloud OnRamp for Colocation]** を選択します。
- ステップ 5** 無効な CSP デバイスがあるクラスタの場合は、**[...]** をクリックし、**[Deactivate]** を選択します。
- クラスタが 1 つ以上のサービスグループに接続されている場合、CSP デバイスで実行されている VM をホストしているサービスチェーンと、クラスタの削除を続行できるかどうかを示すメッセージが表示されます。ただし、クラスタの削除を確認しても、この CSP デバイスでホストされているサービスグループを切り離さずにクラスタを削除することはできません。クラスタがどのサービスグループにも関連付けられていない場合は、クラスタの削除に関する確認を求めるメッセージが表示されます。
- (注) 必要に応じて、クラスタを削除するか、非アクティブ状態のままにすることができません。
- ステップ 6** クラスタを削除するには、**[Delete]** を選択します。
- ステップ 7** クラスタを削除しない場合は、**[Cancel]** をクリックします。
- ステップ 8** 無効なデバイスをデコミッションするには、Cisco SD-WAN Manager のメニューから **[Configuration] > [Devices]** を選択します。
- ステップ 9** 非アクティブ化されたクラスタにあるデバイスについては、**[...]** をクリックし、**[Decommission WAN Edge]** を選択します。
- このアクションにより、デバイスに新しいトークンが提供されます。
- ステップ 10** 次のコマンドを使用して、デバイスを工場出荷時のデフォルトにリセットします。
- factory-default-reset all**
- ステップ 11** ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123 #** を使用して、Cisco NFVIS にログインします。
- ステップ 12** スイッチ構成をリセットし、スイッチをリブートします。『[Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide](#)』の「[Troubleshooting](#)」の章を参照してください。
-

クラスタの再アクティブ化

新しい CSP デバイスを追加する場合、または CSP デバイスが RMA プロセスの対象となる場合は、次の手順を実行します。

手順

-
- ステップ 1** 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 2** 非アクティブ化されたクラスタにあるデバイスを見つけます。
- ステップ 3** デバイス用に Cisco SD-WAN Manager から新しいトークンを取得します。
- ステップ 4** ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123#** を使用して、Cisco NFVIS にログインします。
- ステップ 5** **request activate chassis-number chassis-serial-number token token-number** コマンドを使用します。
- ステップ 6** Cisco SD-WAN Manager を使用して、コロケーションデバイスを設定し、クラスタをアクティブ化します。
『[クラスタの作成とアクティブ化 \(10 ページ\)](#)』を参照してください。
クラスタを削除した場合は、再作成してからアクティブ化します。
- ステップ 7** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Certificates]** の順に選択します。コロケーションデバイスのステータスを見つけて確認します。
- ステップ 8** 有効にする必要がある目的のデバイスの **[Valid]** をクリックします。
- ステップ 9** 有効なデバイスについては、**[Send to Controllers]** をクリックします。
-

サービス グループの管理

サービスグループは、1 つ以上のサービスチェーンで構成されます。Cisco SD-WAN Manager を使用してサービスグループを設定できます。サービスチェーンはネットワークサービスの構造であり、リンクされたネットワーク機能のセットで構成されます。

サービスグループでのサービスチェーンの作成

サービスグループは、1 つ以上のサービスチェーンで構成されます。

表 6: 機能の履歴

機能名	リリース情報	機能説明
サービスチェーンの正常性の監視	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能により、サービスチェーンデータパスの定期的なチェックを設定し、全体的なステータスをレポートできます。サービスチェーンのヘルスマonitoringを有効にするには、クラスタ内のすべての CSP デバイスに NFVIS バージョン 3.12.1 以降をインストールする必要があります。

手順

Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します

- a) **[Service Group]** をクリックし、**[Create Service Group]** をクリックします。サービスグループの名前、説明、およびコロケーショングループを入力します。

サービスグループ名には、128 文字の英数字を含めることができます。

サービスグループの説明には、2048 文字の英数字を含めることができます。

マルチテナントクラスタの場合、ドロップダウンリストからコロケーショングループまたはテナントを選択します。シングルテナントクラスタの場合、コロケーショングループ **[admin]** がデフォルトで選択されます。

- b) **[Add Service Chain]** をクリックします。
 c) **[Add Service Chain]** ダイアログボックスで、次の情報を入力します。

表 7: サービスチェーン情報の追加

フィールド	説明
Name	サービスチェーン名には、128 文字の英数字を含めることができます。
Description	サービスチェーンの説明には、2048 文字の英数字を含めることができます。
Bandwidth	サービスチェーンの帯域幅は Mbps 単位です。デフォルトの帯域幅は 10 Mbps で、5 Gbps の最大帯域幅を設定できます。
Input Handoff VLANs and Output Handoff VLANs	入力 VLAN ハンドオフおよび出力 VLAN ハンドオフは、カンマ区切りの値 (10、20)、または 10 ~ 20 の範囲にすることができます。

フィールド	説明
Monitoring	<p>サービスチェーンのヘルスマonitoringを有効または無効にできるトグルボタン。サービスチェーンのヘルスマonitoringは、サービスチェーンデータパスの正常性をチェックし、サービスチェーン全体の正常性ステータスを報告する定期的なmonitoringサービスです。デフォルトでは、monitoringサービスは無効になっています。</p> <p>SCHM（サービスチェーンヘルスマonitoringサービス）などのサブインターフェイスを持つサービスチェーンは、サブインターフェイス VLAN リストの最初の VLAN を含むサービスチェーンのみをmonitoringできます。</p> <p>サービスチェーンのmonitoringは、エンドツーエンドの接続に基づいてステータスを報告します。したがって、より良い結果を得るために、Cisco Catalyst SD-WAN サービスチェーンに注意しながら、ルーティングとリターントラフィックパスを処理するようにしてください。</p> <p>(注)</p> <ul style="list-style-type: none"> 入力および出力ハンドオフサブネットからの入力および出力monitoring IP アドレスが指定されていることを確認します。ただし、最初と最後の VNF デバイスが VPN で終端されている場合、入力および出力monitoring IP アドレスを指定する必要はありません。 <p>たとえば、ネットワーク機能が VPN 終端されていない場合、入力monitoring IP はインバウンドサブネット 192.0.2.0/24 からの 192.0.2.1/24 である可能性があります。インバウンドサブネットは最初のネットワーク機能に接続し、出力monitoring IP はアウトバウンドサブネットからの 203.0.113.11/24、サービスチェーンの最後のネットワーク機能の 203.0.113.0/24 にすることができます。</p> <ul style="list-style-type: none"> サービスチェーンの最初または最後の VNF ファイアウォールがトランスペアレントモードの場合、これらのサービスチェーンをmonitoringすることはできません。
Service Chain	<p>サービスチェーンのドロップダウンリストから選択するトポロジです。サービスチェーントポロジの場合、ルータ - ファイアウォール - ルータ、ファイアウォール、ファイアウォール - ルータなど、検証済みのサービスチェーンのいずれかを選択できます。『Cisco Catalyst SD-WAN Cloud OnRamp Colocation Solution Guide』の「Validated Service Chains」のトピックを参照してください。カスタマイズされたサービスチェーンを作成することもできます。カスタムサービスチェーンの作成 (48 ページ) を参照してください。</p>

d) [Add Service Chain] ダイアログボックスで、[Add] をクリックします。

サービスチェーンの構成情報に基づいて、すべてのサービスチェーンと VNF を含むサービスグループのグラフィック表現が、デザインビューウィンドウに自動的に表示されます。VNF または PNF は、仮想および物理ネットワーク機能の周囲に「V」または「P」が付いて表示されます。各サービスグループ内に構成されているすべてのサービスチェーンが表示されます。サービスチェーンの横にあるチェックマークは、サービスチェーンの構成が完了していることを示します。

クラスタをアクティブ化したら、CCM が実行されている CSP デバイスを起動するときに、クラスタをサービスグループに接続し、サービスチェーンのモニタリングサービスを有効にします。Cisco SD-WAN Manager は、モニタリングサービスを開始するために同じ CSP デバイスを選択します。モニタリングサービスは、モニタリング間隔を 30 分に設定することにより、すべてのサービスチェーンをラウンドロビン方式で定期的にモニタリングします。『[Cloud OnRamp Colocation クラスタのモニター \(77 ページ\)](#)』を参照してください。

- e) デザインビューウィンドウで、VNF を構成するには、サービスチェーン内の VNF をクリックします。[Configure VNF] ダイアログボックスが表示されます。
- f) 次の情報を使用して VNF を構成し、必要に応じてアクションを実行します。

(注) Cisco vManage リリース 20.7.1 以降では次のフィールドを使用できます。

- Disk Image/Image Package (Select File)
- Disk Image/Image Package (Filter by Tag, Name and Version)
- Scaffold File (Select File)
- Scaffold File (Filter by Tag, Name and Version)

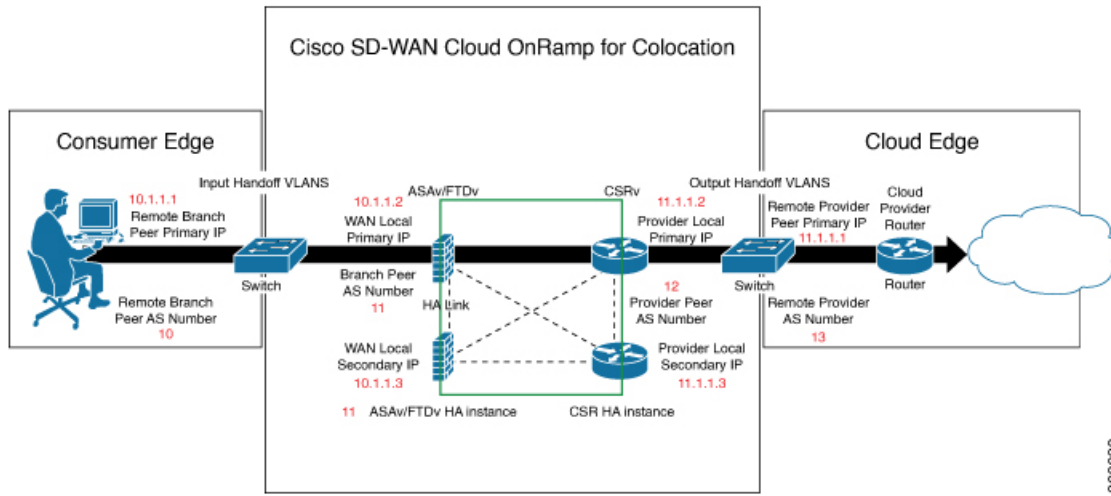
表 8: ルータとファイアウォールの VNF プロパティ

フィールド	説明
Image Package	ルータ、ファイアウォールパッケージを選択します。
Disk Image/Image Package (Select File)	tar.gz パッケージまたは qcow2 イメージファイルを選択します。
Disk Image/Image Package (Filter by Tag, Name and Version)	(オプション) VNF イメージのアップロード時に指定した名前、バージョン、タグに基づいて、イメージまたはパッケージファイルをフィルタリングします。

フィールド	説明
Scaffold File (Select File)	<p>スキヤフォールドファイルを選択します。</p> <p>(注)</p> <ul style="list-style-type: none"> • qcow2 イメージファイルが選択されている場合、このフィールドは必須です。tar.gz パッケージが選択されている場合はオプションです。 • tar.gz パッケージとスキヤフォールドファイルの両方を選択した場合、スキヤフォールドファイルのすべてのイメージプロパティとシステムプロパティは、tar.gz パッケージで指定された Day-0 構成ファイルを含むイメージプロパティとシステムプロパティをオーバーライドします。
Scaffold File (Filter by Tag, Name and Version)	(オプション) VNF イメージのアップロード時に指定した名前、バージョン、タグに基づいて、スキヤフォールドファイルをフィルタリングします。
[Fetch VNF Properties] をクリックします。イメージの利用可能な情報は、[Configure VNF] ダイアログボックスに表示されます。	
Name	VNF イメージ名
CPU	(オプション) VNF に必要な仮想 CPU の数を指定します。デフォルト値は 1 vCPU です。
Memory	(オプション) VNF が使用できる最大プライマリメモリを MB 単位で指定します。デフォルト値は 1024 MB です。
Disk	(オプション) VM に必要なディスクを GB 単位で指定します。デフォルト値は 8 GB です。
入力が必要な、Day-0 からのカスタムトークン化変数を含むダイアログボックスが表示されます。値を指定します。	

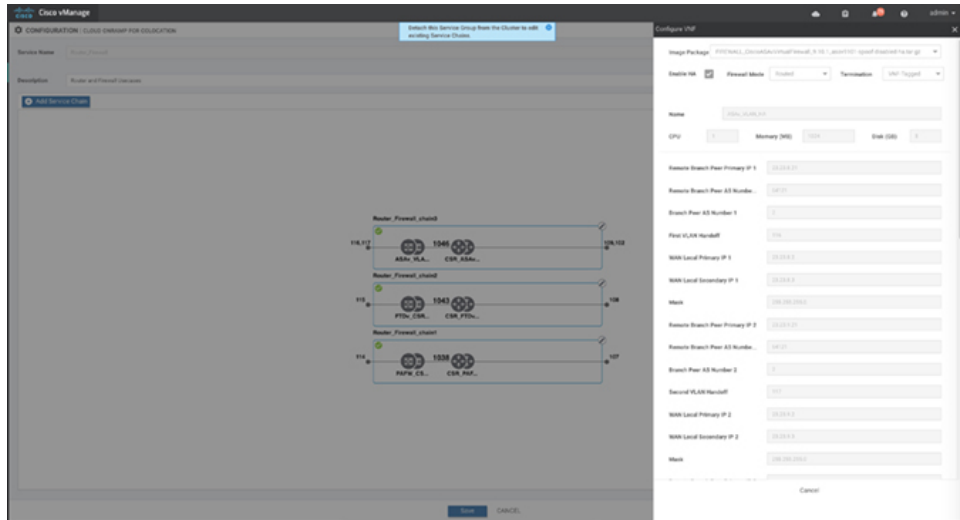
次の図で、緑色のボックス内のすべての IP アドレス、VLAN、および自律システムは、VLAN から生成されたシステム固有の情報、クラスタに提供される IP プールです。この情報は、VM の Day-0 構成に自動的に追加されます。

サービスグループでのサービスチェーンの作成

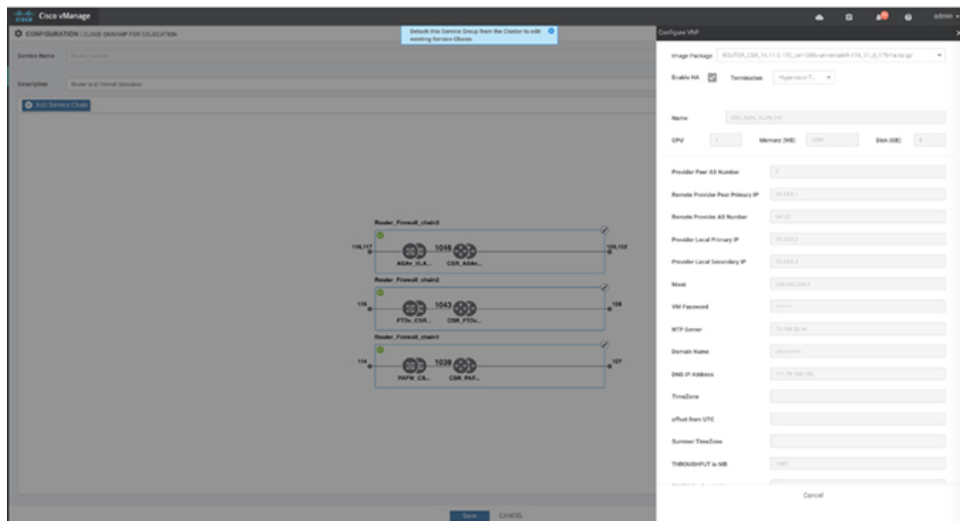


368038

次の図は、Cisco SD-WAN Manager での VNF IP アドレスと自律システム番号の設定例です。



369298



369297

マルチテナントクラスタと共同管理シナリオを使用している場合は、サービスチェーン設計の必要に応じて、次のフィールドと残りのフィールドに値を入力して、Cisco Catalyst SD-WAN VM を設定します。

(注) テナント オーバーレイ ネットワークに参加するには、プロバイダーは次のフィールドに正しい値を指定する必要があります。

フィールド	説明
Serial Number	Cisco Catalyst SD-WAN デバイスの承認済みシリアル番号。サービスプロバイダーは、サービスチェーンを作成する前に、テナントからデバイスのシリアル番号を取得できます。
OTP	Cisco SD-WAN 制御コンポーネントで認証された後に使用できる Cisco Catalyst SD-WAN デバイスの OTP。サービスプロバイダーは、サービスチェーンを作成する前に、テナントから対応するシリアル番号の OTP を取得できます。
Site Id	ブランチ、キャンパス、データセンターなど、Cisco Catalyst SD-WAN デバイスが存在するテナント Cisco Catalyst SD-WAN オーバーレイ ネットワーク ドメイン内のサイトの識別子。サービスプロバイダーは、サービスチェーンを作成する前に、テナントからサイト ID を取得できます。
Tenant ORG Name	証明書署名要求 (CSR) に含まれるテナント組織名。サービスプロバイダーは、サービスチェーンを作成する前に、テナントから組織名を取得できます。
System IP connect to Tenant	テナント オーバーレイ ネットワークに接続するための IP アドレス。サービスプロバイダーは、サービスチェーンを作成する前にテナントから IP アドレスを取得できます。
Tenant vBond IP	テナント Cisco SD-WAN Validator の IP アドレス。サービスプロバイダーは、サービスチェーンを作成する前にテナントから Cisco SD-WAN Validator IP アドレスを取得できます。

サービスチェーンの最初と最後の VM などのエッジ VM の場合、ブランチルータおよびプロバイダールータとピアリングするときに、次のアドレスを指定する必要があります。

表 9: サービスチェーンの最初の VM の VNF オプション

フィールド	必須または任意	説明
Firewall Mode	必須	ルーテッドモードまたはトランスペアレントモードを選択します。 (注) ファイアウォールモードは、ファイアウォール VM にも適用されます。
Enable HA	オプション	VNF の HA モードを有効にします。

フィールド	必須または任意	説明
Termination	必須	<p>次のいずれかのモードを選択します。</p> <ul style="list-style-type: none"> • トランクモードのサブインターフェイスでの L3 モードの選択 <code><type>selection</type> <val help="L3 Mode With Sub-interfaces(Trunked)" display="VNF-Tagged">vlan</val></code> • コンシューマ側からの IPSEC 終端を使用し、プロバイダーゲートウェイに再ルーティングされる L3 モード <code><val help="L3 Mode With IPSEC Termination From Consumer and Routed to Provider GW" display="Tunneled">vpn</val></code> • アクセスモードでの L3 モード (非トランクモード) <code><val help="L3 Mode In Access Mode (Non-Trunked)" display="Hypervisor-Tagged">routed</val></code>

- g) [Configure] をクリックします。サービスチェーンは VNF 構成で構成されます。
- h) 別のサービスチェーンを追加するには、手順 b ~ g を繰り返します。
- i) [Save] をクリックします。

[Service Group] の下のテーブルに新しいサービスグループが表示されます。モニタリングされているサービスチェーンのステータスを表示するには、[Task View] ウィンドウを使用します。このウィンドウには、実行中のすべてのタスクのリストと、成功と失敗の合計数が表示されます。サービスチェーンの正常性ステータスを確認するには、サービスチェーンのヘルスマニタリングが有効になっている CSP デバイスで **show system:system status** コマンドを使用します。

サービスチェーンの QoS

表 10: 機能の履歴

機能名	リリース情報	説明
サービスチェーンの QoS	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能は、レイヤ 2 仮想ローカルエリアネットワーク (VLAN) 識別番号に基づいてネットワークトラフィックを分類します。QoS ポリシーを使用すると、双方向トラフィックにトラフィックポリシングを適用することにより、各サービスチェーンで使用可能な帯域幅を制限できます。双方向トラフィックは、Cisco Catalyst 9500-40X スイッチをコンシューマに接続する入力側とプロバイダーに接続する出力側です。

前提条件

- 共有 VNF および PNF デバイスを持たないサービスチェーンで、サービス品質 (QoS) トラフィックポリシングを使用していることを確認します。



(注) 複数のサービスチェーンで入力 VLAN と出力 VLAN が同じである共有 VNF デバイスを持つサービスチェーンに QoS ポリシーを適用することはできません。

- QoS トラフィックポリシングに次のバージョンのソフトウェアを使用していることを確認してください。

ソフトウェア	リリース
Cisco NFVIS Cloud OnRamp for Colocation	4.1.1 以降
Catalyst 9500-40X	16.12.1 以降

QoS ポリシングポリシーは、次のワークフローに基づいてネットワークトラフィックに適用されます。

1. Cisco SD-WAN Manager は、帯域幅、入力、または出力 VLAN 情報を VNF および PNF デバイスに保存します。帯域幅と VLAN 情報を提供するには、[サービスグループでのサービスチェーンの作成 \(37 ページ\)](#) を参照してください。
2. CCM は、帯域幅、入力、または出力 VLAN 値の情報を Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに保存します。
3. CCM は、VLAN 一致基準に基づいて、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに対応するクラスマップおよびポリシーマップを作成します。
4. CCM は、入力ポートと出力ポートに入力サービスポリシーを適用します。



(注) Cisco vManage リリース 20.7.1 以降、サービスチェーンの QoS トラフィックポリシーは、Cisco Catalyst 9500 スイッチではサポートされていません。

- アクティブクラスタが Cisco vManage リリース 20.7.1 および CSP 4.7.1 にアップグレードされ、アップグレード前にプロビジョニングされたサービスチェーンがある場合、アップグレード中に QoS 設定がスイッチから自動的に削除されます。
- Cisco vManage リリース 20.7.1 で新しいサービスチェーンがプロビジョニングされると、QoS ポリシーはスイッチに設定されません。
- 同様に、Cisco vManage リリース 20.7.1 で作成された新しいクラスタは、スイッチのサービスチェーンの QoS 設定を構成しません。

サービスグループの複製

表 11: 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN Manager のサービスグループの複製	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能を使用すると、同じ設定情報を何度も入力することなく、さまざまな RBAC ユーザーのサービスグループのコピーを作成できます。サービスグループを複製すると、保存されているサービスチェーンテンプレートを利用してサービスチェーンを簡単に作成できます。

サービスチェーンのコピーを複製または作成するときは、次の点に注意してください。

- Cisco SD-WAN Manager は、複製されたサービスグループがクラスタに接続されているかどうかに関係なく、サービスグループのすべての構成情報を複製されたサービスグループにコピーします。
- CSV ファイルを確認し、CSV ファイルのアップロード中に構成情報に一致するサービスグループ名があることを確認します。これを行わないと、サービスグループ名が一致しない場合に CSV ファイルのアップロード中にエラーメッセージが表示される可能性があります。
- サービスグループの設定値の更新されたリストを取得するには、常にサービスグループのデザインビューからサービスグループの構成プロパティをダウンロードします。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud OnRamp for Colocation]** を選択します

ステップ 2 **[Service Group]** をクリックします。

サービスグループの構成ページが表示され、すべてのサービスグループが表示されます。

ステップ 3 目的のサービスグループの **[...]** をクリックし、**[Clone Service Group]** を選択します。

元のサービスグループのクローンがサービスグループのデザインビューに表示されます。次の点に注意してください。

- デフォルトでは、複製されたサービスグループ名と VM 名には、一意の文字列がサフィックスとして付けられます。
- VM 構成を表示するには、サービスチェーン内の VM をクリックします。
- Cisco SD-WAN Manager は、構成が必要なサービスチェーンを、サービスチェーンの編集ボタンの横に **[Unconfigured]** としてマークします。

ステップ 4 必要に応じてサービスグループ名を変更します。サービスグループの説明を入力します。

ステップ 5 サービスチェーンを構成するには、次のいずれかの方法を使用します。

- サービスチェーンの編集ボタンをクリックし、値を入力して、[Save] をクリックします。
- CSV ファイルから設定値をダウンロードし、値を変更してファイルをアップロードし、[Save] をクリックします。CSV ファイルをダウンロード、変更、およびアップロードする方法については、ステップ 6、7、8 を参照してください。

複製されたサービスグループは、サービスグループの構成ページに表示されます。更新されたサービスグループの設定値をダウンロードできるようになりました。

ステップ 6 複製されたサービスグループの設定値をダウンロードするには、次のいずれかを実行します。

(注) CSV ファイルのダウンロードとアップロードは、クラスタに接続されていないサービスグループの作成、編集、および複製のためにサポートされています。

- サービスグループの構成ページで、複製されたサービスグループをクリックし、サービスグループの右側にある [More Actions] をクリックして、[Download Properties (CSV)] を選択します。
- サービスグループのデザインビューで、画面の右上隅にある [Download CSV] をクリックします。

Cisco SD-WAN Manager は、サービスグループのすべての設定値を CSV 形式の Excel ファイルにダウンロードします。CSV ファイルは複数のサービスグループで構成でき、各行は 1 つのサービスグループの設定値を表します。CSV ファイルに行を追加するには、既存の CSV ファイルからサービスグループの設定値をコピーして、このファイルに貼り付けます。

たとえば、各サービスチェーンに 1 つの VM を持つ 2 つのサービスチェーンがある ServiceGroup1_Clone1 は、1 つの行で表されます。

(注) Excel ファイルのサービスチェーンデザインビューでのヘッダーとその表現は次のとおりです。

- sc1/name は、最初のサービスチェーンの名前を表します。
- sc1/vm1/name は、最初のサービスチェーンの最初の VNF の名前を表します。
- sc2/name は、2 番目のサービスチェーンの名前を表します。
- sc2/vm2/name は、2 番目のサービスチェーンの 2 番目の VNF の名前を表します。

ステップ 7 サービスグループの設定値を変更するには、次のいずれかを実行します。

- デザインビューでサービスグループ構成を変更するには、サービスグループ構成ページで複製されたサービスグループをクリックします。

サービスチェーン内の任意の VM をクリックして設定値を変更し、[Save] をクリックします。

- ダウンロードした Excel ファイルを使用してサービスグループ構成を変更するには、Excel ファイルに設定値を手動で入力します。Excel ファイルを CSV 形式で保存します。

ステップ 8 サービスグループのすべての設定値を含む CSV ファイルをアップロードするには、サービスグループ構成ページでサービスグループをクリックし、画面の右隅にある [Upload CSV] をクリックします。

[Browse] をクリックして CSV ファイルを選択し、[Upload] をクリックします。

サービスグループ構成に表示される更新された値を表示できます。

- (注) 同じCSVファイルを使用して、複数のサービスグループの設定値を追加できます。ただし、Cisco SD-WAN Manager を使用して CSV ファイルをアップロードする場合、特定のサービスグループの設定値のみを更新できます。

ステップ 9 CSV ファイルおよび Cisco SD-WAN Manager デザインビューでのサービスグループ構成プロパティの表現を確認するには、サービスグループ構成ページでサービスグループをクリックします。

[Show Mapping Names] をクリックします。

サービスチェーン内のすべての VM の横にテキストが表示されます。Cisco SD-WAN Manager は、このテキストを CSV ファイルの構成プロパティにマッピングした後に表示します。

カスタムサービスチェーンの作成

次の方法でサービスチェーンをカスタマイズできます。

- 追加の VNF を含めるか、他の VNF タイプを追加すること。
- 事前定義されたサービスチェーンの一部ではない新しい VNF シーケンスを作成すること。

手順

ステップ 1 サービスグループとサービスグループ内のサービスチェーンを作成します。『[サービスグループでのサービスチェーンの作成 \(37 ページ\)](#)』を参照してください。

ステップ 2 [Add Service Chain] ダイアログボックスで、サービスチェーン名、説明、帯域幅、入力 VLAN ハンドオフ、出力 VLAN ハンドオフ、サービスチェーンの正常性情報の監視、およびサービスチェーン構成を入力します。[Add] をクリックします。

サービスチェーン構成では、ドロップダウンから [Create Custom] を選択します。デザインビューウィンドウに空のサービスチェーンが表示されます。

ステップ 3 ルータ、ロードバランサ、ファイアウォールなどの VNF を追加するには、VNF アイコンをクリックし、アイコンをサービスグループボックス内の適切な場所にドラッグします。必要なすべての VNF を追加し、VNF サービスチェーンを形成したら、各 VNF を構成します。サービスグループボックスで VNF をクリックします。[Configure VNF] ダイアログボックスが表示されます。次のパラメータを入力します。

- [Disk Image/Image Package] ([Select File]) ドロップダウンリストから、ロードするソフトウェアイメージを選択します。

(注) Cisco vManage リリース 20.7.1 から qcow2 イメージファイルを選択できます。
- qcow2 イメージファイルを選択した場合は、[Scaffold File] ([Select File]) ドロップダウンリストからスキャフォールドファイルを選択します。

(注) このオプションは、Cisco vManage リリース 20.7.1 から入手できます。

- c) 必要に応じて、VNF イメージのアップロード時に指定した名前、バージョン、およびタグに基づいて、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フィルタリングします。
- (注) このオプションは、Cisco vManage リリース 20.7.1 から入手できます。
- d) [Fetch VNF Properties] をクリックします。
- e) [Name] フィールドに、VNF の名前を入力します。
- f) [CPU] フィールドに、VNF に必要な仮想 CPU の数を入力します。
- g) [Memory] フィールドに、VNF に割り当てるメモリの量をメガバイト単位で入力します。
- h) [Disk] フィールドに、VNF に割り当てるストレージのメモリ量をギガバイト単位で入力します。
- i) 必要に応じて、VNF 固有のパラメータを入力します。
- (注) これらの VNF の詳細は、VNF の Day-0 オペレーションに必要なカスタム変数です。
- j) [Configure] をクリックします。
- k) VNF を削除するか、VNF 構成をキャンセルするには、それぞれ [Delete] または [Cancel] をクリックします。

カスタマイズされたサービスチェーンがサービスグループに追加されます。



-
- (注) サービスチェーンで最大 4 つの VNF のみを使用して VNF シーケンスをカスタマイズできません。
-

共有 PNF デバイスによるカスタムサービスチェーン

サポートされている PNF デバイスを追加して、サービスチェーンをカスタマイズできます。



-
- 注意** コロケーションクラスタ間で PNF デバイスを共有しないようにしてください。PNF デバイスは、サービスチェーン間またはサービスグループ間で共有できます。ただし、PNF デバイスは、単一のクラスタ間でのみ共有できるようになりました。
-

表 12: 機能の履歴

機能名	リリース情報	機能説明
サービスチェーンでの PNF デバイスの管理	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能を使用すると、仮想ネットワーク機能 (VNF) デバイスに加えて、物理ネットワーク機能 (PNF) デバイスをネットワークに追加できます。これらの PNF デバイスは、サービスチェーンに追加して、サービスチェーン、サービスグループ、およびクラスタ全体で共有できます。サービスチェーンに PNF デバイスを含めると、サービスチェーンで VNF デバイスのみを使用することによって引き起こされるパフォーマンスとスケーリングの問題を解決できます。

始める前に

検証済みの物理ネットワーク機能の詳細については、『Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Guide』の「Validated Physical Network Functions」のトピックを参照してください。

ルータまたはファイアウォールを既存のサービスチェーンに追加してカスタマイズされたサービスチェーンを作成するには、次の点に注意してください。

- PNF デバイスを Cisco SD-WAN Manager で管理する必要がある場合は、シリアル番号が Cisco SD-WAN Manager ですでに利用可能であることを確認してください。これにより、PNF 設定時に選択できるようになります。
- FTD デバイスは、サービスチェーンの任意の位置に配置できます。
- ASR 1000 シリーズアグリゲーションサービスルータは、サービスチェーンの最初と最後の位置にのみ配置できます。
- PNF デバイスは、サービスチェーンおよびサービスグループ全体に追加できます。
- PNF デバイスは、サービスグループ間で共有できます。同じシリアル番号を入力することで、サービスグループ間で共有できます。
- PNF デバイスは、単一のコロケーションクラスタ間で共有できますが、複数のコロケーションクラスタ間で共有することはできません。

手順

ステップ 1 サービスグループとサービスグループ内のサービスチェーンを作成します。『[サービスグループでのサービスチェーンの作成 \(37 ページ\)](#)』を参照してください。

ステップ 2 [Add Service Chain] ダイアログボックスで、サービスチェーン名、説明、帯域幅、入力 VLAN ハンドオフ、出力 VLAN ハンドオフ、サービスチェーンの正常性情報の監視、およびサービスチェーン構成を入力します。[Add] をクリックします。

サービスチェーン構成では、ドロップダウンリストから [Create Custom] を選択します。デザインビューウィンドウに空のサービスチェーンが表示されます。左側に、サービスチェーンに追加できる VNF デバイスと PNF デバイスのセットが表示されます。VNF デバイスの周囲の「V」は VNF を表し、PNF デバイスの周囲の「P」は PNF を表します。

(注) PNF デバイスを共有してサービスチェーンを作成するには、必ず [Create Custom] オプションを選択してください。

ステップ 3 サービスチェーンで物理ルータ、物理ファイアウォールなどの PNF を追加するには、必要な PNF アイコンをクリックし、アイコンをサービスチェーンボックス内の適切な場所にドラッグします。

必要なすべての PNF デバイスを追加したら、それぞれを設定します。

a) サービスチェーンボックスで PNF デバイスをクリックします。

[Configure PNF] ダイアログボックスが表示されます。PNF を設定するには、次のパラメータを入力します。

b) PNF デバイスで HA が有効になっている場合は、[HA Enabled] をチェックします。

c) PNF で HA が有効になっている場合は、HA シリアル番号を [HA Serial] に追加してください。

PNF デバイスが FTD の場合は、次の情報を入力します。

1. [Name] フィールドに、PNF の名前を入力します。

2. [Firewall Mode] として [Routed] または [Transparent] を選択します。

3. [PNF Serial] フィールドに、PNF デバイスのシリアル番号を入力します。

PNF デバイスが ASR 1000 シリーズ アグリゲーション サービス ルータの場合は、次の情報を入力します。

1. デバイスが Cisco SD-WAN Manager によって管理されている場合は、[vManaged] チェックボックスをオンにします。

2. [Fetch Properties] をクリックします。

3. [Name] フィールドに、PNF の名前を入力します。

4. [PNF Serial] フィールドに、PNF デバイスのシリアル番号を入力します。

d) [Configure] をクリックします。

ステップ 4 サービスチェーンを追加して PNF デバイスを共有するには、ステップ 2 から繰り返します。

ステップ 5 既存の PNF 構成を編集するには、PNF をクリックします。

ステップ 6 [Share NF To] ドロップダウンリストで、PNF を共有するサービスチェーンを選択します。

PNF の共有後、PNF にカーソルを合わせると、それぞれの共有 PNF デバイスが青色で強調表示されます。ただし、異なるサービスグループの PNF は青色で強調表示されません。共有する NF を選択すると、青色の縁が表示されます。同じ PNF が複数のサービスチェーンで共有されている場合は、PNF アイコンをドラッグして特定の位置に配置することで、さまざまな位置で使用できます。

図 7: サービスチェーン内の単一の PNF

次の図は、単一の PNF、Ftd_Pnf（他のサービスチェーンと共有されない）で構成されるサービスチェーンを示しています。



図 8: サービスチェーン内の 2つの PNF デバイス

次の図は、サービスチェーン 1（SC1）とサービスチェーン 2（SC2）で共有される FTdv_PNF と ASR_PNF（非共有）の 2つの PNF で構成されるサービスチェーンを示しています。

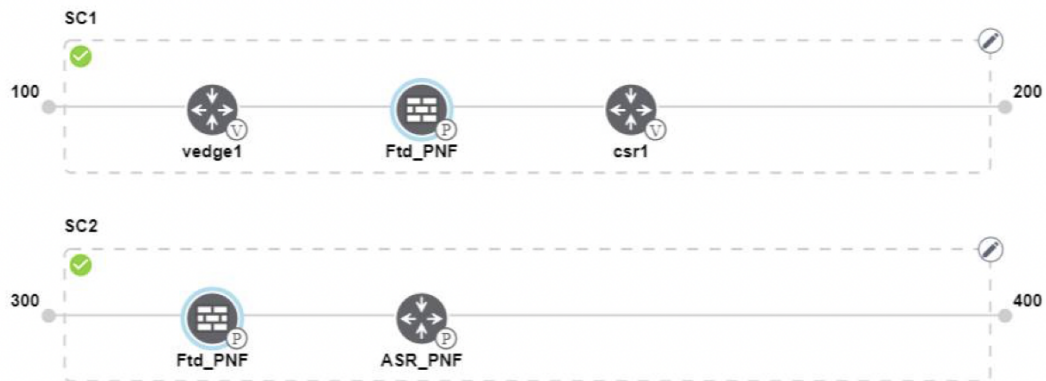
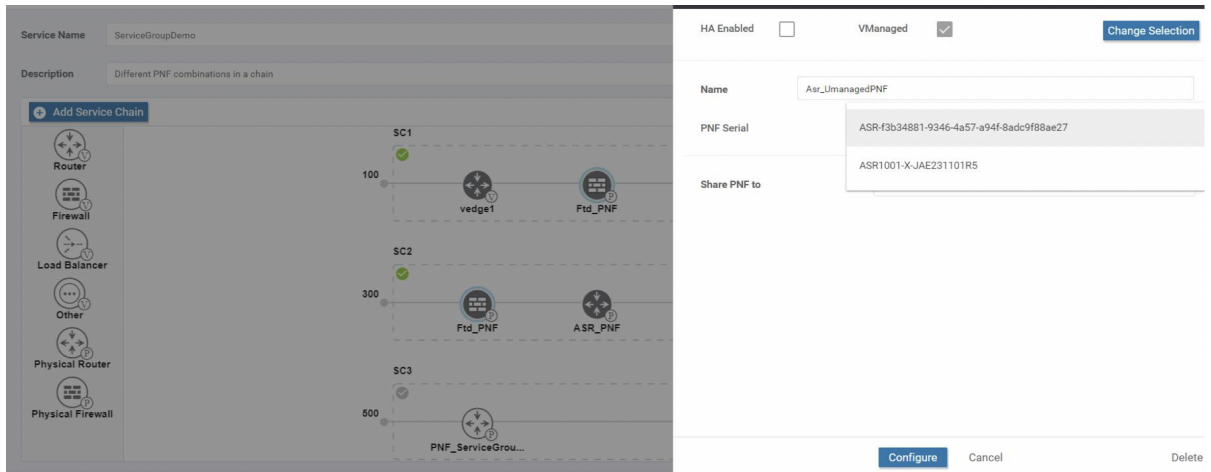


図 9: サービスチェーン内の 3つの PNF デバイス

次の図は、2つの異なる位置にある 3つの PNF デバイスで構成されるサービスチェーンと、Cisco SD-WAN Manager 設定を示しています。



ステップ7 ネットワーク機能構成を削除またはキャンセルするには、それぞれ [Delete] または [Cancel] をクリックします。

サービスグループをコロケーションクラスタに接続する必要があります。PNF デバイスを含むサービスグループを接続した後、VNF デバイスとは異なり、PNF 構成は PNF デバイスに自動的にプッシュされません。代わりに、[Monitor] ウィンドウで生成された構成に注意して、PNF デバイスを手動で構成する必要があります。[Cloud OnRamp Colocation クラスタのモニター \(77 ページ\)](#) VLAN は、Cisco Catalyst 9500-40X スイッチデバイスでも構成する必要があります。特定の PNF 構成の詳細については、『[ASR 1000 Series Aggregation Services Routers Configuration Guides](#)』および『[Cisco Firepower Threat Defense Configuration Guides](#)』を参照してください。

共有 VNF デバイスによるカスタムサービスチェーン

サポートされている VNF デバイスを含めることで、サービスチェーンをカスタマイズできます。

表 13: 機能の履歴

機能名	リリース情報	機能説明
サービスチェーン全体で VNF デバイスを共有する	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能により、サービスチェーン全体で仮想ネットワーク機能 (VNF) デバイスを共有して、リソースの使用率を向上させ、リソースの断片化を減らすことができます。

始める前に

VNF デバイスの共有について、次の点に注意してください。

- サービスチェーンの最初、最後、または最初と最後の両方の VNF デバイスのみを共有できます。

- VNF は、少なくとも 1 つ以上のサービスチェーン、最大 5 つまでのサービスチェーンと共有できます。
- 各サービスチェーンには、サービスチェーン内に最大 4 つの VNF デバイスを含めることができます。
- 同じサービスグループ内でのみ VNF デバイスを共有できます。

手順

ステップ 1 サービスグループとサービスグループ内のサービスチェーンを作成します。『[サービスグループでのサービスチェーンの作成 \(37 ページ\)](#)』を参照してください。

ステップ 2 [Add Service Chain] ダイアログボックスで、サービスチェーン名、説明、帯域幅、入力 VLAN ハンドオフ、出力 VLAN ハンドオフ、サービスチェーンの正常性情報の監視、およびサービスチェーン構成を入力します。[Add] をクリックします。

サービスチェーン構成では、ドロップダウンリストから [Create Custom] を選択します。デザインビューウィンドウに空のサービスチェーンが表示されます。左側に、サービスチェーンに追加できる VNF デバイスと PNF デバイスのセットが表示されます。VNF デバイスの周囲の「V」は VNF を表し、PNF デバイスの周囲の「P」は PNF を表します。

(注) 共有 VNF パッケージを作成するには、必ず [Create Custom] オプションを選択してください。

ステップ 3 ルータ、ロードバランサ、ファイアウォールなどの VNF を追加するには、左側のパネルから VNF アイコンをクリックし、アイコンをサービスチェーンボックス内の適切な場所にドラッグします。

必要なすべての VNF デバイスを追加したら、それぞれを構成します。

a) サービスチェーンボックスで VNF をクリックします。

[Configure VNF] ダイアログボックスが表示されます。VNF を構成するには、次のパラメータを入力します。

b) [Image Package] ドロップダウンリストから、ロードするソフトウェアイメージを選択します。

Cisco SD-WAN Manager でカスタマイズされた VNF パッケージを作成するには、[カスタマイズされた VNF イメージの作成 \(61 ページ\)](#) を参照してください。

c) [Fetch VNF Properties] をクリックします。

d) [Name] フィールドに、VNF の名前を入力します。

e) [CPU] フィールドに、VNF に必要な仮想 CPU の数を入力します。

f) [Memory] フィールドに、VNF に割り当てるメモリの量をメガバイト単位で入力します。

g) [Disk] フィールドに、VNF に割り当てるストレージのメモリ量をギガバイト単位で入力します。

h) 必要に応じて、VNF 固有のパラメータを入力します。VNF 固有のプロパティの詳細については、[サービスグループでのサービスチェーンの作成 \(37 ページ\)](#) を参照してください。

これらの VNF 固有のパラメータは、VNF の Day-0 操作に必要なカスタムユーザー変数です。

さまざまな位置にある場合のさまざまな VNF タイプのユーザー変数およびシステム変数のリストに関する完全な情報については、を参照してください。

(注) ユーザー変数が必須として定義されている場合は、必ずユーザー変数の値を入力してください。システム変数は Cisco SD-WAN Manager によって自動的に設定されます。

i) [Configure] をクリックします。

ステップ 4 VNF デバイスを共有するには、ステップ 2 から繰り返します。

ステップ 5 既存の VNF 構成を編集するには、VNF をクリックします。

ステップ 6 VNF 構成を下にスクロールして、[Share NF To] フィールドを見つけます。[Share NF To] ドロップダウンリストから、VNF を共有するサービスチェーンを選択します。

VNF が共有された後、VNF にカーソルを合わせると、特定の共有 VNF デバイスが青色で強調表示されます。共有する NF を選択すると、青い縁が表示されます。

ステップ 7 VNF を削除するか、VNF 構成をキャンセルするには、それぞれ [Delete] または [Cancel] をクリックします。

サービスグループをクラスタに接続する必要があります。

サービスグループの表示

サービスグループを表示するには、次の手順を実行します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Colocation] を選択します

ステップ 2 [Service Group] をクリックします。

ステップ 3 目的のサービスグループの [...] をクリックし、[View] を選択します。

設計ウィンドウでサービスチェーンを表示できます。

サービスグループの編集

サービスグループをクラスタに接続する前に、すべてのパラメータを編集できます。サービスグループをクラスタに接続した後は、モニタリング構成パラメータのみを編集できます。また、サービスグループを接続した後、新しいサービスチェーンを追加することはできますが、サービスチェーンを編集または接続することはできません。したがって、既存のサービスチェーンを編集する前に、クラスタからサービスグループを切断してください。サービスグループを編集および削除するには、次の手順を実行します。

手順

-
- ステップ 1 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します。
 - ステップ 2 **[Service Group]** をクリックします。
 - ステップ 3 目的のサービスグループの [...] をクリックし、**[Edit]** を選択します。
 - ステップ 4 サービスチェーン構成を変更するか、VNF 構成を変更するには、ルータまたはファイアウォールの VNF アイコンをクリックします。
 - ステップ 5 新しいサービスチェーンを追加するには、**[Add Service Chain]** をクリックします。
-

クラスタ内のサービスグループの接続または切断

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation 構成を完了するには、サービスグループをクラスタに接続する必要があります。サービスグループをクラスタに接続またはクラスタから切り離すには、次の手順を実行します。

手順

-
- ステップ 1 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Cloud OnRamp for Colocation]** を選択します。
 - ステップ 2 対応するクラスタの隣にある [...] をクリックし、**[Attach Service Groups]** を選択します。
 - ステップ 3 **[Attach Service Groups]** ダイアログボックスで、**[Available Service Groups]** で 1 つ以上のサービスグループを選択し、**[Add]** をクリックして、選択したグループを **[Selected Service Groups]** に移動します。
 - ステップ 4 **[Attach]** をクリックします。
 - ステップ 5 サービスグループをクラスタから切り離すには、対応するクラスタの隣にある [...] をクリックし、**[Detach Service Groups]** を選択します。
サービスグループ内の 1 つのサービスチェーンを接続または切り離すことはできません。
 - ステップ 6 表示される **[Config Preview]** ウィンドウで、**[Cancel]** をクリックして、接続または切り離しタスクをキャンセルします。

(注)

- ステップ 7 サービスグループがアタッチまたはデタッチされているかどうかを確認するには、Cisco SD-WAN Manager を使用してステータスを表示します。次の点に注意してください。
 - **[Task View]** ウィンドウのタスクのステータスが長時間にわたって **[FAILURE]** または **[PENDING]** と表示される場合は、Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションガイドの「[Troubleshoot Service Chain Issues](#)」のトピックを参照してください。
 - Cisco Colo Manager タスクが失敗した場合は、『[Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide](#)』の「[Troubleshoot Cisco Colo Manager Issues](#)」のトピックを参照してください。

コロケーションクラスタが [PENDING] 状態に移行した場合は、クラスタの [...] をクリックし、[Sync] を選択します。このアクションにより、クラスタは [ACTIVE] 状態に戻ります。[Sync] オプションは、Cisco SD-WAN Manager とコロケーションデバイスの同期を維持します。

VM カタログとリポジトリの管理



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

Table 14: 機能の履歴

機能名	リリース情報	説明
qcow2 形式での Cisco VM イメージアップロードのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能を使用すると、仮想マシンイメージを qcow2 形式で Cisco SD-WAN Manager にアップロードできます。以前は、事前にパッケージ化された tar.gz 形式のイメージファイルのみをアップロードできました。

Cisco SD-WAN Manager は、事前にパッケージ化された Cisco 仮想マシンイメージ、tar.gz 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) を構成するときに、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。

スキャフォールドファイルには、次のコンポーネントが含まれています。

- VNF メタデータ (image_properties.xml)

- サービスチェーン用のクラスタリソースプールからのシステム生成変数 (system_generated_properties.xml)
- トークン化された Day-0 構成ファイル
- パッケージ マニフェスト ファイル (package.mf)

また、サポートされている形式 (qcow2) でルートディスクイメージを提供することで、VM イメージをパッケージ化することもできます。Linux のコマンドライン NFVIS VM パッケージ ツール **nfvpt.py** を使用して qcow2 をパッケージ化するか、または Cisco SD-WAN Manager を使用してカスタマイズされた VM イメージを作成します。『[カスタマイズされた VNF イメージの作成, on page 61](#)』を参照してください。

VM が SR-IOV 対応であることは、vm パッケージ *.tar.gz の image_properties.xml で sriov_supported が true に設定されていることを意味します。また、サービス チェーン ネットワークは自動的に SR-IOV ネットワークに接続されます。sriov_supported が false に設定されている場合、データポートチャンネル上に OVS ネットワークが作成されます。OVS ネットワークを使用して、サービスチェーンのために VM VNIC に接続されます。Cloud OnRamp for Colocation ソリューションの場合、VM はサービスチェーンで同種タイプのネットワークを使用します。このタイプのネットワークは、SR-IOV と OVS の組み合わせではなく、OVS または SR-IOV のいずれかであることを意味します。

どの VM にも 2 つのデータ VNIC のみが接続されています。1 つはインバウンドトラフィック用で、もう 1 つはアウトバウンドトラフィック用です。3 つ以上のデータインターフェイスが必要な場合は、VM 内のサブインターフェイス構成を使用します。VM パッケージは VM カタログに保存されます。



Note ファイアウォールなどの各 VM タイプには、同じまたは異なるベンダーから Cisco SD-WAN Manager にアップロードされ、カタログに追加される複数の VM イメージを含めることができます。また、同じ VM のリリースに基づく異なるバージョンをカタログに追加できます。ただし、VM 名が一意であることを確認してください。

Cisco VM イメージ形式は *.tar.gz としてバンドルでき、次のものを含めることができます。

- VM を起動するルートディスクイメージ。
- パッケージ内のファイルリストのチェックサム検証用のパッケージ マニフェスト。
- VM メタデータをリストする XML 形式のイメージプロパティファイル。
- (オプション) 0 日目設定、VM のブートストラップに必要なその他のファイル。
- (オプション) VM がステートフル HA をサポートする場合の HA Day-0 構成。
- VM システムプロパティをリストする XML 形式のシステム生成プロパティファイル。

VM イメージは、Cisco SD-WAN Manager がホストする HTTP サーバーローカルリポジトリまたはリモートサーバーの両方でホストできます。

VM が tar.gz などの Cisco NFVIS でサポートされる VM パッケージ形式である場合、Cisco SD-WAN Manager はすべての処理を実行し、VNF プロビジョニング中に変数キーと値を指定できます。



Note Cisco SD-WAN Manager は Cisco VNF を管理します。VNF 内の Day-1 および Day-N 設定は他の VNF ではサポートされません。VM パッケージの形式と内容、および image_properties.xml と マニフェスト (package.mf) のサンプルの詳細については、『Cisco NFVIS Configuration Guide』の「VM Image Packaging」を参照してください。

同じ VM、同じバージョン、Communication Manager (CM) タイプの複数のパッケージをアップロードするには、3つの値 (名前、バージョン、VNFタイプ) のいずれかが異なることを確認します。その後、アップロードする VM *.tar.gz を再パッケージ化できます。

VNF イメージのアップロード

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

手順

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

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

ステップ 3 仮想イメージを保存する場所を選択します。

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

- 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco SD-WAN Manager サーバーから仮想イメージを選択します (例: CSR.tar.gz、ASAv.tar.gz、ABC.qcow2)。
- ファイルをアップロードする場合は、アップロードするファイルのタイプ ([Image Package] または [Scaffold]) を指定します。必要に応じてファイルの説明を指定し、カスタムタグをファイルに追加します。サービスチェーンを作成する際、このタグを使用してイメージとスキャフォールドファイルをフィルタリングできます。
- qcow2 イメージファイルをアップロードする場合は、サービスまたは VNF タイプ ([FIREWALL] または [ROUTER]) を指定します。必要に応じて、以下を指定します。
 - イメージの説明
 - イメージのバージョン番号

- チェックサム
- ハッシュアルゴリズム

また、サービス チェーンの作成時に、イメージやスキュアフォルドファイルのフィルタ処理で使用できるカスタムタグをファイルに追加することもできます。

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

4. [Upload] をクリックして、イメージを仮想イメージリポジトリに追加します。仮想イメージリポジトリテーブルには、追加された仮想イメージが表示され、CSP デバイスにインストールできます。
- イメージをリモートの Cisco SD-WAN Manager サーバーに保存してから CSP デバイスにダウンロードするには、[Remote Server - Manager] をクリックします。[Upload VNF's Package to Remote Server-Manager] ダイアログボックスが表示されます。
 1. [Manager Hostname/IP Address] フィールドに、管理 VPN（通常は VPN 512）にある Cisco SD-WAN Manager サーバー上のインターフェイスの IP アドレスを入力します。
 2. 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco SD-WAN Manager サーバーから仮想イメージを選択します。
 3. ファイルをアップロードする場合は、アップロードするファイルのタイプ ([Image Package] または [Scaffold]) を指定します。必要に応じてファイルの説明を指定し、カスタムタグをファイルに追加します。サービスチェーンを作成する際、このタグを使用してイメージとスキュアフォルドファイルをフィルタリングできます。
 4. qcow2 イメージファイルをアップロードする場合は、サービスまたは VNF タイプ ([FIREWALL] または [ROUTER]) を指定します。必要に応じて、以下を指定します。
 - イメージの説明
 - イメージのバージョン番号
 - チェックサム
 - ハッシュアルゴリズム

また、サービス チェーンの作成時に、イメージやスキュアフォルドファイルのフィルタ処理で使用できるカスタムタグをファイルに追加することもできます。

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

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

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

カスタマイズされた VNF イメージの作成

始める前に

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

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

次のカスタムパッケージの要件が満たされていることを確認します。

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

手順

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

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

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

表 15: VNF パッケージのプロパティ

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

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

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

次の Day-0 構成プロパティを含めます。

表 16: Day-0 構成

フィールド	必須または任意	説明
Mount	必須	ブートストラップファイルがマウントされるパス。
Parseable	必須	Day-0 構成ファイルを解析できるかどうか。 オプションは、[Enable] または [Disable] です。デフォルトでは、[Enable] が選択されています。

フィールド	必須または任意	説明
High Availability	必須	<p>選択する Day-0 構成ファイルのハイアベイラビリティ。</p> <p>指定できる値は、[Standalone]、[HA Primary]、[HA Secondary] です。</p>

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

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

(注) ブートストラップ構成ファイルは XML またはテキスト形式で、VNF と環境に固有のプロパティが含まれています。共有 VNF については、『[Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide](#)』のトピックとその他の関連資料を参照してください。さまざまな VNF タイプに追加する必要があるシステム変数のリストが記載されています。

- a) システム変数を追加するには、[CLI configuration] ダイアログボックスで、テキストフィールドからプロパティを選択して強調表示します。[System Variable] をクリックします。[Create System Variable] ダイアログボックスが表示されます。
- b) [Variable Name] ドロップダウンリストからシステム変数を選択し、[Done] をクリックします。強調表示されたプロパティは、システム変数名に置き換えられます。
- c) カスタム変数を追加するには、[CLI configuration] ダイアログボックスで、テキストフィールドからカスタム変数属性を選択して強調表示します。[Custom Variable] をクリックします。[Create Custom Variable] ダイアログボックスが表示されます。
- d) カスタム変数名を入力し、[Type] ドロップダウンリストからタイプを選択します。
- e) カスタム変数属性を設定するには、次の手順を実行します。
 - サービスチェーンの作成時にカスタム変数が必須になるようにするには、[Mandatory] の横にある [Type] をクリックします。
 - VNF にプライマリとセカンダリの Day-0 ファイルの両方が含まれるようにするには、[Common] の横にある [Type] をクリックします。
- f) [Done] をクリックしてから、[Save] をクリックします。強調表示されたカスタム変数属性は、カスタム変数名に置き換えられます。

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

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

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

表 17: ストレージのプロパティ

フィールド	必須または任意	説明
Size	必須	VM 操作に必要なディスクサイズ。サイズ単位が GiB の場合、最大ディスクサイズは 256 GiB です。
Size Unit	必須	サイズ単位を選択します。サポートされる単位は、MiB、GiB、TiB です。
Device Type	任意	ディスクまたは CD-ROM を選択します。デフォルトでは、ディスクが選択されています。
Location	任意	ディスクまたは CD-ROM の場所。デフォルトでは、ローカルです。
Format	任意	ディスクイメージ形式を選択します。サポートされている形式は、qcow2、raw、および vmdk です。デフォルトでは、raw です。
Bus	任意	ドロップダウンリストから値を選択します。バスでサポートされる値は、virtio、scsi、および ide です。デフォルトでは、virtio です。

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

表 18: VNF イメージのプロパティ

フィールド	必須または任意	説明
SR-IOV Mode	必須	SR-IOV サポートを有効または無効にします。デフォルトでは有効になっています。
Monitored	必須	ブートストラップできる VM の正常性モニタリング。 オプションは enable または disable です。デフォルトでは有効になっています。
Bootup Time	必須	モニタリング対象 VM のモニタリングタイムアウト期間。デフォルトは 600 秒です。
Serial Console	任意	サポートされている、またはされていないシリアルコンソール。 オプションは enable または disable です。デフォルトでは無効になっています。
Privileged Mode	任意	プロミスキャスモードやスヌーピングなどの特別な機能を許可します。 オプションは enable または disable です。デフォルトでは無効になっています。
Dedicate Cores	必須	VM の低遅延（ルータやファイアウォールなど）を補う専用リソース（CPU）の割り当てを容易にします。それ以外の場合は、共有リソースが使用されます。 オプションは enable または disable です。デフォルトでは有効になっています。

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

表 19: VM リソース要件

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

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

表 20: Day-0 構成ドライブオプション

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

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

VNF イメージの表示

手順

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

ステップ 2 **[Virtual Images]** をクリックします。

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

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

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

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

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

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

ステップ4 目的のイメージで [...] をクリックし、[Show Info] を選択します。

VNF イメージの削除

手順

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

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

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



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



(注) また、サービスチェーンによって参照されている VNF イメージは削除できません。

Cisco SD-WAN Manager を使用した Cisco NFVIS のアップグレード

Cisco NFVIS をアップロードしてアップグレードするには、アップグレードイメージが、Cisco SD-WAN Manager を使用して Cisco SD-WAN Manager リポジトリにアップロードできるアーカイブファイルとして利用できる必要があります。Cisco NFVIS イメージをアップロードした後、Cisco SD-WAN Manager の [Software Upgrade] ウィンドウを使用して、アップグレードされたイメージを CSP デバイスに適用できます。Cisco SD-WAN Manager を使用して Cisco NFVIS ソフトウェアをアップグレードする場合、次のタスクを実行できます。

- Cisco NFVIS アップグレードイメージをアップロードします。『[NFVIS アップグレードイメージのアップロード, on page 69](#)』を参照してください。
- アップロードされたイメージで CSP デバイスをアップグレードします。『[Cisco NFVIS アップグレードイメージを使用した CSP デバイスのアップグレード, on page 69](#)』を参照してください。
- Cisco SD-WAN Manager ツールバーにある [Tasks] アイコンをクリックして、CSP デバイスのアップグレードステータスを表示します。

NFVIS アップグレードイメージのアップロード

手順

-
- ステップ 1** 所定の場所からローカルシステムに Cisco NFVIS アップグレードイメージをダウンロードします。ソフトウェアイメージをネットワーク内の FTP サーバーにダウンロードすることもできます。
- ステップ 2** Cisco SD-WAN Manager のメニューから、**[Maintenance] > [Software Repository]** を選択します。
- ステップ 3** **[Add New Software] > [Remote Server/Remote Server - Manager]** をクリックします。
- ソフトウェアイメージは、リモートファイルサーバー、リモート Cisco SD-WAN Manager サーバー、または Cisco SD-WAN Manager サーバーに保存できます。
- Cisco SD-WAN Manager サーバー：ソフトウェアイメージをローカルの Cisco SD-WAN Manager サーバーに保存します。
- リモートサーバー：ソフトウェアイメージの場所を指す URL を保存し、FTP または HTTP URL を使用してアクセスできます。
- リモート Cisco SD-WAN Manager サーバー：ソフトウェアイメージをリモート Cisco SD-WAN Manager サーバーに保存し、リモート Cisco SD-WAN Manager サーバーの場所はローカル Cisco SD-WAN Manager サーバーに保存されます。
- ステップ 4** イメージをソフトウェアリポジトリに追加するには、ステップ 1 でダウンロードした Cisco NFVIS アップグレードイメージを参照して選択します。
- ステップ 5** **[Add|Upload]** をクリックします。

ソフトウェアリポジトリテーブルには、追加された NFVIS アップグレードイメージが表示され、CSP デバイスにインストールできます。『[Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide](#)』の「Manage Software Upgrade and Repository」のトピックを参照してください。

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

始める前に

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

手順

- ステップ 1** Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Upgrade]** > **[WAN Edge]** を選択します。
- ステップ 2** 選択するデバイスの 1 つ以上の CSP デバイスチェックボックスをオンにします。
- ステップ 3** **[Upgrade]** をクリックします。**[Software Upgrade]** ダイアログボックスが表示されます。
- ステップ 4** CSP デバイスにインストールする Cisco NFVIS ソフトウェアバージョンを選択します。ソフトウェアがリモートサーバーにある場合は、適切なリモートバージョンを選択します。
- ステップ 5** 新しい Cisco NFVIS ソフトウェアバージョンで自動的にアップグレードおよびアクティブ化し、CSP デバイスを再起動するには、**[Activate and Reboot]** チェックボックスをオンにします。

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

- ステップ 6** **[Upgrade]** をクリックします。

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

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

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

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

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



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

サポートされるアップグレードシナリオと推奨される接続

規範的接続またはフレキシブルな接続の使用を決定するさまざまなアップグレードシナリオとクラスタの状態を以下に示します。

表 21: サポートされる接続

Cisco SD-WAN Manager	Cisco NFVIS	クラスタの状態	サポートされる接続
リリース 19.3 または 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 3.12 または 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	リリース 19.3 または 20.1.1.1 で作成され、アクティブなクラスタ	規範的接続を使用する
最新のリリース 20.3.1 を使用する	最新のリリース 4.2.1 を使用する	Cisco vManage リリース 20.3.1 で作成され、アクティブなクラスタ	規範的接続またはフレキシブルな接続を使用できる
リリース 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	リリース 20.1.1.1 で作成され、アクティブなクラスタ	規範的接続を使用する
リリース 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	リリース 20.1.1.1 で作成され、アクティブなクラスタ。 アップグレード後に新しい Cisco CSP デバイスを追加するには、「 Cisco SD-WAN Manager および Cisco NFVIS のアップグレード後のクラスタへの Cisco CSP デバイスの追加 」を参照してください。	規範的接続を使用する
リリース 20.1.1.1 からリリース 20.3.1 へのアップグレード	リリース 4.1 からリリース 4.1.1 または 4.2.1 へのアップグレード	Cisco vManage リリース 20.3.1 で作成され、アクティブなクラスタ	規範的接続またはフレキシブルな接続を使用できる

Cisco SD-WAN Manager および Cisco NFVIS のアップグレード後のクラスタへの Cisco CSP デバイスの追加

Cisco SD-WAN Manager をリリース 20.3.1 にアップグレードする前にクラスタが作成された場合に、Cisco CSP デバイスをクラスタに追加するには、次の手順を実行します。

1. 規範的接続に従って、新しく追加された Cisco CSP デバイスのケーブルを接続します。
2. Cisco NFVIS をリリース 4.2.1 にアップグレードする
3. Cisco NFVIS にログインして、新しく追加された Cisco CSP デバイスで次のコマンドを使用します。

- **request csp-prescriptive-mode**

新しく追加された Cisco CSP デバイスを規範モードで実行するように要求します。

- **request activate chassis-number chassis number token serial number**

Cisco CSP デバイスをアクティブ化する

例

```
request activate chassis-number 71591a3b-7d52-24d4-234b-58e5f4ad0646
token e0b6f073220d85ad32445e30de88a739
```

クラスタを更新する前の推奨事項

- Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションの最新リリースにアップグレードするときにすでにアクティブなクラスタを使用するには、Cisco SD-WAN Manager および Cisco NFVIS を最新リリースにアップグレードしてください。
- Cisco Catalyst SD-WAN Cloud OnRamp for Colocation ソリューションの最新リリースにアップグレードするときに新しいクラスタを作成するには、フレキシブルな接続のために Cisco SD-WAN Manager および Cisco NFVIS を最新リリースにアップグレードしてください。

Cisco Catalyst SD-WAN Manager からの Cloud OnRamp for Colocation デバイスの動作ステータスのモニター



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

コロケーションデバイスのモニタリングは、クラウドサービスプラットフォーム (CSP) デバイスや Cisco Colo Manager などのデバイスの正常性、インベントリ、可用性、およびその他

の運用関連プロセスを確認および分析するプロセスです。CPU、メモリ、ファン、温度など、CSP デバイスのコンポーネントを監視することもできます。Cisco SD-WAN Manager モニタリング画面の詳細については、『[Cisco Catalyst SD-WAN Configuration Guides](#)』を参照してください。

すべての通知は、Cisco SD-WAN Manager 通知ストリームに送信されます。通知ストリームコマンドを使用するには、『[Cisco Catalyst SD-WAN Command Reference](#)』を参照してください。

手順

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。

Cisco SD-WAN リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから [**モニター (Monitor)**] > [**ネットワーク (Network)**] の順に選択します。

Cisco SD-WAN Manager が CSP デバイスに到達できず、Cisco Colo Manager がスイッチに到達できない場合、CSP デバイスと Cisco Colo Manager は到達不能として表示されます。

ステップ 2 ホスト名をクリックして、リストから CSP デバイスまたはスイッチをクリックします。

デフォルトでは、VNF ステータスウィンドウが表示されます。

ステップ 3 [Select Device] をクリックし、デバイスの検索結果をフィルタリングするには、検索バーの [Filter] オプションを使用します。

表示されるデバイスに関する情報のカテゴリは次のとおりです。

- VNF ステータス：各 VNF のパフォーマンス仕様、必要なリソース、およびコンポーネントネットワーク機能を表示します。[VNF に関する情報の表示 \(75 ページ\)](#) を参照してください。
- インターフェイス：インターフェイスのステータスと統計情報を表示します。『[Cisco Catalyst SD-WAN Configuration Guides](#)』の「[View Interfaces](#)」を参照してください。
- 制御接続：制御接続のステータスと統計を表示します。『[Cisco Catalyst SD-WAN Configuration Guides](#)』の「[View Control Connections](#)」のトピックを参照してください。
- システムステータス：リポートとクラッシュの情報、ハードウェアコンポーネントのステータス、CPU とメモリの使用状況を表示します。『[Cisco Catalyst SD-WAN Configuration Guides](#)』の「[View Control Connections](#)」のトピックを参照してください。
- Cisco Colo Manager：Cisco Colo Manager の正常性ステータスを表示します。[Cisco Colo Manager の正常性の表示 \(74 ページ\)](#) を参照してください。
- イベント：最新のシステムログ (syslog) イベントを表示します。『[Cisco Catalyst SD-WAN Configuration Guides](#)』の「[View Events](#)」のトピックを参照してください。
- トラブルシューティング：ping および traceroute トラフィック接続ツールに関する情報を表示します。『[Cisco Catalyst SD-WAN Configuration Guides](#)』の「[Troubleshoot a Device](#)」のトピックを参照してください。

- リアルタイム：機能固有の操作コマンドのリアルタイムデバイス情報を表示します。『[Cisco Catalyst SD-WAN Configuration Guides](#)』の「View Real-Time Data」のトピックを参照してください。

ステップ 4 コロケーションクラスタを監視するには、Cisco SD-WAN Manager メニューから **[Monitor]** > **[Devices]** を選択し、**[Colocation Cluster]** をクリックします。

Cisco vManage リリース 20.6.1 以前：コロケーションクラスタをモニターするには、Cisco SD-WAN Manager メニューから **[Monitor]** > **[Network]** を選択し、**[Colocation Clusters]** をクリックします。

ステップ 5 目的のクラスタ名をクリックします。詳細については、「[Cloud OnRamp Colocation クラスタのモニター \(77 ページ\)](#)」を参照してください。

Cisco Colo Manager の正常性の表示

デバイス、CCM ホストシステム IP、CCM IP、および CCM 状態に関する Cisco Colo Manager (CCM) の正常性を表示できます。この情報を確認すると、ネットワーク サービスチェーンの設計時に使用する VNF を決定するのに役立ちます。VNF に関する情報を表示するには、次の手順を実行します。

手順

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

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

すべてのデバイスの情報が表形式で表示されます。

ステップ 2 表から CSP デバイスをクリックします。

ステップ 3 左ペインで、**[Colo Manager]** をクリックします。

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

VNFに関する情報の表示

表 22:機能の履歴

機能名	リリース情報	説明
VNF の状態とカラーコード	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能を使用すると、展開された VM の状態を、[Monitor]>[Devices] ページで表示できるカラーコードを使用して判断できます。これらのカラーコードは、VM の状態に基づいてサービスチェーンの作成を決定するのに役立ちます。

表 23:機能の履歴

機能名	リリース情報	説明
SR-IOV 対応の NIC および OVS スイッチのネットワーク使用率チャート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	この機能により、SR-IOV 対応の NIC と OVS スイッチの両方に接続された VM VNIC のネットワーク使用率チャートを表示できます。これらのチャートは、VM の使用率がサービスチェーンの作成に最適かどうかを判断するのに役立ちます。

各 VNF のパフォーマンス仕様と必要なリソースを表示できます。この情報を確認すると、ネットワークサービスの設計時に使用する VNF を決定するのに役立ちます。VNF に関する情報を表示するには、次の手順を実行します。

手順

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。

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

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

ステップ 2 表から CSP デバイスをクリックします。

ステップ 3 左側のペインで、[VNF Status] をクリックします。

ステップ 4 表から、VNF 名をクリックします。Cisco SD-WAN Manager が特定の VNF に関する情報を表示します。ネットワーク使用率、CPU 使用率、メモリ使用率、およびディスク使用率をクリックして、VNF リソースの使用率を監視できます。

次の VNF 情報が表示されます。

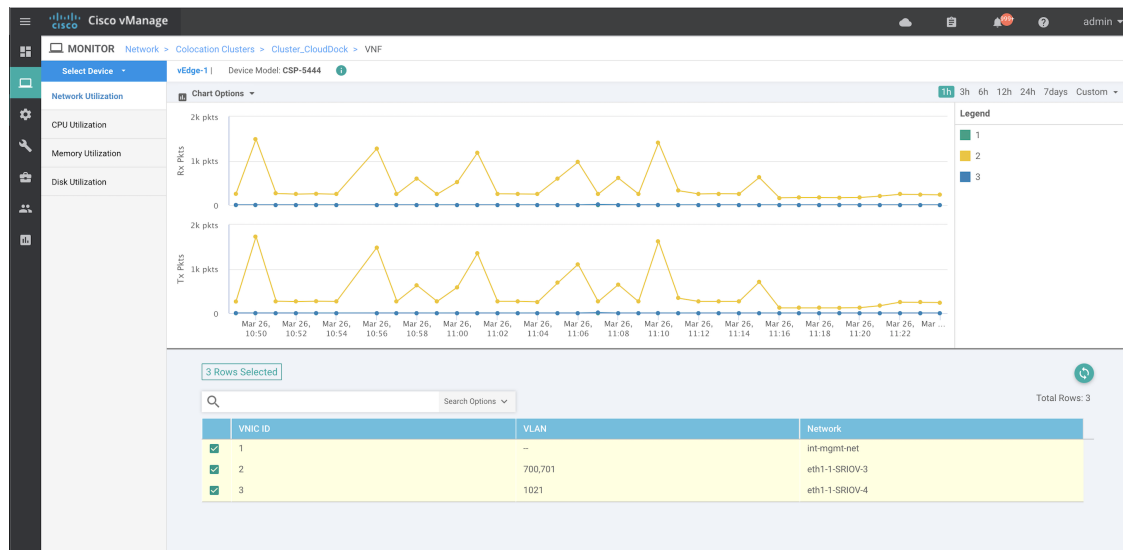
表 24: VNF 情報

チャートオプションバー	グラフ形式の VNF 情報	色分けされた形式の VNF 情報
<ul style="list-style-type: none"> • [Chart Options] ドロップダウン: [Chart Options] ドロップダウンリストをクリックして、表示するデータのタイプを選択します。 • 期間: データを表示する事前定義された期間またはカスタム期間をクリックします。 	<p>[Select Device] ドロップダウンリストから VNF を選択して、VNF の情報を表示します。</p>	<p>VNF は、VNF ライフサイクルの次の運用ステータスに基づいて特定の色で表示されます。</p> <ul style="list-style-type: none"> • 緑: VNF は正常に展開され、正常に起動されています。 • 赤: VNF の展開またはその他の操作が失敗するか、VNF が停止しています。 • 黄色: VNF はある状態から別の状態に移行中です。

右側のペインには、以下が表示されます。

- フィルタ基準
- すべての VNF または VM に関する情報を一覧表示する VNF テーブル。デフォルトでは、最初の 6 つの VNF が選択されています。SR-IOV が有効な NIC および OVS スイッチに接続された VNIC のネットワーク使用率チャートが表示されます。

図 10: VNF 情報



チェックボックスをオンにすると選択した VNF の情報がグラフィック表示にプロットされます。

- 左側のチェックボックスをクリックして、VNF を選択または選択解除します。一度に最大 6 つの VNF の情報を選択して表示できます。

- 列のソート順を変更するには、列のタイトルをクリックします。

Cloud OnRamp Colocation クラスターのモニター

表 25: 機能の履歴

機能名	リリース情報	説明
ネットワーク アシュアランス-VNF: 停止/開始/再起動	Cisco IOS XE Catalyst SD-WAN リ リース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、[Colocation Cluster] タブから Cisco CSP デバイスの VNF を停止、開始、または再起動できます。Cisco SD-WAN Manager を使用して VNF の操作を簡単に実行できます。

クラスタ情報とその正常性状態を表示できます。この情報を確認すると、サービスチェーン内の各 VNF をホストする Cisco CSP デバイスを判断するのに役立ちます。クラスタに関する情報を表示するには、次の手順を実行します。

手順

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。

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

ステップ 2 クラスタを監視するには、**[Colocation Cluster]** をクリックします。

Cisco vManage リリース 20.6.1 以前: **[Colocation Clusters]** をクリックします。

関連する情報を保有するすべてのクラスタが表形式で表示されます。クラスタ名をクリックします。**[Config View]** および **[Port Level View]** をクリックすると、クラスタを監視できます。

- **[Config View]**: ウィンドウの主要部分に、クラスタを形成する CSP デバイスとスイッチデバイスが表示されます。右側のペインでは、コロケーションサイズに基づいて、使用可能な CPU リソースと合計 CPU リソース、使用可能メモリと割り当て済みメモリなどのクラスタ情報を表示できます。

ウィンドウの詳細部分には以下が含まれます。

- 検索: 検索結果をフィルタリングするには、検索バーの **[Filter]** オプションを使用します。
- クラスタ内のすべてのデバイス (Cisco CSP デバイス、PNF、およびスイッチ) に関する情報を一覧表示する表。

Cisco CSP デバイスをクリックします。VNF 情報が表形式で表示されます。この表には、VNF 名、サービスチェーン、CPU の数、メモリ消費量、およびネットワーク サービスチェーンのパフォー

マンスを定義するその他のコアパラメータなどの情報が含まれています。 [VNFに関する情報の表示 \(75 ページ\)](#) を参照してください。

VNFを開始、停止、またはリブートするには、目的のVNFの[...]をクリックし、次のいずれかの操作を選択します。

- [Start]
- [Stop]
- [Restart]

(注) サービスチェーンのいずれかのVNFで開始、停止、再開の操作を実行する前に、サービスチェーンのプロビジョニングが完了し、VMが展開されていることを確認します。

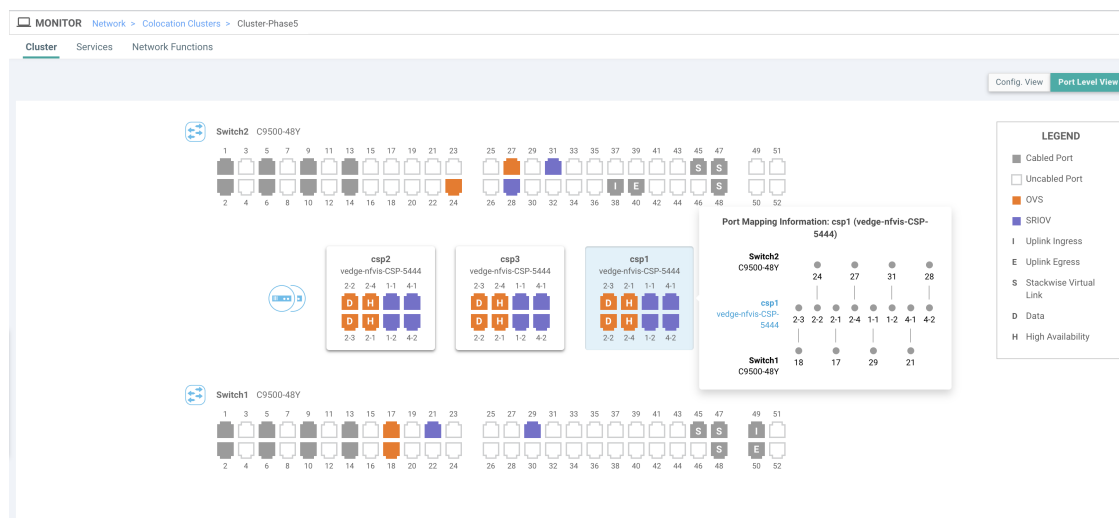
VNFで操作を選択したら、操作が完了するまで待ってから、別の操作を実行します。[Task View] ウィンドウから操作の進行状況を表示できます。

- [Port Level View] : クラスターをアクティブ化した後、ポート接続の詳細を表示するには、[Port Level View] をクリックします。

スイッチとCSPデバイスの詳細なポート接続情報を、SR-IOVおよびOVSモードに基づいて色分けされた形式で表示できます。

Catalyst 9500スイッチとCSPデバイス間のポートのマッピングを表示するには、CSPデバイスをクリックするか、カーソルを合わせます。

図 11: クラスターのポート接続の詳細の監視



ステップ 3 [Services] をクリックします。

ここでは、次の情報を表示できます。

- サービスチェーンの完全な情報。最初の 2 列には、サービスグループ内のサービスチェーンの名前と説明が表示され、残りの列には、VNF、PNF ステータス、モニタリングサービスイネーブルメント、およびサービスチェーンの全体的な正常性が表示されます。サービスチェーンに関連付けられたコロ

セッションユーザーグループを表示することもできます。さまざまな正常性ステータスとその表現は次のとおりです。

- **Healthy** : 緑の上向き矢印。すべての VNF、PNF デバイスが実行されていて、正常な状態の場合、サービスチェーンは「Healthy」状態になります。ルーティングとポリシーが正しく構成されていることを確認してください。
- **Unhealthy** : 赤の下向き矢印。VNF または PNF の 1 つが異常な状態にある場合、サービスチェーンは「Unhealthy」状態であると報告されます。たとえば、サービスチェーンを展開した後、ネットワーク機能の IP アドレスの 1 つが WAN または LAN 側で変更された場合、またはファイアウォールポリシーがトラフィックを通過させるように構成されていない場合、異常な状態が報告されます。これは、ネットワーク機能またはサービスチェーン全体が異常であるか、両方が異常な状態にあるためです。
- **Undetermined** : 黄色の下向き矢印。この状態は、サービスチェーンの正常性を判断できない場合に報告されます。この状態は、一定期間にわたって監視対象のサービスチェーンで正常または異常などの使用可能なステータスがない場合にも報告されます。ステータスが未確定のサービスチェーンをクエリまたは検索することはできません。

サービスチェーンが 1 つの PNF で構成されていて、PNF が Cisco SD-WAN Manager の到達可能範囲外にある場合は、モニターできません。サービスチェーンが単一のネットワーク機能で構成されている場合、ファイアウォールの両側に VPN 終端があり、監視できない場合は、Undetermined として報告されます。

(注) サービスチェーンのステータスが未確定の場合、サービスチェーンを選択して詳細な監視情報を表示することはできません。

- 監視フィールドを有効にしてサービスチェーンを構成した場合は、Healthy または Unhealthy 状態のサービスグループをクリックします。サービスチェーンの監視ウィンドウの主要な部分には、次の要素が含まれています。

サービスチェーン、VNF、PNF の遅延情報をプロットするグラフィック表示。

サービスチェーンの監視ウィンドウの詳細部分には、以下が含まれます。

- 検索 : 検索結果をフィルタリングするには、検索バーの [Filter] オプションを使用します。
- すべてのサービスチェーン、VNF、PNF、それらの正常性ステータス、およびタイプに関する情報を一覧表示する表。
 - 選択するサービスチェーン、VNF、PNF のサービスチェーン、VNF、PNF チェックボックスをオンにします。
 - 列のソート順を変更するには、列のタイトルをクリックします。

ステータスの詳細列は、監視対象のデータパスを示し、ホップごとの分析を提供します。

- [Diagram] をクリックして、サービスグループおよびすべてのサービスチェーンと VNF をデザインビューウィンドウに表示します。

- VNF をクリックすると、VNF に割り当てられた CPU、メモリ、およびディスクがダイアログボックスに表示されます。
- [Service Group] ドロップダウンリストからサービスグループを選択します。デザインビューには、選択したサービスグループと一緒にすべてのサービスチェーンと VNF が表示されます。

ステップ 4 [Network Functions] をクリックします。

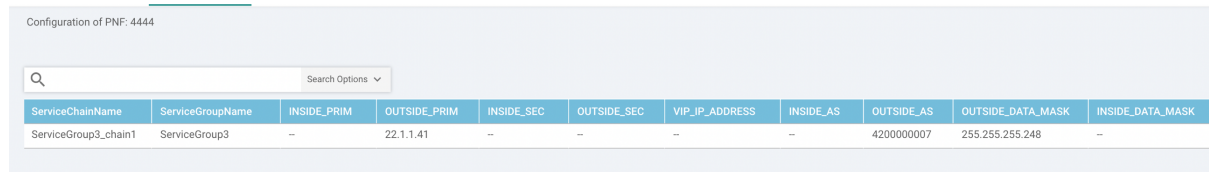
ここでは、次の情報を表示できます。

- 表形式のすべての仮想または物理ネットワーク機能。[Show] ボタンを使用して、VNF または PNF を選択して表示します。

VNF 情報が表形式で表示されます。この表には、VNF 名、サービスチェーン、コロケーションユーザーグループ、CPU 使用率、メモリ消費量などの情報、およびネットワークサービスのパフォーマンスを明確に示すその他の主要パラメータが記載されています。VNF の詳細を表示するには、VNF 名をクリックします。[VNF に関する情報の表示 \(75 ページ\)](#) を参照してください。

- PNF 情報が表形式で表示されます。この表には、シリアル番号や PNF タイプなどの情報が含まれています。特定の PNF の構成を表示してメモするには、目的の PNF シリアル番号をクリックします。PNF のすべての構成を手動でメモしてから、PNF デバイスを構成するようにしてください。たとえば、サービスチェーンのさまざまな場所に PNF を配置する PNF 構成の一部を次に示します。PNF を手動で設定するには、「[ASR 1000 Series Aggregation Services Routers Configuration Guides](#)」および「[Cisco Firepower Threat Defense Configuration Guides](#)」を参照してください。

図 12: サービスチェーン側のパラメータを持つ最初の位置にある PNF



ServiceChainName	ServiceGroupName	INSIDE_PRIM	OUTSIDE_PRIM	INSIDE_SEC	OUTSIDE_SEC	VIP_IP_ADDRESS	INSIDE_AS	OUTSIDE_AS	OUTSIDE_DATA_MASK	INSIDE_DATA_MASK
ServiceGroup3_chain1	ServiceGroup3	--	22.1.1.41	--	--	--	--	4200000007	255.255.255.248	--

図 13: 外部ネイバー情報を持つ最初の位置にある PNF



OUTSIDE_AS	OUTSIDE_DATA_MASK	INSIDE_DATA_MASK	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_SEC	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_SEC
4200000007	255.255.255.248	--	--	--	22.1.1.43	22.1.1.44	22.1.1.43	22.1.1.44

図 14: 2つのサービスチェーンで共有される PNF

ServiceGroup2_chain3 は PNF のみのサービスチェーンであるため、構成は生成されません。PNF は ServiceGroup2_chain1 の最後の位置にあるため、INSIDE 変数のみが生成されます。

Configuration of PNF: 33334

Search Options

ServiceChainName	ServiceGroupName	INSIDE_PRIM	OUTSIDE_PRIM	INSIDE_SEC	OUTSIDE_SEC	VIP_IP_ADDRESS	INSIDE_AS	OUTSIDE_AS	OUTSIDE_DATA_MA
ServiceGroup2_chain3	ServiceGroup2	--	--	--	--	--	--	--	--
ServiceGroup2_chain1	ServiceGroup2	22.1.1.27	--	--	--	--	4200000002	--	--

図 15: 外部ネイバー情報を持つ 2 つのサービスチェーン間で共有される PNF

Configuration of PNF: 33334

Search Options

OUTSIDE_AS	OUTSIDE_DATA_MASK	INSIDE_DATA_MASK	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_SEC	INSIDE_VLAN
--	--	--	--	--	--	--	[1830]
12	--	255.255.255.248	22.1.1.25	--	--	--	[1032]

Cloud OnRamp Colocation クラスタの packets キャプチャ

表 26: 機能の履歴

機能名	リリース情報	説明
Cloud OnRamp Colocation クラスタの packets キャプチャ	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	<p>この機能を使用すると、コロケーションクラスタの Cloud Services Platform (CSP) デバイスで、物理ネットワークインターフェイスカード (PNIC) レベルまたは仮想ネットワーク インターフェイスカード (VNIC) レベルで packets をキャプチャできます。同じデバイスの 1 つ以上の PNIC または VNIC で packets をキャプチャすることも、異なるブラウザを使用する異なるデバイスで同時に packets をキャプチャすることもできます。この機能により、packets の形式に関する情報を収集し、アプリケーションの分析、セキュリティ、トラブルシューティングに役立てることができます。</p>

コロケーションクラスターの CSP デバイスとの間で送受信されるパケットをキャプチャできます。CSP デバイスの PNIC または VNIC レベルでパケットをキャプチャできます。

Cloud OnRamp Colocation クラスターのパケットキャプチャでサポートされるポート

パケットキャプチャは、次のポートでサポートされています。

表 27: パケットキャプチャでサポートされるポート

モード	VNIC レベル	PNIC レベル
シングルテナント	OVS-DPDK、HA-OVS-DPDK、SR-IOV、OVS-MGMT	SR-IOV、MGMT
マルチテナント（ロールベース アクセス コントロール）	OVS-DPDK、HA-OVS-DPDK、OVS-MGMT	MGMT

Cisco SD-WAN Manager でパケットキャプチャを有効にする

コロケーションクラスターの CSP デバイスで PNIC または VNIC レベルでパケットをキャプチャする前に、Cisco SD-WAN Manager でパケットキャプチャ機能を有効にします。

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** を選択します。
2. **[Data Stream]** で、**[Enabled]** を選択します。

Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、トグルボタンをクリックしてデータストリームを有効にします。

PNIC レベルでパケットをキャプチャする

1. Cisco SD-WAN Manager メニューから**[Monitor]** > **[Devices]**の順に選択します。
2. **[Colocation Cluster]** をクリックし、クラスターを選択します。
3. 表示されるデバイスのリストから、CSP デバイス名をクリックします。
4. 左側のペインで、**[Packet Capture]** をクリックします。
5. **[PNIC ID]** ドロップダウンリストから、PNIC を選択します。
6. （オプション）**[Traffic Filter]** をクリックして、キャプチャするパケットを IP ヘッダーの値に基づいてフィルタ処理します。

表 28: パケットキャプチャフィルタ

フィールド	説明
Source IP	パケットの送信元 IP アドレス。
Source Port	パケットの送信元ポート番号。

フィールド	説明
Protocol	パケットのプロトコル ID。 サポートされているプロトコルは、ICMP、IGMP、TCP、UDP、ESP、AH、ICMP バージョン 6 (ICMPv6)、IGRP、PIM、および VRRP です。
Destination IP	パケットの宛先 IP アドレス。
Destination Port	パケットの宛先ポート番号。

7. [Start] をクリックします。

パケットキャプチャが開始され、その進行状況が表示されます。

- **Preparing file to download** : ファイルサイズが 20 MB に達した後、またはパケットキャプチャを開始してから 5 分後、または [Stop] をクリックすると、パケットキャプチャが停止します。
- **Preparing file to download** : Cisco SD-WAN Manager は libpcap 形式のファイル (.pcap ファイル) を作成します。
- 「File ready, click to download the file」 : ダウンロードアイコンをクリックして、生成されたファイルをダウンロードします。

VNIC レベルでパケットをキャプチャする

1. Cisco SD-WAN Manager メニューから **[Monitor]** > **[Devices]** の順に選択します。
2. **[Colocation Cluster]** をクリックし、クラスタを選択します。
3. 表示されるデバイスのリストから、CSP デバイス名をクリックします。
4. VNF を選択し、左側のペインで **[Packet Capture]** をクリックします。
5. または、**[Monitor]** > **[Devices]** > **[Colocation Cluster]** を選択します。次に、クラスタを選択して **[Network Functions]** をクリックし、VNF を選択してから、左側のペインで **[Packet Capture]** をクリックします。
6. **[VNIC ID]** ドロップダウンリストから、VNIC を選択します。
7. (オプション) **[Traffic Filter]** をクリックして、IP ヘッダーの値に基づいてキャプチャするパケットをフィルタ処理します。これらのフィルタの詳細については、上記のセクションを参照してください。
8. **[Start]** をクリックします。パケットキャプチャが開始され、進行状況が表示されます。

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation マルチテナント機能



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

表 29: 機能の履歴

機能名	リリース情報	説明
ロールベースのアクセス制御を使用したコロケーション マルチテナント機能	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、サービスプロバイダーは複数のコロケーションクラスタを管理し、複数のコロケーショングループを使用してこれらのクラスタをテナント間で共有できます。マルチテナント設定では、サービスプロバイダーはテナントごとに一意のコロケーションクラスタを展開する必要はありません。代わりに、コロケーションクラスタのハードウェアリソースは複数のテナント間で共有されます。マルチテナント機能では、サービスプロバイダーは、個々のテナントユーザーの役割に基づいてアクセスを制限することにより、テナントが自分のデータのみを表示できるようにします。

コロケーション マルチテナント機能の概要

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation マルチテナント機能では、サービスプロバイダーはシングルテナントモードで Cisco SD-WAN Manager を使用して複数のコロケーションクラスタを管理できます。サービスプロバイダーは、シングルテナントモードでクラスタを起動するのと同じ方法でマルチテナントクラスタを起動できます。マルチテナントクラスタは、複数のテナント間で共有できます。「[Create and Activate Clusters](#)」を参照してください。

テナントは、コロケーションクラスタの Cisco Cloud Services Platform (CSP) デバイスや Cisco Catalyst 9500 デバイスなどのハードウェアリソースを共有します。この機能の重要なポイントは次のとおりです。

- サービスプロバイダーは、有効な証明書を使用して Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager、Cisco Catalyst SD-WAN Validator、および Cisco Catalyst SD-WAN コントローラ）を展開および設定します。
- サービスプロバイダーは、Cisco CSP デバイスと Cisco Catalyst 9500 スイッチをオンボードした後、コロケーションクラスタをセットアップします。
- Cisco Catalyst SD-WAN はシングルテナントモードで動作し、Cisco SD-WAN Manager はシングルテナントモードで表示されます。
- コロケーションマルチテナント展開では、サービスプロバイダーは、ロールを作成することにより、テナントがサービスチェーンのみを参照できるようにします。サービスプロバイダーは、コロケーショングループ内の各テナントのロールを作成します。これらのテナントは、ロールに基づいてサービスチェーンにアクセスして監視することが許可されています。ただし、サービスチェーンを構成したり、システムレベルの設定を変更したりすることはできません。ロールにより、テナントは表示が許可されている情報のみにアクセスできるようになります。
- 各テナントトラフィックは、コンピューティングデバイス全体で VXLAN を使用してセグメント化され、Cisco Catalyst スイッチファブリック全体で VLAN を使用してセグメント化されます。
- サービスプロバイダーは、特定のクラスタにサービスチェーンをプロビジョニングできません。

コロケーション マルチテナント セットアップの 2 つのシナリオを以下に示します。

- サービスプロバイダーが所有する Cisco Catalyst SD-WAN デバイス：このシナリオでは、サービスチェーンで使用される Cisco Catalyst SD-WAN デバイスは、対応するサービスプロバイダーに属します。CSP デバイスと Catalyst 9500 スイッチは、サービスプロバイダーが所有、監視、保守します。仮想マシン（VM）パッケージは、サービスプロバイダーが所有、アップロード、および保守します。『[共同管理されたマルチテナント環境でのコロケーションクラスタ デバイスと Cisco Catalyst SD-WAN デバイスのモニター（94 ページ）](#)』を参照してください。
- 共同管理された Cisco Catalyst SD-WAN デバイス：このシナリオでは、サービスチェーンで使用される Cisco Catalyst SD-WAN デバイスはテナント オーバーレイ ネットワークに属します。コロケーションクラスタ デバイスはサービスプロバイダーが所有しますが、サービスチェーンの Cisco Catalyst SD-WAN はテナントの Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager、Cisco Catalyst SD-WAN Validator、および Cisco Catalyst SD-WAN コントローラ）によって制御されます。CSP デバイスと Catalyst 9500 スイッチは、サービスプロバイダーが所有、監視、保守します。VM パッケージは、サービスプロバイダーが所有、アップロード、および保守します。[共同管理されたマルチテナント環境でのコロケーションクラスタ デバイスと Cisco Catalyst SD-WAN デバイスのモニター（94 ページ）](#)を参照してください。

マルチテナント環境での役割と機能

マルチテナント環境には、サービスプロバイダーと複数のテナントが含まれます。各ロールには、明確な責任と関連する機能があります。

サービス プロバイダ

サービスプロバイダーは、すべてのハードウェアインフラストラクチャを所有し、クラスタを管理します。また、サービスプロバイダーは、ロールを作成してテナントをオンボーディングし、テナントのサービスチェーンをプロビジョニングし、すべてのテナントのすべてのサービスチェーンを表示できます。

サービスプロバイダーは、**管理ユーザー**または**管理ユーザー権限**の書き込み権限を持つユーザーとして **Cisco SD-WAN Manager** にログインします。サービスプロバイダーは、**Cisco SD-WAN Manager** サーバーからユーザーおよびユーザーグループを追加、編集、または削除でき、通常は次のアクティビティを担当します。

- テナントのクラスタを作成および管理します。
- 事前にパッケージ化された VM イメージパッケージと Cisco Enterprise NFV インフラストラクチャ ソフトウェア (NFVIS) ソフトウェアイメージを CSP デバイスにアップロードします。
- カスタムのコロケーショングループとロールベースのアクセス制御 (RBAC) ユーザーを作成します。
- サービスグループを作成し、コロケーショングループを複数のサービスグループに関連付けます。
- CSP デバイスと Catalyst 9500 スイッチをアップグレードします。
- すべてのテナントのサービスチェーンと VM を監視します。
- テナントの仮想ネットワーク機能 (VNF) のいずれかで操作を開始、停止、または再開します。
- Cisco SD-WAN Manager を管理し、Cisco Catalyst SD-WAN デバイスのシステム全体のログを記録します。

テナント

テナントは、自分自身に属するサービスチェーンの VNF で操作を開始できますが、別のテナントに属するサービスチェーンの VNF で表示、アクセス、または操作を開始することはできません。テナントは、以下のアクティビティを担当します。

- すべてのサービスグループと、テナントに属するサービスチェーンの正常性ステータスを監視します。
- テナントに属するサービスチェーンの一部である VNF のイベントまたはアラームを監視します。
- テナントに属するサービスチェーンの一部である VNF で、開始、停止、または再起動の操作を開始します。

- クラスタ、サービスチェーン、または VNF に問題がある場合は、対応するサービスプロバイダーと協力します。

マルチテナント環境での推奨仕様

サービスプロバイダーは、次の情報を使用して、テナント、クラスタ、テナントごとのサービスチェーン、およびさまざまなコロケーションサイズの VLAN 数を決定することをお勧めします。

表 30: マルチテナント環境の仕様

テナント	クラスタ (CPU)	テナントあたりのサービスチェーン (CPU)	VLAN
150	2 (608)	1 (4) : 小	~ 300
75 ~ 150	2 (608)	2 ~ 3 (4 ~ 8) : 中	300 ~ 450
25 ~ 50	2 (608)	4 ~ 6 (12 ~ 24) : 大	~ 400
300	4 (1216)	小	~ 600
150 ~ 300	4 (1216)	中	600 ~ 900
50 ~ 100	4 (1216)	大	~ 800
600	8 (2432)	小	~ 1200
300 ~ 600	8 (2432)	中	900 ~ 1200
100 ~ 200	8 (2432)	大	~ 1050
750	10 (3040)	小	~ 1500
375 ~ 750	10 (3040)	中	600 ~ 1500
125 ~ 230	10 (3040)	大	~ 1250

たとえば、サービスプロバイダーが、1つの VM で構成されるサービスチェーンのテナントごとに4つの vCPU をプロビジョニングする場合、サービスプロバイダーは、8つの CSP デバイスを備えた2つのクラスタで約150のテナントをオンボードできます。これらの各テナントまたはサービスチェーンには、サービスチェーンごとに300のハンドオフ VLAN、1つの入力 VLAN、および1つの出力 VLAN が必要です。

コロケーション マルチテナント機能の前提条件と制限事項

次のセクションでは、コロケーションマルチテナント環境での前提条件と制限事項について詳しく説明します。

前提条件

- Cisco CSP デバイスと Cisco Catalyst 9500 スイッチ間の配線は、規範的接続またはフレキシブルなトポロジに従って完了します。複数のクラスタを起動するには、クラスタの CSP デバイスと Catalyst 9500 スイッチ間の配線が単一のクラスタと同じであることを確認してください。配線の詳細については、「[Wiring Requirements](#)」を参照してください。
- 各 Cisco CSP デバイスには、アウトオブバンド (OOB) 管理スイッチへのポートチャンネルとして手動で構成された 2 つの 1 GB 管理ポートがあります。
- テナントは、所有するサービスチェーンの一部である VNF の [Monitor] ウィンドウからイベントまたはアラームを監視のみできます。テナント監視ウィンドウには、テナントがサービスチェーンを表示しているときに、対応するコロケーショングループが表示されません。



- (注) 共同管理されたマルチテナントセットアップでは、サービスプロバイダーはテナントから必要な情報を収集することにより、テナントのサービスチェーンをプロビジョニングします。たとえば、テナントは、テナント組織名、テナント Cisco SD-WAN Validator IP アドレス、テナントサイト ID、システム IP アドレスなどをアウトオブバンドで提供します。[サービスグループでのサービスチェーンの作成 \(37 ページ\)](#) を参照してください。

制約事項

- シングルテナントモードからマルチテナントモードへのコロケーションクラスタの変更、およびその逆の変更はサポートされていません。
- 複数のテナント間での VNF デバイスの共有はサポートされていません。
- サービスプロバイダーは、テナントに対して複数のサービスグループをプロビジョニングできます。ただし、同じサービスグループを複数のテナントにプロビジョニングすることはできません。
- シングルテナントモードの Cisco Catalyst SD-WAN Cloud OnRamp for Colocation リリース 20.4.1 から、マルチテナントモードのリリース 20.5.1 以降へのアップグレードはサポートされていません。この制限は、シングルテナントモードからマルチテナントモードにアップグレードできないことを意味します。
- シングルルート IO 仮想化対応 (SR-IOV 対応) の物理ネットワーク インターフェイスカード (PNIC) のマルチテナント機能はサポートされていません。VNF VNIC のオープン仮想

スイッチ (OVS) のみがサポートされています。現在の SR-IOV ドライバは VXLAN をサポートしていないため、CSP デバイスのすべての PNIC は OVS モードです。VNF VNIC は OVS ネットワークに接続されていて、必要な速度でトラフィックを転送する機能が低下する可能性があります。

- テナントが使用するリソースの課金とサブスクリプションの管理はサポートされていません。
- 共同管理されたマルチテナントセットアップでは、テナントは、テナントが所有する VNF デバイスのみを監視できます。

サービスプロバイダー機能

新しいテナントのプロビジョニング

サービスプロバイダーは、コロケーショングループを作成して新しいテナントをプロビジョニングし、コロケーショングループに関連付けられたユーザーグループの RBAC ユーザーを作成してテナントへのアクセスを提供できます。RBAC ユーザーは、独自のテナント環境内で制限付きの管理業務を実行できます。

始める前に

サービスプロバイダーは、CSP デバイスとの制御接続を確立し、クラスタをアクティブ化することにより、クラスタを共有モードで起動する必要があります。サービスプロバイダーは複数のクラスタを作成でき、これらの各クラスタには 2 ~ 8 台の CSP デバイスと 2 台の Catalyst 9500 スイッチを含めることができます。クラスタ作成操作では、クラスタがマルチテナント展開またはシングルテナント展開のどちらであるかを選択するオプションがサポートされています。「[Create and Activate Clusters](#)」を参照してください。

手順

ステップ 1 テナントをオンボーディングするには、コロケーショングループを作成します。詳細については、「[Create Colocation Group](#)」を参照してください。このグループは、テナントのサービスグループと VM を監視するためのアクセスをテナントに提供します。

ステップ 2 RBAC ユーザーを追加し、ステップ 1 で作成したコロケーショングループに関連付けます。詳細については、「[Create an RBAC User and Associate to Colocation Group](#)」を参照してください。

(注) Cisco SD-WAN Manager の代わりに TACACS サーバーを使用してユーザーを認証している場合は、RBAC ユーザーを追加しないでください。TACACS サーバーを使用してユーザーを認証している場合は、ユーザーをステップ 1 で作成したコロケーショングループに関連付けます。

ステップ 3 サービスグループを作成し、それをコロケーショングループに関連付け、サービスグループを特定のクラスタに接続します。「[Create Service Chain in a Service Group](#)」を参照してください。

テナントが新しいサービスチェーンを必要とする場合は、テナントに固有のハンドオフ VLAN を使用します。

コロケーショングループの作成

シングルテナント Cisco SD-WAN Manager では、コロケーショングループを使用して、複数のテナント間でコロケーションクラスタを共有できます。コロケーショングループは、サービスチェーンを特定のテナントに関連付けるメカニズムです。テナント用に作成された RBAC ユーザーは、コロケーショングループと呼ばれます。これらのユーザーは、ログイン情報を使用して Cisco SD-WAN Manager にログインし、テナント固有のサービスチェーンと VNF 情報のみを表示できます。サービスプロバイダーがテナントにサービスグループを使用することを選択した場合、コロケーショングループをサービスグループに関連付けることができるように、サービスグループを作成する前にコロケーショングループを作成する必要があります。

手順

ステップ 1 Cisco SD-WAN Manager のメニューで、**[Administration] > [Colo Groups]** を選択します。

ステップ 2 **[Add Colo Group]** をクリックします。

ステップ 3 コロケーショングループ名、コロケーショングループを関連付ける必要があるユーザーグループの名前、および説明を入力します。

(注) ここで指定するコロケーショングループ名は、マルチテナント設定のサービスグループを作成するときに表示されます。

ステップ 4 **[Add]** をクリックします。

ユーザーグループの権限の表示

手順

ステップ 1 Cisco SD-WAN Manager メニューから **[Administration] > [Manage Users]** を選択します。

ステップ 2 **[User Groups]** をクリックします。

ステップ 3 ユーザーグループの権限を表示するには、**[Group Name]** リストで、作成したユーザーグループの名前をクリックします。

(注) ユーザーグループとその権限が表示されます。マルチテナント環境でのユーザーグループの権限のリストについては、『Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide』の「[Manage Users](#)」のトピックを参照してください。

RBAC ユーザーの作成とコロケーショングループへの関連付け

手順

-
- ステップ 1** Cisco SD-WAN Manager メニューから **[Administration] > [Manage Users]** を選択します。
- ステップ 2** **[Add User]** をクリックします。
- ステップ 3** **[Add User]** ダイアログボックスに、ユーザーのフルネーム、ユーザー名、パスワードを入力します。
- (注) ユーザー名に大文字を入力することはできません。

ステップ 4 **[User Groups]** ドロップダウンリストから、ユーザーが属する必要のあるグループを追加します。たとえば、コロケーション機能用に作成したユーザーグループなど、グループを 1 つずつ選択します。デフォルトでは、リソースグループ **[global]** が選択されています。

ステップ 5 **[Add]** をクリックします。

Cisco SD-WAN Manager では **[Users]** テーブルにあるユーザーが一覧表示されるようになりました。

- (注) テナントまたはコロケーショングループ用に作成された RBAC ユーザーは、ログイン情報を使用して Cisco SD-WAN Manager にログインできます。これらのユーザーは、テナントに関連付けられたサービスグループがクラスタにアタッチされた後、テナント固有のサービスチェーンと VNF 情報を表示できます。

コロケーション ユーザー グループからの RBAC ユーザーの削除

RBAC ユーザーを削除するには、ユーザーが Cisco SD-WAN Manager を使用して設定されている場合、コロケーショングループから RBAC ユーザーを削除します。ユーザーが TACACS サーバーを使用して認証されている場合は、TACACS サーバーのユーザーグループからユーザーの関連付けを解除します。

RBAC ユーザーが削除されると、そのユーザーはクラスタのデバイスにアクセスしたり、デバイスを監視したりできなくなります。RBAC ユーザーが Cisco SD-WAN Manager にログインしている場合、ユーザーを削除しても RBAC ユーザーはログアウトされません。

手順

-
- ステップ 1** Cisco SD-WAN Manager メニューから **[Administration] > [Manage Users]** を選択します。
- ステップ 2** 削除する RBAC ユーザーをクリックします。
- ステップ 3** 削除する RBAC ユーザーの **[...]** をクリックし、**[Delete]** を選択します。
- ステップ 4** **[OK]** をクリックして RBAC ユーザーの削除を確認します。
-

テナントの削除

テナントを削除するには、テナントに関連付けられているサービスグループを削除してから、テナントのコロケーショングループを削除します。

手順

ステップ 1 削除するテナントに関連付けられているサービスグループのリストを見つけます。「[View Service Groups](#)」を参照してください。

(注) テナントは、同じコロケーショングループに関連付けられた1つ以上のRBACユーザーを持つコロケーショングループです。サービスグループの構成ページでは、テナントのコロケーショングループを表示できます。

ステップ 2 削除したいテナントのクラスタからサービスグループを切り離します。『[クラスタ内のサービスグループの接続または切断 \(56 ページ\)](#)』を参照してください。

(注) サービスグループを別のテナントに再利用する場合は、サービスグループに関連付けられているコロケーショングループを変更します。サービスグループを削除した場合は、再作成する必要があります。

ステップ 3 テナントのコロケーショングループを削除します。『[Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide](#)』の「[Manage a User Group](#)」トピックを参照してください。

テナントコロケーションクラスタの管理

サービスプロバイダーは、次の管理タスクを実行できます。

- クラスタのアクティブ化：サービスプロバイダーは、デバイス、リソースプール、システム設定を構成し、マルチテナントモードまたは共有モードでクラスタをアクティブ化できます。「[Create and Activate Clusters](#)」を参照してください。
- サービスグループを作成し、RBACユーザーをコロケーショングループに関連付ける：サービスプロバイダーは、コロケーショングループを作成し、RBACユーザーをコロケーショングループに関連付け、サービスグループを作成し、サービスグループをマルチテナントモードのコロケーショングループに関連付け、サービスグループを特定のクラスタに接続できます。「[Create Service Chain in a Service Group](#)」を参照してください。



(注) サービスプロバイダーは、テナントごとに特定のサービスグループを関連付ける必要があります。

- VMパッケージの作成：サービスプロバイダーは、VMパッケージを作成してCisco SD-WAN Manager リポジトリにアップロードできます。同じパッケージを使用して、複数のテナントのサービスチェーンにVNFをプロビジョニングできます。



(注) サービスグループがコロケーショングループに関連付けられている場合、VNF の構成に使用される VM パッケージ作成の SR-IOV オプションは無視されます。マルチテナントモードでは、VNF パッケージは VXLAN を使用した OVS-DPDK のみをサポートします。

- サービスチェーンとテナントの VNF を監視する：サービスプロバイダーは、すべてのテナントサービスチェーンを監視し、これらのサービスチェーンに関連付けられているテナントとともに、正常でないサービスチェーンを特定できます。サービスプロバイダーは、Cisco SD-WAN Manager または CSP デバイスからログを収集し、テナントに通知することもできます。
- Cisco CSP デバイスの追加と削除：サービスプロバイダーは、コロケーションクラスタを管理するために、CSP デバイスを追加または削除できます。

テナント機能

テナントとしてのコロケーションクラスタの管理

すべてのテナントは、サービスチェーンとサービスチェーンに関連付けられている VM を監視し、サービスチェーンで正常性の問題が発生した場合はサービスプロバイダーと協力する必要があります。テナントは、テナントに属するサービスチェーンの一部である VNF のイベントまたはアラームのみを監視できます。

テナントには管理者権限がなく、サービスプロバイダーが作成するサービスチェーンのみを表示できます。テナント監視ウィンドウには、テナントがサービスチェーンを表示しているときに、対応するコロケーショングループが表示されます。テナントは、次のタスクを実行できます。

1. RBAC ユーザー名とパスワードを入力してテナントとして Cisco SD-WAN Manager にログインします。
2. VNF の正常性ととも、テナントサービスチェーンの正常性を表示および監視します。さまざまなサービスチェーンの正常性ステータスの詳細については、[Cloud OnRamp Colocation クラスタのモニター \(77 ページ\)](#) を参照してください。

[Monitor.Network] ウィンドウで、サービスチェーンの [Diagram] をクリックして、すべてのテナントサービスグループとサービスチェーンと VNF をデザインビューに表示します。

3. テナントの VNF 正常性を表示します。
 1. [Monitor] ウィンドウで、[Network Functions] をクリックします。
 2. [Virtual NF] テーブルから VNF 名をクリックします。

左側のペインで、[CPU Utilization]、[Memory Utilization]、および [Disk Utilization] をクリックして、VNF のリソース使用率を監視します。

左ペインから VM 固有のアラームとイベントを表示することもできます。

4. VNF を開始、停止、またはリブートします。
 1. [Monitor] ウィンドウで、[Virtual NF] テーブルから VNF 名をクリックします。
 2. クリックした VNF 名について、[...] をクリックし、次のいずれかの操作を選択します。
 - [Start]
 - [Stop]
 - [Restart]

共同管理されたマルチテナント環境でのコロケーションクラスタ デバイスと Cisco Catalyst SD-WAN デバイスのモニター

始める前に

- サービスプロバイダー Cisco SD-WAN Manager を使用してサービスチェーンを作成する場合、サービスプロバイダーは、サービスチェーン内の Cisco Catalyst SD-WAN VM の正しい UUID とデバイス OTP が入力されていることを確認する必要があります。サービスプロバイダーはテナントオーバーレイにアクセスできないため、テナントはこの情報を提供する必要があります。
- サービスプロバイダーがサービスグループをコロケーションクラスタから切り離す場合、サービスプロバイダーは、テナント Cisco SD-WAN Manager を使用して対応する VM デバイスをデコミッションする必要があることをテナントに通知する必要があります。
- サービスプロバイダーがサービスグループをコロケーションクラスタに再アタッチする必要がある場合は、Cisco Catalyst SD-WAN VM の新しい OTP を入力する必要があります。この OTP はテナントによって提供されます。サービスプロバイダー Cisco SD-WAN Manager のサービスグループを編集して、Cisco SD-WAN VM の新しい OTP を保存する必要があります。

手順

-
- ステップ 1 サービスチェーンを作成するときに、テナントの Cisco Catalyst SD-WAN デバイスをサービスプロバイダーのサービスグループに関連付けます。「[Create Service Chain in a Service Group](#)」を参照してください。
 - ステップ 2 サービスプロバイダー Cisco SD-WAN Manager からの VNF を監視します。「[Monitor Cloud OnRamp Colocation Clusters](#)」を参照してください。

ステップ 3 テナント Cisco SD-WAN Manager からの VNF の Cisco Catalyst SD-WAN デバイスに関する情報をモニターします。

(注) サービスプロバイダーは、VNF の Cisco Catalyst SD-WAN デバイスに関する情報をサービスプロバイダーの **[Configuration] > [Devices]** ウィンドウの **[WAN Edge List]** から表示できません。これらのデバイスはテナントによって制御されているためです。

翻訳について

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