Cisco vManage を使用した Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスの設定

Cisco vManage を使用した Cloud OnRamp Colocation デバイスの追加

Cisco vManage 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 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 vManage 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 vManage IP アドレスとログイン情報、Cisco vBond IP アドレスとログイン情報などの Cisco 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

ステップ 1 [Cisco vManage] メニューから、**[Tools]** > **[SSH Terminal]**を選択して、Cisco vManage 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                                  Technology-package
Current                       Type                     Next reboot
------------------------------------------------------------------------------
network-advantage    Smart License                  network-advantage
dna-advantage        Subscription Smart License     dna-advantage
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR 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 vManage 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。

Cisco vManage からの Cloud OnRamp for Colocation デバイスの削除

Cisco vManage 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 （63 ページ）』を参照してください。
- 削除される CSP デバイスが Cisco Colo Manager をホストしている場合は、Cisco Colo Manager のリカバリを参照してください。

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

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 vManage からも構成が完全に削除されます。

Cisco vManage でのクラスタの管理

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 （6 ページ）』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 （38 ページ）』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 （63 ページ）』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

（注） 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。

（注） 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 vManage 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 vManage 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 vManage 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

クラスタの作成、クラスタのクリア、およびクラスタの削除中に、両方のスイッチの構成を消去してください。以前に使用されたスイッチ構成の消去の詳細については、Catalyst 9500 の問題のトラブルシューティングを参照してください。

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 vManage を使用して構成できます。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。

（注） 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。サービスチェーンは Mbps で構成され、最大 10 Gbps、最小 10 M を割り当てることができます。デフォルトのサービスチェーン帯域幅は 10 Mbps です。「Ordering and Sizing of Network Hub Devices」のトピックを参照してください。

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 vBond Orchestrator 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 vManage 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 vManage および Cisco vBond Orchestrator の NTP サーバーを構成していることを確認してください。NTP サーバーを構成するには、『Cisco 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。
- 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。

ステップ 1 [Cisco vManage] メニューから、Cisco vManage を選択し、**[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 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 vManage と統合されます。これらのシリアル番号は、CCW で Cisco 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 （9 ページ）を参照してください。

k) [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 vManage 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 vManage 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 （21 ページ）を参照してください。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、Cisco Colo Manager（CCM）および CSP デバイス構成タスクは、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 デバイス構成タスクは、Cisco vManage 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。

Resource Pool

表 *2:* 機能の履歴

機能名	リリース情報	説明
クラスタリソースプールの Day-N 拡張	Cisco vManage リリース 20.9.1 Cisco NFVIS リリース 4.9.1	この機能は、クラスタ状態がアクティブな場合のリソースプールパラメータの編集をサポートします。

（注） Cisco vManage リリース 20.9.1 以降では、クラスタ状態がアクティブな場合にリソースプールパラメータを編集できます。この機能は、アクティブな Day-N クラスタリソースプールの拡張のみをサポートします。IP および VLAN プールの削減はサポートされていません。VNF 管理 IP プールを除くすべての IP プールには、day-N 編集で新しいサブネットを追加できます。

[Name]、[Description]、[Management Subnet Gateway]、[Management Mask]、および [Switch PNP Server IP] フィールドは編集できません。

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、これを変更できます。

9. [Save] をクリックします。

ポート接続

表 *3:* 機能の履歴

機能名	リリース情報	説明
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 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。
入力および出力トラフィックの共通ポートチャネル	Cisco vManage リリース 20.9.1 Cisco NFVIS リリース 4.9.1	この機能により、コロケーションクラスタの作成時から、入力および出力トラフィックに共通のポートチャネルが導入されます。この機能は、接続されているすべてのメンバーリンクを 1 つのポートチャネルにまとめ、トラフィックのロードバランシングを行うことで、中断のないトラフィックフローを促進します。入力ポート番号は、単一のポートチャネルを作成するために使用されます。

入力および出力トラフィックの共通ポートチャネル

Cisco vManage リリース 20.8.1 以前のリリースでは、入力ポートチャネルと出力ポートチャネルは分離されています。入力ポートチャネルと出力ポートチャネルの両方、およびサービスチェーンに同じ VLAN を使用できます。これにより、スパニングツリープロトコル（STP）ループが発生し、ポートチャネルの 1 つがシャットダウンされ、トラフィックが中断されます。

Cisco vManage リリース 20.9.1 以降では、単一のポートチャネルが Stackwise Virtual Switch Link（SVL）スイッチの入力および出力トラフィックに使用されます。クラスタを作成してアクティブにするか、クラスタを Cisco vManage リリース 20.9.1 にアップグレードすると、Cisco Colocation Manager は 2 つのポートチャネルを 1 つのポートチャネルに自動的に結合します。クラスタのアップグレードまたはアクティブ化の後、入力と出力の両方の VLAN ハンドオフが単一のポートチャネルで構成されます。Cisco vManage でクラスタを作成するときは、引き続き入力と出力のそれぞれのポートを選択できます。この機能は、接続されているすべてのメンバーリンクを1つのポートチャネルにまとめ、トラフィックのロードバランシングを行うことで、中断のないトラフィックフローを促進します。

Cisco vManage リリース 20.9.1 へのアップグレード後、Cisco 1000 シリーズ アグリゲーション サービス ルータや Cisco Nexus 9000 シリーズ スイッチなどのデバイスのトポロジ構成を変更し、リンク アグリゲーション グループ（LAG）を使用して 4 つのリンクすべてを単一のポートチャネルにバンドルし、VLAN を適切に設定してください。Cisco vManage で入力ポートと出力ポートの両方を引き続き追加できます。ソフトウェアは、デバイスに送信する前に、それらをバックエンドで単一のポートチャネルに結合します。

次に、4 つのリンクを 1 つのポートチャネルに結合する設定例を示します。

```
switch1#show running-config int twe1/0/35

interface TwentyFiveGigE1/0/35
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end

switch1#show running-config int twe2/0/35
Building configuration...

Current configuration : 177 bytes
!
interface TwentyFiveGigE2/0/35
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end

switch1#show running-config int twe1/0/37
Building configuration...

Current configuration : 177 bytes
!
interface TwentyFiveGigE1/0/37
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end

switch1#show running-config int twe2/0/37
Building configuration...

Current configuration : 177 bytes
!
interface TwentyFiveGigE2/0/37
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end
```

Cisco vManage 画面に次の警告が表示されます。

20.9.1 以降、I & E（4 つのインターフェイス）のメンバーを持つ単一ポートチャネルが形成され、サービスチェーンの両方の入力/出力 VLAN ハンドオフで構成されます。クラスタをアクティブ化または20.9.1にアップグレードするときにネクストホップデバイス（router.switch）構成がポートチャネル構成および VLAN 構成と一致していることを確認してください。

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 vManage 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。

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 Release 20.7.x 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.x 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す。

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（CCM）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 vManage 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 *4*: 機能の履歴

機能名	リリース情報	説明
TACACS Authentication	Cisco SD-WAN リリース 20.3.1 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 （9 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 vManage 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 vManage 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 vManage にデバイスが表示されるまで待ちます。

- クラスタ内の CSP デバイスに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 vManage で、**[Tools]** > **[SSH Terminal]**の画面をクリックして、Cisco vManage 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。「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」を参照してください。

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 vManage **[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.x 以前のリリースでは、Cisco vManage **[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 デバイスのバックアップと復元の前提条件と制限事項 （32 ページ）を参照してください。

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 *5 :* 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ブ化の進行状況を監視する	Cisco SD-WAN リリース 20.1.1	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 vManage タスクビューウィンドウを使用して進行状況を監視し、[Monitoring] ページからイベントを監視できます。

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.x 以前のリリースでは、Cisco Colo Manager（CCM）が起動し、アクティブ化の進行状況が CLOUD ONRAMP CCM タスクの一部として報告されます。このタスクは、CCM 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 以降、Cisco vManage がターゲット CSP デバイスから CCM Healthy を受信すると、CLOUD ONRAMP CCM 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、CCM 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 *1*：クラスタのアクティブ化（*Cisco vManage* リリース *20.7.x* 以前）

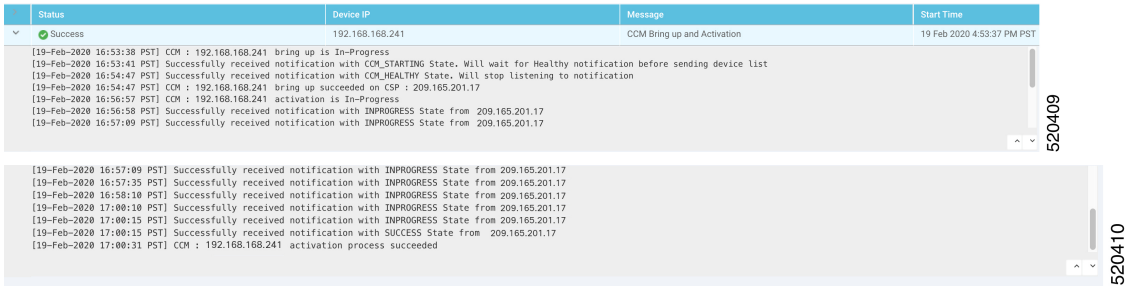


図 *2*：*CLOUD ONRAMP CCM* タスク（*Cisco vManage* リリース *20.8.1* 以降）

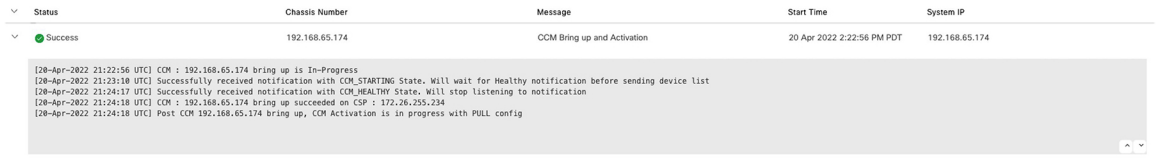


図 *3*：プッシュ機能テンプレート構成タスク（*Cisco vManage* リリース *20.8.1* 以降）

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 vManage] 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 vManage メニューから **[Monitor]** > **[Devices]** > **[Colocation Cluster]**を選択します。

   Cisco vManage リリース 20.6.x 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 vManage 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 vManage 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 vManage 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、Cisco Cloud サービスプラットフォームの問題のトラブルシューティング 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（CCM）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 CCM 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 vManage メニューから**[Monitor]** > **[Devices]**の順に選択します。

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

   2. [Colocation Cluster] をクリックします。

      Cisco vManage リリース 20.6.x 以前：[Colocation Cluster] をクリックします。

      特定の CSP デバイスに対して CCM が有効になっているかどうかを表示します。

5. CCM の正常性を監視するには、以下の手順を実行します。

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

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

2. [Colocation Cluster] をクリックします。

   Cisco vManage リリース 20.6.x 以前：[Colocation Cluster] をクリックします。

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

3. CCM 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. CCM の正常性を表示するには、[Colo Manager] をクリックします。

「STARTING」の後に Cisco Colo Manager のステータスが「HEALTHY」に変わらない場合は、Cisco Colo Manager の問題のトラブルシューティングを参照してください。

「STARTING」の後に Cisco Colo Manager のステータスは「HEALTHY」に変わったが、スイッチの構成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、スイッチデバイスが PNP または Cisco Colo Manager にコールホームしていない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。

ステップ 1 [Cisco vManage] 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。

Cisco vManage でのクラスタの編集

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。

ステップ 1 [Cisco vManage] 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：
   - Cisco vManage 20.8.1 以前のリリース：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。

   - Cisco vManage 20.9.1 以降：すべてのグローバルパラメータと一部のリソースプールパラメータを編集します。

     （注） アクティブな Day-N クラスタリソースプールの拡張がサポートされています。IP および VLAN プールの削減はサポートされていません。VNF 管理 IP プールを除くすべての IP プールには、day-N 編集で新しいサブネットを追加できます。

     次のリソースプールパラメータは編集できません。

     - **名前**
     - **説明**
     - **管理サブネットゲートウェイ**
     - **管理マスク**
     - **スイッチ PNP サーバー IP**

   - 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 vManage を使用して、CSP デバイスを追加および構成できます。

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 デバイスで同じであることを確認してください。

ステップ 1 [Cisco vManage] 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。

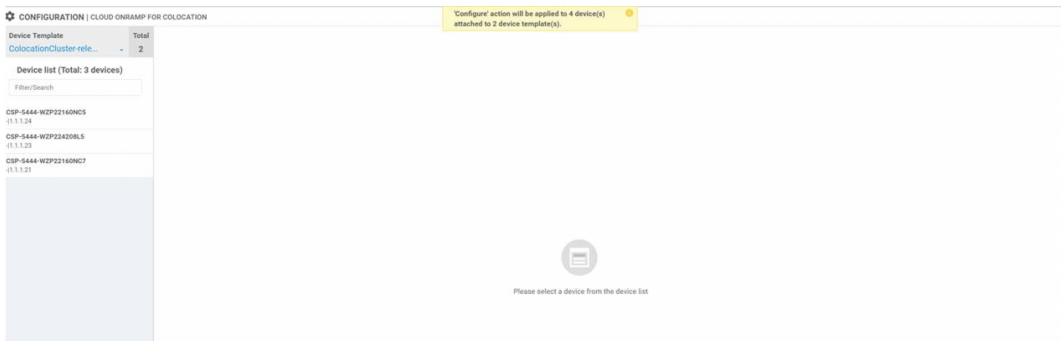
名前には、128 文字の英数字を含めることができます。

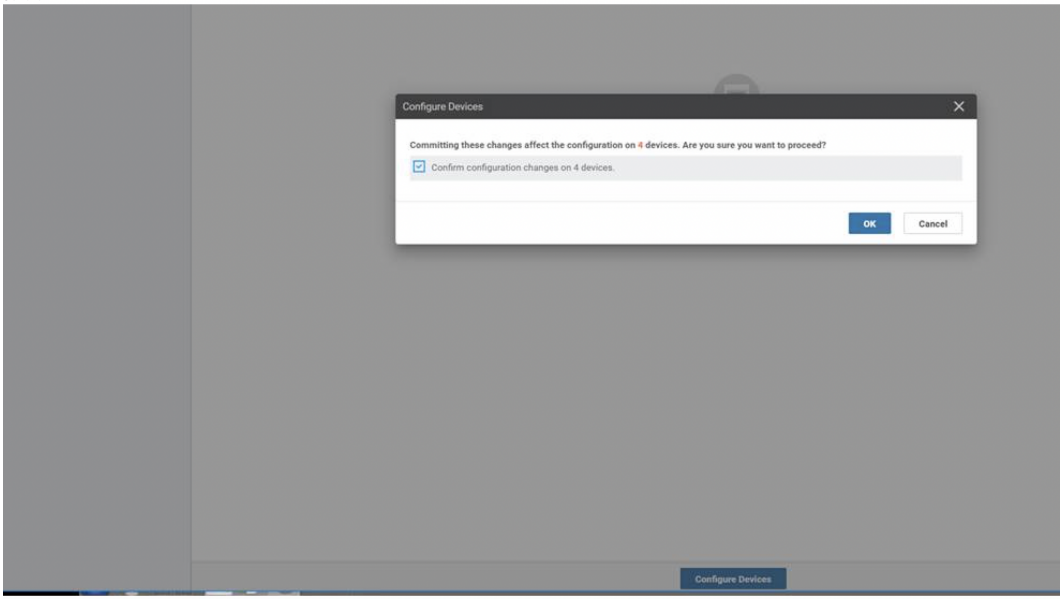
（注） CSP デバイスを起動するには、デバイスの OTP を設定してください。

図 *4 : 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。



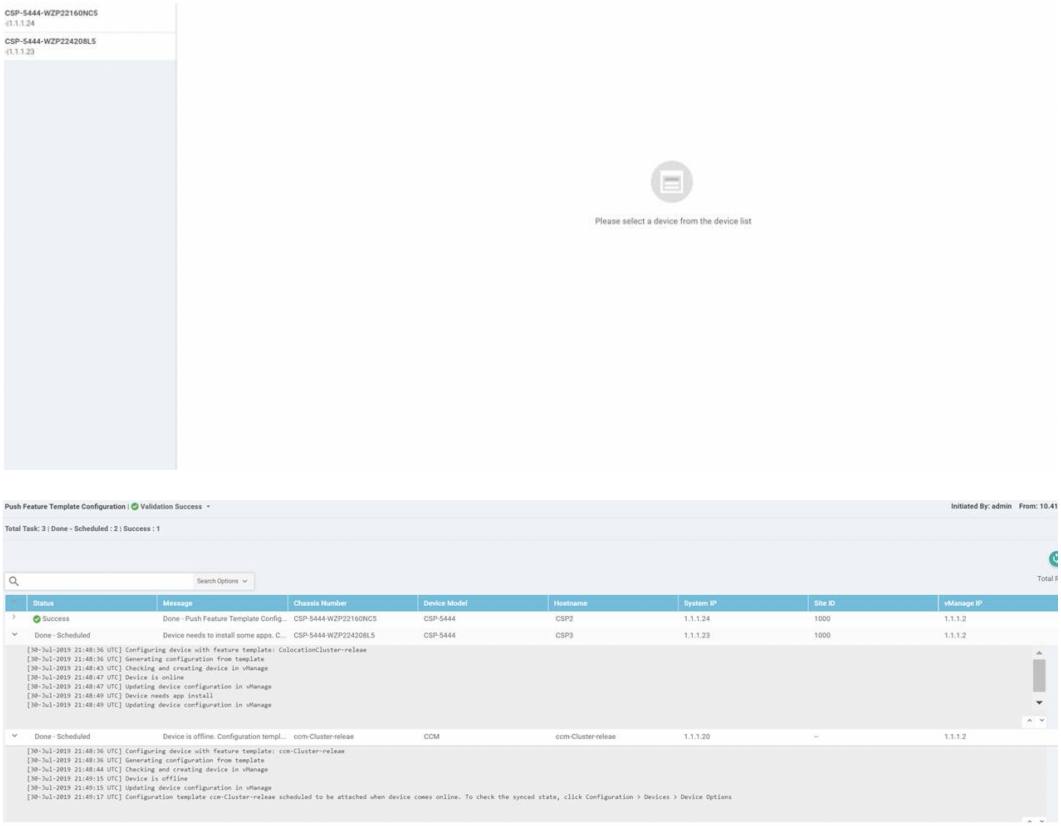


ステップ 7 CSP デバイスが追加されているかどうかを確認するには、実行中のすべてのタスクのリストを表示する [Task View] ウィンドウを使用します。

クラスタからの CSP デバイスの削除

Cisco vManage を使用して CSP デバイスを削除できます。

ステップ 1 [Cisco vManage] 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。



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。CSP デバイスの工場出荷時設定へのリセットを参照してください。

ステップ 8 無効な CSP デバイスを使用停止するには、[Cisco vManage] 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。

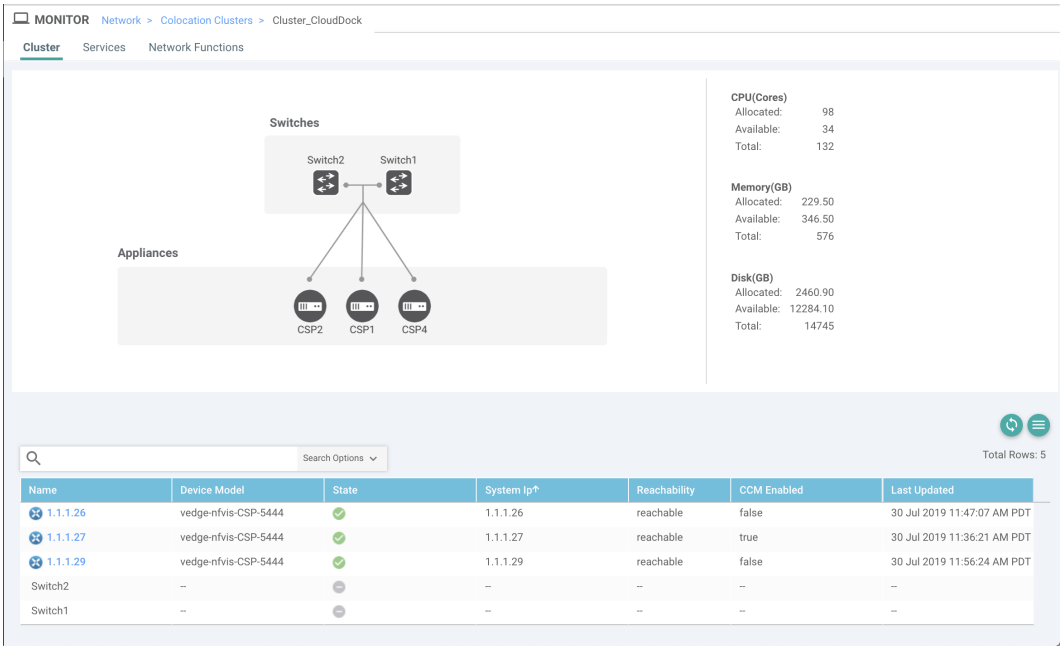
CCM がある CSP の削除

ステップ 1 CCM 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、CCM が有効になっているかどうかを確認できます。次の図は、CCM ステータスを表示できる場所を示しています。

図 *5 : CCM* 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 CCM 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 CCM インスタンスを起動できるように、Cisco vManage 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.x 以前のリリースでは、CCM 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 CCM インスタンスを起動する必要があります。

CCM がある CSP デバイスを削除すると、CCM 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 CCM 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 vManage] 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

ステップ 1 [Cisco vManage] 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 *6 :* 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 SD-WAN リリース 20.5.1 Cisco vManage リリース 20.5.1	この機能を使用すると、デバイスの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 vManage 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 vManage 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 （18 ページ）』を参照してください。

（注） CSP デバイスの交換時、Cisco vManage 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。配線に関する要件を参照してください。
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 vManage 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 コントローラ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。

クラスタからの PNF デバイスの削除

ステップ 1 PNF を持つすべてのサービスグループとサービスチェーンを切り離します。

ステップ 2 （オプション）サービスグループを削除します。

削除された PNF が Cisco vManage を使用してオーケストレーションされた ASR ルータである場合は、[Device] ウィンドウからデバイスを無効にしてデコミッションします。

ステップ 3 PNF を Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに接続しているケーブルを取り外し、インターフェイスに対応する Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C から VLAN 構成を手動で削除します。

Cisco vManage からのクラスタの削除

Cisco vManage 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。

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

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 vManage] 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す。

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 無効なデバイスを使用停止するには、[Cisco vManage] 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。 スイッチの構成を消去し、スイッチを工場出荷時のデフォルトにリセットする を参照してください。

スイッチの取り外しと交換

Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C シリーズのスイッチは、サービスチェーン内の異なる VNF デバイス間でトラフィックを切り替えるためのデータパスで使用されます。Stackwise Virtual（SVL）技術を使用してスタックされた 2 つのスイッチがあります。

冗長スタックを実現するために、スイッチは 2 つのスタックワイズ仮想リンク（SV リンク）と 1 つのデュアルアクティブ検出（DAD リンク）のセットを使用します。Cisco Catalyst 9500-40X 上の規範的接続の場合、ポート 38、39 は SVL リンク、ポート 40 は DAD リンクです。Cisco Catalyst 9500-48Y4C 上の規範的接続の場合、ポート 46、47 は SVL リンク、ポート 48 は DAD リンクです。

スタックには2つのスイッチがあり、一方のスイッチがアクティブで、もう一方がスタンバイです。コントロール プレーン データベースはスイッチ間で同期されます。各スイッチには、スタックの一部としてスイッチ番号が割り当てられます。現在のシナリオでは、スイッチには 1 と 2 の番号が付けられています。SVL 冗長性の詳細については、『High Availability Switch Configuration Guide』を参照してください。

（注） スイッチに障害が発生した場合は、障害が発生したスイッチ番号を確認してください。このスイッチは、代替としてセットアップするために使用できます。

スタック内のスイッチを交換するには、次の手順を実行します。

ステップ 1 スイッチ 1 コンソールで、**show switch** コマンドを使用して構成を表示します。

```
Switch# show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------------
*1       Active   c4b3.6a71.0b00     1      V01     Ready
 2       Member   0000.0000.0000     0      V01     Removed
```

（注） ここで、取り外されるスイッチ番号は 2 です。このスイッチ番号は、新しいスイッチを構成するときに必要です。

ステップ 2 障害が発生したユニットを交換するスイッチで、スイッチ番号が 1 であることを確認します。これは、新しいユニットで **show switch** コマンドを再度使用することで確認できます。

```
Switch# show switch
Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------------
*1       Active   5486.bc78.c900     1      V01     Ready
```

ステップ 3 新しいスイッチの番号が 2 の場合は、番号を 1 に変更してから、スイッチをリロードしてください。次のコマンドを使用してスイッチ番号を表示し、スイッチの番号を 1 に変更します。

```
Switch# show switch
Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------
*2       Active   5486.bc78.c900     1      V01     Ready


Switch# switch 2 renumber 1
WARNING: Changing the switch number may result in a configuration change for that switch.  The
interface configuration associated with the old switch number will remain as a provisioned
configuration. New Switch Number will be effective after next reboot. Do you want to continue?[y/n]?
 [yes]:
Switch#reload

System configuration has been modified. Save? [yes/no]: no
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

Jun 17 19:41:01.793: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command
```

ステップ 4 SVL に必要なケーブルを接続します。これは、最初の Cisco Catalyst 9500-40X スイッチから 2 番目のスイッチへのポート 38、39、および 40 です。

ステップ 5 2 番目のスイッチで、構成を設定して保存します。

```
Switch(config)#
stackwise-virtual
domain 10
!
interface TenGigabitEthernet1/0/38
stackwise-virtual link 1
!
interface TenGigabitEthernet1/0/39
stackwise-virtual link 1
!
interface TenGigabitEthernet1/0/40
stackwise-virtual dual-active-detection
```

ステップ 6 交換するユニットと同じになるように新しいユニットの番号を付け直し、ボックスを再ロードします。

```
Switch# switch 1 renumber 2
WARNING: Changing the switch number may result in a configuration change for that switch.  The
interface configuration associated with the old switch number will remain as a provisioned
configuration. New Switch Number will be effective after next reboot. Do you want to continue?[y/n]?
 [yes]: yes
Switch# reload
```

新しいスイッチが起動すると、スタックに参加し、構成と同期します。

次に、**show switch** コマンドからの出力例を示します。

```
Switch# show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------
*1       Active   c4b3.6a71.0b00     1      V01     Ready
 2       Member   5486.bc78.c900     1      V01     Ready
```

```
Switch#
*Jun 17 21:00:57.696: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
*Jun 17 21:00:57.694: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2
has been elected STANDBY.
*Jun 17 21:01:02.651: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))

*Jun 17 21:01:02.651: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Jun 17 21:01:53.686: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
*Jun 17 21:01:54.688: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
Switch#
Switch# show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-------------------------------------------------------------------------------------
*1       Active   c4b3.6a71.0b00     1      V01     Ready
 2       Standby  5486.bc78.c900     1      V01     Ready
```

Cisco vManage からの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。

ステップ 1 Cisco vManage 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 デバイスの Cisco vManage 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 vManage 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 （6 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 vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。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 vManageを使用してサービスグループを構成できます。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。

Cisco vManage でのサービスチェーンの VNF 配置

サービスチェーン配置コンポーネントは、サービスチェーン内の各 VNF をホストする CSP デバイスを選択します。配置の決定は、使用可能な帯域幅、冗長性、および計算リソース（CPU、メモリ、ストレージ）の可用性に基づいています。Cloud OnRamp for Colocation 用に構成されたサービスチェーン内のすべての VNF の帯域幅、CPU、メモリ、およびストレージのニーズが満たされていない場合、配置ロジックはエラーを返します。リソースが使用できず、サービスチェーンが展開されていない場合は、通知を受け取ります。

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 *7:* 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 SD-WAN リリース 19.2.1	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モニタリングを有効にするには、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。

[Cisco vManage] 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 *8*: 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。
Monitoring	サービスチェーンのヘルスモニタリング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モニタリングは、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モニタリングサービスです。デフォルトでは、モニタリングサービスは無効になっています。 SCHM（サービスチェーンヘルスモニタリングサービス）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モニタリングできます。 サービスチェーンのモニタリングは、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 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。 （注） • 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モニタリング 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、入力および出力モニタリング IP アドレスを指定する必要はありません。 たとえば、ネットワーク機能が VPN 終端されていない場合、入力モニタリング 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、出力モニタリング 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。 • 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モニタリングすることはできません。

フィールド	説明
Service Chain	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。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。

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 vManage 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 クラスタの監視』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。

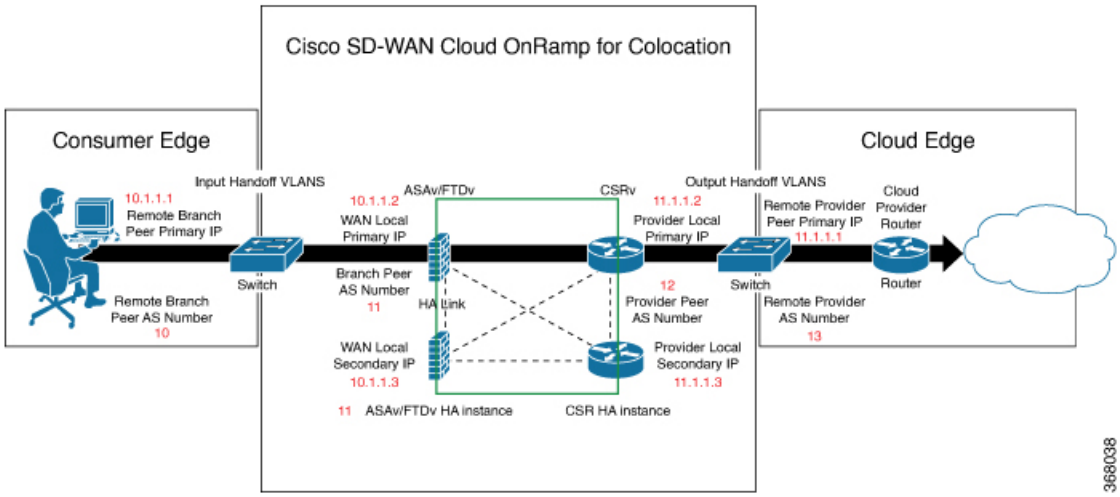
- Disk Image/Image Package (Select File)
- Disk Image/Image Package (Filter by Tag, Name and Version)
- Scaffold File (Select File)
- Scaffold File (Filter by Tag, Name and Version)

表 *9:* ルータとファイアウォールの *VNF* プロパティ

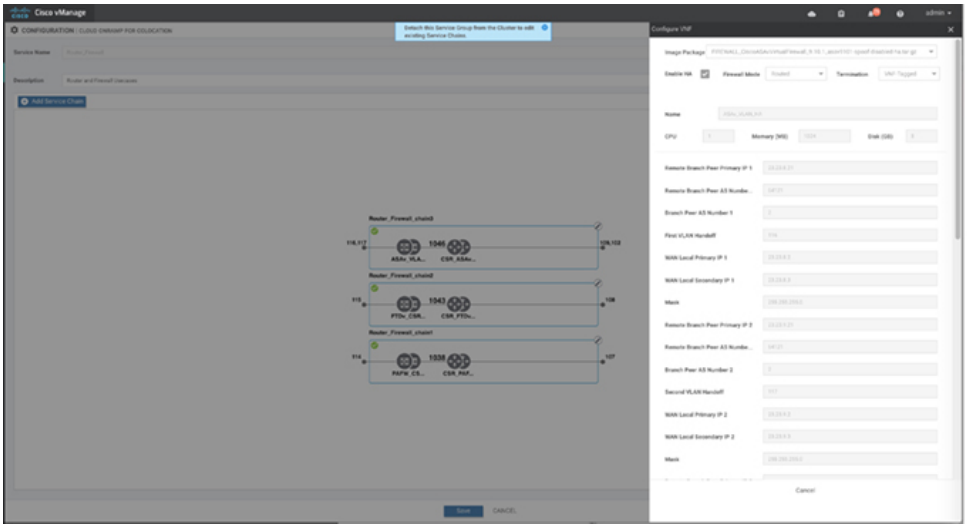
フィールド	説明
Image Package	ルータ、ファイアウォールパッケージを選択します。
Disk Image/Image Package (Select File)	tar.gz パッケージまたは qcow2 イメージファイルを選択します。
Disk Image/Image Package (Filter by Tag, Name and Version)	（オプション）VNF イメージのアップロード時に指定した名前、バージョン、タグに基づいて、イメージまたはパッケージファイルをフィルタリングします。

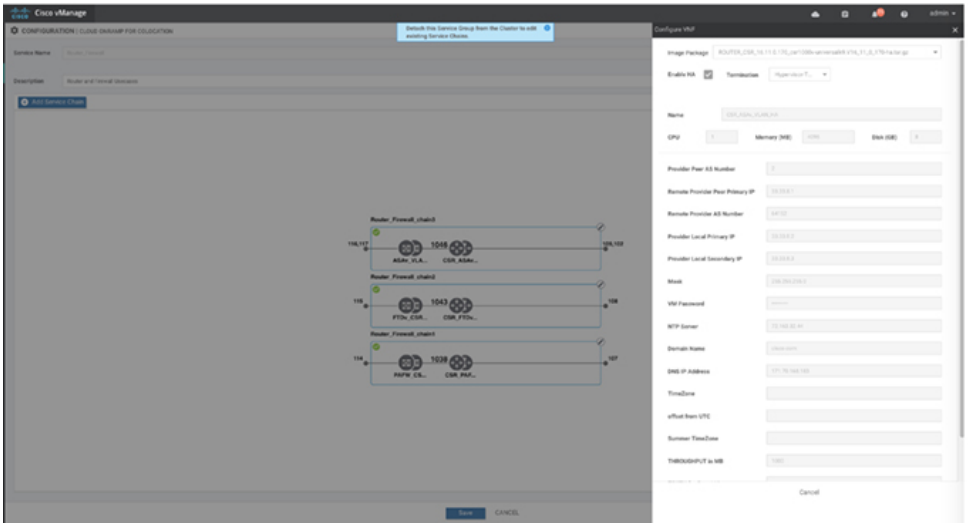
フィールド	説明
Scaffold File (Select File)	スキャフォールドファイルを選択します。 （注） • qcow2 イメージファイルが選択されている場合、このフィールドは必須です。tar.gz パッケージが選択されている場合はオプションです。 • tar.gz パッケージとスキャフォールドファイルの両方を選択した場合、スキャフォールドファイルのすべてのイメージプロパティとシステムプロパティは、tar.gz パッケージで指定された Day-0 構成ファイルを含むイメージプロパティとシステムプロパティをオーバーライドします。
Scaffold File (Filter by Tag, 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、スキャ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。



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





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 SD-WAN VM を構成します。

（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 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 コントローラで認証された後に使用できる Cisco 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 SD-WAN デバイスが存在するテナント Cisco 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 vBond Orchestrator 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 vBond Orchestrator の 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 *10*：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	必須またはオプション	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 にのみ適用されます。
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	必須またはオプション	説明

Termination	必須	次のいずれかのモードを選択します。
		• 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
		`<type>selection</type> <val help="L3 Mode With Sub-interfaces(Trunked)" display="VNF-Tagged">vlan</val>`
		• 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
		`<val help="L3 Mode With IPSEC Termination From Consumer and Routed to Provider GW" display="Tunneled">vpn</val>`
		• アクセスモードでの L3 モード（非トランクモード）
		`<val help="L3 Mode In Access Mode (Non-Trunked)" display="Hypervisor-Tagged">routed</val>`

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モ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 *11* : 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 SD-WAN リリース 20.1.1	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 vManage 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 （38 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 *12 :* 機能の履歴

機能名	リリース情報	説明
Cisco vManage のサービスグループの複製	Cisco SD-WAN リリース 20.5.1 Cisco vManage リリース 20.5.1	この機能を使用すると、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 vManage 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。

ステップ 1 [Cisco vManage] 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 vManage 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 vManage 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 vManage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 vManage 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 vManage 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。

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 （38 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。

a) [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。

b) 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す。

物理ネットワーク機能のワークフロー

このトピックでは、共有 PNF デバイスの作成、構成、および監視に必要な一連の操作の概要を説明します。PNF ワークフローが有効であることを確認するには、ケーブル接続が正しいこと、および VLAN ポートが Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C の適切なポートにあることを確認してください。

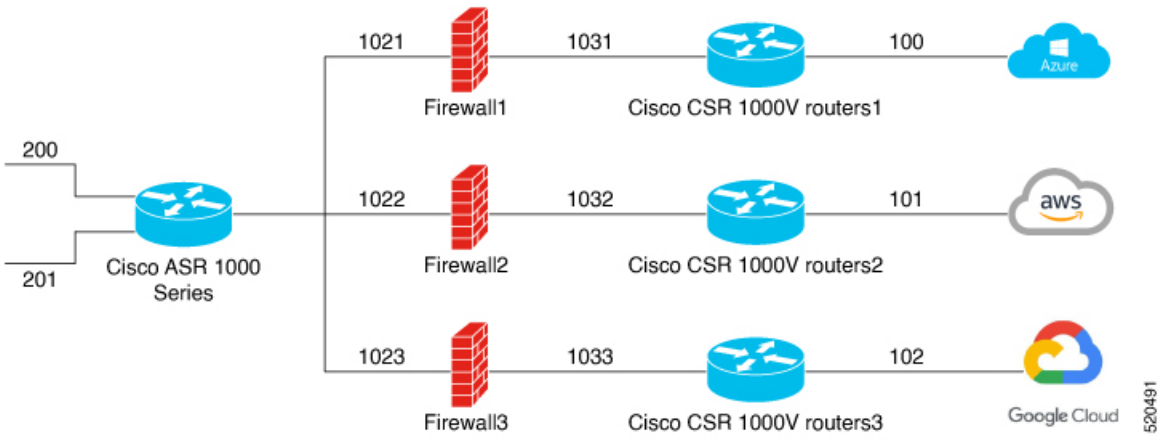
1. PNF デバイスを Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチデバイスに接続します。
2. Cisco ASR 1000 シリーズ ルータを Cisco vManage で管理するには、Cisco スマートアカウントから WAN エッジルータの認証済みシリアル番号をアップロードします。『System and Interfaces Configuration Guide』の「Upload WAN Edge Router Serial Numbers from Cisco Smart Account」を参照してください。
3. 追加した PNF デバイスを使用してサービスチェーンを作成します。『共有 PNF デバイスによるカスタムサービスチェーン （50 ページ）』を参照してください。
4. サービスグループをクラスタに接続し、生成された構成パラメータを確認します。『クラスタ内のサービスグループの接続または切断 （63 ページ）』を参照してください。
5. 生成された構成パラメータに従って、PNF および Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチデバイスを構成します。『PNF および Cisco Catalyst 9500 スイッチの構成 （54 ページ）』を参照してください。

次の図では、最初の PNF が複数のサービスチェーンで共有されています。これらのサービスチェーンは、Microsoft Azure、AWS、Google Cloud のさまざまなクラウドアプリケーションにアクセスします。VLAN 200 からのトラフィックは、SD-WAN ポリシー定義に基づいて Cisco ASR 1000 シリーズ PNF に入り、VRF 構成と対応する宛先アプリケーションに基づいてネクスト ホップ ファイアウォールを取得します。リターントラフィックは、アプリケーション トラフィックごとに同じパスを通過する必要があります。

PNF を構成するには、以下の手順を実行します。

1. ASR1000 シリーズ デバイスにログインし、Cisco vManage から入手可能な VLAN および IP アドレス情報に基づいて設定します。
2. インバウンドトラフィックとアウトバウンドトラフィックの両方で特定の VLAN を許可するには、PNF デバイスが接続されている Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチポートを構成します。

図 *6 :* 複数のサービスチェーンで共有される *PNF*



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 *13* : 機能の履歴

機能名	リリース情報	機能説明
サービスチェーンでの PNF デバイスの管理	Cisco SD-WAN リリース 19.2.1	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

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 vManage で管理する必要がある場合は、シリアル番号が Cisco vManage 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 構成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。

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 （38 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 vManage 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。

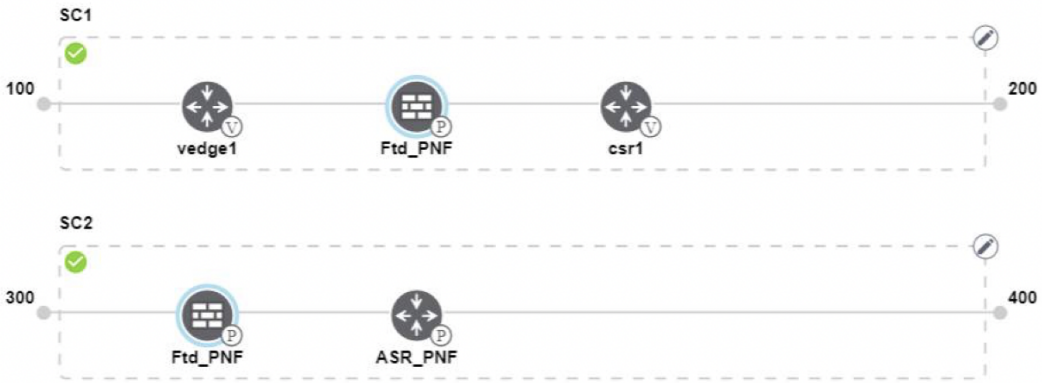
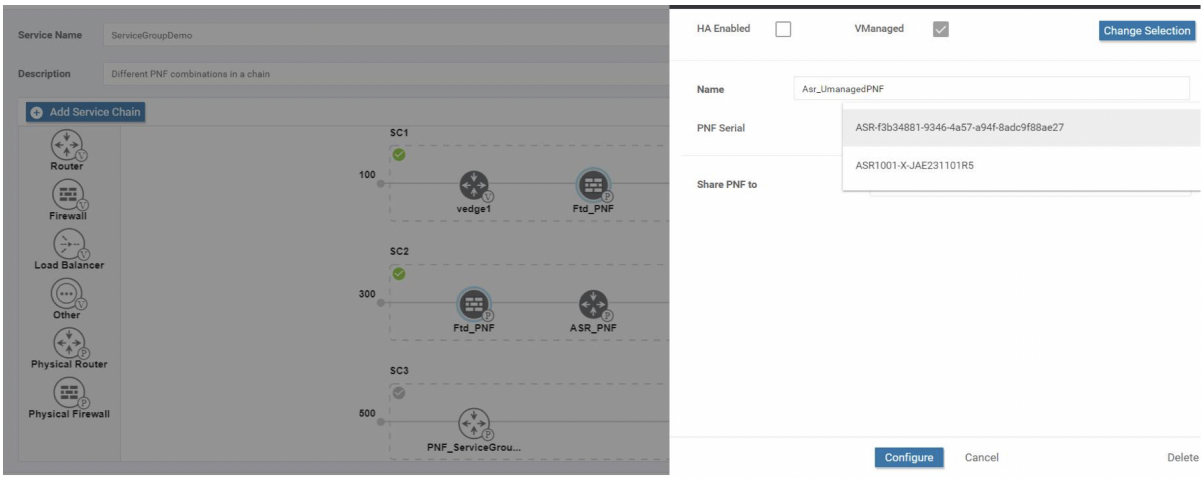


図 *9* : サービスチェーン内の *3* つの *PNF* デバイス

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 vManage 構成を示しています。



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 クラスタの監視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。

PNF および Cisco Catalyst 9500 スイッチの構成

ステップ 1 サービスチェーンの一部である PNF デバイスを追加する必要があるスイッチからポートを識別します。ポートの可用性を確認するには、を参照してください。

ステップ 2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチのいずれかのターミナルサーバーを使用して Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C と接続するか、アクティブスイッチの IP アドレスを指定して **vty session** コマンドを使用します。

ステップ 3 PNF に接続されているインターフェイスを持つ Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチで生成された構成パラメータから VLAN を構成します。生成された VLAN 構成については、「モニター」画面を参照してください。

ステップ 4 FTD または ASR 1000 シリーズのデバイスを設定するには、[Monitor] ウィンドウの構成をメモしてから、デバイスで手動で構成します。

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 *14*：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 SD-WAN リリース 19.2.1	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。

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 （38 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 vManage から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 （38 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、共有 VNF のユースケース （56 ページ）および共有 VNF のカスタムパッケージの詳細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 vManage 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。

共有 VNF のユースケース

一部の共有 VNF ユースケースとそれらの事前定義された変数リストのサンプルイメージを次に示します。

図 *10* : 共有 - 最初の位置の *Cisco vEdge* ルータ *VNF*

最初の位置にある Cisco vEdge ルータ VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバー（ASAv ファイアウォール）は HA モードです。

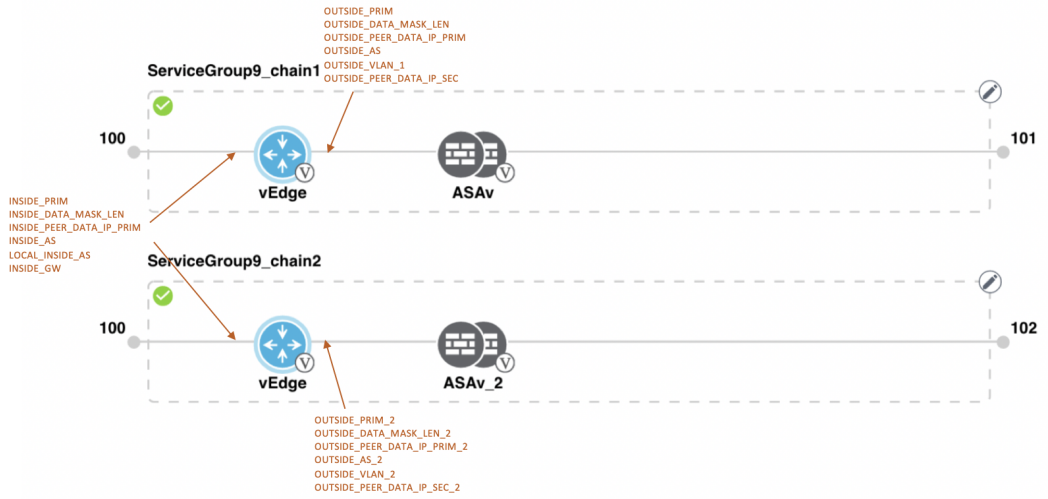


図 *11* : 共有 - 最初の位置の *Cisco vEdge* ルータ *VNF*

最初の位置にある Cisco vEdge ルータ VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバーはスタンドアロンモードです。

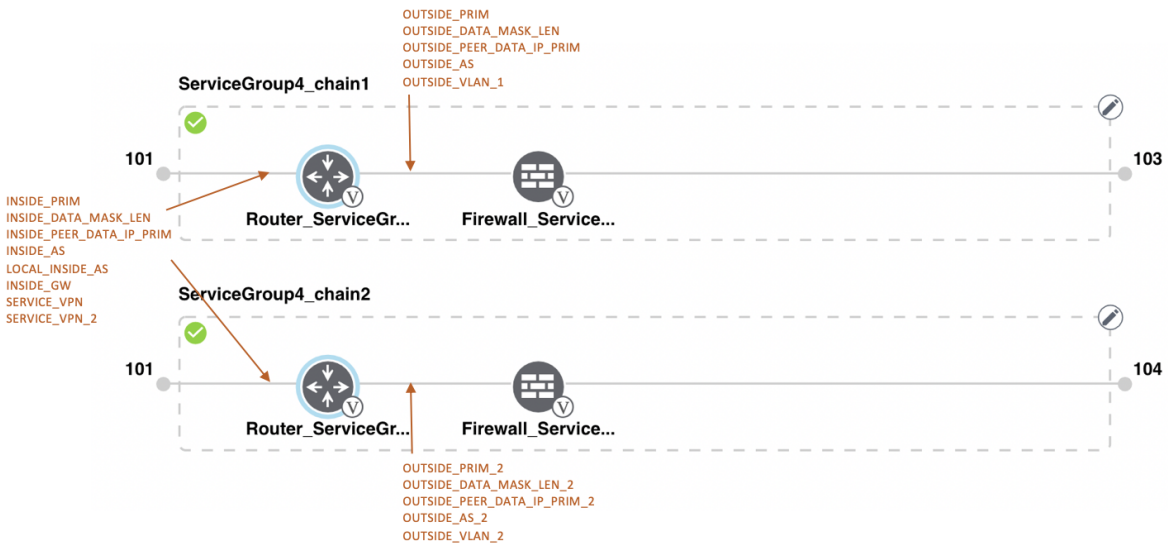


図 *12* : 共有 - 最初の位置の *Cisco vEdge* ルータ *VNF*

最初の位置にある Cisco vEdge ルータ VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はトランクモード（VNF タグ付き）であり、ネイバーはスタンドアロンモードです。

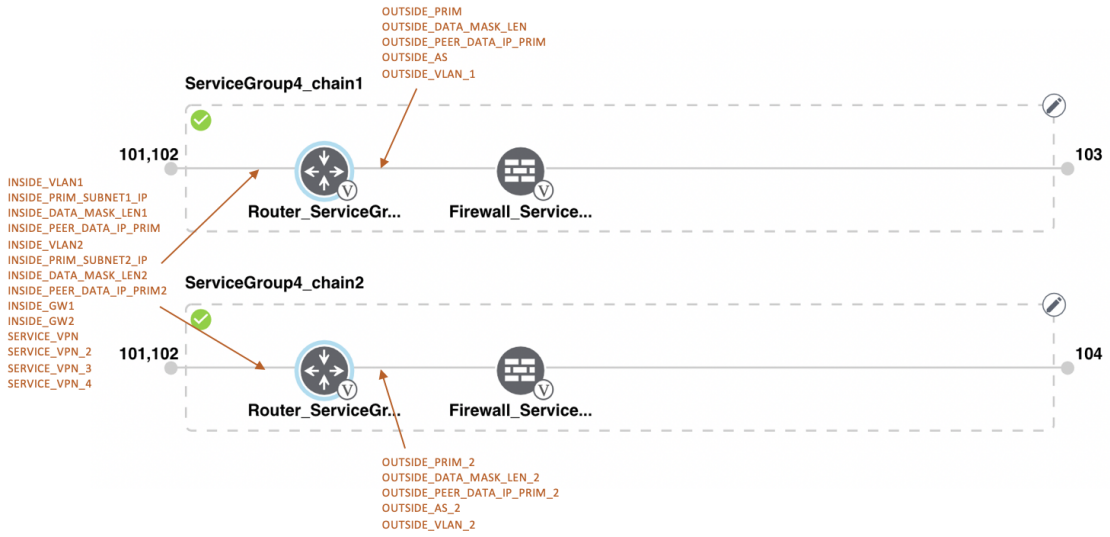


図 *13* : 共有 - 最初の位置の *Cisco vEdge* ルータ *VNF*

最初の位置にある Cisco vEdge ルータ VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はトランクモード（VNF タグ付き）であり、ネイバーは HA モードです。

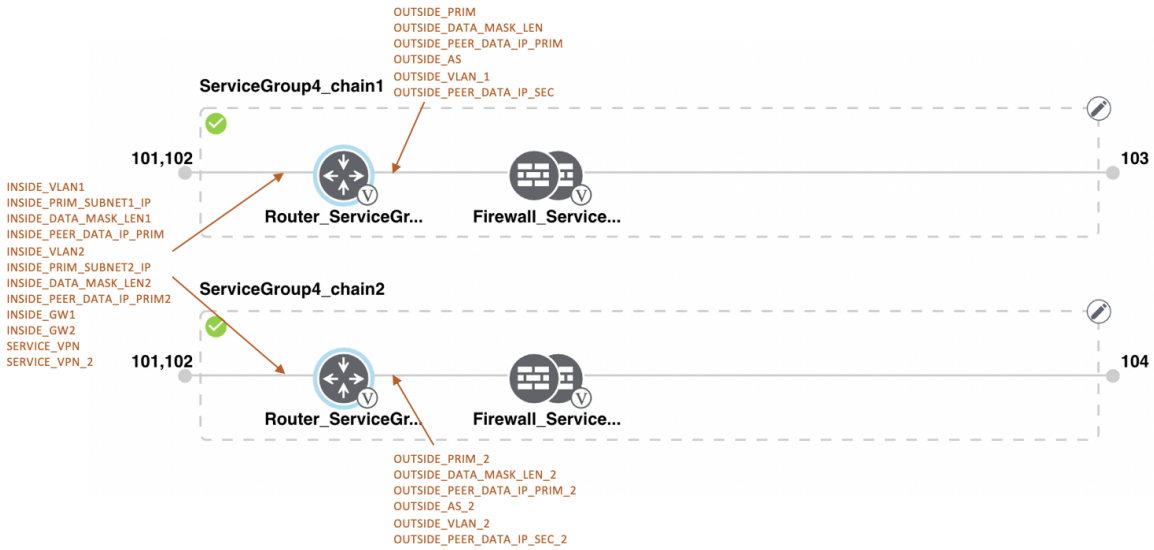


図 *14* : 共有 - 最後の位置の *Cisco CSR1000V VNF*

最後の位置にある Cisco CSR1000V VNF は、2 番目の位置にある 2 番目のサービスチェーンと共有されます。最後の VNF からの出力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバー（ASAv ファイアウォール）はスタンドアロンモードです。

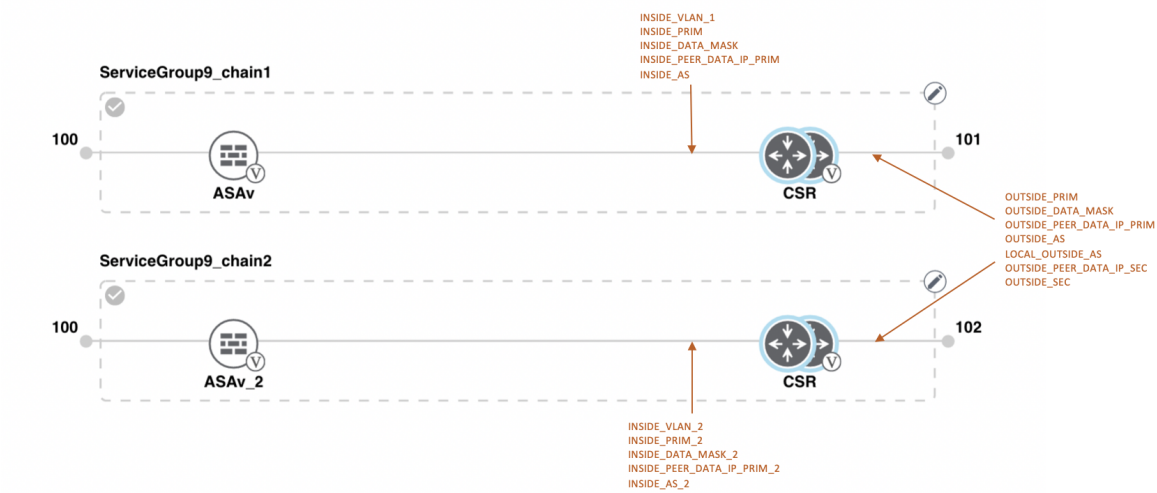


図 *15* : 共有 - 最後の位置の *Cisco CSR1000V VNF*

最後の位置にある Cisco CSR1000V VNF は、2 番目の位置にある 2 番目のサービスチェーンと共有されます。最後の VNF からの出力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバーはスタンドアロンモードです。

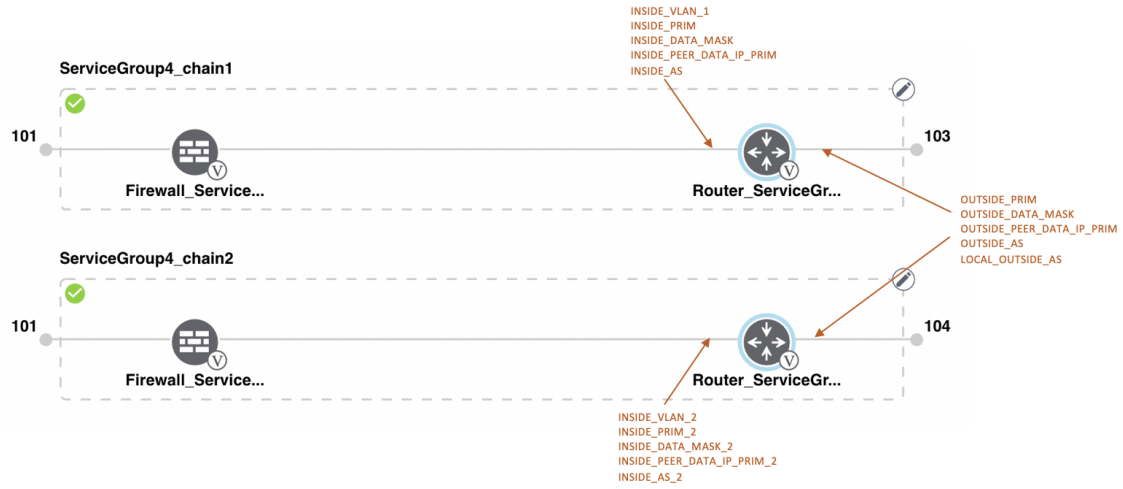


図 *16* : 共有 - 最後の位置の *Cisco CSR1000V VNF*

最後の位置にある Cisco CSR1000V VNF は、2 番目の位置にある 2 番目のサービスチェーンと共有されます。最後の VNF からの出力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバー（Firewall_Service）は HA モードです。

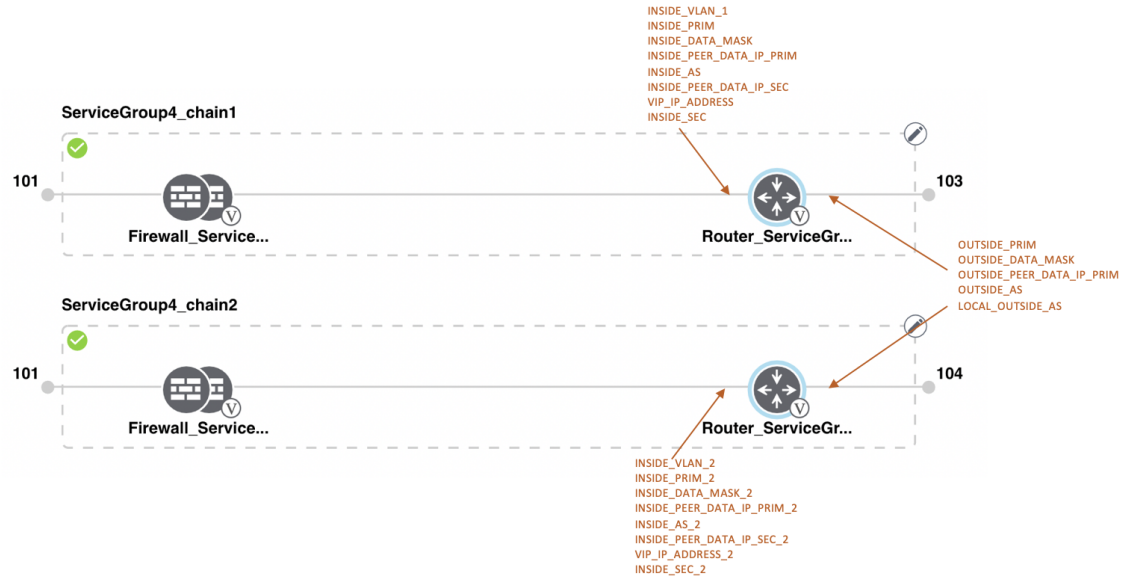


図 *17 :* 共有 - 最後の位置の *Cisco CSR1000V VNF*

最後の位置にある Cisco CSR1000V VNF は、2 番目の位置にある 2 番目のサービスチェーンと共有されます。最後の VNF からの出力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバー（Firewall_Service）は HA モードです。

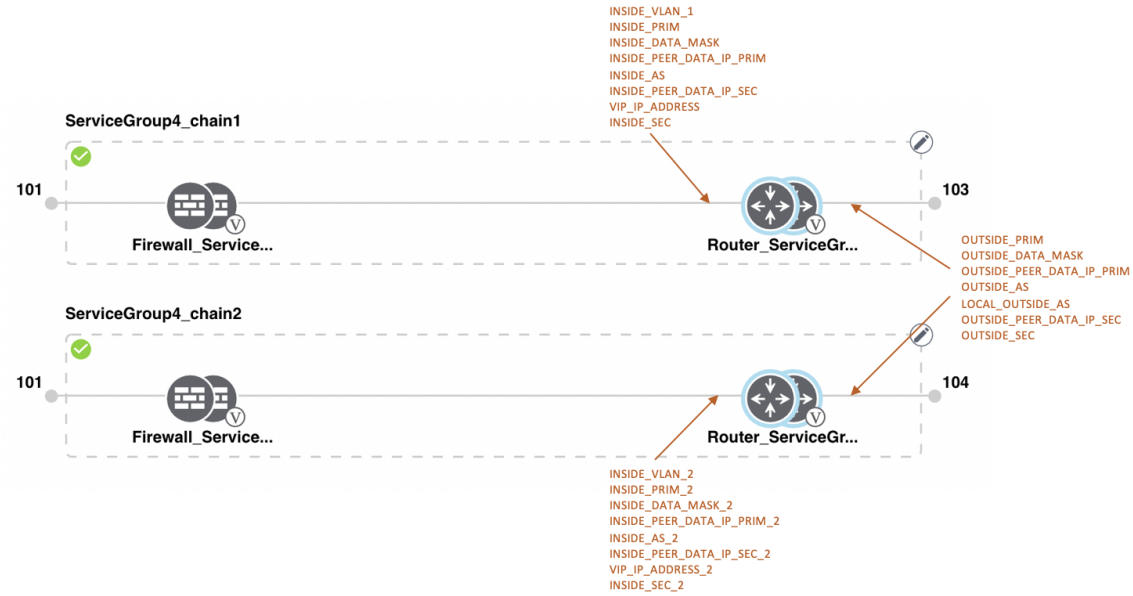


図 *18* : 共有 - 最初の位置の *ASAv VNF*

最初の位置にある ASAv VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバーは冗長モードです。

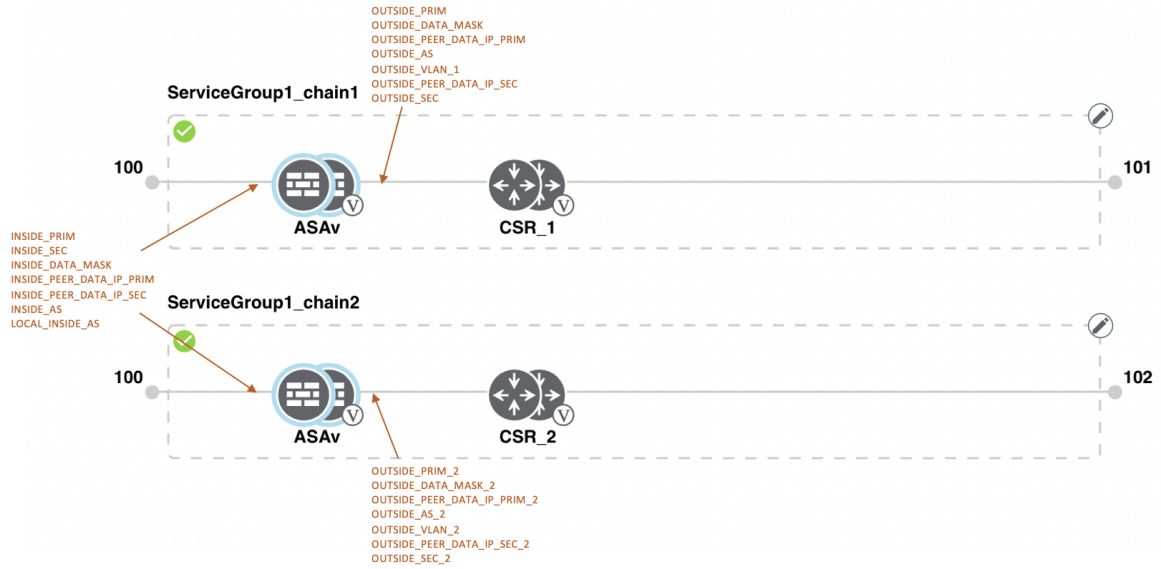


図 *19* : 共有 - 最初の位置の *ASAv VNF*

最初の位置にある ASAv（Firewall_Service）VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はアクセスモード（ハイパーバイザタグ付き）であり、ネイバーはスタンドアロンモードです。

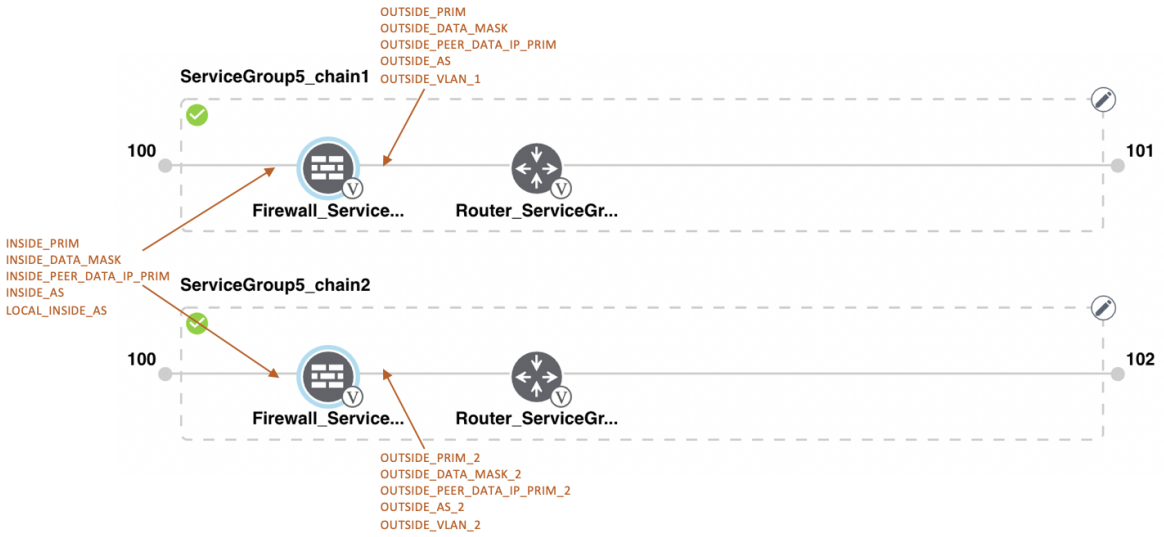


図 *20 :* 共有 - 最初の位置の *ASAv VNF*

最初の位置にある ASAv（Firewall_Service）VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はアクセスモード（ハイパーバイザタグ付き）であり、ルータであるネイバーは冗長モードです。

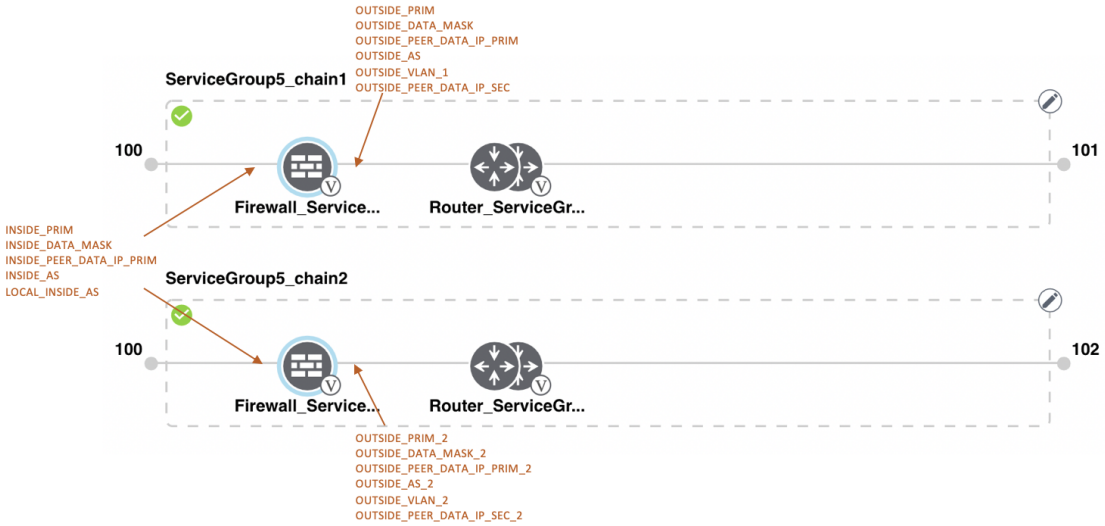
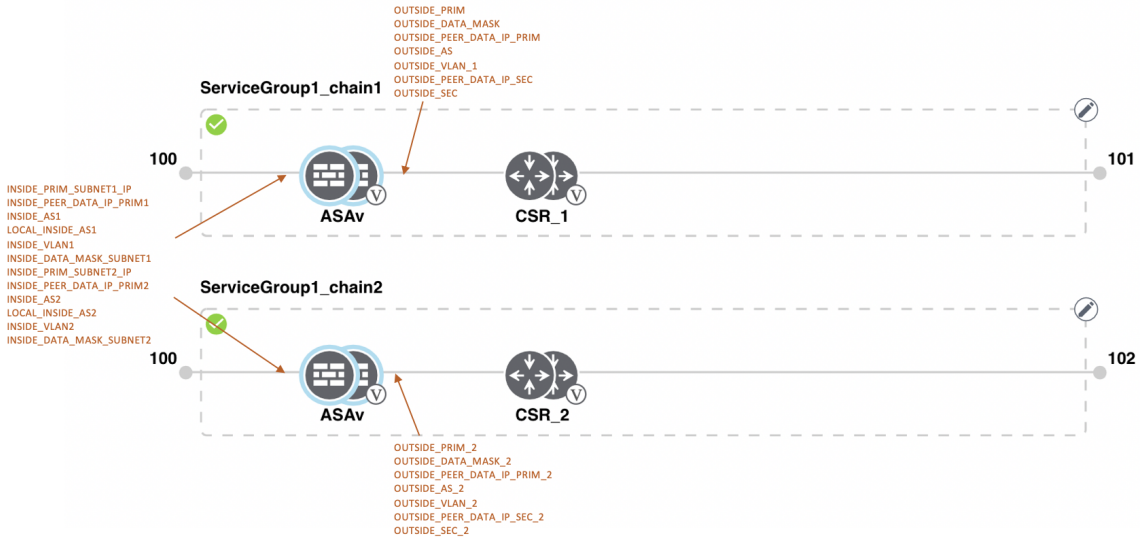


図 *21 :* 共有 - 最初の位置の *ASAv VNF*

HA モードの最初の位置にある ASAv VNF は、最初の位置にある 2 番目のサービスチェーンと共有されます。最初の VNF への入力はトランクモード（vnf タグ付き）であり、ネイバーは冗長モードです。



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。

ステップ 1 [Cisco vManage] 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。

ステップ 1 [Cisco vManage] 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 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。

ステップ 1 [Cisco vManage] 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接続または切り離しされているかどうかを確認するには、Cisco vManage 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、サービスチェーンの問題のトラブルシューティングを参照してください。
- Cisco Colo Manager タスクが失敗した場合は、Cisco Colo Manager の問題のトラブルシューティング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 vManage とコロケーションデバイスの同期を維持します。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションの Day-N 構成ワークフロー

Day-N 構成のバックグラウンドプロセスを以下に示します。

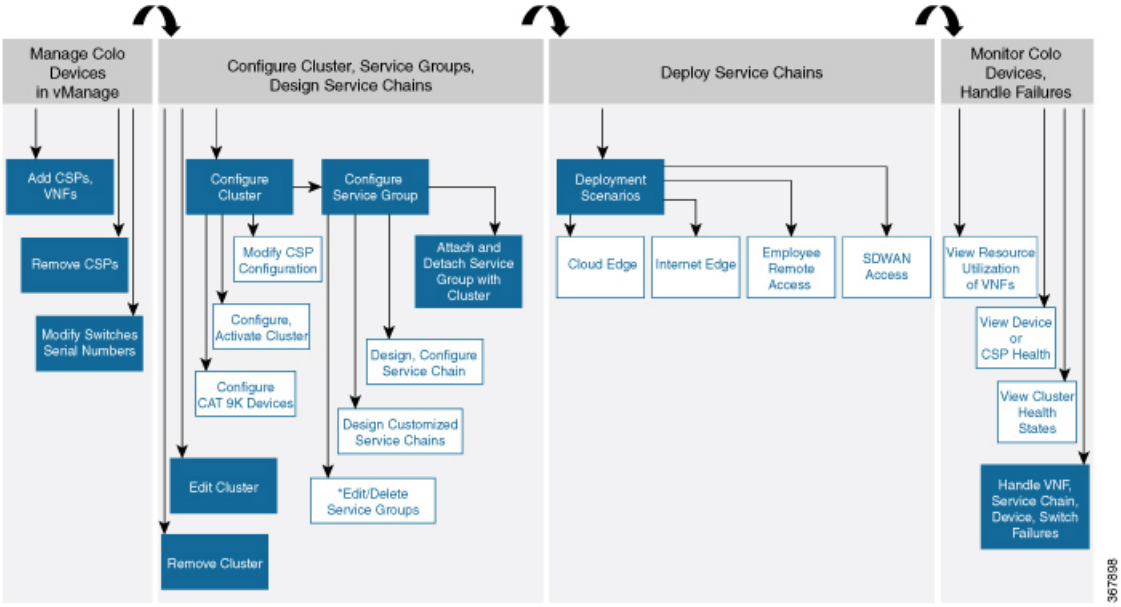
- Cisco vManage からのすべての Day-N 構成では、クラスタが同期状態にある必要があります（デバイスは Cisco vManage と同期している必要があります）。
- サービスグループをクラスタに接続すると、Cisco vManage は配置ロジックを実行して、特定の CSP デバイスに配置される VM を決定します。
- Cisco vManage からのスイッチ関連の Day-N 構成では、Cisco Colo Manager が正常な状態である必要があります。
- Cisco vManage は、すべてのスイッチ関連のサービスチェーン、クラスタ、スイッチ構成を Cisco Colo Manager に保存します。
- Cisco Colo Manager は、Cisco vManage から受信したすべての設定について、進行中の状態に移行します。
- Cisco Colo Manager は、Cisco Colo Manager のすべてのグローバルおよびサービスチェーン構成をデバイス固有の構成に変換します。
- Cisco Colo Manager は、構成のプッシュが成功したか失敗したかにかかわらず、状態を Cisco vManage に報告します。

- すべての Day-N サービスチェーンまたは VM 構成が CSP デバイスに送信されます。
- CSP デバイスは、VM ファイルのダウンロードステータスに関する通知を Cisco vManage に送信します。
- すべての VM がダウンロードされると、Cisco vManage は一括構成を送信してすべての VM を起動します。
- CSP デバイスは、起動された VM と状態に関する通知を Cisco vManage に送信します。
- いずれかのスイッチデバイスがエラーを返した場合、Cisco vManage は詳細情報とともにエラーを報告し、クラスタは FAILURE 状態に移行します。

通知とエラーメッセージに基づくエラーを修正したことを確認してから、Cloud OnRamp for Colocation クラスタを再度アクティブ化します。

（注） Day-N 構成中に、両方のスイッチデバイスのスイッチのシリアル番号を変更できます。

図 *22 : Day-N* ワークフロー



（注） * サービスグループは、クラスタから切り離した後にのみ編集できます。

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