



Cisco SD-WAN Cloud OnRamp for Colocation リリース 20.9.1 ソ リューションガイド

初版：2022年8月15日

最終更新：2022年8月25日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	最初にお読みください	1
-------	------------	---

第 2 章	Cisco SD-WAN Cloud onRamp for Colocation ソリューションに関する情報	3
	Cisco SD-WAN Cloud onRamp for Colocation ソリューション	3
	Cisco SD-WAN Cloud onRamp for Colocation ソリューションのコンポーネント	5

第 3 章	Cisco SD-WAN Cloud onRamp for Colocation ソリューションの前提条件と要件	9
	Cisco SD-WAN Cloud onRamp for Colocation ソリューションの要件	9
	ハードウェア要件	9
	ソフトウェア要件	11
	配線に関する要件	13
	規範的接続	13
	フレキシブルな接続	14
	ソリューションを展開するための前提条件	16
	Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのサイジング要件	17

第 4 章	Cisco SD-WAN Cloud onRamp for Colocation ソリューションの利用を開始	19
	Cisco SD-WAN Cloud onRamp for Colocation ソリューション – 展開ワークフロー	19
	Cisco CSP での Cisco NFVIS Cloud OnRamp for Colocation のインストール	21
	CIMC ユーザーインターフェイスのログイン	21
	仮想デバイスのアクティブ化	23
	NFVIS Cloud OnRamp for Colocation イメージのマッピング	23
	Cisco Cloud サービス プラットフォーム デバイスの起動	24
	プラグアンドプレイプロセスを使用した CSP デバイスのオンボード	24

USB ブートストラッププロセスを使用した CSP デバイスのオンボード	25
オンボードデバイスの確認とデバイスのアクティブ化	27
スイッチデバイスの起動	28
Cisco Colo Manager の起動	31
Cisco SD-WAN Cloud onRamp for Colocation ソリューションのプロビジョニングと構成	31
コロケーションごとの DHCP サーバーのプロビジョニング	32
規範的接続のためのデバイスポート接続の詳細とサービスチェーン	32
検証済みサービスチェーン	37
検証済み VM パッケージ	38
カスタマイズされたサービスチェーン	39

第 5 章

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 41

Cisco vManage を使用した Cloud OnRamp Colocation デバイスの追加	41
Cisco vManage からの Cloud OnRamp for Colocation デバイスの削除	43
Cisco vManage でのクラスタの管理	44
クラスタのプロビジョニングと構成	45
クラスタの作成とアクティブ化	46
クラスタの設定	49
ログインクレデンシャル	49
Resource Pool	50
ポート接続	52
NTP	56
Syslog サーバ	56
TACACS 認証	57
バックアップサーバー設定	58
クラスタアクティベーションの進行状況	61
クラスタの表示	64
Cisco vManage でのクラスタの編集	64
CSP デバイスのクラスタへの追加	66
クラスタからの CSP デバイスの削除	67

CCM がある CSP の削除	68	
RMA 後の Cisco CSP デバイスの交換	70	
Cisco CSP デバイスの返却	70	
Cisco CSP デバイスの RMA プロセス	71	
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	72	
クラスタからの PNF デバイスの削除	73	
Cisco vManage からのクラスタの削除	74	
スイッチの取り外しと交換	75	
Cisco vManage からのクラスタの再アクティブ化	77	
サービス グループの管理	78	
Cisco vManage でのサービスチェーンの VNF 配置	78	
サービスグループでのサービスチェーンの作成	78	
サービスチェーンの QoS	84	
サービスグループの複製	86	
カスタムサービスチェーンの作成	88	
物理ネットワーク機能のワークフロー	89	
共有 PNF デバイスによるカスタムサービスチェーン	90	
PNF および Cisco Catalyst 9500 スwitch の構成	94	
共有 VNF デバイスによるカスタムサービスチェーン	95	
共有 VNF のユースケース	96	
サービスグループの表示	103	
サービスグループの編集	103	
クラスタ内のサービスグループの接続または切断	103	
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	104	
第 6 章	クラスタコンポーネントおよび SWIM のソフトウェアイメージ管理	107
	VM カタログとリポジトリの管理	107
	VNF イメージ形式	109
	VNF イメージのアップロード	109
	カスタマイズされた VNF イメージの作成	111
	VNF イメージの表示	117

VNF イメージの削除	118
Cisco vManage を使用した Cisco NFVIS のアップグレード	118
NFVIS アップグレードイメージのアップロード	118
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	119
Cisco Catalyst 9500 スイッチのアップグレード	120
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	123

第 7 章

Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのモニタリング	127
Cisco vManage からの Cloud OnRamp for Colocation デバイスの動作ステータスの監視	128
Cisco vManage からの VNF に関する情報の表示	129
Cisco Colo Manager の正常性の表示	131
Cloud onRamp Colocation クラスタの監視	132
Cloud onRamp Colocation クラスタのパケットキャプチャ	136
スイッチ構成のための Cisco Colo Manager の状態	138
ホストからの Cisco Colo Manager の状態と遷移	139
Cisco Colo Manager の通知	139
VM アラーム	143
VM 状態	145
クラウド サービス プラットフォームのリアルタイムコマンド	145

第 8 章

ハイ アベイラビリティ	147
冗長性	147
ネットワークファブリックの冗長性	148
x86 コンピューティング ハードウェアの冗長性	148
物理 NIC またはインターフェイスの冗長性	148
NFVIS、仮想化インフラストラクチャの冗長性	148
サービスチェーンまたは VNF の冗長性	149
Cisco Colo Manager のリカバリ	151
さまざまな障害シナリオの処理	152

第 9 章

Cisco SD-WAN Cloud onRamp for Colocation マルチテナント機能	155
---	------------

コロケーション マルチテナント機能の概要	155
マルチテナント環境での役割と機能	157
マルチテナント環境での推奨仕様	158
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	159
サービスプロバイダー機能	160
新しいテナントのプロビジョニング	160
コロケーショングループの作成	161
ユーザーグループの権限の表示	161
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	162
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	162
テナントの削除	163
テナント コロケーション クラスタの管理	163
c-tenant-functionalities	164
テナントとしてのコロケーションクラスタの管理	164
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 SD-WAN デバイスの監視	165

 第 10 章

Cisco SD-WAN Cloud onRamp for Colocation ソリューションのトラブルシューティング	167
コロケーション マルチテナント機能の問題のトラブルシューティング	167
Catalyst 9500 の問題のトラブルシューティング	168
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	174
DHCP IP アドレス割り当て	182
Cisco Colo Manager の問題のトラブルシューティング	183
サービスチェーンの問題のトラブルシューティング	185
物理ネットワーク機能管理の問題のトラブルシューティング	187
CSP からのログ収集	188
Cisco vManage の問題のトラブルシューティング	188

 第 11 章

共有 VNF のカスタムパッケージの詳細	189
Cisco vEdge ルータ変数リスト	189
Cisco CSR1000V 変数リスト	193

ASAv 変数リスト 197



第 1 章

最初にお読みください

参考資料

- [Release Notes](#)[英語]
- [Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations](#)[英語]

ユーザマニュアル

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

通信、サービス、およびその他の情報

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

マニュアルに関するフィードバック

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



第 2 章

Cisco SD-WAN Cloud onRamp for Colocation ソリューションに関する情報

- [Cisco SD-WAN Cloud onRamp for Colocation ソリューション \(3 ページ\)](#)
- [Cisco SD-WAN Cloud onRamp for Colocation ソリューションのコンポーネント \(5 ページ\)](#)

Cisco SD-WAN Cloud onRamp for Colocation ソリューション

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。

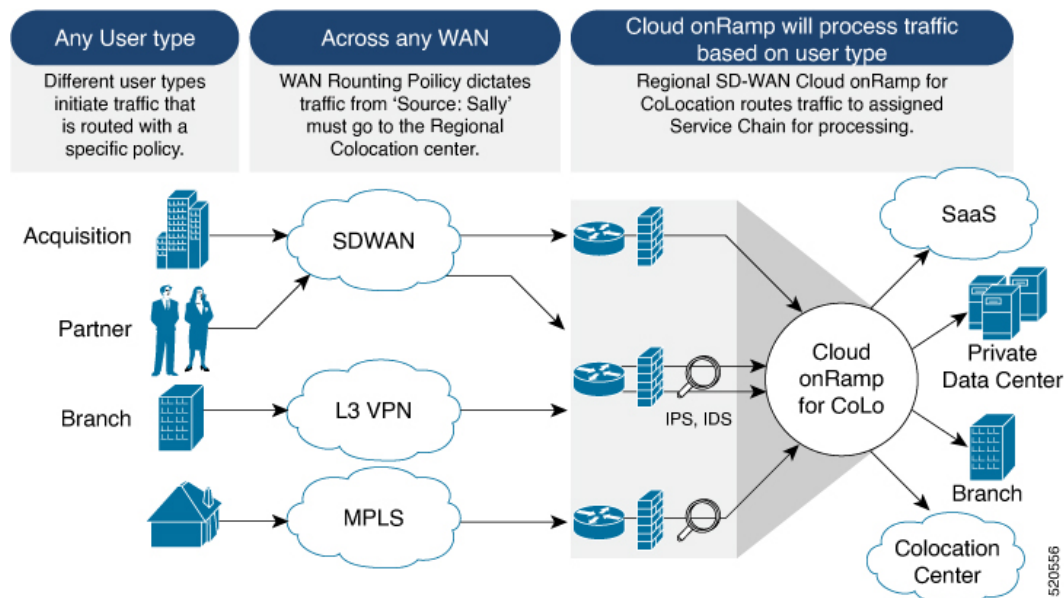
このソリューションでは、コロケーション設備向けに特別に構築された Cisco SD-WAN Cloud onRamp for Colocation ソリューションにより、ブランチおよびリモートワーカーからすべてのアプリケーションがホストされている場所への最適なパスにトラフィックをルーティングします。また、このソリューションにより、分散型企業はブランチで直接インターネットアクセスが可能になり、Infrastructure-as-a-Service (IaaS) プロバイダーおよび Software as a Service (SaaS) プロバイダーへの接続を強化できます。

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 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 SD-WAN Cloud onRamp for CoLocations



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 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 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。

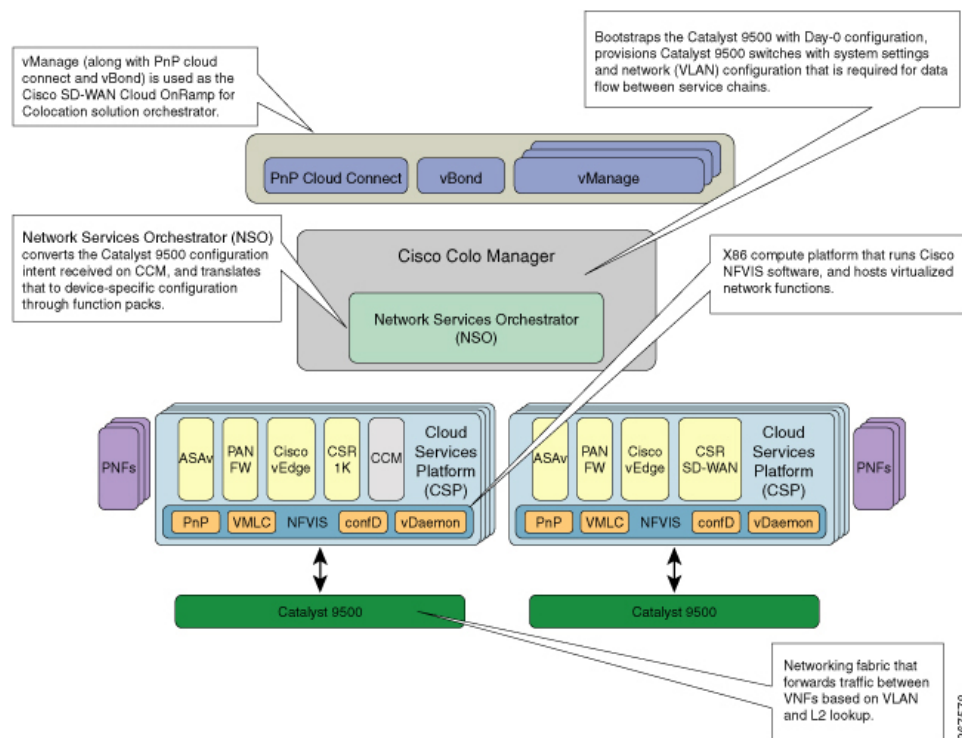
Cisco SD-WAN Cloud onRamp for Colocation ソリューションは、コロケーション IaaS プロバイダーによって特定のコロケーション設備内でホストできます。必要なコンポーネントをサポートしている限り、地域ごとにニーズを満たすコロケーションプロバイダーを選択できます。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションのコンポーネント

Cisco SD-WAN Cloud onRamp for Colocation ソリューションは、複数のコロケーションに展開できます。コロケーションは、複数の仮想ネットワーク機能と複数のサービスチェーンを起動する、コンピューティングとネットワーキングファブリックのスタックです。このスタックは、ブランチユーザー、エンドポイントをハイブリッドクラウドまたはデータセンターに接続します。Cisco vManage は、コロケーション内のデバイスをプロビジョニングするためのオーケストレータとして使用されます。各コロケーションは、同じサイト内またはサイト間で他のコロケーションを表示できません。

次の図は、Cisco SD-WAN Cloud onRamp for Colocation ソリューションのコンポーネントを示しています。

図 2 : Cisco SD-WAN Cloud onRamp for Colocation ソリューションアーキテクチャの概要



- **Cisco Cloud Services Platform, CSP-5444 and CSP-5456** : Cloud Services Platform (CSP) は、NFVIS ソフトウェアを実行する x86 Linux ハードウェアプラットフォームです。これは、Cisco SD-WAN Cloud onRamp for Colocation ソリューションで仮想ネットワーク機能をホストするためのコンピューティングプラットフォームとして使用されます。Cisco SD-WAN Cloud onRamp for Colocation 展開では、複数の CSP システムを使用できます。

Cisco Network Function Virtualization Infrastructure Software : Cisco Network Function Virtualization Infrastructure Software (NFVIS) ソフトウェアは、x86 コンピューティングプ

プラットフォーム上で実行されるベース仮想化インフラストラクチャソフトウェアとして使用されます。Cisco NFVIS ソフトウェアは、VM ライフサイクル管理、VM サービスチェーン、VM イメージ管理、プラットフォーム管理、デバイスをブートストラップするための PNP、AAA 機能、および syslog サーバーを提供します。NFVIS ドキュメントの「NFVIS Functionality Changes for SD-WAN Cloud OnRamp for Colocation」を参照してください。

- **Virtual Network Functions** : Cisco SD-WAN Cloud onRamp for Colocation ソリューションは、シスコが開発した仮想ネットワーク機能 (VNF) をサポートします。次の表に、検証済みの VNF とそのバージョンを示します。

表 1: 検証済みの仮想ネットワーク機能

仮想ネットワーク機能	バージョン
Cisco CSR1000V	17.1.1、17.2、17.3
Cisco Catalyst 8000V	17.4.1a
Cisco IOS XE SD-WAN デバイス	16.12.1、16.12.2r、17.2.1r、17.3.1a
Cisco ASA v	9.12.2、9.13.1、9.15.1
チェックポイント	R80.30、R80.40
Cisco FTDv/NGFW	6.4.0.1、6.5.0-115
Cisco vEdge Cloud ルータ	19.2.1、20.1.1、20.3.1、20.4.1
Palo Alto ファイアウォール (PAFW)	9.0.0
Fortinet ファイアウォール	6.0.2

Cisco SD-WAN Cloud onRamp for Colocation ソリューションでサードパーティの VNF を検証するには、シスコの認定プログラムを使用します。サードパーティの VNF の検証の詳細については、<https://developer.cisco.com/site/nfv/#the-ecosystem-program> を参照してください。

- **Physical Network Functions** : 物理ネットワーク機能 (PNF) は、ルータやファイアウォールなどのコロケーション サービス チェーンの一部として特定のネットワーク機能を提供することに特化した物理デバイスです。検証済みの PNF とそのバージョンは次のとおりです。

表 2: 検証済みの物理ネットワーク機能

物理ネットワーク機能	バージョン
Cisco FTD モデル : FPR-9300	6.4.0.1、6.5
Cisco ASR 1000 シリーズ	16.12.1、17.1、17.2、17.3

- **Network Fabric** : L2 および VLAN ベースのルックアップを使用して、サービスチェーン内の VNF 間のトラフィックを転送します。最後の VNF は、L2 または L3 転送を介してネットワークファブリックにトラフィックを転送できます。ネットワークファブリックには、次のいずれかを含めることができます。
 - Cisco Catalyst 9500-40X スイッチ : 40 個の 10G ポートと 2 個の 40G ポートをサポートし、ネットワークファブリックとして使用します
 - Cisco Catalyst 9500-48Y4C スイッチ : 48 個の 1G/10G/25G ポートと 4 個の 40G/100G ポートをサポートし、ネットワークファブリックとして使用します。
- **Management Network** : 独立した管理ネットワークが、CSP システムで実行されている NFVIS ソフトウェア、仮想ネットワーク機能、およびファブリック内のスイッチを接続します。この管理ネットワークは、システムとの間でファイルやイメージを転送するためにも使用されます。アウトオブバンド管理スイッチは、管理ネットワークを構成します。CSP デバイス、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに割り当てられた IP アドレスは、DHCP 構成を通じて管理ネットワークプールによって取得されます。オーケストレータは、VNF 管理 IP アドレスを管理し、VNF Day-0 構成ファイルを介して割り当てます。
- **Virtual Network Function Network Connectivity** : VNF は、Single Root IO Virtualization (SR-IOV) を使用するか、ソフトウェア仮想スイッチを介して、物理ネットワークに接続できます。VNF には、物理ネットワーク インターフェイスに直接または間接的に接続できる 1 つ以上の仮想ネットワーク インターフェイス (VNIC) を含めることができます。物理ネットワーク インターフェイスはソフトウェア仮想スイッチに接続でき、1 つ以上の VNF が仮想スイッチを共有できます。Cisco SD-WAN Cloud onRamp for Colocation ソリューションは、接続を作成するための仮想スイッチインスタンスと仮想 NIC メンバーシップの作成を管理します。デフォルトでは、CSP システムのすべての物理インターフェイスと管理インターフェイスを VNF で使用できます。

Cisco SD-WAN Cloud onRamp for Colocation 展開では、SR-IOV インターフェイスは仮想イーサネット ポート アグリゲーター (VEPA) モードで構成されます。このモードでは、NIC は VNF から受信したすべてのトラフィックを外部の Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに送信します。Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C は、L2 MAC アドレスと VLAN に基づくトラフィックを転送します。トラフィックを CSP または外部接続ネットワークに送り返すことができます。CSP インターフェイスに接続されている Catalyst 9500 スイッチポートは、VEPA モードで構成されています。VNF VNIC で VLAN が構成されている場合、VLAN は Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチの接続されたポートで構成する必要があります。

SR-IOV インターフェイスを使用する VNF とソフトウェアスイッチを使用する VNF は、外部スイッチファブリックを介してサービスチェーン化できます。
- **Physical Network Function Network Connectivity** : PNF は、右側から使用できる空きデータポートである Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチポートに接続できます。
- **Service Chains** : Cisco SD-WAN Cloud onRamp for Colocation ソリューション展開では、VNF 間のトラフィックは、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C を介して外

部でサービスチェーン化されます。サービスチェーン化要件は、単一の CSP またはクラスタ内の複数の CSP システムで実行されている VNF 全体のトラフィックにサービスチェーン機能を提供します。サービスチェーン化は、サービスチェーン内の送信元エンドポイントと宛先エンドポイントに基づいていて、プロバイダーのアプリケーションには基づいていません。Cisco SD-WAN Cloud onRamp for Colocation ソリューションでは、L2 (VLAN、宛先 MAC アドレス) ベースのサービスチェーン化が使用されています。

- **Cisco Colocation Manager** : Cisco Colocation Manager (CCM) コンポーネントは、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチを管理するソフトウェアスタックです。このソリューションでは、Cisco Colocation Manager は Docker コンテナ内の NFVIS ソフトウェアでホストされています。CSP デバイスは、ソリューションアーキテクチャの概要に示すように、PNF および VNF とともに Cisco Colocation Manager をホストします。クラスタをアクティブ化すると、クラスタごとに 1 つの CCM インスタンスが CSP デバイスの 1 つで起動されます。CCM ソフトウェアは Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C の構成を受け入れ、それらを監視します。詳細については、「[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](#)」を参照してください。
- **Orchestration through Cisco vManage** : Cisco vManage サーバーは、Cisco SD-WAN Cloud onRamp for Colocation ソリューションのオーケストレーションに使用されます。詳細については、『[Cisco SD-WAN Configuration Guides](#)』を参照してください。



第 3 章

Cisco SD-WAN Cloud onRamp for Colocation ソリューションの前提条件と要件

- [Cisco SD-WAN Cloud onRamp for Colocation ソリューションの要件 \(9 ページ\)](#)
- [ソリューションを展開するための前提条件 \(16 ページ\)](#)
- [Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのサイジング要件 \(17 ページ\)](#)

Cisco SD-WAN Cloud onRamp for Colocation ソリューション の要件

Cisco SD-WAN Cloud onRamp for Colocation ソリューションを展開するためのハードウェア、ソフトウェア、Cloud OnRamp for Colocation クラスタ、およびケーブル接続の要件を以下に示します。

ハードウェア要件

次の表に、ハードウェア要件を示します。

表 3: 機能の履歴

機能名	リリース情報	説明
Cisco Cloud Services Platform、CSP-5456 のサポート	Cisco SD-WAN リリース 20.4.1	このリリース以降、Cisco CSP-5456 は Cloud onRamp for Colocation ソリューションでサポートされています。CSP-5456 は 56 コアのより高いキャパシティを提供し、サービスチェーン内の VNF の配置を最大化します。

表 4:ハードウェア要件

コンポーネント	ハードウェア要件
コンピューティングプラットフォームフォーム	CSP-5444 および CSP-5456
物理フォームファクタ	Cisco UCS C240 M5SX (2RU)
プロセッサ コア数	CSP-5444 : 44 個の物理コア CSP-5456 : 56 個の物理コア
PCIe NIC スロット	6
ディスク	8 × 1.2 TB = 9.6 TB
ディスクスロット数	26 (24 使用可)
メモリ	192 GB の RAM
RAID	12 Gbps SAS HW コントローラ、4 GB フラッシュバックライト キャッシュ (FBWC)、RAID 10。
ベースネットワーキング	M5 6 x 1GE Intel i350 ポートの 4 x 1PCIe カード、2 x 1GE LoM (注) NFVIS および VM 管理トラフィックには、ポートチャネル構成の 2-GigE インターフェイスが必要です。

コンポーネント	ハードウェア要件
ネットワークインターフェイスカード (NIC)	<p>2 x Intel X520 2 ポート 10G (Niantic) および Intel XL710 4 ポート 10G SFP+ (Fortville)</p> <p>(注) ポートチャネル構成で仮想スイッチに接続された 2 つの Fortville 10G インターフェイス。この接続は、virtio インターフェイスのみをサポートする VM との間の実働トラフィックに必要です。</p> <p>(注) ポートチャネル構成で仮想スイッチに接続された 2 つの Fortville 10G インターフェイス。この構成は、2 つの異なる CSP システムでホストされている VNF 間の VNF HA 状態の同期に必要です。</p> <p>(注) SR-IOV モードの 4 つの Niantic 10G インターフェイス。ハイパーバイザまたは仮想スイッチをバイパスするために、高性能で低遅延のネットワーク接続を必要とする VM には、これらのインターフェイスが必要です。SR-IOV をサポートできる VM は、SR-IOV 仮想機能 (VF) に接続する必要があります。このモードでは、リンクの冗長性は利用できません。</p> <p>(注) 規範的接続の場合、Fortville NIC (X710) がライザー 1、スロット 2、および Niantic カード (X520) がライザー 1、スロット 1、およびライザー 2、スロット 4 に配置されていることを確認します。</p>
プロセッサ (2)	2 x Intel Xeon Gold 6152 シリーズ
電源	デュアル電源
ネットワークファブリック	<p>Catalyst 9500-40X</p> <p>40 個の 10G ポートと 2 個の 40G ポートをサポート</p> <p>Catalyst 9500-48Y4C</p> <p>48 個の 1G/10G/25G ポートと 4 個の 40G/100G ポートをサポート</p>
管理ネットワーク	十分な数の 1G ポートとポートチャネル機能を備えたスイッチは、管理スイッチとして使用できます。ハードウェアとリンクの冗長性をサポートするには、2 つのスイッチを推奨します。

ソフトウェア要件

次の表に、ソフトウェア要件を示します。

表 5: ソフトウェア要件

コンポーネント	ソフトウェア要件
仮想化インフラストラクチャ ソフトウェア	Cisco NFVIS Cloud OnRamp for Colocation 「 Release Notes for Cisco SD-WAN Cloud OnRamp for Colocation Solution 」を参照してください。
オーケストレーション	Cisco vManage ビジネスインサイトの <ul style="list-style-type: none"> 詳細については、「Cisco SD-WAN Product Documentation」を参照してください。 最新の Cisco vManage 機能の詳細については、「Cisco SD-WAN Release Notes」を参照してください。

すべての CSP デバイスとスイッチは、Cloud OnRamp for Colocation ソリューションで同じバージョンのソフトウェアを実行する必要があります。コロケーション内のすべてのデバイスの新しいソフトウェアバージョンは、対応可否に応じて Cisco vManage でホストされます。

サポートされているプラットフォームおよびファームウェア

次の表に、サポートされている Cisco NFVIS のプラットフォームとファームウェアバージョンを示します。

プラットフォーム	ファームウェア	バージョン
CSP-5444、CSP-5456	BIOS	C240M5.4.2.2b.0.0613220203
	CIMC	4.2 (2a)

CIMC バージョンをアップグレードするには、『[Cisco Host Upgrade Utility User Guide](#)』を参照してください。



(注) CIMC バージョンをアップグレードするときは、テクニカルアシスタンスセンター (TAC) に連絡することをお勧めします。

配線に関する要件

表 6: 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。

このソリューションは、Cisco CSP デバイスと Cisco Catalyst 9500 スイッチ間のフレキシブルな接続と規範的接続の両方をサポートします。

規範的接続

規範的接続は、Cisco Catalyst 9500-48Y4C および Cisco Catalyst 9500-40X スイッチの両方でサポートされています。

次の情報に基づいて、Catalyst 9500 スイッチの SVL ポートとアップリンクポートを接続していることを確認してください。

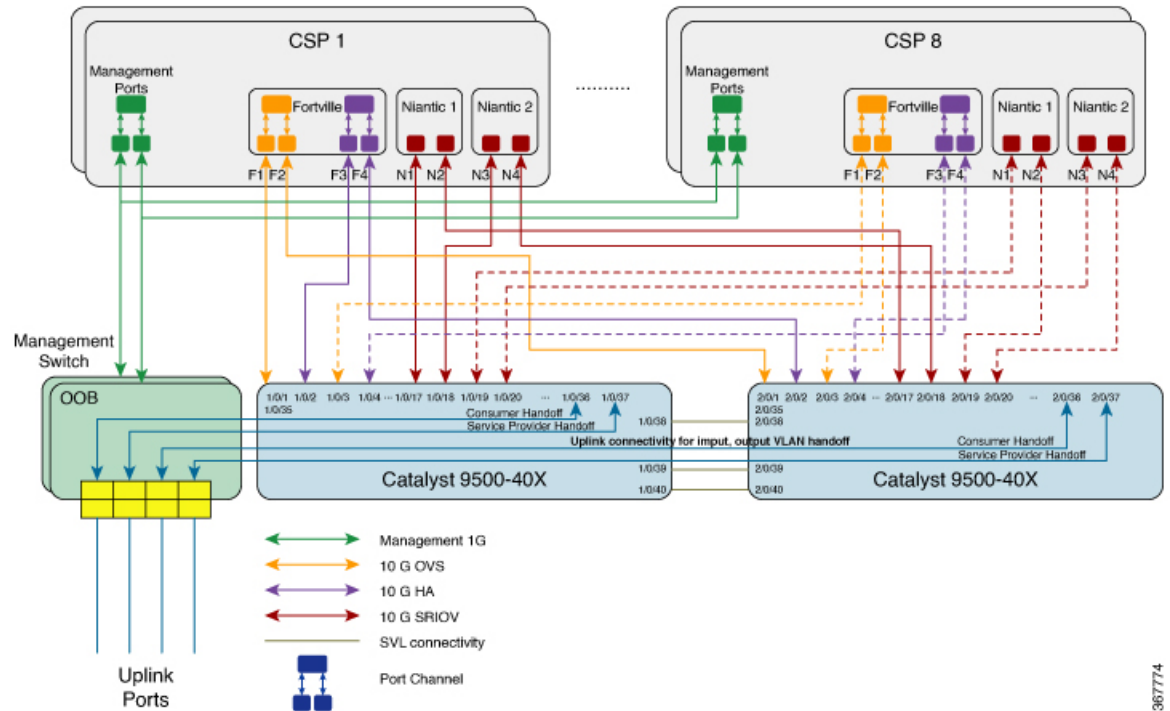
Cisco Catalyst 9500-40X

- Stackwise Virtual Switch Link (SVL) ポート : 1/0/38 ~ 1/0/40、および 2/0/38 ~ 2/0/40
- アップリンクポート : 1/0/36、2/0/36 (入力 VLAN ハンドオフ) および 1/0/37、2/0/37 (出力 VLAN ハンドオフ)

Cisco Catalyst 9500-48Y4C

次の図は、Cisco Catalyst 9500-40X スイッチの物理接続の概要設計を示しています。

図 3: Cisco Catalyst 9500-40X の規範的接続



上記のトポロジでは、各 CSP に OOB 管理スイッチへのポートチャネルとして構成された 2 つの 1 GB 管理ポートがあります。各 Cisco Catalyst 9500-40X スイッチは 1 GB ポートに接続されています。この接続には、Cloud onRamp for Colocation ごとに管理スイッチに 2 つのポートが必要です。サービスプロバイダーのハンドオフは、このスイッチの 10 GB ポートに接続されています。すべてのサービスプロバイダーのポートは、Cisco Catalyst 9500-40X スイッチにトランクされます。すべての VLAN は、Cisco Catalyst 9500-40X スイッチのすべてのポートで構成されます。

同様に、CSP デバイスを所定の方法で Cisco Catalyst 9500-48Y4C スイッチに接続できます。



- (注) 管理スイッチはオーケストレーションされていないため、手動でプロビジョニングする必要があります。管理スイッチはオーケストレーションされていませんが、管理スイッチとデバイスが定義された接続に従って接続されていることを確認してください。

フレキシブルな接続

Cisco Catalyst 9500-40X および Cisco Catalyst 9500-48Y4C スイッチでフレキシブルな接続がサポートされています。フレキシブルな接続の場合、以下に従います。

- 正確に 2 枚の Niantic カードと 1 枚の Fortville カードを Cisco CSP デバイスのライザカードスロットに挿入する必要があります。



(注) Niantic カードをライザスロット 1 と 4 以外のスロットに挿入し、Fortville カードをスロット 2 以外のスロットに挿入する場合は、すべてのカードを接続した後で、Cisco NFVIS を Cisco CSP デバイスにクリーンインストールします。

- Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチの使用可能なポートに接続された Cisco CSP デバイスのすべてのデータポート。

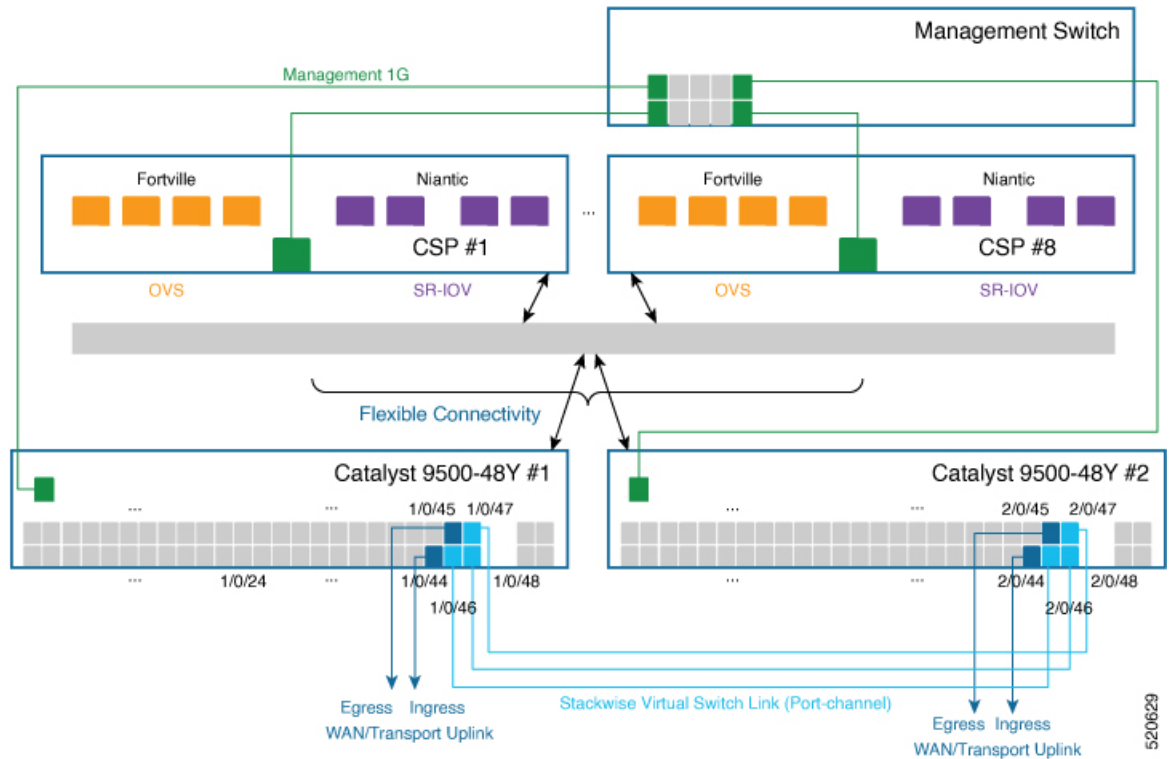


(注) Cisco CSP デバイスのすべてのポートを接続し、それらがプライマリおよびセカンダリスイッチポートに冗長な方法で接続されていることを確認します。すべての Cisco CSP ポートが接続されていない場合、クラスタのアクティブ化プロセスは失敗します。

- 1/0/1 ~ 1/0/48 と 2/0/1 ~ 2/0/48 または 1/0/48 ~ 1/0/52 と 2/0/48 ~ 2/0/52 の間の任意の SVL ポートを接続します。
- 10G/25G スループットの場合は 1/0/1 ~ 1/0/48 と 2/0/1 ~ 2/0/48 の間、または 40G/100G スループットの場合は 1/0/49 ~ 1/0/52 と 2/0/49 ~ 2/0/52 の間の任意のアップリンクポートを接続します
- 冗長性を確保するために、Cisco CSP デバイスのすべての Niantic ポートと Fortville ポートを接続します。たとえば、Niantic ポートがライザスロット 1 と 2 に接続され、Fortville ポートがライザスロット 4 に接続されている場合、次のいずれかの方法で Cisco CSP インターフェイスをスイッチに接続できます。
 - プライマリスイッチ : eth1-1、eth2-1、eth4-1、eth4-3
セカンダリスイッチ : eth1-2、eth2-2、eth4-2、eth4-4
 - プライマリスイッチ : eth1-2、eth2-1、eth4-1、eth4-2
セカンダリスイッチ : eth1-1、eth2-2、eth4-3、eth4-4
- 物理ネットワーク機能 (PNF) を利用可能な Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチに接続します
- Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチをそれぞれ 1 GB 管理ポートに接続します。各 Cisco CSP デバイスには、OOB 管理スイッチへのポートチャネルとして構成された 2 つの 1 GB 管理ポートがあります。管理スイッチは Cisco vManage によってオーケストレーションされません。したがって、次の図に示すように、管理スイッチと管理ポートを接続してください。

次の図は、SVL ポートとアップリンクポートがデフォルトポートに接続されている Cisco CSP デバイスと Cisco Catalyst 9500-48Y4C スイッチ間のフレキシブルな接続を示しています。

図 4: Cisco SD-WAN Cloud onRamp for Colocation ソリューションのフレキシブルな接続



520629

ソリューションを展開するための前提条件

Cisco SD-WAN Cloud onRamp for Colocation ソリューションを展開するための前提条件は次のとおりです。

- 少なくとも2つの CSP PID (2つの Niantics と 1つの Fortville) が必要です。クラスタ (HA インスタンスを含む) ごとに必要なサービスチェーンの数に応じて、より多くの CSP デバイスを注文できます。また、CSP デバイスの数を注文するときは、スループット要件または Cloud onRamp for Colocation を終了するセッション数を考慮してください。
- 注文したデバイスを PNP クラウドと vOrchestrator に反映するために必要なスマートアカウント。
- 2つの Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C および OOB スイッチと、クラスタごとに1つの DHCP サーバーが必要です。
- ポートチャネル、RJ45 およびデータ SFP と、接続用のケーブルが必要です。
- WAN 終端用のルータが必要です。
- スイッチと CIMC を設定するためのターミナルサーバーが必要です。

- クラスタごとの管理 IP プールを 2 つの部分に分割します。クラスタ内の物理デバイスの数とブロードキャストとゲートウェイに必要な IP アドレスを考慮して、DHCP サーバー上の一部を構成します。VNF および Cisco Colo Manager の Cisco vManage で、管理 IP プールの他の部分を構成します。Cisco vManage 管理プールの最初の IP アドレスは、Cisco Colo Manager に使用されます。この IP アドレスと PNP サーバーをスイッチに設定していることを確認してください。

Cisco SD-WAN Cloud onRamp for Colocation ソリューション デバイスのサイジング要件

Cloud onRamp for Colocation クラスタ要件は、スループットとコンピューティングの需要に基づいて、小規模、中規模、大規模、および超大規模のクラスタに分類できます。

次の基準を考慮して、さまざまな Cloud onRamp for Colocation のサイズカテゴリを決定します。



(注) Cloud onRamp for Colocation のサイズは、CSP デバイス、Cisco Catalyst 9500-40X および Cisco Catalyst 9500-48Y4C スイッチなどのデバイスを注文するときに、オーケストレーションの前に決定する必要があります。

- パブリッククラウドに必要な接続の数と、これらのクラウドに到達しようとする顧客の数に応じて、必要なサービスチェーンの数を決定します。
- 適用する必要があるポリシーに応じて、各サービスチェーンで必要な VM の数を決定します。
- 上記の 2 つの基準から、サービスチェーンごとに必要なスループットを平均して判断できます。

単一の Cisco SD-WAN Cloud onRamp for Colocation Solution ソリューションの展開では、4 つの CSP システムをクラスタに展開できます。



第 4 章

Cisco SD-WAN Cloud onRamp for Colocation ソリューションの利用を開始

- [Cisco SD-WAN Cloud onRamp for Colocation ソリューション – 展開ワークフロー \(19 ページ\)](#)
- [Cisco CSP での Cisco NFVIS Cloud OnRamp for Colocation のインストール \(21 ページ\)](#)
- [Cisco Cloud サービス プラットフォーム デバイスの起動 \(24 ページ\)](#)
- [スイッチデバイスの起動 \(28 ページ\)](#)
- [Cisco Colo Manager の起動 \(31 ページ\)](#)
- [Cisco SD-WAN Cloud onRamp for Colocation ソリューションのプロビジョニングと構成 \(31 ページ\)](#)

Cisco SD-WAN Cloud onRamp for Colocation ソリューション – 展開ワークフロー

このトピックでは、colo デバイスの使用を開始し、Cisco vManage 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。「[Cisco SD-WAN Cloud onRamp for Colocation ソリューションの前提条件と要件 \(9 ページ\)](#)」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。「[コロケーションごとの DHCP サーバーのプロビジョニング \(32 ページ\)](#)」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。「[Cisco CSP での Cisco NFVIS Cloud OnRamp for Colocation のインストール \(21 ページ\)](#)」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。「[Cisco SD-WAN Cloud onRamp for Colocation ソリューションの利用を開始 \(19 ページ\)](#)」を参照してください。
 - CSP デバイスを起動します。「[プラグアンドプレイプロセスを使用した CSP デバイスのオンボード \(24 ページ\)](#)」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。「[スイッチデバイスの起動 \(28 ページ\)](#)」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。「[クラスタのプロビジョニングと構成 \(45 ページ\)](#)」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。「[クラスタの設定 \(49 ページ\)](#)」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 \(46 ページ\)](#)』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 \(78 ページ\)](#)』を参照してください。



(注) 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 \(103 ページ\)](#)』を参照してください。



(注) 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 \(103 ページ\)](#)』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。[Cisco vManage を使用した Cloud OnRamp Colocation デバイスの追加 \(41 ページ\)](#) および [Cisco vManage からの Cloud OnRamp for Colocation デバイスの削除 \(43 ページ\)](#) を参照してください。

- クラスタを非アクティブ化します。『[Cisco vManage からのクラスタの削除 \(74 ページ\)](#)』を参照してください。
- クラスタを再アクティブ化します。『[Cisco vManage からのクラスタの再アクティブ化 \(77 ページ\)](#)』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 \(78 ページ\)](#)』を参照してください。

Cisco CSP での Cisco NFVIS Cloud OnRamp for Colocation のインストール

このセクションでは、NFVIS Cloud OnRamp for Colocation を Cisco CSP デバイスにインストールするために実行する必要がある一連のタスクに関する情報を提供します。

CIMC ユーザーインターフェイスのログイン

始める前に

- CIMC にアクセスするための IP アドレスが設定済みであることを確認します。
- ローカルシステムに Adobe Flash Player 10 以降がインストールされていない場合はインストールします。

CIMC の IP アドレスを設定する方法の詳細については、[cisco.com](#) の『[Set up CIMC for UCS C-Series Server](#)』ガイドを参照してください。

CIMC のアップグレードについては、[cisco.com](#) の『[CIMC Firmware Update Utility](#)』ガイドを参照してください。

-
- ステップ 1** 初期セットアップ時に CIMC へのアクセス用に設定した IP アドレスを Web ブラウザに入力します。
- ステップ 2** セキュリティ ダイアログボックスが表示された場合は、次の操作を実行します。
- a) **オプション**: チェックボックスをオンにして、シスコからのすべてのコンテンツを受け入れます。
 - b) [Yes] をクリックして証明書を受け入れ、続行します。
- ステップ 3** ログイン ウィンドウで、ユーザ名とパスワードを入力します。
- 未設定のシステムに初めてログインする場合は、ユーザー名に **admin**、パスワードに **password** を使用します。
- ステップ 4** [Log In] をクリックします。
- [Change Password] ダイアログボックスは、CIMC に初めてログインしたときのみ表示されます。
- ステップ 5** パスワードを適宜変更して保存します。

CIMC のホームページが表示されます。

- ステップ 6** [CIMC Server] タブで、[Summary] を選択し、[Launch KVM Console] をクリックします。
[KVM Console] が別ウィンドウで開きます。
- ステップ 7** KVM コンソールの [Virtual Media] メニューから、[Activate Virtual Devices] を選択します。
暗号化されていない仮想メディアセッションメッセージが表示されたら、[Accept this session] を選択し、[Apply] をクリックします。仮想デバイスがアクティブになります。
- ステップ 8** KVM コンソールの [Virtual Media] メニューから、[Map CD/DVD] を選択します。
- ステップ 9** ローカルシステム上のインストールファイル (ISO) を参照して選択します。
- ステップ 10** [Map Device] をクリックします。
これで、ISO イメージファイルが CD/DVD にマップされました。
- ステップ 11** [CIMC Server] タブから、[BIOS] を選択します。
BIOS のアップグレードの詳細については、cisco.com の「[BIOS Upgrade](#)」ガイドを参照してください。
- ステップ 12** [BIOS Actions] エリアから、[Configure Boot Order] を選択します。
[Configure Boot Order] ダイアログボックスが表示されます。
- ステップ 13** [Device Types] エリアから、[CD/DVD Linux Virtual CD/DVD] を選択し、[Add] をクリックします。
- ステップ 14** [HDD] を選択し、[Add] をクリックします。
- ステップ 15** [Up] および [Down] オプションを使用して、起動の順序を設定します。[CD/DVD Linux Virtual CD/DVD] 起動順序オプションは、最初の選択肢である必要があります。
- ステップ 16** 起動順序の設定を完了するには、[Apply] をクリックします。
- ステップ 17** CIMC の [Server Summary] ページから [Power Off Server] オプションを選択して、サーバーをリブートします。
- ステップ 18** サーバーがダウンしたら、CIMC で [Power On Server] オプションを選択します。
サーバーがリブートすると、KVM コンソールによって、仮想 CD/DVD ドライブから Cisco Enterprise NFVIS が自動的にインストールされます。インストールが完了するまで 30 分～1 時間ほどかかることがあります。
- ステップ 19** インストールが完了すると、システムはハードドライブから自動的にリブートします。リブート後、コマンドプロンプトが「localhost」から「nfvis」に変わったら、システムにログインします。
システムがコマンドプロンプトを自動的に変更するまでしばらく待ちます。自動的に変更されない場合は、Enter キーを押して、コマンドプロンプトを「localhost」から「nfvis」に手動で変更します。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 #** を使用します。
- (注) 初めてログインすると、デフォルトのパスワードを変更するように求められます。アプリケーションを続行するには、画面の指示に従って強力なパスワードを設定する必要があります。最初のログイン時にデフォルトのパスワードを変更しない限り、API コマンドを実行したり、タスクを続行したりすることはできません。デフォルトのパスワードがリセットされていない場合、API は 401 未承認エラーを返します。

ステップ 20 システム API を使用するか、Cisco Enterprise NFVIS ポータルからシステム情報を表示して、インストールを確認できます。



(注) RAID 構成が 4.8 TB RAID-10 であることを確認します。CIMC を介して RAID を構成するには、cisco.com の『[Cisco UCS Servers RAID Guide](#)』を参照してください。

仮想デバイスのアクティブ化

仮想デバイスをアクティブ化するには、KVM コンソールを起動する必要があります。

始める前に

Java 1.6.0_14 以降のバージョンがローカルシステムにインストールされていることを確認します。

ステップ 1 所定の場所からローカルシステムに Cisco Enterprise NFVIS イメージをダウンロードします。

ステップ 2 CIMC から、[Server] タブを選択し、[Launch KVM Console] をクリックします。

(注) JNLP ファイルがシステムにダウンロードされます。セッションタイムアウトを回避するには、ダウンロードした直後にファイルを開く必要があります。

ステップ 3 名前を変更した .jnlp ファイルを開きます。Cisco Virtual KVM Console をダウンロードするように求められたら、[Yes] をクリックします。すべてのセキュリティ警告を無視して、起動を続行します。

KVM コンソールが表示されます。

ステップ 4 KVM コンソールの [Virtual Media] メニューから、[Activate Virtual Devices] を選択します。

暗号化されていない仮想メディアセッションメッセージが表示されたら、[Accept this session] を選択し、[Apply] をクリックします。仮想デバイスがアクティブになります。

NFVIS Cloud OnRamp for Colocation イメージのマッピング

ステップ 1 KVM コンソールの [Virtual Media] メニューから、[Map CD/DVD...] を選択します。

ステップ 2 ローカルシステム上のインストールファイル (ISO) を参照して選択します。

ステップ 3 [Map Device] をクリックします。

これで、ISO イメージファイルが CD/DVD にマップされました。

ステップ 4 KVM コンソールから、電源の再投入（ウォームリブート）とシステムのインストールプロセスが開始され、NFVIS がインストールされます。

Cisco Cloud サービス プラットフォーム デバイスの起動

表 7: 機能の履歴

機能名	リリース情報	Description
USB ドライブを使用した Day-0 構成での CSP デバイスのオンボーディング	Cisco SD-WAN リリース 20.4.1	この機能により、Day-0 構成ファイルを USB ドライブにロードすることにより、CSP デバイスをオンボードできます。インターネットにアクセスして Plug-and-Play Connect サーバーに到達できない場合は、このオンボーディングオプションを使用します。

Cisco Cloud Services Platform (CSP) デバイスを起動するには、次のオプションを使用できます。

- **自動展開**：Day-0 構成時に、工場出荷時の設定で CSP デバイスを Cisco SD-WAN ネットワークに安全にオンボードして展開します。この展開では、Cisco CSP デバイスのプラグアンドプレイ (PnP) プロセスを使用して Cisco vBond オーケストレーションの IP アドレスを動的に検出します。
- **ブートストラップ展開**：構成ファイルを CSP デバイスと共有する必要があります。構成ファイルを作成して起動可能 USB にコピーするか、構成ファイルを USB に追加することができます。起動可能 USB が接続されていて、起動時にデバイスで使用できます。

プラグアンドプレイプロセスを使用した CSP デバイスのオンボード

このトピックでは、PnP プロセスを使用して Cisco CSP デバイスの起動を自動化する方法について説明します。

始める前に

- 所定のトポロジに従って CSP デバイスを接続し、電源をオンにします。
- プラグアンドプレイ (PnP) 対応インターフェイスを WAN トランスポート（通常はインターネット）に接続します。

Cisco CSP デバイスの電源を入れます。次のプロセスが発生します。

ステップ 1 デバイスが起動すると、デバイスのサポートされている PnP インターフェイス上の DHCP プロセスを介して、IP アドレス、デフォルトゲートウェイ、および DNS 情報を取得します。

- ステップ 2** デバイスは、Cisco Cloud でホストされている PnP Connect サーバーに接続し、そのシャーシまたはシリアル番号を PnP サーバーと共有して認証を受けます。
- ステップ 3** 認証後、PnP Connect ポータルは Cisco vBond オーケストレーション、組織名、およびルート証明書に関する情報をデバイスに提供します。
- エンタープライズルート CA 証明書を使用する展開の場合、Cisco vBond オーケストレーションの IP アドレスまたは DNS、組織名、およびエンタープライズルート CA 証明書に関する情報は、HTTPS プロトコルを使用して PnP Connect ポータルからデバイスにダウンロードされます。デバイスはこの情報を使用して、Cisco vBond オーケストレーションとの制御接続を開始します。
- PnP 接続ポータルを介して、PnP インターフェイスでデバイスの可用性と Cisco vBond オーケストレーションとの関連付けを表示できます。
- ステップ 4** デバイスが PnP 経由で Cisco vBond オーケストレーションにリダイレクトされると、PnP 接続ポータルに [Redirect Successful] ステータスが表示されます。
- ステップ 5** Cisco vBond オーケストレーションでの認証後、デバイスには Cisco vManage と Cisco vSmart コントローラ情報が提供され、登録してセキュアな接続を確立します。
- ステップ 6** デバイスは、Cisco vManage サーバーとのセキュアな制御接続を確立しようとします。
- ステップ 7** Cisco vBond オーケストレーションでの認証後、Cisco vManage サーバーはデバイスのシステム IP でデバイスに応答し、共有システム IP 情報を使用してデバイスを再認証します。
- ステップ 8** Cisco SD-WAN オーバーレイネットワークに参加するために、デバイスは、設定された system-ip IP アドレスを使用して、すべての SD-WAN コントローラへの制御接続を再開します。

USB ブートストラッププロセスを使用した CSP デバイスのオンボード

自動検出オプションを使用できない場合は、この展開オプションを使用して、構成なしで出荷される工場出荷時のデバイスを構成します。

次の場合に、この展開オプションをお勧めします。

- デバイスが、動的 IP アドレスを提供できないプライベート WAN トランスポート (MPLS) に接続されている。
- プラグアンドプレイ接続サーバーにアクセスするためのインターネットアクセスが利用できない。

考慮すべき点

- USB ドライブには、ファイル名のデバイスのシリアル番号で識別される複数の Day-0 構成ファイルを含めることができます。この命名規則により、複数のデバイスのブートストラップに同じ USB ドライブを使用できます。
- 構成ファイルに含まれるサポートされている Day-0 構成は次のとおりです。
 - デバイスの静的 IP 構成
 - Cisco vBond オーケストレーション IP アドレスとポート構成

- DNS サーバーとドメイン名構成
- ブートストラップ構成は、USB キーにアップロードして、インストールサイトのデバイスに挿入できます。

始める前に

- デバイスは、構成が追加されていない工場出荷時のデフォルト状態である必要があります。
- デバイスには、Cisco NFVIS の新しいイメージをインストールする必要があります。
- USB ドライブは、ドライブを認識して自動マウントするために仮想ファイルアロケーションテーブル (VFAT) でフォーマットされている必要があります。USB ドライブをラップトップまたはデスクトップに挿入してフォーマットします。
- デバイスは Cisco vBond オーケストレーション に到達できる必要があります。

ステップ 1 USB ドライブのルートフォルダに構成ファイルを作成します。

構成ファイル名が *nfvis_config_SERIAL.xml* であることを確認します。ここで、

SERIAL は、CSP デバイスのシリアル番号を表します。

次に例を示します。

nfvis_config_WZP232903K6.xml

ステップ 2 以下を構成ファイルにコピーします。

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <vm_lifecycle xmlns="http://www.cisco.com/nfvis/vm_lifecycle">
    <networks>
      <network>
        <name>int-mgmt-net</name>
        <subnet>
          <name>int-mgmt-net-subnet</name>
          <address>192.168.30.6</address>
          <netmask>255.255.255.0</netmask>
          <gateway>192.168.30.1</gateway>
        </subnet>
      </network>
    </networks>
  </vm_lifecycle>

  <system xmlns="http://viptela.com/system">
    <organization-name>vIPTela Inc Regression</organization-name>
    <sp-organization-name>vIPTela Inc Regression</sp-organization-name>
    <vbond>
      <remote>172.23.191.87</remote>
      <port>12346</port>
    </vbond>
  </system>

  <vpn xmlns="http://viptela.com/vpn">.
    <vpn-instance>
      <vpn-id>0</vpn-id>
```

```
<interface>
  <if-name>colo-mgmt</if-name>
  <tunnel-interface>
    <encapsulation>
      <encap>ipsec</encap>
    </encapsulation>
  </tunnel-interface>
  <shutdown>>false</shutdown>
</interface>
</vpn-instance>
</vpn>
</config>
```

(注) デバイスの上記の静的 IP 構成を構成ファイルにコピーすることが必須です。デバイスの静的 IP 構成は、次の Day-0 構成で表されます。

```
<address></address>, <netmask></netmask>, and <gateway></gateway>
```

ステップ 3 USB ドライブを Cisco CSP デバイスに挿入し、デバイスの電源を入れます。

デバイスが起動すると、デバイスはブート可能な USB ドライブで構成ファイルを検索します。ファイルが見つかったら、デバイスは PnP プロセスを一時停止し、ブートストラップ構成ファイルをロードします。

ステップ 4 USB ドライブを取り外します。

(注) 構成の適用後に USB ドライブをアンマウントしてデバイスをリブートしないと、USB ドライブの構成は再適用されません。CSP デバイスが出荷時データリセット (FDR) 状態ではないか、元のシステム状態に復元されていません。

ステップ 5 CSP デバイスにアクセスするには、ステップ 2 で指定した静的 IP アドレス (192.168.30.6 など) に SSH で接続します。

ステップ 6 最初のログイン時にシステムから変更を求めるプロンプトが表示されたら、デフォルトのパスワードを変更します。

画面の指示に従って、強力なパスワードを設定してください。最初のログイン時にデフォルトのパスワードを変更しない限り、API コマンドを実行したり、タスクを続行したりすることはできません。

次のタスク

デバイスのオンボーディングプロセスを確認するには、[オンボードデバイスの確認とデバイスのアクティブ化 \(27 ページ\)](#) に進みます。

オンボードデバイスの確認とデバイスのアクティブ化

ステップ 1 URL `HTTPS://vManage-ip-address/` を使用して、管理者ログイン情報で Cisco vManage にログインします。

ステップ 2 **[Configuration] > [Devices]** をクリックします。

デバイスのリストから、トークンという単語を含むシリアル番号を持つ CSP デバイスは、まだオンボードされていません。これらのデバイスを SD-WAN コントローラで認証するために、Cisco vManage はワンタ

イムパスワード (OTP) を提供します。OTP は、SD-WAN コントローラの承認済みデバイスリストに CSP デバイスを追加した後に Cisco vManage によって自動生成されます。

ステップ 3 [Valid] 列で、一覧表示されているすべての CSP デバイスのインストール済み証明書の有効性を確認します。[証明書](#)のインストールの失敗 (177 ページ) を参照してください。また、ルート CA がインストールされているかどうかを確認します。[CSP が Cisco vManage との接続を確立していない](#) (179 ページ) を参照してください。

(注) エンタープライズルート CA 証明書を使用するデバイスオンボーディングの場合、CSP デバイスは、PnP Connect ポータルからルート証明書と、Cisco vBond オーケストレーション および組織名情報を受け取ります。

ステップ 4 CSP デバイスをアクティブ化し、シャシ番号とシリアル番号 (ワンタイムパスワード) を CSP デバイスに関連付けるには、CSP デバイスの CLI で次のコマンドを使用します。

```
request activate chassis-number chassis-number token token-number
```

request device コマンドの詳細については、「[request device](#)」を参照してください。

例 :

```
request activate chassis-number CSP-5444-serial-number token 70d43cfbd0b3b426da63dba2dd4f4c49
```

ステップ 5 残りの CSP デバイスを起動するには、CSP デバイスごとにステップ 1 ~ 4 を繰り返します。

スイッチデバイスの起動

このセクションでは、Day-0 構成を通じて Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチデバイスを起動する方法について説明します。

始める前に

スイッチデバイスを起動する前に、次の点に注意してください。

- Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチデバイスには、Network-Advantage と Cisco DNA-Advantage の両方のライセンスがあります。スイッチデバイスで使用可能なライセンスを確認するには、次のコマンドを使用します。

```
Device# show license status
```

ライセンス使用情報については、**show license usage** コマンドを参照してください。

- PNP リダイレクトセットアップまたはスイッチデバイスで設定されている手動 PNP プロファイルのいずれかが必要です。PNP リダイレクトセットアップの場合、スイッチ SN と Cisco Colo Manager IP アドレスを PNP に追加し、`devicehelper.cisco.com` のエントリをネットワークの OOB ルータに追加します (DHCP サーバーが OOB ルータ上にある場合)。次に例を示します。

```
#conf t
#ip host devicehelper.cisco.com <OOB router of the network>
```

- 両方のスイッチが SVL モード構成に従って接続されていることを確認します。

ステップ 1 以前に使用したことがある場合は、スイッチ構成をクリーニングします。

- a) SVL スタックモードに必要なスイッチの番号を付け直します。

(注) SVL モード中はスイッチに触れないようにしてください。また、Enter キーやスペースキーを押すなどの操作を実行しないでください。これにより、スイッチで SVL が完了する可能性があります。

show switch コマンドを使用して、スイッチ番号とスイッチスタックにプロビジョニングされたスイッチが存在するかどうかを特定します。スイッチ番号が 2 の場合は、**switch 2 renumber 1** コマンドを使用し、次に構成を消去します。

- b) スwitchのスタートアップ構成を消去して初期状態に戻すには、**write erase** コマンドを使用します。
 c) 新しい構成でスイッチをリロードするには、特権 EXEC モードで次のコマンドを使用し、変更された構成を保存しないために **no** を入力します。

```
switch(config)#reload
```

(注) 構成を保存する必要はありません。

- d) スwitchスタックのリロードが完了したら、セカンダリスイッチデバイスで手順 b および c を実行します。このアクションにより、セカンダリスイッチデバイスが 2 回リロードされます。

ステップ 2 Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スwitchの起動後、ローカル DHCP サーバーから IP アドレスを取得し、PNP 検出を開始します。

ステップ 3 オプション 43 を使用する DHCP サーバーにより、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スwitchは Cisco Colo Manager の PNP サーバーに到達できます。

Cisco Colo Manager の IP アドレスは、Cisco vManage 上のクラスタの PNP サーバーの IP アドレスです。オプション 43 の DHCP サーバーが常にポート 9191 を指すようにします。

例：

次に、スイッチのローカル PNP サーバーの例を示します。

```
ip dhcp pool Cat9k
network 10.114.11.39 255.255.255.0
dns-server 172.31.232.182
default-router 172.31.232.182
option 43 ascii "5A;B2;K4;I10.114.11.40;J9191"
```

ここで、10.114.11.40 はローカル PNP サーバーまたは Cisco Colo Manager の IP アドレスです。

オプション 43 を使用する DHCP サーバーをポート 9191 に設定した後の出力は次のとおりです。

```
ip dhcp excluded-address 172.31.232.182 172.31.232.185
ip dhcp excluded-address 172.31.233.182
ip dhcp excluded-address 172.31.232.254
ip dhcp excluded-address 172.31.23.10 172.31.23.49
ip dhcp excluded-address 172.31.23.52 172.31.23.100
ip dhcp excluded-address 172.31.23.252
ip dhcp excluded-address 172.31.23.253
ip dhcp excluded-address 172.31.23.230 172.31.23.250
!
```

ステップ 4 スイッチが Cisco Colo Manager の PNP サーバーに到達すると、Day-0 構成がプッシュされます。Day-0 構成のプッシュは、クラスタが Cisco vManage でアクティブ化されている場合に発生します。クラスタがアクティブ化されていない場合、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチは Cisco Colo Manager の PNP サーバーに 1 分ごとに到達し、バックオフモードのままになります。

スイッチデバイスが起動すると、スイッチデバイス上の SSH 接続と NETCONF セッションが有効になり、Cisco Colo Manager が Day-N 構成をプッシュし、継続的なスイッチ管理が続行されます。

例

規範的接続のアップリンクポート 36 および 37 について

規範的接続の場合、ポート 36（入力 VLAN ハンドオフ）および 37（出力 VLAN ハンドオフ）はアップリンクポート用に予約されています。



(注) 1/0/36、1/0/37 および 2/0/36、2/0/37 スイッチポートは「アクティブ」モードで構成されません。ユーザーがポートチャネルを使用しておらず、ポート 36 および 37 に接続していない場合、ポート 36 または 37 の Cisco Catalyst 9500-40X に接続されている OOB スイッチポートを「パッシブ」モードとして構成する必要があります。

次に例を示します。

- **interface Port-channel1 switchport trunk allowed VLAN 100-106**

```
example VLANs
switchport mode trunk
!
```

- **interface TenGigabitEthernet1/0/1**

```
port connected to cat9k 1/0/36 or 1/0/37
switchport mode trunk
channel-group 1 mode passive
spanning-tree portfast
!
```

- **interface TenGigabitEthernet1/0/2**

```
interface TenGigabitEthernet1/0/2
switchport mode trunk
channel-group 1 mode passive
spanning-tree portfast
!
```

次のタスク

別のスイッチを起動するには、次のスイッチに対して、前述のすべての手順を順番に繰り返します。

Cisco Colo Manager の起動

このセクションでは、Cisco Colo Manager の起動方法について説明します。Cisco Colo Manager は、クラスタ内の Catalyst 9K スイッチの PNP エージェントとして機能します。Catalyst 9K スイッチへの Day-0 構成のプッシュを処理し、Cisco vManage から Catalyst 9K に構成をリレーします。



(注) クラスタのアクティブ化プロセス中に、Cisco Colo Manager が自動的に起動します。

- ステップ 1** Cloud onRamp for Colocation 内のすべての CSP デバイスは、Cisco vManage との DTLS トンネルを確立します。
- ステップ 2** Cisco vManage は、NETCONF アクション API を送信して、その CSP デバイスで Cisco Colo Manager を起動することにより、1 つの CSP デバイスを選択します。
- ステップ 3** Cisco Colo Manager は、起動時は「Starting」状態です。Cisco Colo Manager は、正常性チェックのステータスに応じて、「Healthy」または「Unhealthy」状態に移行できます。

次のタスク

スイッチの構成後、Colo Manager が起動すると、両方のスイッチが Colo Manager に到達します。Cisco Colo Manager の PNP リストをチェックして、両方のスイッチデバイスがホームにコールしたことを確認してください。『[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 \(168 ページ\)](#)』を参照してください。



(注) アクティベーションを続行するには、両方のスイッチがホームにコールする必要があります。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションのプロビジョニングと構成

Cisco SD-WAN Cloud onRamp for Colocation PID を注文するには、Cisco Commerce Workspace (CCW) で Cisco SD-WAN Cloud onRamp for Colocation を選択します。

注文時に、スマートアカウント名、バーチャルアカウント名などの顧客固有の注文の詳細を指定する必要があります。

Cisco SD-WAN Cloud onRamp for Colocation ソリューション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. Cloud Service Platform (CSP) デバイスおよび Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチが、所定の接続またはフレキシブルな接続に従ってケーブル接続され、電源がオンになっていることを確認します。
2. スマートアカウントは、顧客固有のデバイス注文の詳細を PNP Connect および vOrchestrator と同期します。

コロケーションごとの DHCP サーバーのプロビジョニング

スイッチ、VNF、CSP デバイスなどの物理デバイスの IP アドレスを管理するには、コロケーションごとに DHCP サーバーを構成する必要があります。Cisco Colo Manager の IP アドレスは、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C の DHCP オプション 43 で、Cisco Colo Manager に到達するように設定できます。

Cisco vManage は、コロケーションの Cisco Colo Manager IP アドレスを修正して割り当てます。これは、Day-0 構成を通じてすべての VNF の IP アドレスを管理および割り当てます。



-
- (注) 物理 (CSP デバイス、スイッチ) と仮想アプライアンス (Cisco Colo Manager、VNF) の両方のサブネットは同じである必要があります。
-

コロケーションに適切なサブネットを選択し、コロケーション内の CSP デバイスとスイッチの数に応じて IP アドレスのプールを制限できます。Cisco vManage は、Cisco vManage インターフェイスの VNF 管理 IP プールに入力された最初の IP アドレスを選択し、(スイッチ PNP サーバー IP) Cisco Colo Manager IP アドレスとして構成します。管理プールの 2 番目と 3 番目の IP アドレスは、スイッチ管理 IP アドレスに使用されます。スイッチの PNP の DHCP サーバーで別の IP アドレスが構成されている場合は、[Switch PNP Server IP] フィールドを編集して、代替の IP アドレスを指定できます。Cisco vManage プールの残りの IP アドレスは、コロケーション内の残りの VNF に割り当てられます。



-
- (注) 各コロケーションに DNS サーバーを設定してください。
-

規範的接続のためのデバイスポート接続の詳細とサービスチェーン

Cisco SD-WAN Cloud onRamp for Colocation ソリューション展開では、CSP システムに接続された Cisco Catalyst 9500-40X スイッチがサービスチェーンを実行します。VM が SR-IOV をサポートしている場合、Cisco Catalyst 9500-40X スイッチはサービスチェーンを実行しますが、SR-IOV をサポートしていない VM は、オープン仮想スイッチ (OVS) によってサービスチェーンを実行します。

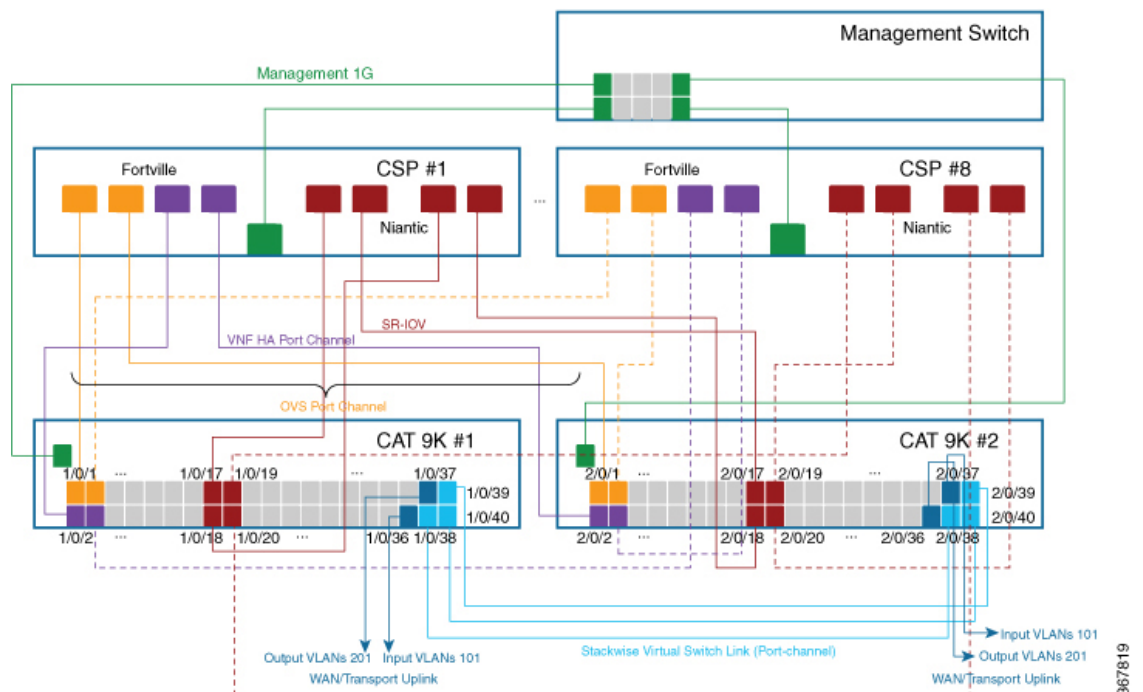
仮想スイッチベースのサービスチェーンは、高可用性トラフィックと制御トラフィックに使用されます。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションには、Cisco Catalyst 9500-40X スイッチからの VLAN ベースの L2 サービスチェーンが使用されます。このサービスチェーンでは、サービスチェーン内の VM の各仮想 NIC インターフェイスが、CSP 仮想スイッチ上の同じアクセス VLAN 上に構成されます。スイッチは、vNIC インターフェイスに出入りするパケットの VLAN タグをプッシュします。VNF は、サービスチェーンの次のサービスを認識しないままにすることができます。同じ CSP でホストされている VNF 間、またはクラスタ内の異なる CSP デバイス間でトラフィックを転送するには、一致する VLAN を持つ物理スイッチを構成します。

Cisco SD-WAN Cloud onRamp for Colocation ソリューションの展開では、ユニキャストトラフィック用の CSP デバイスに接続されているスイッチポートで `deja-vu` チェックが無効になっています。

次のトポロジは、CSP ポートから Cisco Catalyst 9500-40X スイッチおよび OOB スイッチへの接続を示しています。

図 5: OVS、VEPA 対応スイッチポートによるサービスチェーン接続



スイッチのインターフェイスの場所は次のとおりです。

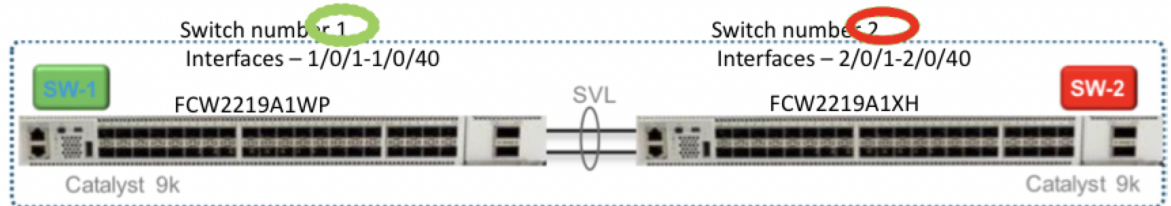


- (注) インターフェイスの場所は、クラスタが正常にアクティブ化された後、スイッチが SVL モードになると適用されます。

```

SW-1#show platform
Switch Ports Model Serial No. MAC address Hw Ver. Sw Ver.
-----
1 50 C9500-40X FCW2219A1WP 848a.8da0.c200 V01 16.12.X
2 50 C9500-40X FCW2219A1XH 848a.8da0.d000 V01 16.12.X
Switch/Stack Mac Address : 848a.8da0.c200 - Local Mac Address
Mac persistency wait time: Indefinite

```



次のポートは VEPA が無効になっていて、ポートチャンネルで構成されています。

- 1/0/1 ~ 1/0/16
- 2/0/1 ~ 2/0/16

次のポートは VEPA が有効になっていて、ポートチャンネル構成は無効になっています。

- 1/0/17 ~ 1/0/32
- 2/0/17 ~ 2/0/32



(注) VEPA ポートは、SRIOV インターフェイスにのみ適用されます。

次のポートは、WAN 接続ポートです。

- 1/0/36、2/0/36 : ポート 1/0/36 を接続して、ブランチ/VPN 接続からの外部トラフィックを受信します (OOB スイッチ経由)。
- 1/0/37、2/0/37 : ポート 1/0/37 を接続して、サービス チェーン トラフィックを、OOB スイッチ上のプロバイダーネットワークにマッピングされている特定の VLAN に転送します。

ポートは次のように接続できます。

- データポート : ポート 1/0/1 ~ 1/0/35 を CSP デバイスに接続します。スイッチ全体で冗長性と HA を実現するには、2 つのポートを 1 つの CSP に接続し、他の 2 つのポートを次の CSP に接続します。たとえば、ポート 1/0/1 と 2/0/1 はデータに使用され、HA はそれぞれ最初の CSP、CSP #1 に接続できます。次に、1/0/2 および 2/0/2 は、次の CSP、CSP #2 などに接続される別のポートチャンネルです。したがって、OVS ポートは 8 つの CSP デバイスすべてを使用します。

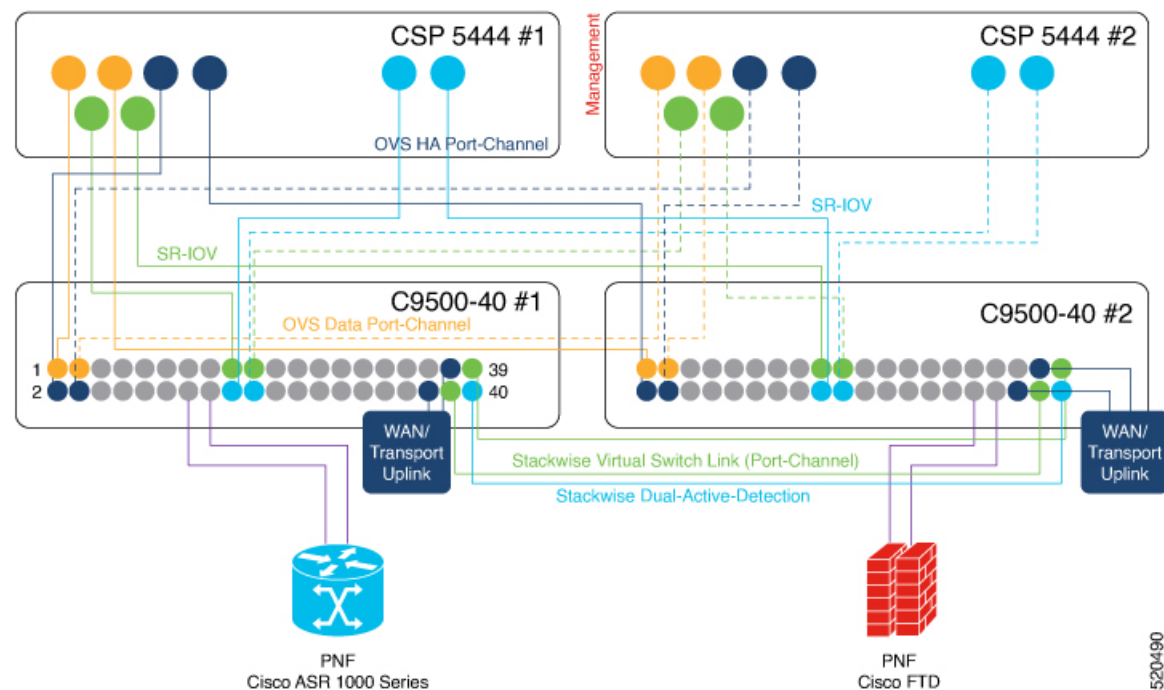
- WAN 接続ポート：構成された VLAN のポート 1/0/36 を接続して、外部トラフィックを受信します（入力 VLAN ハンドオフ）。ポート 1/0/37 を接続して、サービスチェーントラフィックをプロバイダーネットワークにマッピングされている特定の VLAN に転送します（出力 VLAN ハンドオフ）。外部入力または出力 VLAN トラフィックは、ブランチまたは VPN 接続から来ることができ、プロバイダーネットワークは、OOB スイッチを介して Cloud OnRamp for Colocation で終端します。クラスタに構成された各サービスチェーンと、各サービスチェーンに構成された入力または出力 VLAN の場合、ポート 36 および 37 の構成は、サービスチェーンの展開中に発生します。

ポート 36 または 37 が OOB スイッチに接続されていて、ポートチャネルを使用していない場合は、すべての VLAN ハンドオフが、入力または出力 VLAN ハンドオフに対応して設定されていることを確認します。たとえば、ポート 36 が接続されている場合、サービスチェーンの入力 VLAN ハンドオフですべての VLAN ハンドオフを構成します。ポート 37 が接続されている場合、サービスチェーンの出力 VLAN ハンドオフですべての VLAN ハンドオフを構成します。

- Stackwise Virtual Switch Link (SVL) 構成でポート 1/0/38 ~ 1/0/40 を接続します。

次のケーブル接続イメージは、物理ネットワーク機能が Cisco Catalyst 9500-40X スイッチにどのように接続されているかを示しています。

図 6: PNF ケーブル接続イメージ



次の表に、PNF で使用できるポートを示します。

表 8: Cisco Catalyst 9500-40X スイッチ上の PNF のポート

CSP デバイスの数	PNF の数	最初のスイッチの PNF に使用可能なスイッチポート	2 番目のスイッチの PNF に使用可能なスイッチポート
7	1	1/0/15 ~ 1/0/16、 1/0/31 ~ 1/0/32	2/0/15 ~ 2/0/16、 2/0/31 ~ 2/0/32
6	2	1/0/13 ~ 1/0/16、 1/0/29 ~ 1/0/32	2/0/13 ~ 2/0/16、 2/0/29 ~ 2/0/32
4	4	1/0/11 ~ 1/0/16、 1/0/27 ~ 1/0/32	2/0/11 ~ 2/0/16、 2/0/27 ~ 2/0/32

CSP デバイスを削除してポートを入れ替えるには、次の手順を実行します。

1. 8 つすべての CSP デバイスがスイッチに接続されていて、PNF デバイスをスイッチに接続する場合は、次の手順を実行します。
 1. Cisco vManage の RMA ワークフローを使用して、クラスタから 8 番目の CSP（スイッチの右端のデータポートに接続されている CSP）を非アクティブ化または削除します。
 2. Cisco Catalyst 9500-40X スイッチの CSP 物理接続を切断します。
 3. 切断された CSP の代わりに PNF デバイスを接続します。
2. 追加のポートを PNF で使用できるようにするために、最初の 7 つの CSP デバイスのいずれかを削除する必要がある場合は、次の手順を実行します。
 1. 1 に記載されている手順を実行します。
 2. 8 番目の CSP である右端の接続された CSP を、削除された CSP によって使用可能になるポートに移動します。

たとえば、1 番目の CSP が削除されている場合は、8 番目の CSP を 1 番目の CSP の位置に移動し、8 番目の CSP の代わりに PNF を接続します。

Cisco SD-WAN Cloud onRamp for Colocation ソリューション展開の最初のフェーズでは、フルチェーン VNF 構成がサポートされます。フルチェーン構成では、プロデューサチェーンとコンシューマチェーンのすべての VNF は、単一のサービスチェーンの一部です。VNF は、異なるタイプのプロデューサとコンシューマ間で共有されません。サービスチェーンの個別のインスタンスは、コンシューマタイプとプロデューサタイプの各組み合わせをサポートします。フルチェーン構成の場合、チェーン内のすべての VNF は L2 サービスチェーンです。

Cisco vManage は、Cisco SD-WAN Cloud onRamp for Colocation ソリューションのサービスチェーン構成を管理します。Cisco vManage は、コロケーション用に提供された VLAN プールから個々の VM VNIC に VLAN を割り当て、適切な VLAN でスイッチを構成します。VNF は、サー

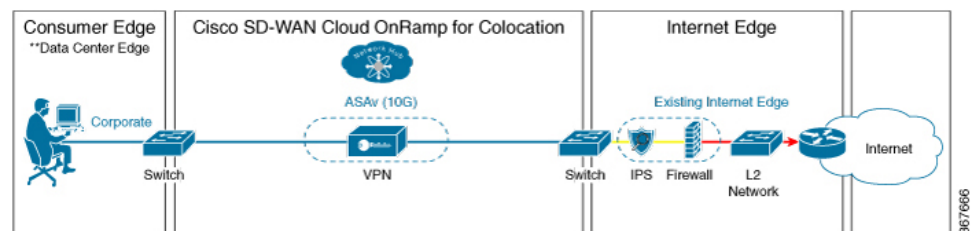
ビスチェーンを認識しないままにすることができます。Day-0 VNF 構成とは別に、Cisco vManage はサービスチェーンの一部である個々の VNF を構成しません。

検証済みサービスチェーン

Cisco SD-WAN Cloud onRamp for Colocation ソリューション展開で、Cisco vManage からクラスター内に展開できる4つの検証済みサービスチェーンを次に示します。すべての検証済みサービスチェーンについて、各 VM は HA またはスタンドアロンモードでインスタンス化できます。

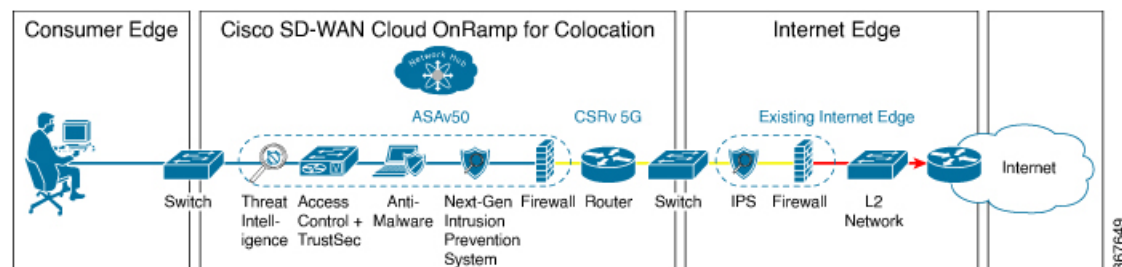
- 従業員のリモート VPN アクセス：このサービスチェーンには、L3 VPN HA または L3 VPN 非 HA モードのファイアウォールがあります。ファイアウォール VNF は、ASA v、パロアルト ネットワークス ファイアウォール、Firepower Threat Defense Virtual (FTDv) にすることができます。ここでは、ASA v はルーテッドモードであり、VPN 接続に対する Day-0 構成のサポート、コンシューマチェーン上の BGP、および VLAN はありません。

図 7: 従業員リモート VPN アクセスサービスチェーン



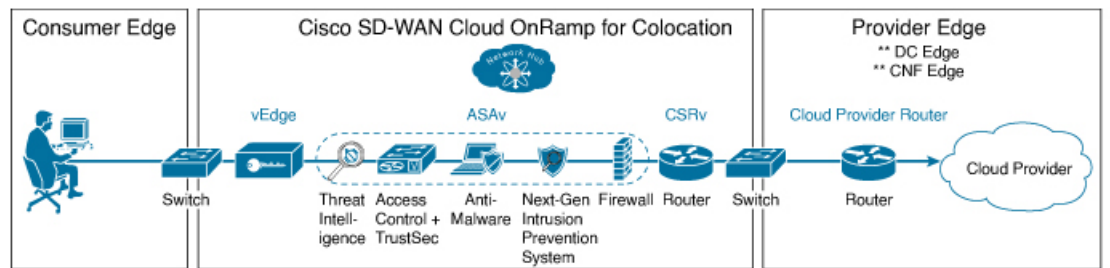
- インターネットエッジ（アウトバウンドインターネット、eコマース、SaaS） - このサービスチェーンでは、ファイアウォールの後にルータが続きます。ファイアウォールモードは、L3-VLAN HA および L3-VLAN 非 HA にすることができます。ルータは、L3 HA モードおよび L3 非 HA モードにすることができます。ここで、ASA v は常にルーテッドモードです。1つの VLAN ハンドオフが必要であり、インバウンドサブインターフェイスは最大4つまで可能です。終端は、最大4つのサブインターフェイスがあるルーテッドモードまたはトランクモードにすることができます。ハイパーバイザのタグ付き VLAN と、VLAN のタグ付けを行うために VNF のどちらかを選択できます。VNF の VLAN タグ付けでは、最小1つの VLAN、最大4つの VLAN に終端できます。ハイパーバイザのタグ付き VLAN では、すべての VLAN が同じインバウンド VNF インターフェイスでタグ付けされます。

図 8: インターネットエッジサービスチェーン



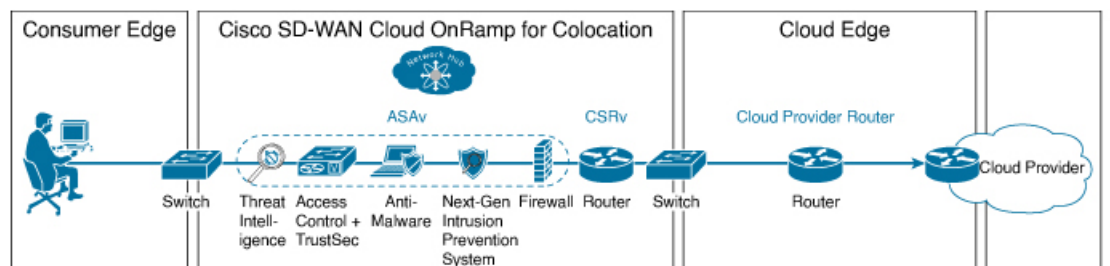
- SD-WAN アクセス：このサービスチェーンでは、vEdge の後にファイアウォールが続き、その後にルータが続きます。ファイアウォールモードは、L2 HA、L2 非 HA、L3 HA、および L3 非 HA にすることができます。ルータは、L3 HA モードおよび L3 非 HA モードにすることができます。

図 9: SD-WAN アクセスサービスチェーン



- クラウドエッジ（パブリッククラウドアクセス）：このサービスチェーンでは、ファイアウォールの後にルータが続き、ファイアウォールはルーテッドモードです。ファイアウォールモードは、L3 HA および L3 非 HA にすることができます。ルータは、L3 HA モードおよび L3 非 HA モードにすることができます。このサービスチェーンは、ファイアウォールモードが L3 のインターネットエッジ（アウトバウンドインターネット、e コマース、SaaS）です。

図 10: クラウドエッジ（パブリッククラウドアクセス）サービスチェーン



Cisco vManage を介して検証済みのサービスチェーンを選択する方法については、[サービスグループでのサービスチェーンの作成（78 ページ）](#) のトピックを参照してください。

検証済み VM パッケージ

VM パッケージは、ユースケースごとに作成されます。これらのパッケージには、サポートされているユースケースごとに推奨される Day-0 構成が含まれています。すべてのユーザーは、必要なカスタム Day-0 構成を持ち込み、要件に従って VM をパッケージ化できます。検証済みパッケージでは、さまざまな Day-0 構成が単一の VM パッケージにバンドルされています。たとえば、VM がファイアウォール VM である場合、サービスチェーンの途中にある場合は、トランスペアレントモードまたはルーテッドモードで使用できます。VM がサービスチェーンの最初または最後の VM である場合、ブランチまたはプロバイダーへの終端トンネルになるか、ルーティングされたトラフィックになるか、複数のブランチまたはプロバイダーを終端することができます。各ユースケースは、展開時またはサービスチェーンのプロビジョニング中に

ユーザーが選択できるように、イメージメタデータの特別なタグとして設定されます。VMがサービスチェーンの中心にある場合、Cisco vManage はそれらのセグメントの IP アドレスと VLAN を自動化できます。VM がブランチまたはプロバイダーに終端している場合、ユーザーは IP アドレス、ピアアドレス、自律システム番号などを構成する必要があります。

カスタマイズされたサービスチェーン

サービスチェーンは、パケットが通過するサービス機能と関連するエンドポイントグループの名前付きリストです。サービスチェーンをカスタマイズし、サービスチェーンテンプレートを作成できます。サービスチェーンテンプレートは、入力トラフィックをクラウドに接続する目的でサービスを提供する VM のチェーンです。サービスチェーンテンプレートには、検証済みの VM を含む事前定義されたサービスチェーンを含めることができます。

カスタマイズされたサービスチェーンの最初の VNF と最後の VNF は、ルータ（またはファイアウォール）にすることができます。SD-WAN の場合、最初の VM はオーケストレーションされた vEdge です。非 SD-WAN の場合、最初の VM は、オーケストレーションされないゲートウェイルータとしてモデル化できます。

サービスチェーンテンプレートを選択し、1 つ以上の VM を挿入して 1 つ以上の VM を削除することでテンプレートを変更できます。サービスチェーン内の各 VM について、VM カタログから取得された VM イメージを選択できます。たとえば、サービスチェーンの最初の VM がルータである場合、Cisco 1000v を選択するか、VM リポジトリから選択するか、サードパーティルータを選択できます。



第 5 章

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 \(41 ページ\)](#)
- [Cisco vManage からの Cloud OnRamp for Colocation デバイスの削除 \(43 ページ\)](#)
- [Cisco vManage でのクラスタの管理 \(44 ページ\)](#)
- [サービス グループの管理 \(78 ページ\)](#)
- [クラスタ内のサービスグループの接続または切断 \(103 ページ\)](#)
- [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 \(104 ページ\)](#)

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 Current	Type	Technology-package 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 \(103 ページ\)](#)』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 \(151 ページ\)](#) 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 \(46 ページ\)](#)』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 \(78 ページ\)](#)』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 \(103 ページ\)](#)』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 \(168 ページ\)](#) 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ポイン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。「[Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのサイジング要件](#)」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。

- [**Configure & Provision Cluster**] をクリックします。
- 次の情報を入力します。

表 9: 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 \(49 ページ\)](#) 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 \(61 ページ\)](#) 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 10: 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。

- [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。
- [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)。
- [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 11: 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ンネル	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ン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 つのポートチャンネルにまとめ、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、単一のポートチャン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ンネル

Cisco vManage リリース 20.8.1 以前のリリースでは、入力ポートチャンネルと出力ポートチャンネルは分離されています。入力ポートチャンネルと出力ポートチャンネルの両方、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、ポートチャンネルの 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、単一のポートチャンネルが 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 つのポートチャンネルを 1 つのポートチャン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ン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 つのポートチャンネルにまとめ、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ンネルにバンドルし、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ンネルに結合します。

次に、4つのリンクを1つのポートチャン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ンネルが形成され、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) 構成がポートチャンネル構成および 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 12: 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 \(49 ページ\)](#) 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 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。「[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せん。

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 \(72 ページ\)](#) 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 NFWIS 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 13: 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 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ベーション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ベーション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 11: クラスタのアクティブ化 (Cisco vManage リリース 20.7.x 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 12: CLOUD ONRAMP CCM 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 13: 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 (C9500-48Y-CAT324L269), switch2 : 10.0.5.151 (C9500-48Y-CAT324L2H3) [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 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 \(174 ページ\)](#) 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 \(183 ページ\)](#) 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 \(168 ページ\)](#) 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。

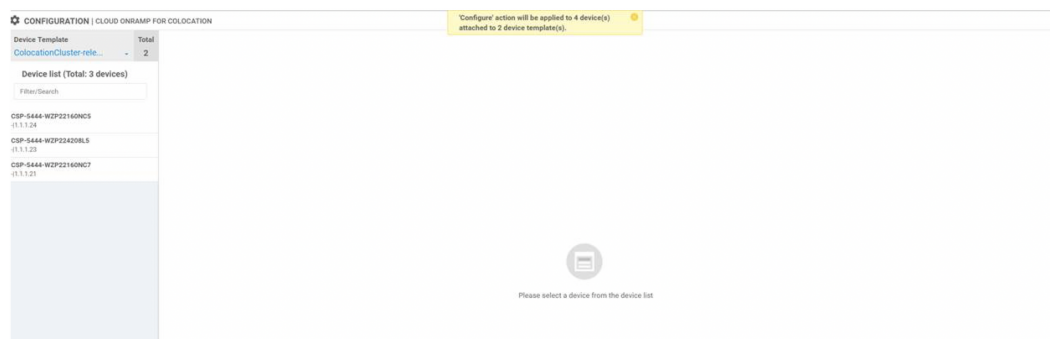
名前には、128 文字の英数字を含めることができます。

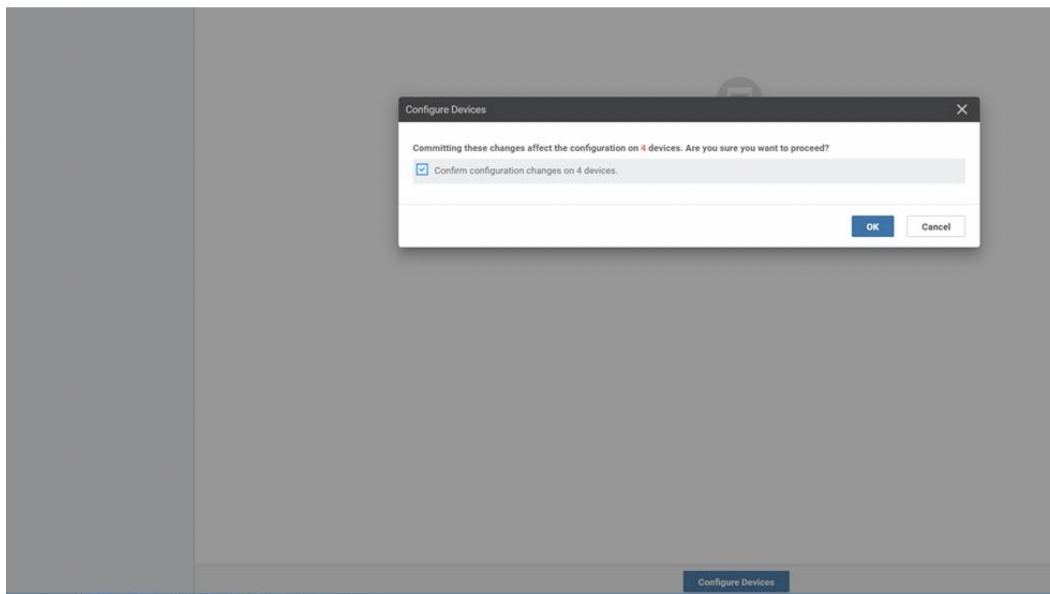
(注) CSP デバイスを起動するには、デバイスの OTP を設定してください。

図 14: 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。

CCM がある CSP の削除

Push Feature Template Configuration Validation Success Initiated By: admin From: 10.41

Total Task: 3 (Done - Scheduled: 2) Success: 1

State	Message	Cluster Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Template Config.	CSP-5444-WZP22160NCS	CSP-5444	CSP2	1.1.1.24	1000	1.1.1.2
Done - Scheduled	Device needs to install some apps. C...	CSP-5444-WZP22420RL5	CSP-5444	CSP3	1.1.1.23	1000	1.1.1.2
Done - Scheduled	Device is offline. Configuration templ...	CCM	CCM	ccm-Cluster-release	1.1.1.20	-	1.1.1.2

Log messages for the 'Done - Scheduled' row:

- [30-741-2023 21:48:36 UTC] Configuring device with Feature template: ColocationCluster-release
- [30-741-2023 21:48:36 UTC] Generating configuration from template
- [30-741-2023 21:48:35 UTC] Checking and creating device in vmanage
- [30-741-2023 21:48:47 UTC] Device is online
- [30-741-2023 21:48:47 UTC] Updating device configuration in vmanage
- [30-741-2023 21:48:48 UTC] Device needs app install.
- [30-741-2023 21:48:49 UTC] Updating device configuration in vmanage

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 (179 ページ) 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 15: CCM を使用する CSP デバイス

Name	Device Model	State	System IP	Reachability	CCM Enabled	Last Updated
1.1.1.26	vedge-nfvis-CSP-5444	✓	1.1.1.26	reachable	false	30 Jul 2019 11:47:07 AM PDT
1.1.1.27	vedge-nfvis-CSP-5444	✓	1.1.1.27	reachable	true	30 Jul 2019 11:36:21 AM PDT
1.1.1.29	vedge-nfvis-CSP-5444	✓	1.1.1.29	reachable	false	30 Jul 2019 11:56:24 AM PDT
Switch2	-	○	-	-	-	-
Switch1	-	○	-	-	-	-

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マ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 14: 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 \(58 ページ\)](#)』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 \(13 ページ\)](#) 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 \(172 ページ\)](#) 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witch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witch 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
```

Switch#	Role	Mac Address	Priority	H/W Version	Current 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
```

Switch#	Role	Mac Address	Priority	H/W Version	Current 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。

■ スイッチの取り外しと交換

```
Switch# show switch
Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
Mac persistency wait time: Indefinite

Switch# 
-----
Switch#  show switch
Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
Mac persistency wait time: Indefinite

Switch# 
-----
Switch#  show switch
Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
Mac persistency wait time: Indefinite
-----
Switch#  Role      Mac Address      Priority Version  Current 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

Switch# 
-----
Switch#  show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
-----
Switch#  show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
-----
Switch#  Role      Mac Address      Priority Version  Current 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

Switch# Role Mac Address Priority H/W Current 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 \(46 ページ\)](#)』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 15: 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。

[Cisco vManage] メニューから、[Configuration] > [Cloud OnRamp for Colocation] を選択します

- [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。

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

表 16: 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	<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。</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モニタリングできます。</p> <p>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。</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。 <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。</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 (88 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 \(132 ページ\)](#)』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)

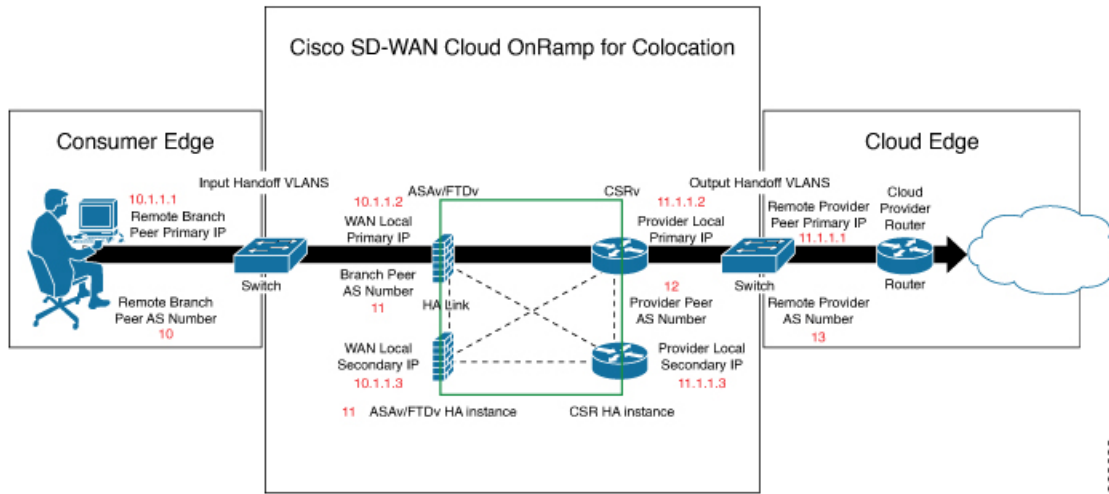
表 17: ルータとファイアウォールの VNF プロパティ

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。

フィールド	説明
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。
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。	

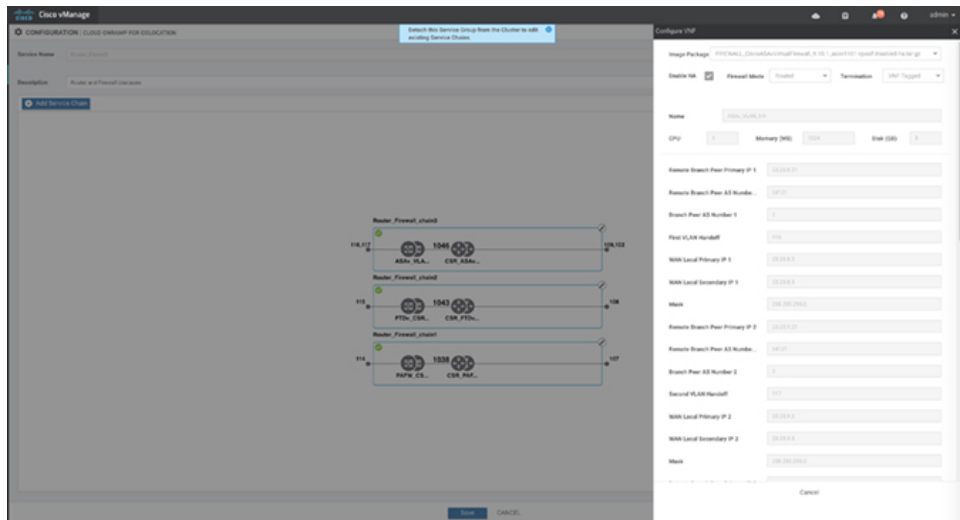
次の図で、緑色のボックス内のすべての IP アドレス、VLAN、および自律システムは、VLAN から生成されたシステム固有の情報、クラスタに提供される IP プールです。この情報は、VM の Day-0 構成に自動的に追加されます。

サービスグループでのサービスチェーンの作成

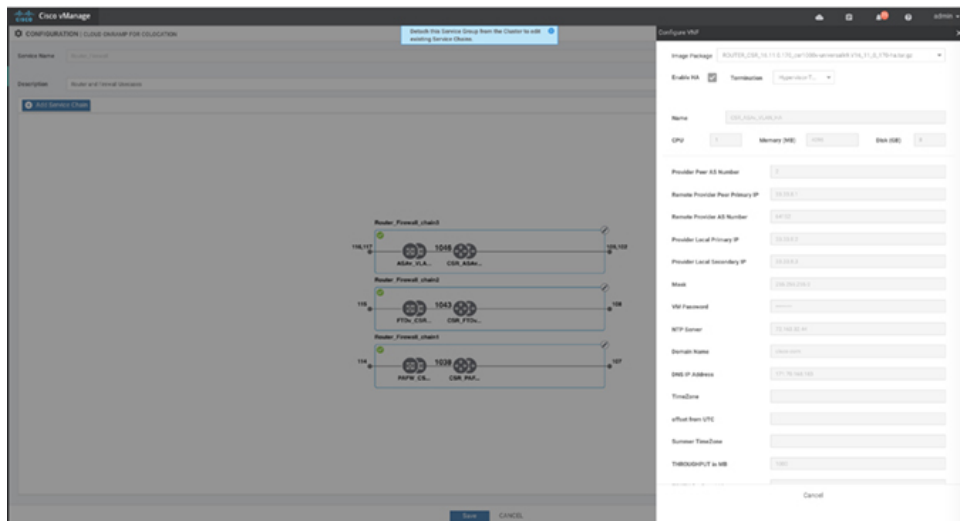


368038

次の図は、Cisco vManage 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 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 18: 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	<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 19: 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 \(78 ページ\)](#) 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 20: 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 \(78 ページ\)](#)』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。

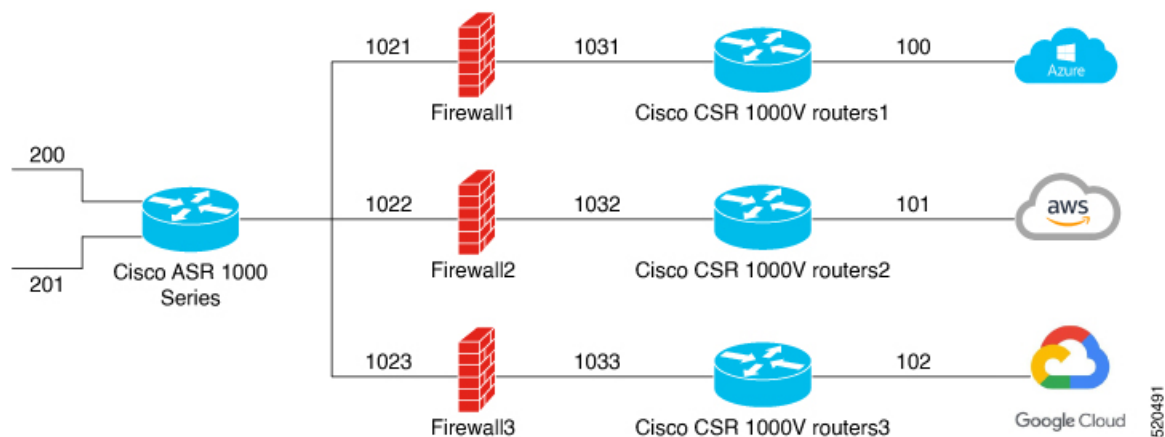
1. PNF デバイスを Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチデバイスに接続します。
2. Cisco ASR 1000 シリーズルータを Cisco vManage で管理するには、Cisco スマートアカウントから WAN エッジルータの認証済みシリアル番号をアップロードします。『[System and Interfaces Configuration Guide](#)』の「Upload WAN Edge Router Serial Numbers from Cisco Smart Account」を参照してください。
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 \(90 ページ\)](#)』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 \(103 ページ\)](#)』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 \(94 ページ\)](#)』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 16: 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 21: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 \(78 ページ\)](#)』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 17: 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 18: 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。

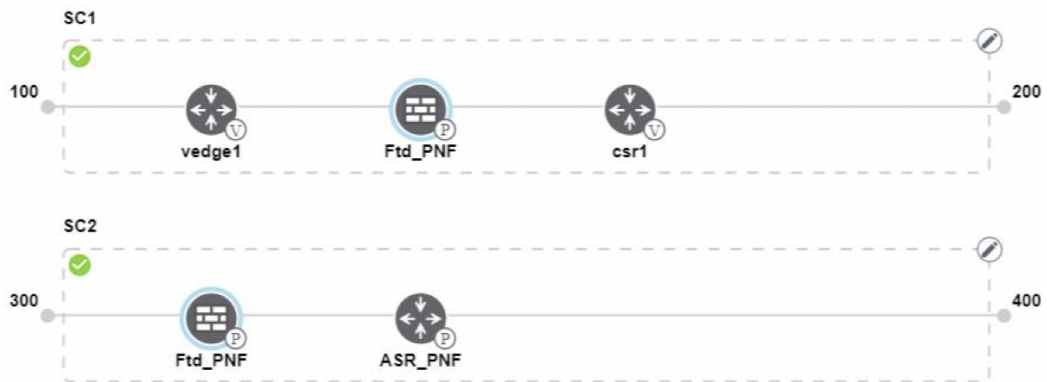
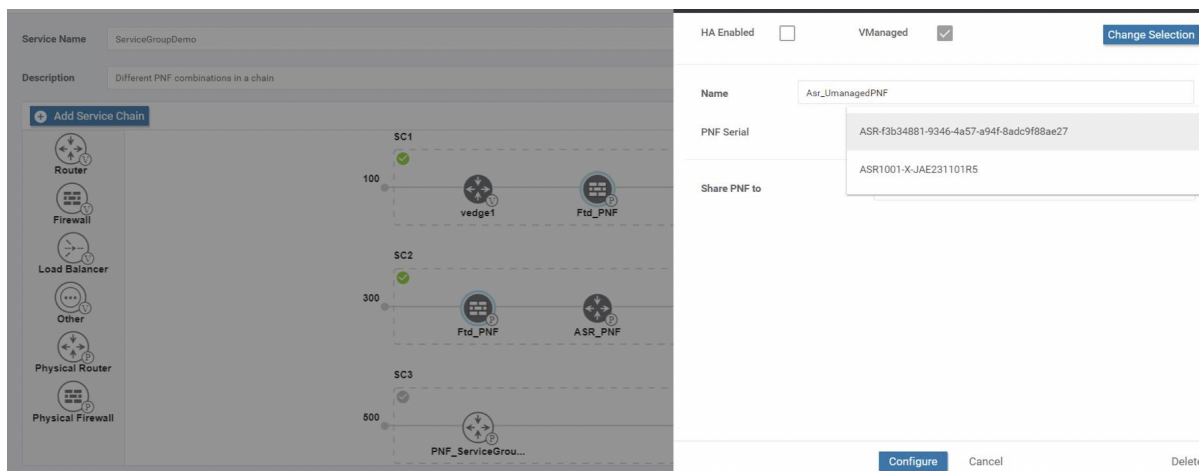


図 19: サービスチェーン内の 3 つの PNF デバイス

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。

PNF および Cisco Catalyst 9500 スイッチの構成



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 \(132 ページ\)](#) 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。

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、[こちら](#)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、「[Cloud onRamp Colocation クラスタの監視](#)」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 22: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 \(78 ページ\)](#)』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 \(111 ページ\)](#) 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 \(78 ページ\)](#) 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 \(96 ページ\)](#) および [共有 VNF のカスタムパッケージの詳細 \(189 ページ\)](#) 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 20: 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 (ASA v ファイアウォール) は HA モードです。

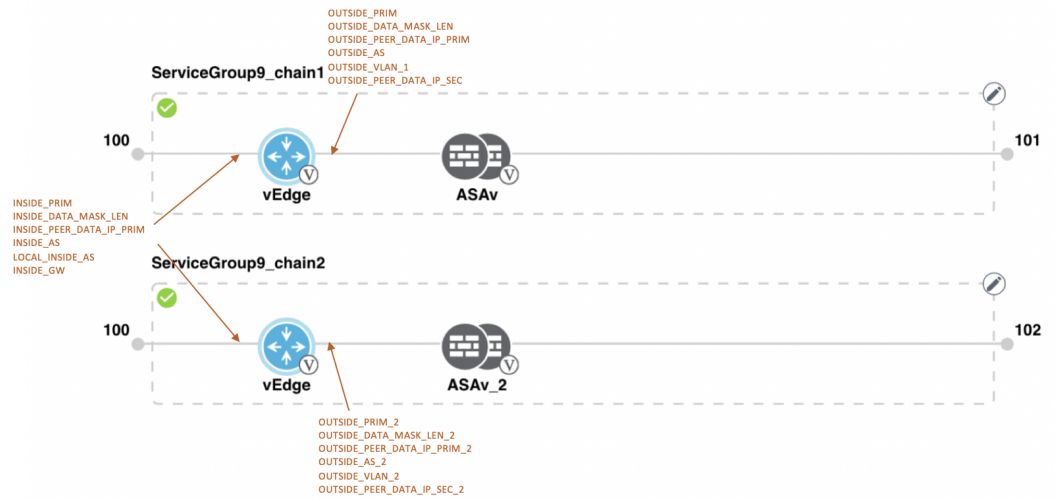


図 21: 共有 - 最初の位置の Cisco vEdge ルータ VNF

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。

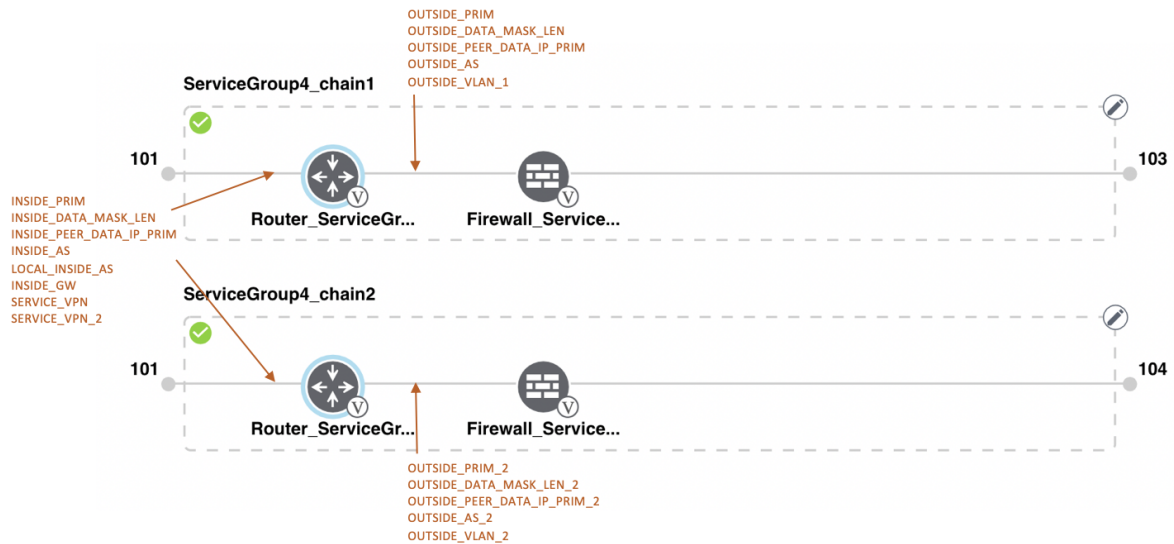


図 22: 共有 - 最初の位置の Cisco vEdge ルータ VNF

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 への入力アクセスモード（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。

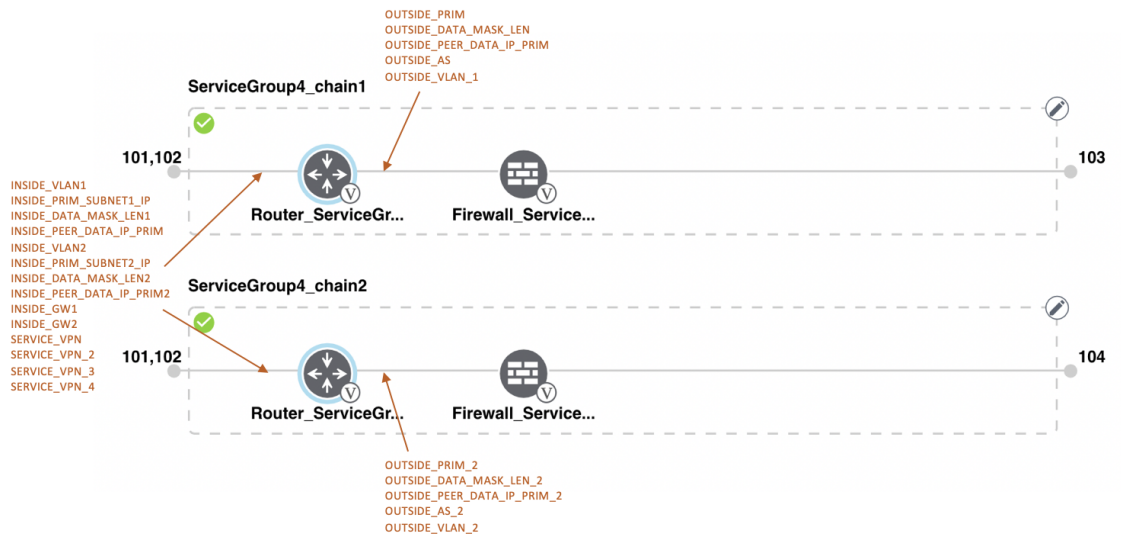


図 23: 共有 - 最初の位置の Cisco vEdge ルータ VNF

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 への入力にはトランクモード (VNF タグ付き) であり、ネイバーは HA モードです。

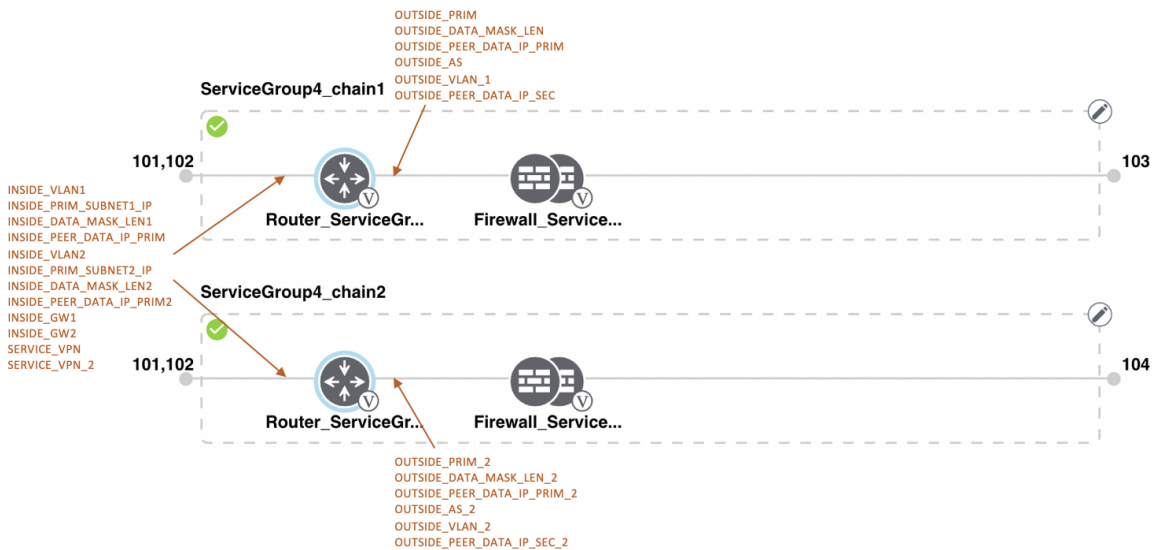


図 24: 共有 - 最後の位置の Cisco CSR1000V VNF

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 (ASA v ファイアウォール) はスタンドアロンモードです。

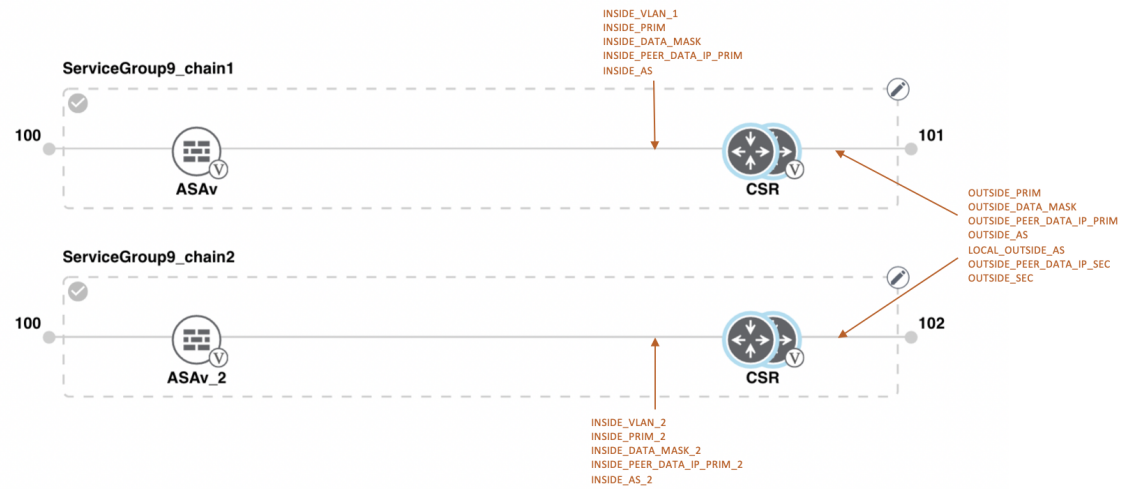


図 25: 共有 - 最後の位置の Cisco CSR1000V VNF

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。

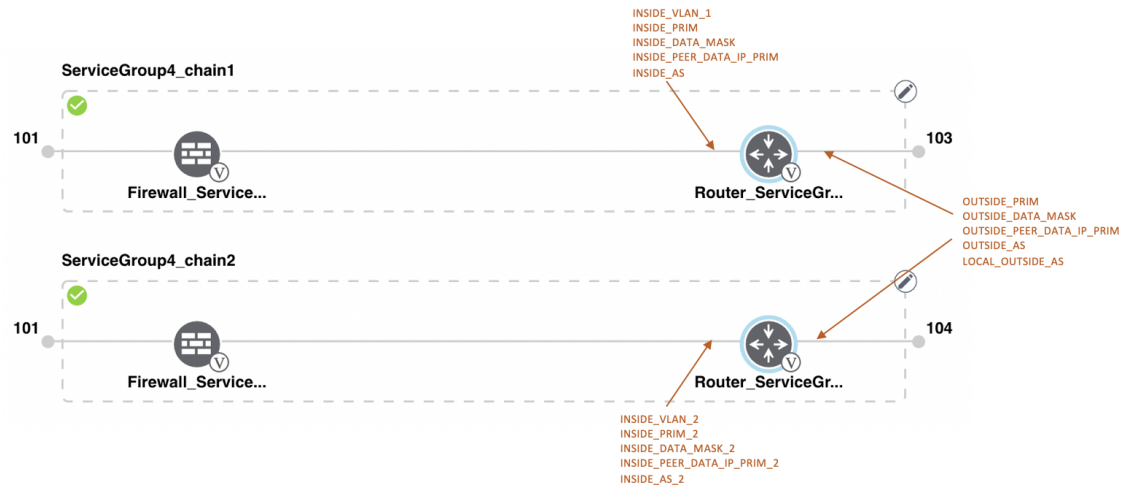


図 26: 共有 - 最後の位置の Cisco CSR1000V VNF

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。

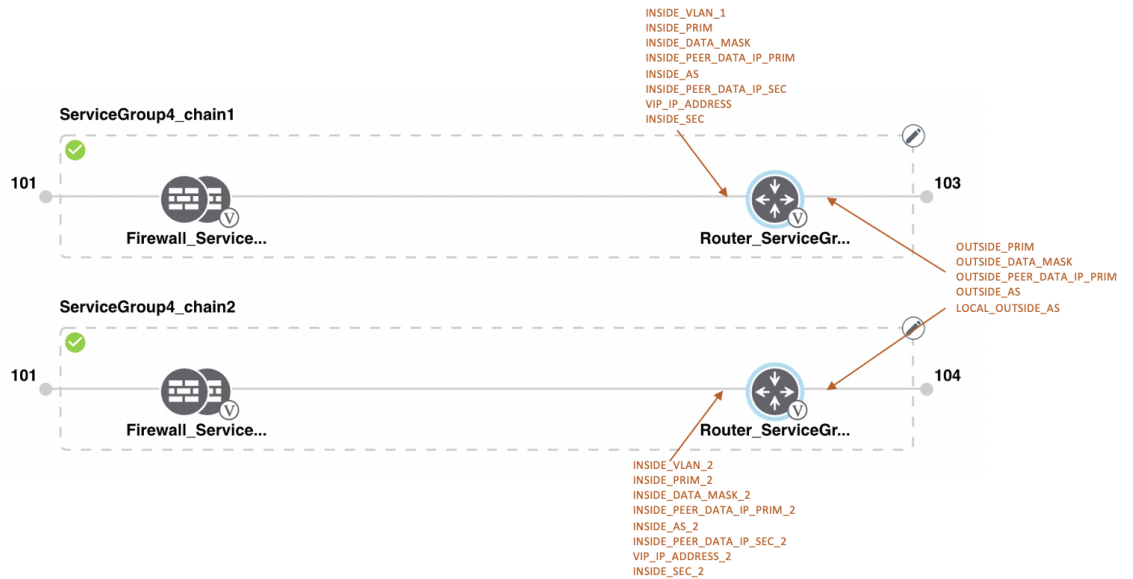


図 27: 共有 - 最後の位置の Cisco CSR1000V VNF

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。

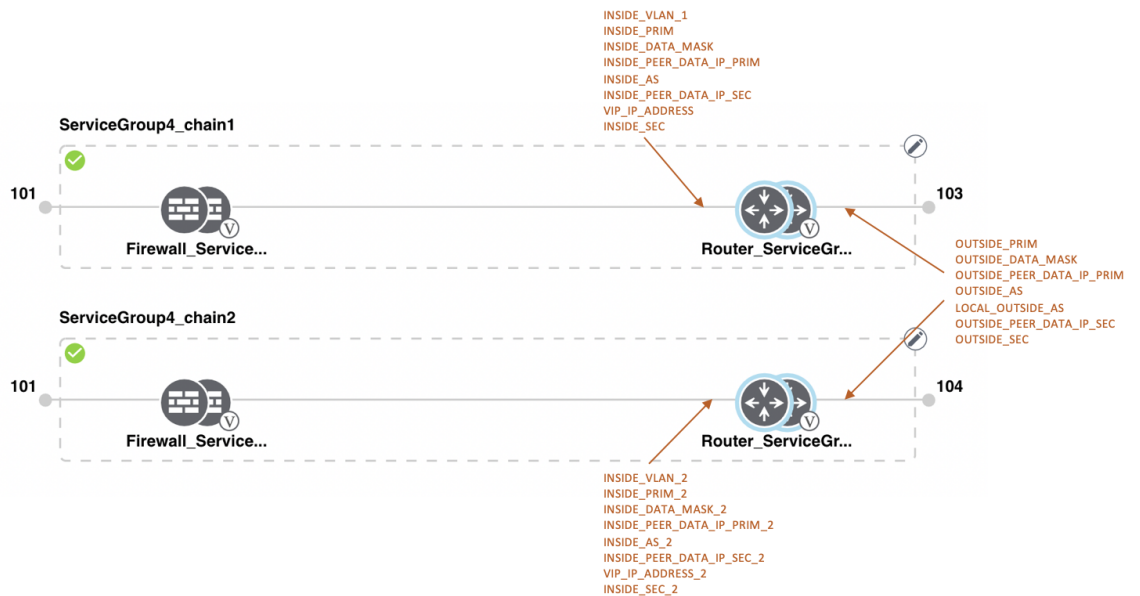


図 28: 共有 - 最初の位置の ASA v VNF

最初の位置にある ASA v 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。

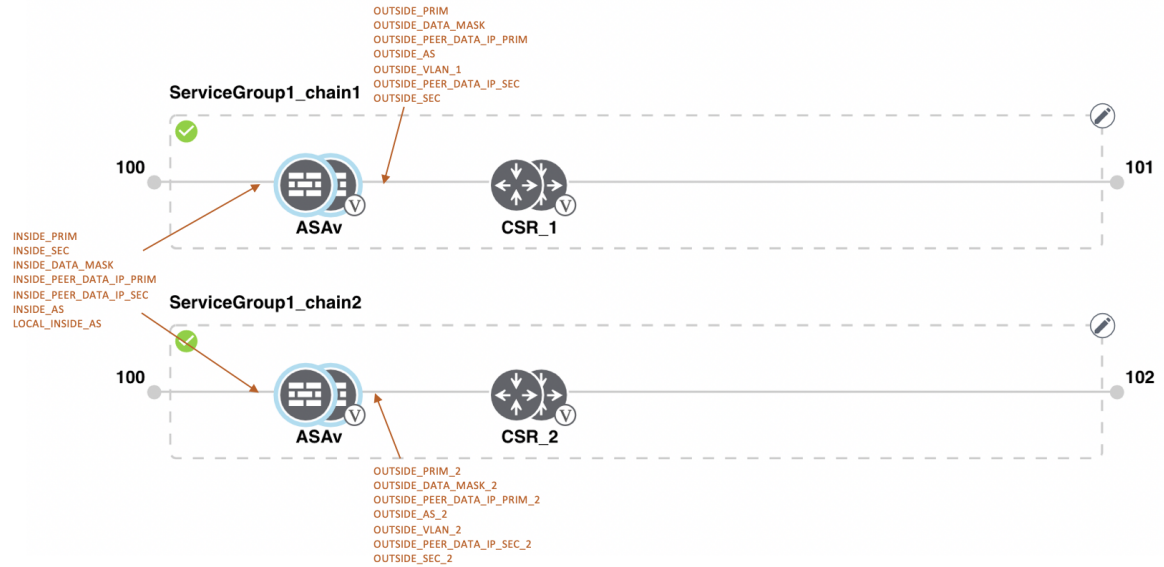


図 29: 共有 - 最初の位置の ASA v VNF

最初の位置にある ASA v (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。

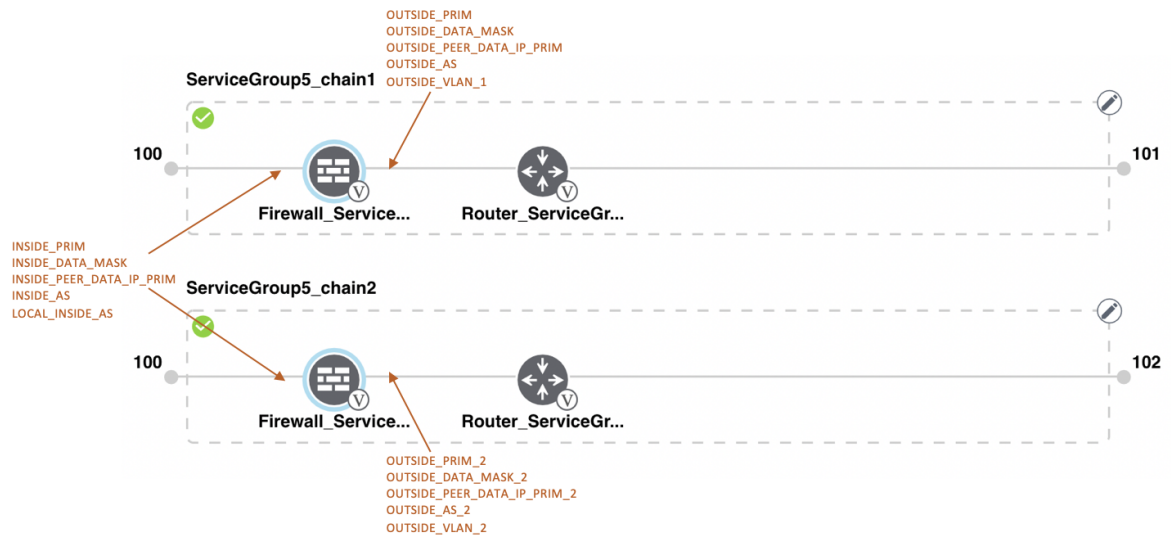


図 30: 共有 - 最初の位置の ASA v VNF

最初の位置にある ASA v (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。

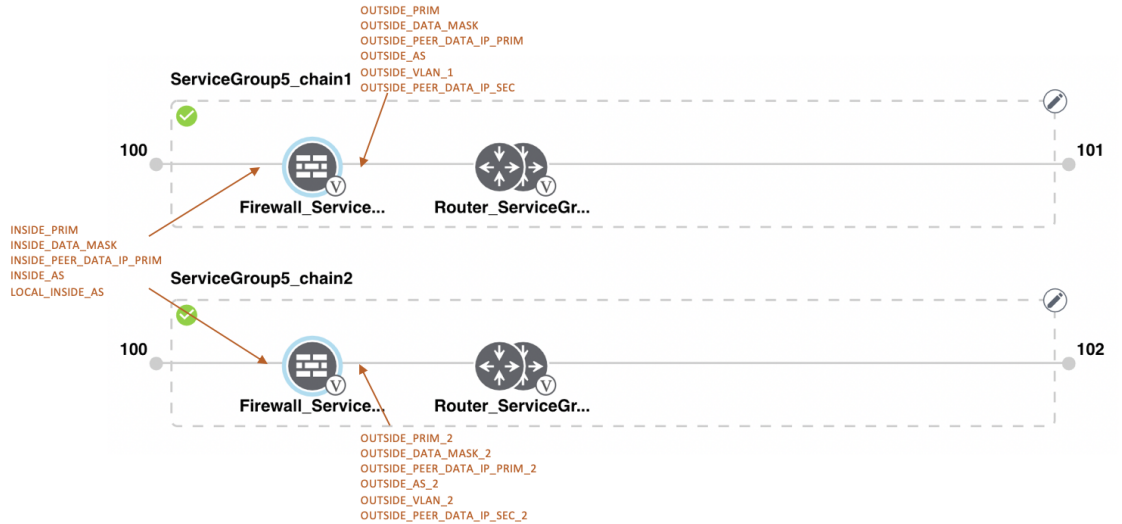
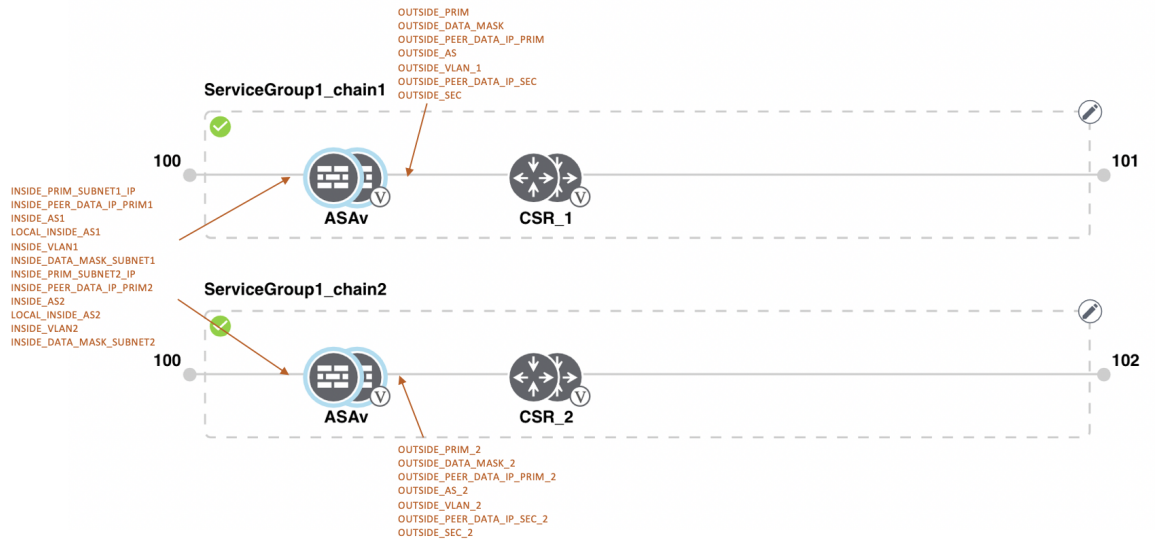


図 31: 共有 - 最初の位置の ASA v VNF

HA モードの最初の位置にある ASA v 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 \(185 ページ\)](#) 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 \(183 ページ\)](#) 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。

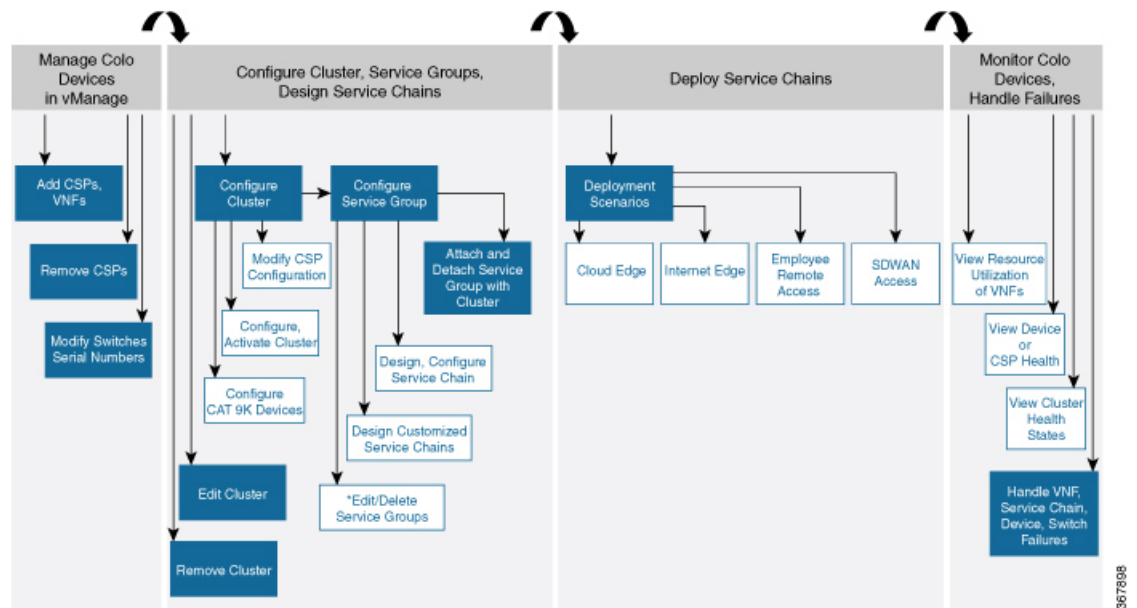
- Cisco Colo Manager は、構成のプッシュが成功したか失敗したかにかかわらず、状態を Cisco vManage に報告します。
- すべての Day-N サービスチェーンまたは VM 構成が CSP デバイスに送信されます。
- CSP デバイスは、VM ファイルのダウンロードステータスに関する通知を Cisco vManage に送信します。
- すべての VM がダウンロードされると、Cisco vManage は一括構成を送信してすべての VM を起動します。
- CSP デバイスは、起動された VM と状態に関する通知を Cisco vManage に送信します。
- 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 32: 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れた後にものみ編集できます。



第 6 章

クラスタコンポーネントおよびSWIMのソフトウェアイメージ管理

- [VM カタログとリポジトリの管理 \(107 ページ\)](#)
- [Cisco vManage を使用した Cisco NFVIS のアップグレード \(118 ページ\)](#)
- [Cisco Catalyst 9500 スイッチのアップグレード \(120 ページ\)](#)
- [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 \(123 ページ\)](#)

VM カタログとリポジトリの管理

表 23: 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 リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能を使用すると、仮想マシンイメージを qcow2 形式で Cisco vManage 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 vManage 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 vManage 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 \(111 ページ\)](#)』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。Cisco SD-WAN 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。



-
- (注) 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 vManage 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 vManage 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 vManage 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。



- (注) Cisco vManage は Cisco VNF を管理します。VNF 内の Day-1 および Day-N 構成は他の 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 イメージ形式

Cisco vBond Orchestrator は、Cisco VNF とサードパーティの VNF を区別しません。すべての VNF は、ルータ、ファイアウォール、ロードバランサなど、VNF によって提供されるサービスに基づいて分類されます。パッケージメタデータには VM 固有の属性があります。パッケージメタデータ ファイルで指定された HA NIC と管理 NIC に基づいて、Cisco vBond Orchestrator は管理 NIC と HA NIC を接続します。デフォルトでは、管理 NIC は 0 で、HA NIC は 1 です。指定された数の HA NIC が、VNF プロビジョニング中に接続されます。

VNF イメージのアップロード

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

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

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

ステップ 3 仮想イメージを保存する場所を選択します。

- 仮想イメージをローカルの Cisco vManage サーバーに保存し、コントロールプレーン接続を介して CSP デバイスにダウンロードするには、[vManage] をクリックします。[Upload VNF's Package to vManage] ダイアログボックスが表示されます。
 1. 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco vManage サーバーから仮想イメージを選択します。例：CSR.tar.gz、ASAv.tar.gz、または ABC.qcow2
 2. ファイルをアップロードする場合は、アップロードするファイルのタイプ (イメージパッケージまたはスキャフォールド) を指定します。必要に応じて、ファイルの説明を指定し、カスタムタグをファイルに追加します。タグは、サービスチェーンを作成するときに、イメージとスキャフォールドファイルをフィルタリングするために使用できます。

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

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

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

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

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

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

1. [vManage Hostname/IP Address] フィールドに、管理 VPN (通常は VPN 512) にある Cisco vManage サーバー上のインターフェイスの IP アドレスを入力します。
2. 仮想イメージファイルまたは qcow2 イメージファイルをダイアログボックスにドラッグアンドドロップするか、[Browse] をクリックしてローカルの Cisco vManage サーバーから仮想イメージを選択します。
3. ファイルをアップロードする場合は、アップロードするファイルのタイプ (**イメージパッケージ** または **スキャフォールド**) を指定します。必要に応じて、ファイルの説明を指定し、カスタムタグをファイルに追加します。タグは、サービスチェーンを作成するときに、イメージとスキャフォールドファイルをフィルタリングするために使用できます。
4. qcow2 イメージファイルをアップロードする場合は、サービスまたは VNF タイプ (**FIREWALL** または **ROUTER**) を指定します。必要に応じて、以下を指定します。

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

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

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

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

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

カスタマイズされた VNF イメージの作成

始める前に

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

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

次のカスタムパッケージの要件が満たされていることを確認します。

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

- ステップ 1 [Cisco vManage] メニューから、[Maintenance] > [Software Repository] を選択します。
- ステップ 2 [Virtual Images] > [Add Custom VNF Package] をクリックします。
- ステップ 3 次の VNF パッケージプロパティを使用して VNF を構成し、[Save] をクリックします。

表 24: VNF パッケージのプロパティ

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

- ステップ 4 VM qcow2 イメージをパッケージ化するには、[File Upload] をクリックし、qcow2 イメージファイルを参照して選択します。
- ステップ 5 VNF のブートストラップ構成ファイルを選択するには、[Day 0 Configuration] をクリックし、[File Upload] をクリックし、ファイルを参照して選択します。
次の Day-0 構成プロパティを含めます。

表 25: Day-0 構成

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

フィールド	必須またはオプション	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>サポートされている値は、スタンダードアロン、HA プライマリ、HA セカンダリです。</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] をクリックし、[Save] をクリックします。Day-0 構成が [Day 0 Config File] テーブルに表示されます。システム変数とカスタム変数を使用して、ブートストラップ構成変数をトークン化できます。Day-0 構成ファイルの変数をトークン化するには、目的の Day-0 構成ファイルの横にある [View Configuration File] をクリックします。[Day 0 configuration file] ダイアログボックスで、次のタスクを実行します。

(注) ブートストラップ構成ファイルは XML またはテキストファイルで、VNF と環境に固有のプロパティが含まれています。共有 VNF については、[共有 VNF のカスタムパッケージの詳細 \(189 ページ\)](#) でさまざまな VNF タイプに追加する必要があるシステム変数のリストについて参照してください。

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

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

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

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

表 26: ストレージのプロパティ

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

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

表 27: VNF イメージのプロパティ

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

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

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

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

VNF イメージの表示

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

ステップ 2 [Virtual Images] をクリックします。

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

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

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

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

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

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

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

VNF イメージの削除

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

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

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



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



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

Cisco vManage 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 vManage を使用して Cisco vManage 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 vManage 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 vManage 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 \(118 ページ\)](#)』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 \(119 ページ\)](#)』を参照してください。
- Cisco vManage 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

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 vManage] 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 - vManage] 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 vManage サーバー、または Cisco vManage サーバーに保存できます。

Cisco vManage サーバー：ソフトウェアイメージをローカルの Cisco vManage 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 vManage サーバー：ソフトウェアイメージをリモート Cisco vManage サーバーに保存し、リモート Cisco vManage サーバーの場所はローカル Cisco vManage 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 SD-WAN Configuration Guides](#)』のソフトウェアリポジトリ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。

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

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

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

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

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

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

ステップ 6 [Upgrade] をクリックします。

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

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

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

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

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



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

Cisco Catalyst 9500 スイッチのアップグレード

Cisco Catalyst 9500-40X および Cisco Catalyst 9500-48Y4C スイッチの両方に対してソフトウェアアップグレードを実行できます。

始める前に

- 両方のスイッチで実行中の構成をバックアップします
- Cisco Catalyst 9500 アップグレードソフトウェア (.bin ファイル) を cisco.com Web サイトからダウンロードし、アーカイブファイルとして使用できることを確認してください。

ステップ 1 アップグレードされたソフトウェアを Trivial File Transfer Protocol (TFTP) からスイッチ 1 のフラッシュにコピーするには、次のコマンドを使用します。

a) **conf t**

コンフィギュレーション モードを 1 行に 1 つずつ開始します。CNTL/Z で終了します。

例 :

```
c9500-1#conf t
```

b) **blocksize value**

グローバル構成のブロックサイズを手動で変更して、転送プロセスを高速化します。

例：

```
c9500-1(config)#ip tftp blocksize 8165
c9500-1(config)#end
```

c) **copy scp**

スイッチイメージファイルをスイッチ 1 のフラッシュに安全にコピーします。

例：

```
c9500-1#copy scp://<cec-id>@172.16.0.151//auto/tftp-xxx-users2/yyyy/Switch_Image/
cat9k_iosxe.17.03.01.SPA.bin flash: vrf Mgmt-vrf
```

ステップ 2 スイッチが SVL モードの場合に、アップグレードされたソフトウェアをスイッチから別のスイッチにコピーするには、次のコマンドを使用します。

両方のスイッチが SVL モードでない場合は、スイッチ 2 に対してステップ 1 を繰り返します。

- Cisco Catalyst 9500-40X

copy

スイッチ 1 のフラッシュからスイッチ 2 のフラッシュにコピーします。

```
c9500-1#copy flash-1:cat9k_iosxe.17.03.01.SPA.bin flash-2:
```

- Cisco Catalyst 9500-48Y4C

copy

スイッチ 1 からスイッチ 2 のブートフラッシュにコピーします

```
switch1#copy bootflash:cat9k_iosxe.17.03.01.SPA.bin stdby-bootflash:
cat9k_iosxe.17.03.01.SPA.bin
```

ステップ 3 スタートアップスイッチ ソフトウェアの仕様を削除するには、Catalyst 9500 スイッチで **boot system** コマンドの **no** 形式を使用します。

a) **config t**

コンフィギュレーション モードを開始します。

b) **no boot system**

すべてのスタートアップソフトウェア構成をクリアします。

ステップ 4 スイッチを構成し、コピーしたソフトウェアをリロードするには、次のコマンドを使用します。

- Cisco Catalyst 9500-40X

1. boot system switch all flash

新しくコピーしたソフトウェアでスイッチをブートするようにブート変数を設定します。

```
c9500-1(config)#boot system switch all flash:
cat9k_iosxe.17.03.01.SPA.bin
```

2. end

スイッチのグローバル コンフィギュレーション モードを終了します。

```
c9500-1(config)#end
```

3. **wr mem**

行ったスイッチ構成の変更をコピーし、フラッシュの構成に保存します。

```
c9500-1#wr mem
```

• Cisco Catalyst 9500-48Y4C

1. **boot system bootflash**

アップグレードされたソフトウェアをインストールし、構成を保存して、コピーされたソフトウェアをリロードします。

```
switch1(config)#boot system bootflash:  
cat9k_iosxe.17.03.01.SPA.bin
```

2. **end**

スイッチのグローバル コンフィギュレーション モードを終了します。

```
switch1(config)#end
```

3. **wr mem**

行ったスイッチ構成の変更をコピーし、ブートフラッシュの構成に保存します。

```
switch1#wr mem
```

• SVL 構成のないスイッチ。コピーしたソフトウェアをリロードするように両方のスイッチを構成します。両方のスイッチで次のコマンドを使用します。

1. **boot system flash**

フラッシュメモリからイメージを起動するようにスイッチを構成します。

```
Switch(config)#boot system flash:  
cat9k_iosxe.17.03.01.SPA.bin
```

2. **end**

スイッチのグローバル コンフィギュレーション モードを終了します。

```
Switch(config)#end
```

3. **wr mem**

行ったスイッチ構成の変更をコピーし、フラッシュの構成に保存します。

```
Switch#wr mem
```

ステップ 5 実行中の構成にブートシステム構成が1つだけ存在することを確認するには、次のコマンドを使用します。

a) **show run | i boot**

アップグレードされたソフトウェアが最初のブートイメージであることを確認します。

例 :

```
c9500-1#show run | i boot
```

b) **license boot level**

Cisco DNA Essentials を使用してスイッチで新しいソフトウェアライセンスを起動します

例：

```
c9500-1#license boot level network-advantage addon dna-advantage
```

c) **diagnostic bootup level**

スイッチの起動時に、診断テストが開始されるように起動診断レベルを設定します。

例：

```
c9500-1#diagnostic bootup level minimal
```

ステップ 6 スイッチ構成の変更をリロードして適用するには、次のコマンドを使用します。Cisco Catalyst 9500-40X および Cisco Catalyst 9500-48Y4C スイッチの両方に適用されます。

例：

```
c9500-1#reload
```

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 30: サポートされる接続

Cisco vManage	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	Cisco vManage 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	Cisco vManage 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

Cisco vManage	Cisco NFVIS	クラスタの状態	サポートされる接続
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 20.1.1.1 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 vManage およ び Cisco NFVIS のアッ プグレード後に Cisco CSP デバイスをクラ スタに追加する」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 vManage および Cisco NFVIS のアップグレード後に Cisco CSP デバイスをクラスタに追加する

Cisco vManage 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

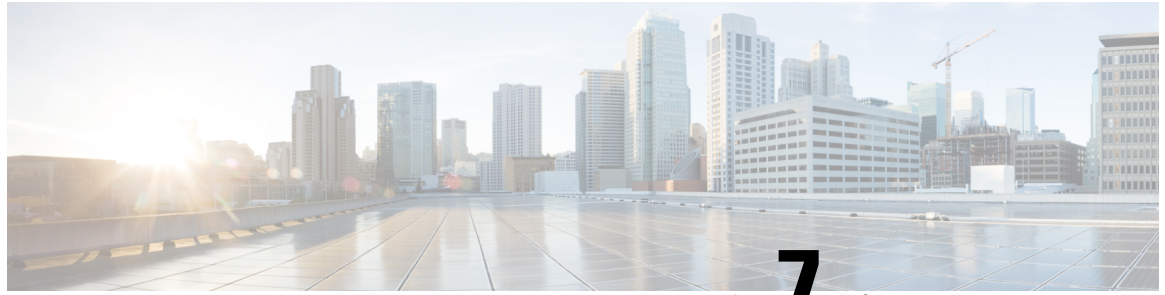
例

```
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 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すでにアクティブなクラスタを使用するには、Cisco vManage 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 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 vManage 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。

■ 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



第 7 章

Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのモニタリング

Cisco vManage は、各デバイスの正常性を示すクラスタレベルで Cloud OnRamp for Colocation のステータスを表示します。クラスタレベルのリソースが表示され、割り当てられた CPU や使用可能な CPU などのリソースの可用性が示されます。クラスタ内のサービスグループを表示できます。クラスタの下のすべてのサービスグループは、サービスチェーン内の稼働中または停止している VM の数を示すテーブルビューに表示されます。また、サービスグループのダイアグラムビューを表示できます。このダイアグラムビューには、VM に割り当てられているリソースを確認できるサービスチェーン内のすべてのサービスチェーンと VM が表示されます。ビューには、VM に接続されている各 VNIC の VLAN が表示されます。VNF の詳細を表示する表形式の VNF ビューを見ることができます。VM にカーソルを合わせると、管理 IP、CPU、メモリ、ディスク、HA、VM タイプに関する情報を取得できます。

CPU、メモリ、ディスク、VNIC 使用率チャートなどの履歴およびリアルタイムの運用統計は、VM および CSP デバイスごとに利用できます。VNF ビューは、クラスタビューの下のデバイスから、またはサービスビューからナビゲートできます。『[Cisco vManage からの Cloud OnRamp for Colocation デバイスの動作ステータスの監視 \(128 ページ\)](#)』を参照してください。

- [Cisco vManage からの Cloud OnRamp for Colocation デバイスの動作ステータスの監視 \(128 ページ\)](#)
- [スイッチ構成のための Cisco Colo Manager の状態 \(138 ページ\)](#)
- [ホストからの Cisco Colo Manager の状態と遷移 \(139 ページ\)](#)
- [Cisco Colo Manager の通知 \(139 ページ\)](#)
- [VM アラーム \(143 ページ\)](#)
- [VM 状態 \(145 ページ\)](#)
- [クラウドサービスプラットフォームのリアルタイムコマンド \(145 ページ\)](#)

Cisco vManage からの Cloud OnRamp for Colocation デバイスの動作ステータスの監視

コロケーションデバイスの監視は、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 vManage モニタリング画面の詳細については、『[Cisco SD-WAN Configuration Guides](#)』を参照してください。

すべての通知は、Cisco vManage 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 SD-WAN Command Reference](#)』を参照してください。

ステップ 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。

Cisco vManage が CSP デバイスに到達できず、Cisco Colo Manager（CCM）がスイッチに到達できない場合、CSP デバイスと CCM 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。[Cisco vManage からの VNF に関する情報の表示（129 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 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 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 SD-WAN Configuration Guides](#)』の「View Control Connections」のトピックを参照してください。
- **Colo Manager**：Cisco Colo Manager のヘルスステータスを表示します。[Cisco Colo Manager の正常性の表示（131 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 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 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 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 vManage 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.x 以前 : コロケーションクラスタを監視するには、Cisco vManage 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 クラスタの監視 \(132 ページ\)](#)」を参照してください。

Cisco vManage からの VNF に関する情報の表示

表 31: 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 SD-WAN リリース 20.1.1	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。

表 32: 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 SD-WAN リリース 20.1.1	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。

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。

ステップ 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。

Cisco vManage 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明確に示すその他の主要パラメータなどの情報が含まれています。

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 vManage は、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。

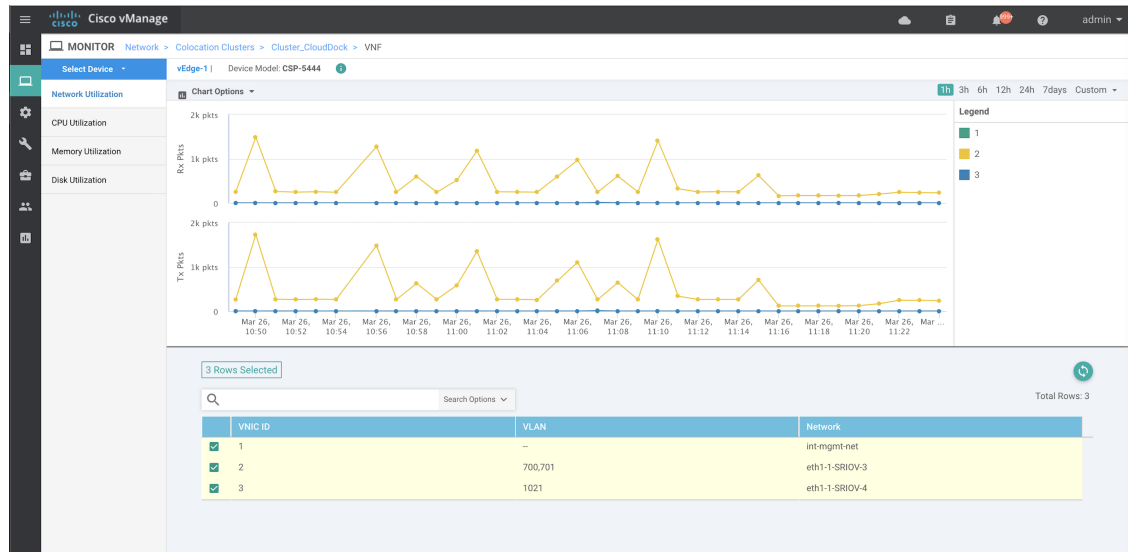
表 33: VNF 情報

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。

- Filter criteria
- 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 33: 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。

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。

ステップ 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。
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、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。

Cloud onRamp Colocation クラスタの監視

表 34: 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 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、[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 vManage 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。

ステップ 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。

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.x 以前: **[Colocation Cluster]** をクリックします。

関連する情報を保有するすべてのクラスタが表形式で表示されます。クラスタ名をクリックします。**[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。 [Cisco vManage からの VNF に関する情報の表示 \(129 ページ\)](#) 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。

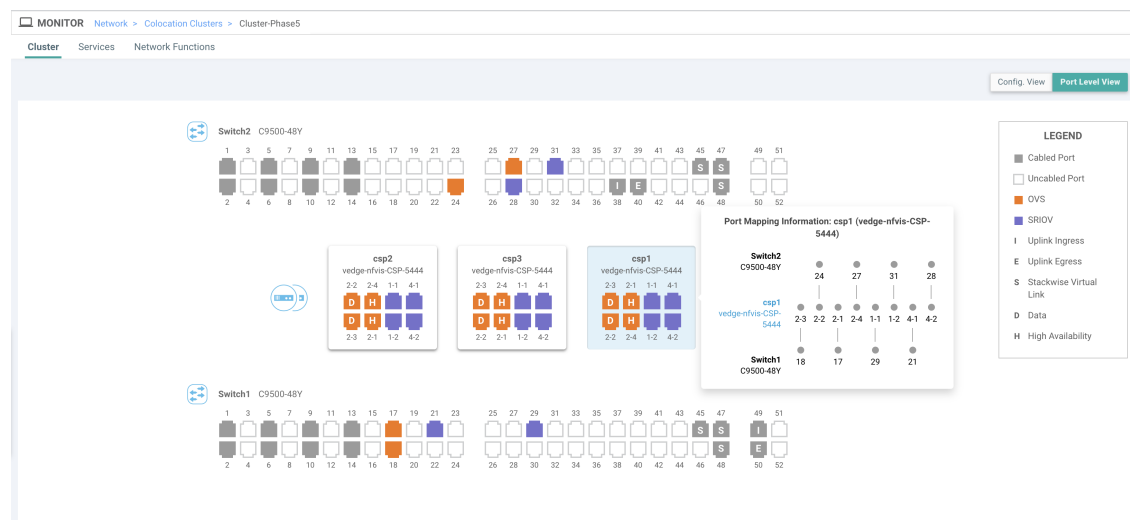
VNF で操作を選択したら、操作が完了するまで待つから、別の操作を実行します。[Task View] ウィンドウから操作の進行状況を表示できます。

- [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。

Catalyst9500 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 34: クラスタ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、監視サービスの有効性、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ケー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 vManage の到達可能範囲外にある場合は、監視できません。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** をクリックします。ダイアログボックスで、VNF に割り当てられた CPU、メモリ、およびディスクを確認できます。
- **[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。[Cisco vManage からの VNF に関する情報の表示 \(129 ページ\)](#) 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 35: 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

Configuration of PNF: 4444

Q Search Options

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 36: 外部ネイバー情報を持つ最初の位置にある PNF

Configuration of PNF: 4444

Q 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
4200000007	255.255.255.248	--	--	--	22.1.1.43	22.1.1.44	[200]

図 37: 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

Q Search Options

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

図 38: 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

Q 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 クラスタのパケットキャプチャ

表 35: 機能の履歴

機能名	リリース情報	説明
Cloud onRamp Colocation クラスタのパケットキャプチャ	Cisco IOS XE リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能を使用すると、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) レベルでパケット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 でパケット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パケットをキャプチャすることもできます。この機能により、パケットの形式に関する情報を収集し、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。

コロケーションクラスタの 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 36: 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 vManage 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 vManage でパケットキャプチャ機能を有効にします。

1. Cisco vManage 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。

PNIC レベルでパケットをキャプチャする

1. Cisco vManage 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. 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 37: 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。
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 vManage 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 vManage 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。

スイッチ構成のための Cisco Colo Manager の状態

Cisco vManage からさまざまなプロセスをトリガーしたときのさまざまな Cisco Colo Manager (CCM) の状態と遷移は次のとおりです。

- INIT 状態 : Cisco Colo Manager コンテナが正常に初期化されたとき。
- IN-PROGRESS 状態 : 構成のプッシュが不可能な場合。
- SUCCESS 状態 : Cisco Colo Manager コンテナが Cisco vManage から受信したインテントを正常に変換し、Cisco Catalyst 9500-40X または Cisco Catalyst 9500-48Y4C スイッチにプッシュしたとき。
- FAILURE 状態 : Cisco Colo Manager での処理または構成のプッシュに障害が発生した場合。

Cisco vManage が Cloud OnRamp for Colocation 構成インテントを CCM に初めてプッシュすると、INIT 状態から IN-PROGRESS 状態に移行します。Cisco Colo Manager が構成をプッシュすると、SUCCESS または FAILURE 状態に戻ります。増分構成をプッシュするたびに、IN-PROGRESS 状態になります。いずれかの構成のプッシュが失敗すると、Cisco Colo Manager は FAILURE 状態になります。



- (注) Cisco Colo Manager の状態が変化すると、通知が送信されます。『[Cisco Colo Manager の通知 \(139 ページ\)](#)』を参照してください。

ホストからの Cisco Colo Manager の状態と遷移

Cisco vManage は、起動する Cisco Colo Manager のさまざまな CSP ホストの状態に依存します。

- **Starting** : Cisco Colo Manager が起動し、ヘルスチェックスクリプトが実行されていないとき。このフェーズ中、Cisco vManage は CSP の状態が正常に変わるのを待ちます。
- **Healthy** : ヘルスチェックスクリプトが実行され、チェックに合格した場合。この状態は、構成ステータスの運用モデルをクエリできるか、構成をプッシュできることを意味します。このフェーズ中に、Cisco Colo Manager が INIT 状態の場合、Cisco vManage はデバイスリストをプッシュします。Cisco Colo Manager が INIT 状態でない場合、Cloud OnRamp for Colocation は性能が低下した状態である可能性があり、リカバリフローが開始される必要があります。
- **Unhealthy** : Network Services Orchestrator (NSO) の必要なパッケージがすべて稼働していない場合。この状態は、NSO が起動しなかった、Cisco Colo Manager パッケージが起動しなかった、またはその他の理由など、さまざまな理由が原因である可能性があります。この状態は、構成ステータス操作が実行されておらず、構成をプッシュできないことを意味します。

Cisco Colo Manager の通知

`show notification stream viptela` コマンドを使用して、Cisco Colo Manager コンソールから Cisco Colo Manager 通知を表示できます。

以下に、さまざまな Cisco Colo Manager の内部状態を示します。

表 38: CCM 通知

Cisco Colo Manager の状態	通知トリガー	通知出力の例
INIT	<p>Init : Cloud OnRamp for Colocation がアクティブ化され、Cisco vManage が Cisco CSP で Cisco Colo Manager を起動します。</p> <p>(注) Cisco Colo Manager の状態は、docker コンテナが最初に起動されたときにのみ「Init」である必要があります、コンテナが削除されて再度起動されない限り、この状態になってはいけません。</p>	<pre>admin@ncs# show notification stream viptela last 50 notification eventTime 2019-04-08T17:15:15.982292+00:00 ccmEvent severity-level minor host-name ccm user-id vmanage_admin config-change false transaction-id 0 status SUCCESS status-code 0 status-message init details Initializing CCM event-type CCM-STATUS !</pre>

Cisco Colo Manager の状態	通知トリガー	通知出力の例
INPROGRESS	<p>Cisco vManage はインテントをプッシュし、Cisco Colo Manager は進行中の状態に移行します。</p> <p>(注) Cisco Colo Manager は、稼働中のスイッチに対して複数の進行中の通知を生成します。</p>	<pre>notification eventTime 2019-04-08T17:37:54.536953+00:00 ccmEvent severity-level minor host-name ccm user-id vmanage_admin config-change false transaction-id 0 status SUCCESS status-code 0 status-message IN-PROGRESS details Received configuration from vManage event-type CCM-STATUS !</pre>
SUCCESS	<p>クラスタのアクティブ化中に、Cisco Catalyst 9500 スイッチが正常にオンボードされると、ステータスは SUCCESS に移行します。増分構成の場合、構成がスイッチデバイスに正常に保存された場合のみ、ステータスが SUCCESS に移行します。</p>	<pre>notification eventTime 2019-04-08T17:51:48.044286+00:00 ccmEvent severity-level minor host-name ccm user-id vmanage_admin config-change false transaction-id 0 status SUCCESS status-code 0 status-message SUCCESS details Devices done onboarding event-type CCM-STATUS ! ! admin@ncs#</pre>

Cisco Colo Manager の状態	通知トリガー	通知出力の例
FAILURE	<p>クラスタのアクティブ化中にスイッチのオンボーディングが失敗した場合、CCM ステータスは FAILURE に移行します。増分構成が保存されていない場合、CCM ステータスは FAILURE に移行します。</p> <p>(注) 障害状態は、エンドユーザーの介入なしに別の状態に遷移することはできません。</p>	<pre>notification eventTime 2019-04-08T18:01:44.943198+00:00 ccmEvent severity-level critical host-name ccm user-id vmanage_admin config-change false transaction-id 0 status FAILURE status-code 0 status-message FAILURE details SVL bringup not successful. Could not sync TenGigabitEthernet2/0/* interfaces. event-type CCM-STATUS ! ! admin@ncs#</pre>
	<p>フレキシブルな接続の配線エラーが原因でクラスタのアクティブ化中にスイッチのオンボーディングが失敗し、CCM ステータスが FAILURE に移行します。</p>	

Cisco Colo Manager の状態	通知トリガー	通知出力の例
		<pre>admin@ncs# show notification stream viptela last 100 include Step notification details Step 5 of 7: Device switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM) connected after SVL reload. details Step 6 of 7: Started sync-from for primary device switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM) details Step 6 of 7: Sync-from done for primary device switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM) Device list : switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM), switch2 : 192.168.100.19 (C9500-48Y4C-CAT2316L2F2) details Step 6 of 7: Devices ready for LLDP query Device list : switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM), switch2 : 192.168.100.19 (C9500-48Y4C-CAT2316L2F2) details Step 6.1 of 7: LLDP Query Details: csp2 has 8/8 interfaces connected, 2/4 sriov, 2/4 fortville to primary switch; 2/4 sriov, 2/4 fortville to secondary switch; Found devices with not optimum connections:- csp1 has 6/8 interfaces connected, 2/4 sriov, 2/4 fortville to primary switch; 2/4 sriov, 0/4 fortville to secondary switch; Minimum Requirement is to have 8/8 interfaces per CSP in cluster. Recommended action: Please refer to recommended topologies and minimum requirements details Step 7 of 7: Devices done onboarding Device list : switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM), switch2 : 192.168.100.19 (C9500-48Y4C-CAT2316L2F2)</pre>

VM アラーム

以下は VM アラームであり、Cisco vManage がアラームを受信すると、Cisco vManage からそれらを表示できます。

表 39: アラーム

アラーム	トリガー条件	syslog メッセージ
INTF_STATUS_CHANGE	インターフェイスステータスの変更	<pre>nfvis %SYS-6-INTF_STATUS_CHANGE: Interface eth0, changed state to up</pre>
VM_STOPPED	VM の停止	<pre>nfvis %SYS-6-VM_STOPPED: VM stop successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c</pre>

アラーム	トリガー条件	syslog メッセージ
VM_STARTED	VM の起動	nfvis %SYS-6-VM_STARTED: VM start successful: SystemAdminTera_ROUTER_0_d8733c1- 0768-4ae6-8dce-b223ecdb036c
VM_REBOOTED	VM のリブート	nfvis %SYS-6-VM_REBOOTED: VM reboot successful: SystemAdminTera_ROUTER_0_d8733c1- 0768-4ae6-8dce-b223ecdb036c
VM_RECOVERY_INIT	VM リカバリの開始	nfvis %SYS-6-VM_RECOVERY_INIT: VM recovery initiation successful: SystemAdminTera_ROUTER_0_d8733c1- 0768-4ae6-8dce-b223ecdb036c
VM_RECOVERY_REBOOT	VM リカバリのリブート	nfvis %SYS-6-VM_RECOVERY_REBOOT: VM recovery reboot successful: SystemAdminTera_ROUTER_0_d8733c1- 0768-4ae6-8dce-b223ecdb036c
VM_RECOVERY_COMPLETE	VM リカバリの完了	nfvis %SYS-6-VM_RECOVERY_COMPLETE: VM recovery successful: SystemAdminTera_ROUTER_0_d8733c1- 0768-4ae6-8dce-b223ecdb036c
VM_MONITOR_UNSET	VM モニタリングの設定解除	nfvis %SYS-6-VM_MONITOR_UNSET: Unsetting VM monitoring successful: SystemAdminTera_ROUTER_0_d8733c1- 0768-4ae6-8dce-b223ecdb036c
VM_MONITOR_SET	VM モニタリングの設定	nfvis %SYS-6-VM_MONITOR_SET: Setting VM monitoring successful: SystemAdminTera_ROUTER_0_d8733c1- 0768-4ae6-8dce-b223ecdb036c

syslog サポートと VM アラームの詳細については、『[Cisco NFVIS Configuration Guide](#)』を参照してください。

VM 状態

展開された VM のライフサイクルの動作ステータスは次のとおりです。Cisco SD-WAN では、Cisco vManage から VM の状態を表示および監視できます。

表 40: VM 状態

VM 状態	説明
VM_UNDEF_STATE	VM または VNF は、ある状態から別の状態に移行中です。
VM_INERT_STATE	VM または VNF は展開されていますが、稼働していません。
VM_ALIVE_STATE	VM または VNF が展開され、正常に起動または稼働しています。
VM_ERROR_STATE	展開またはその他の操作が失敗した場合、VM または VNF はエラー状態になります。

クラウドサービスプラットフォームのリアルタイムコマンド

表 41: リアルタイムコマンド

System Information
Container status
show control connections
Control connection history
Control local properties
Control summary
Control statistics
Control valid vEdges
valid vManage ID

HW Alarms
HW Environments
PNICs
System Status
Host System Mgmt Info
Host System settings
Host System processes
Resource CPU allocation
RBAC Authentication
Resource CPU VNFs
Hardware Inventory
Hardware Temperature thresholds
Control affinity stats



第 8 章

ハイ アベイラビリティ

Cisco SD-WAN Cloud onRamp for Colocation ソリューションにより、さまざまなコンシューマがさまざまな繰り返しアプリケーションに安全にアクセスできます。Cisco SD-WAN Cloud onRamp for Colocation ソリューションの高可用性 (HA) は、クラスタ展開で発生する可能性のあるいくつかのタイプの障害を処理するように設計されています。Cisco SD-WAN Cloud onRamp for Colocation ソリューションの展開では、次のタイプの障害が発生する可能性があります。

- 計算の障害
- スイッチの障害
- サービスチェーンの障害

障害を解決するには、次のメカニズムを使用します。

- 冗長性
- 障害検出
- [冗長性 \(147 ページ\)](#)
- [さまざまな障害シナリオの処理 \(152 ページ\)](#)

冗長性

コンポーネントの障害に対処するために冗長性が追加されたコンポーネントを以下に示します。

- **x86 コンピューティング ハードウェア** : [x86 コンピューティング ハードウェアの冗長性 \(148 ページ\)](#) を参照してください。
- **ネットワークファブリック** : [ネットワークファブリックの冗長性 \(148 ページ\)](#) を参照してください。
- **物理NIC/インターフェイス** : [物理NICまたはインターフェイスの冗長性 \(148 ページ\)](#) を参照してください。

- NFVIS 仮想化インフラストラクチャ : [NFVIS、仮想化インフラストラクチャの冗長性 \(148 ページ\)](#) を参照してください。
- サービスチェーン/VNF : [サービスチェーンまたは VNF の冗長性 \(149 ページ\)](#) を参照してください。
- Cisco Colo Manager : [Cisco Colo Manager のリカバリ \(151 ページ\)](#) を参照してください。

ネットワークファブリックの冗長性

ネットワークファブリック : ハードウェアスイッチの冗長性機能は、ネットワークファブリックの障害を処理するために使用されます。スイッチに障害が発生した場合、スタンバイスイッチが、障害が発生したスイッチを通過するトラフィックを引き継ぐようにします。

x86 コンピューティング ハードウェアの冗長性

x86 コンピューティング ハードウェア : x86 コンピューティング ハードウェアで使用されるプロセッサ、ストレージなどのハードウェアコンポーネントが故障し、完全な Cisco Cloud Services Platform (CSP) システム障害につながる可能性があります。Cisco vBond オーケストレータは、管理インターフェイスを介して ICMP ping を使用して、x86 コンピューティングプラットフォームの正常性を継続的に監視します。システム障害では、オーケストレータはデバイスの状態と、影響を受けるサービスチェーンと VM を表示します。サービスチェーンを立ち上げるために必要なアクションを実行します。『[Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのモニタリング \(127 ページ\)](#)』を参照してください。VNF (仮想ネットワーク機能) の動作状態に応じて、十分なリソースが利用可能な場合は、VM を別の CSP で起動する必要があります。このアクションにより、VNF は Day-N 構成を保持できます。VNF ディスクがローカルストレージを使用している場合、サービスグループ全体を、オーケストレータに保存されている Day-0 構成を使用して別の CSP デバイスで再スピンする必要があります。

物理 NIC またはインターフェイスの冗長性

物理 NIC またはインターフェイス : 物理 NIC (PNIC) またはインターフェイスまたはケーブルに障害が発生したり、切断されたりすると、これらのインターフェイスを使用している VNF が影響を受けます。VNF が OVS ネットワークを使用している場合、リンクの冗長性を実現するためにポートチャネル構成が使用されます。VNF が OVS ネットワークを使用していて、VNF に HA インスタンスがある場合、そのインスタンスはすでに別の CSP で起動されています。フェールオーバーは、2 番目の CSP 上のこの VNF に対して発生します。2 番目の VNF インスタンスがない場合は、障害が発生した VNF を含むサービスチェーンを削除して再インスタンス化する必要があります。

NFVIS、仮想化インフラストラクチャの冗長性

Cisco NFVIS 仮想化インフラストラクチャ : NFVIS ソフトウェアレイヤで複数のタイプの障害が発生する可能性があります。CSP の重要なコンポーネントの1つがクラッシュしたり、ホス

トの Linux カーネルがパニックになったり、重要なコンポーネントの1つが応答しなくなったりする可能性があります。重大なコンポーネント障害が発生した場合、NFVIS ソフトウェアは netconf 通知を生成します。オーケストレータはこれらの通知を使用して、vManage ダッシュボードに障害を表示します。Cisco CSP または Cisco NFVIS がクラッシュするか、制御接続がダウンすると、オーケストレータはデバイスの到達可能性がダウンしていることを示します。ネットワークの問題（ある場合）を解決するか、CSP デバイスをリブートします。デバイスが回復しない場合は、CSP デバイスの削除に進む必要があります。

サービスチェーンまたは VNF の冗長性

表 42: 機能の履歴

機能名	リリース情報	説明
スイッチ冗長性のための HA VNF NIC の配置	Cisco SD-WAN リリース 20.5.1 Cisco vManage リリース 20.5.1	この機能は、サービスチェーンの最適な配置を提供するため、スイッチの冗長性を考慮しながら、リソースの使用率を最大化します。HA プライマリおよびセカンダリインスタンスの VNIC は、代替 CSP インターフェイスに配置され、スイッチレベルでの冗長性を実現します。
HA VNF NIC 配置の変更	Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	このリリースでは、冗長スイッチインターフェイスに接続されている CSP デバイスの物理 NIC 上のプライマリおよびセカンダリ VNF VNIC の配置が変更されています。

サービスチェーンまたは VNF：ファイアウォールなどのコロケーション サービスチェーン内の一部の VNF は、スタンバイ VNF を使用してステータスフルな冗長性機能をサポートしている可能性があります。Cisco CSR1000V などの VNF はステータスフルな冗長性をサポートしていない可能性があります。Cisco SD-WAN Cloud onRamp for Colocation ソリューションは、VNF に依存して VNF の高可用性を実現します。サービスチェーンレベルでの HA サポートは利用できません。VNF がステータスフル HA をサポートしている場合、障害を検出してスイッチオーバーを実行します。VNF をホストしている CSP デバイスが機能し、すべての NIC またはインターフェイス接続が機能している場合、以前にアクティブだった VNF がダウンし、スタンバイ VNF としてレポートすることが前提です。VNF が動作していない場合、VNF の HA はその時点から機能していないため、問題を修正する必要があります。

VNF が HA をサポートしていない場合、VNF 内で重要なプロセスが失敗し、そのような VNF で使用できる HA サポートがない場合、VNF はリブートすると想定されます。

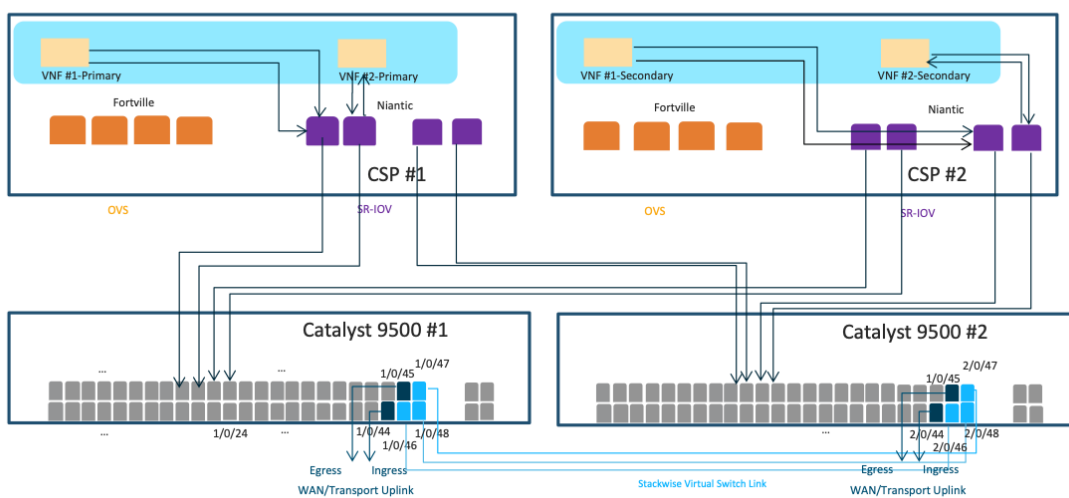
スイッチ冗長性のため的高可用性 VNF NIC の配置

Cisco SD-WAN Cloud onRamp for Colocation Release 20.5.1 以降、サービスチェーン内のネットワークサービスは、スイッチに障害が発生しても中断することなくトラフィックを転送します。HA 仮想インスタンスの仮想 NIC (VNIC) は、プライマリ HA インスタンスがあるスイッチとは異なるスイッチに配置されるため、トラフィックフローは中断されません。たとえば、

スイッチ 1 に接続されている CSP1 の物理 NIC にプライマリ VNF が配置されている場合、スイッチ 2 に接続されている CSP2 の物理 NIC にセカンダリ VNF が配置されます。

次の図は、次のことを示しています。

- このソリューションは、VNF #1 と VNF #2 のプライマリインスタンスを、スイッチ #1 に接続されている CSP #1 の SR-IOV ポートにプロビジョニングします。
- VNF1 と VNF2 のセカンダリインスタンスは、スイッチ 2 に接続されている CSP2 の SR-IOV ポートに配置されます。
- スイッチ #1 に障害が発生した場合、トラフィックは 2 番目のスイッチを使用して、1 番目の VNF と 2 番目の VNF のスイッチ #2 から引き続き流れます。



スイッチ冗長化のための HA VNF NIC に関する注意事項

- この機能は、VNF が SR-IOV インターフェイスを使用し、スイッチへのデュアルホーミングがサポートされていないシングルテナントクラスタにのみ適用されます。マルチテナントクラスタでは、ポートチャネルの一部である OVS インターフェイスがすでに使用されていて、スイッチにデュアルホーム接続されるため、この機能は必要ありません。
- ソリューションの配置アルゴリズムは、上で指定された冗長要件に基づいてサービスチェーンを自動的に配置します。手動構成は必要ありません。
- Cisco vManage を以前のリリースからリリース 20.5.1 にアップグレードする場合、HA VNF NIC 冗長性機能を使用するときに次の点が適用されます。
 - 作成する新しいサービスグループの場合、代替スイッチに接続する CSP インターフェイスでの HA 仮想インスタンスの VNIC の配置は自動的に行われます。

- 既存のサービスグループの場合、サービスグループをクラスタから切り離してから、クラスタに再接続して、サービスチェーンのスイッチの冗長性を実現します。
- 出力ポートを配置するときに、ソリューションは最初に入力 VNF ポートをホストするのと同じ CSP ポートに出力ポートを配置しようとします。CSP ポートに十分な帯域幅がない場合、ソリューションは、同じスイッチに接続されている同じ CSP デバイスの追加ポートに出力ポートを配置しようとします。

Cisco SD-WAN Cloud onRamp for Colocation Release 20.6.1 以降、ソリューションは最大 10 Gbps の帯域幅のサービスチェーンをサポートします。必要な帯域幅が 5 Gbps を超え、10 Gbps 以下である場合、VNF の入力および出力 VNIC の配置は、同じ CSP デバイスの異なる CSP ポートにある可能性があります。

スイッチの冗長性のために HA VNF NIC の配置を使用するための推奨事項

- すべてのサービスチェーンリソースを最大容量まで使用できるように、できるだけ多くのサービスチェーンを設計し、これらのチェーンをプロビジョニングします。これにより、コロケーションソリューションは、各ポートに未使用の帯域幅を残すことなく、VM の帯域幅を完全に連続した順序で利用できます。
- 高帯域幅のサービスチェーンをコロケーションクラスタに接続し、続いて低帯域幅のサービスチェーンを接続します。リソースを最適に使用するには、可用性の高いサービスチェーンをコロケーションクラスタに接続し、その後スタンドアロンサービスチェーンを接続します。

Cisco Colo Manager のリカバリ

Cisco Colo Manager のリカバリ : Cisco Colo Manager は、Cloud OnRamp for Colocation 内の CSP デバイスで起動されます。Cisco vManage は、DTLS トンネルを持つ CSP を選択して Cisco Colo Manager を起動します。次のシナリオでは、Cisco Colo Manager のリカバリフローが必要です。

Cisco Colo Manager をホストしている CSP が返品許可 (RMA) プロセスの対象と見なされ、この CSP を削除した後にクラスタ内に少なくとも 2 つの他の CSP デバイスがある場合、新しい Cisco Colo Manager は、既存の 2 つの CSP デバイスのうちのいずれかの Cisco vManage によって新しい構成のプッシュ中に自動的に起動されます。



- (注) RMA プロセスの対象と見なされた CSP デバイスの電源を切るか、CSP デバイスで工場出荷時のデフォルトリセットを実行する必要があります。このタスクにより、クラスタ内に Cisco Colo Manager が 1 つだけあることが保証されます。



- (注) Cisco Colo Manager が実行されているホストは再起動またはリブートできます。Cisco Colo Manager はすべての構成データと運用データをそのまま使用する必要があるため、このアクションはリカバリシナリオではありません。

クラスタが正常にアクティブ化された後、Cisco Colo Manager が異常になった場合は、[Cisco Colo Manager の問題のトラブルシューティング \(183 ページ\)](#) を参照してください。

さまざまな障害シナリオの処理

• VNF 障害

- HA 対応のサービスチェーン内の VM がダウンした場合、スタンバイ VM が引き継ぎます。このスタンバイサービスチェーンは、数秒以内に機能します。CSP デバイス上の Cisco NFVIS ソフトウェアは、モニタリング対象の VM である場合、機能不全なアクティブ VM を起動しようとします。VM が正常に回復すると、アクティブモードとスタンバイモードに正常に切り替わります。VM が正常に回復せず、この VM で HA 機能を起動する場合は、サービスチェーンを削除して、HA 機能を備えた新しいサービスチェーンを起動します。ここで、VM は障害がハートビートに基づいていることを検出し、トラフィックに影響を与えることはありません（数秒を除く）。アクティブな VM が回復した場合、この VM は再びアクティブになるか、スタンバイのままになる可能性があり、この状態は VM ごとに異なります。
- VM が HA に対応していない場合、サービスチェーンは失敗し、トラフィックはブラックホールになります。Cisco Colo Manager はこの障害を検出するため、Cisco vManage は VM がダウンしサービスチェーンがダウンしているという通知を受け取ると、アラートを送信します。VM が正常に回復すると、同じ通知が送信され、サービスチェーンは介入なしで機能します。VM が正常に回復しない場合は、サービスチェーンを削除し、新しいサービスチェーンを起動します。

• サービスチェーンの障害

- サービスチェーン内のすべての VM が HA をサポートしている場合、サービスチェーンはアクティブおよびスタンバイのサービスチェーンを持つことができます。アクティブなサービスチェーンがダウンすると、スタンバイサービスチェーンが引き継ぎ、数秒以内に機能します。この動作は VM レベルの HA であり、VM フェールオーバーの動作が引き継がれます。CSP 上の Cisco NFVIS ソフトウェアも、（モニタリング対象の VM の場合）機能不全なアクティブ VM の起動を試み、それらが正常に回復すると、VM はアクティブモードとスタンバイモードに正常に切り替わります。
- VM が HA に対応していない場合、サービスチェーンは失敗し、トラフィックはブラックホールになります。Cisco NFVIS と Cisco Colo Manager は、VM がダウンしているという通知を送信し、Cisco vManage はアラートを送信します。通知に基づいて、別のアクティブなサービスチェーンを起動します。サービスチェーンが正常に回復すると、同じ通知が送信され、サービスチェーンは介入なしで機能します。

- Cisco CSP デバイスの障害

Cisco CSP がダウンすると、その CSP で実行されているすべてのサービスチェーンと VM もダウンします。Cisco Colo Manager は、CSP デバイスに到達不可という通知を Cisco vManage に送信し、Cisco vManage は CSP デバイスとの DTLS 接続の損失を検出します。Cisco vManage は CSP デバイスに関するアラートを送信します。サービスチェーンを作成し、構成をコロケーションにプッシュすることにより、別の CSP デバイスでサービスチェーンを起動する必要があります。十分な計算ハードウェアがない場合は、別の CSP デバイスをコロケーションに追加し、サービスチェーン構成を他の CSP デバイスにプッシュします。

リリース 20.5.1 以降、コロケーションクラスタにデバイスのバックアップコピーを作成することで、障害のある CSP デバイスを置き換えることができます。したがって、CSP デバイスに障害が発生した場合、新しい CSP デバイスを Cisco vManage に追加して、デバイスを交換前の状態に復元することができます。CSP デバイスの交換方法の詳細については、「[Cisco CSP デバイスの返却](#)」を参照してください。

- スイッチリンクの障害

スイッチからのリンクがダウンした場合、他のスイッチが引き継ぎ、サービスチェーントラフィックが継続します。



第 9 章

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

表 43: 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 リリース 17.5.1a Cisco SD-WAN リリース 20.5.1 Cisco vManage リリース 20.5.1	この機能により、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 \(155 ページ\)](#)
- [マルチテナント環境での役割と機能 \(157 ページ\)](#)
- [マルチテナント環境での推奨仕様 \(158 ページ\)](#)
- [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 \(159 ページ\)](#)
- [サービスプロバイダー機能 \(160 ページ\)](#)
- [テナント コロケーションクラスタの管理 \(163 ページ\)](#)
- [c-tenant-functionalities \(164 ページ\)](#)
- [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 SD-WAN デバイスの監視 \(165 ページ\)](#)

コロケーション マルチテナント機能の概要

Cisco 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 vManage 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。「[クラスタの作成とアクティブ化](#)」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 コントローラ (Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ) を展開および構成します。
- 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 SD-WAN はシングルテナントモードで動作し、Cisco vManage ダッシュボード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す。

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 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 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 SD-WAN デバイスの監視 \(165 ページ\)](#)』を参照してください。
- 共同管理された Cisco 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 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 SD-WAN デバイスはテナントの Cisco SD-WAN コントローラ (Cisco vManage、Cisco vBond オーケストレーション および Cisco vSmart 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 SD-WAN デバイスの監視 \(165 ページ\)](#)』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 vManage にログインします。サービスプロバイダーは、Cisco vManage 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 vManage を管理し、Cisco 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 44: 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。さまざまなコロケーションサイズのサービスチェーンごとの VM の数については、「[Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのサイジング要件](#)」を参照してください。

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、「[配線に関する要件](#)」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 vBond Orchestrator 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 \(78 ページ\)](#) 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 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

以下のセクションでは、サービスプロバイダーが実行できるタスクについて説明します。

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。「[クラスタの作成とアクティブ化](#)」を参照してください。

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、「[コロケーショングループの作成](#)」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、「[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](#)」を参照してください。

(注) Cisco vManage 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に接続します。「[サービスグループでのサービスチェーンの作成](#)」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 vManage 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 vManage 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。

ステップ 1 Cisco vManage 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

ステップ 1 Cisco vManage 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 SD-WAN Systems and Interfaces Configuration Guide』の「[Manage Users Using Cisco vManage](#)」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

ステップ 1 Cisco vManage 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 **[UserGroups]** ドロップダウンリストから、ユーザーが属する必要が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 vManage 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 vManage 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 vManage を使用して構成されている場合、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 vManage 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。

ステップ 1 Cisco vManage 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。

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。「[サービスグループの表示](#)」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 \(103 ページ\)](#)』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 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。「[クラスタの作成とアクティブ化](#)」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。「[サービスグループでのサービスチェーンの作成](#)」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 vManage 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 vManage 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。

c-tenant-functionalities

以下のセクションでは、テナントが実行できるタスクについて説明します。

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 vManage にログインします。
2. VNF の正常性とともに、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 クラスタの監視 \(132 ページ\)](#) 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 SD-WAN デバイスの監視

始める前に

- サービスプロバイダー Cisco vManage 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 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 vManage 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接続する必要がある場合は、Cisco 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 vManage 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。

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 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。「[サービスグループでのサービスチェーンの作成](#)」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 vManage 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 vManage からの VNF の Cisco SD-WAN デバイスに関する情報を監視します。

(注) サービスプロバイダーは、VNF の Cisco SD-WAN デバイスに関する情報をサービスプロバイダーの **[Cisco vManage] > [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。



第 10 章

Cisco SD-WAN Cloud onRamp for Colocation ソリューションのトラブルシューティング

- コロケーションマルチテナント機能の問題のトラブルシューティング (167 ページ)
- Catalyst 9500 の問題のトラブルシューティング (168 ページ)
- 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 (174 ページ)
- DHCP IP アドレス割り当て (182 ページ)
- Cisco Colo Manager の問題のトラブルシューティング (183 ページ)
- サービスチェーンの問題のトラブルシューティング (185 ページ)
- 物理ネットワーク機能管理の問題のトラブルシューティング (187 ページ)
- CSP からのログ収集 (188 ページ)
- Cisco vManage の問題のトラブルシューティング (188 ページ)

コロケーションマルチテナント機能の問題のトラブル シューティング

次のコマンドを使用して、出力を表示し、問題を特定できます。

- 存在するブリッジなど、各 VNF の VNIC と VLAN の概要を表示するには、`support ovs vsctl show` コマンドを使用します。

```
nfvis# support ovs vsctl show
```

- ブリッジ、ネットワーク、または VLAN を使用したサービスチェーンの展開の詳細を確認するには、`show service-chains` コマンドを使用します。
- コロケーションクラスタ内の CSP デバイスとピア CSP デバイスのデータと HA VTEP IP アドレスを表示するには、`show cluster-compute-details` コマンドを使用します。
- 各 HA ブリッジの送信元および宛先のシリアル番号と、対応する VLAN および VNID の関連付けを表示するには、`show vxlan tunnels` コマンドを使用します。
- VLAN のユーザー ID、VNID マッピングによって識別できるテナントごとのデータフローを表示するには、`show vxlan flows` コマンドを使用します。

- VXLAN フロー統計を表示するには、`support ovs ofctl dump-flows vxlan-br` コマンドを使用します。
- VM ライフサイクルの全体的な展開ステータスを表示するには、`show vm_lifecycle deployments` コマンドを使用します。

エンドツーエンドの Ping が失敗する

1. `show vm_lifecycle deployments all` コマンドを使用して、VM が展開されているかどうかを確認します。
2. `show service-chains` コマンドを使用して、サービスチェーンに接続されているチェーン名が表示されることを確認します。
3. `show notification stream viptela` を使用して、Cisco SD-WAN デバイスで発生したイベントに関する通知を確認します。
4. `show cluster-compute-details` コマンドを使用して、CSP ピアデバイスの `data-vtep-ip` と `ha-vtep-ip` に ping を実行します。
5. ブリッジ、ネットワーク、または VLAN ごとの VLAN の関連付けが、各 VNF の VNIC および VLAN と一致していることを確認します。`show service-chain chain-name` コマンドの出力が `support ovs vsctl show` コマンドの出力と一致することを確認します。
6. 接続に失敗し、ピア CSP デバイスに ping できない場合は、テクニカルサポートにお問い合わせください。

Catalyst 9500 の問題のトラブルシューティング

ここでは、一般的な Catalyst 9500 の問題とそのトラブルシューティング方法について説明します。

一般的な Catalyst 9500 の問題

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

Cisco Colo Manager の PNP リストを確認して、スイッチデバイスがコールホームしていないかどうかを判断します。次に、`show pnp list` コマンドを使用した場合の良いシナリオと悪いシナリオをそれぞれ示します。

デバイスがコールホームした

```
admin@ncs# show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
-----
FCW2223A3VN 192.168.10.40 true true true 2018-12-18 22:53:26
FCW2223A4B3 192.168.30.42 true true true 2018-12-11 00:41:19
```

デバイスがコールホームしていない


```
admin@ncs# show pnp list
```

```
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
```

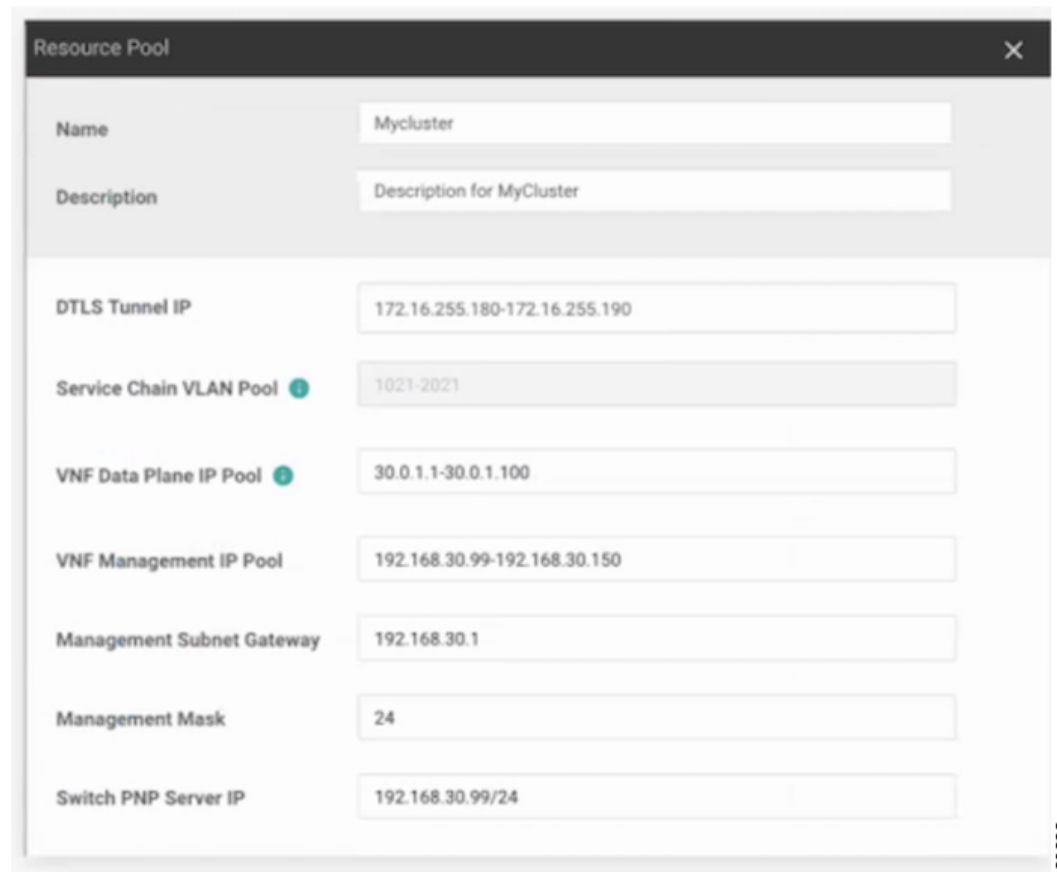
<- 空のリスト

Action:

1. 両方のスイッチの管理インターフェイスがシャットダウンされておらず、IPアドレスがあることを確認します。
2. スイッチで **write erase** コマンドを実行してから、リロードしてみます。IPアドレスが管理インターフェイスに表示されることを確認します。
3. DHCP オプション43の構成が有効であることを確認します。PNP IP アドレスが 192.168.30.99 であるサンプル DHCP 構成を次に示します。

```
ip dhcp pool 192_NET network 192.168.30.0 255.255.255.0 dns-server 192.168.30.1
default-router 192.168.30.1 option 43 ascii "5A;B2;K4;I192.168.30.99;J9191" lease
infinite
```

4. 次のように、リソースプールの Cisco vManage で提供される PNP IP アドレスが DHCP 構成の IP アドレスと一致することを確認します。



Field	Value
Name	Mycluster
Description	Description for MyCluster
DTLS Tunnel IP	172.16.255.180-172.16.255.190
Service Chain VLAN Pool	1021-2021
VNF Data Plane IP Pool	30.0.1.1-30.0.1.100
VNF Management IP Pool	192.168.30.99-192.168.30.150
Management Subnet Gateway	192.168.30.1
Management Mask	24
Switch PNP Server IP	192.168.30.99/24

5. ping を実行して、両方のスイッチに到達可能かどうかを確認します。

Catalyst 9500 は DHCP オプション 43 を使用して到達できなかった

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は進行中です。クラスタがすでにアクティブ化されている場合は、クラスタがアクティブ化保留状態にあることを示します。クラスタがアクティブ化されていない場合は、クラスタがアクティブ化されていない状態であることを示します。

Action:

1. 管理ユーザーとしてNFVISにSSHで接続します。`ccm-console` コマンドを使用して、Cisco Colo Manager にログインします。`show pnp list` コマンドを実行します。
2. PNP リストが空の場合は、OOB スイッチで Cisco Colo Manager の IP アドレスが正しく設定されているかどうかを OOB ステータスで確認します。

Day-0 構成のプッシュが両方の Catalyst 9500 スイッチで失敗した

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は進行中です。PnP 構成のプッシュはエラーで失敗し、Cisco Colo Manager は進行中の状態です。

Action:

1. `renumber` コマンドと `write erase` コマンドを使用して、Catalyst 9500 スイッチをクリーニングします。
2. Cisco vManage からクラスタを非アクティブ化してから再度アクティブ化して、Day-0 構成を再プッシュします。

セカンダリ Catalyst 9K スイッチで Day-0 構成のプッシュが失敗する

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は「Failure」を示しています。Cisco Colo Manager は、1つのスイッチのみが正常に起動し、セカンダリスイッチの障害を検出できないことを示しています。

Action:

1. `renumber` コマンドと `write erase` コマンドを使用して、セカンダリ Catalyst 9500 スイッチをクリーニングします。
2. vManage からクラスタを非アクティブ化してから再度アクティブ化して、Day-0 構成を再プッシュします。

Catalyst9500 スイッチの1つが稼働している。セカンダリスイッチがSVL構成になっておらず、SVL リンクケーブルが接続されていない

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は「Failure」を示しています。どちらのスイッチも IP アドレスを使用してオンボードされています。スイッチの SVL リンクが見つからないため、Cisco Colo Manager は両方のスイッチが接続されているときにエラーを検出します。Cisco vManage で両方のスイッチが「緑」として表示されます。

Action:

1. SVL リンクケーブルを確認します。
2. 両方の Catalyst 9500 スイッチのライセンスを確認します。

Day-0 構成のプッシュが失敗し、スイッチへの接続がダウンしている

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は、次の Day-0 構成プッシュまで「Failure」と表示されます。NSO は、構成をプッシュできないという通知を送信します。Cisco vManage でスイッチが「赤」として表示されます。これは、接続がダウンしていることを意味します。

Action:

1. Catalyst 9500 スイッチの正常性を確認します。
2. スイッチをオンラインに戻します。
3. Day-0 構成のプッシュを再開します。

Cisco vManage から PNP 後に Catalyst 9500 にログインできない

PNP の後、Cisco vManage が Catalyst 9500 にさらに構成をプッシュできない場合は、スイッチからロックアウトされている可能性があります。

Action:

1. 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、NFVIS にログインします。



(注) 初めてログイン試行すると、デフォルトのパスワードを変更するように求められます。画面の指示に従って強力なパスワードを設定してください。

2. Cisco NFVIS で **ccm console** コマンドを使用して、Cisco Colo Manager にログインします。Cisco Colo Manager で次のコマンドを実行して、ユーザーを Catalyst 9500 スイッチに追加します。

```
• config t
  cluster <cluster-name>
  system rbac users user admin password
  $9$yYkZqj7lQcrRL3$sZ23jqv5buK4lYCkt0dCbO6xYEfxRHQJiQnrlFdYHBg
```



(注) パスワードは必ずスクリプト文字列として設定してください。

これで、対応するユーザーが Catalyst 9500 スイッチに追加され、ユーザーとパスワードを使用してスイッチに SSH で接続できます。

クラスタのアクティブ化の問題、管理者およびパスワードを **Catalyst 9500** にプッシュできない

Action:

1. クラスタのアクティブ化がまだ保留状態の場合は、colo-config-status が進行中状態であるかどうかを確認します。状態が進行中の場合、同期は行われておらず、新しい構成をプッシュできません。このプロセスには最大 20 分かかります。
 1. CloudOnRamp for Colocation の構成ステータスが長時間進行中の状態になっている場合は、管理者ユーザーとして NFVIS に SSH で接続します。 **ccm-console** コマンドを使用して、Cisco Colo Manager にログインします。 **show pnp list** コマンドを実行します。2 つのスイッチが追加されているかどうかを確認します。
 2. スイッチが 1 つしか表示されない場合は、 **write erase** コマンドを使用して他のスイッチ構成が消去され、リロードされていることを確認してください。セカンダリスイッチのスタートアップ構成を消去して、初期状態に戻す必要があります。
 3. Cisco Colo Manager の PNP サーバーとのスイッチ接続を確認します。
2. クラスタが正常にアクティブ化されている場合は、colo-config-status が「SUCCESS」状態であるかどうかを確認します。ステータスが Success と表示されている場合は、管理者パスワードがスイッチにプッシュされている必要があります。そうでない場合は、Cisco vManage で新しいログイン情報をスイッチに追加してから、新しい構成をプッシュします。
3. クラスタのアクティブ化が失敗し、colo-config-status が「FAILED」状態の場合は、RBAC を使用して ccm コンソールから新しい認証をプッシュします。次の例では、パスワードは「Cisco-123」の暗号化です。

```
cluster cluster system rbac users user Alpha password
$9$Z9Sr2VOuwjwC74$qEYAmxgoaW4m07.UjPGR9gL2ksFkcCIcIcEYOUWxDfo role
administrators
```



(注) クラスタがアクティブ状態の場合、RBAC 構成をプッシュすることはできません。Cisco vManage は、Cisco Colo Manager への境界外の変更を許可しません。

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

クラスタの作成、クラスタのクリア、クラスタの削除中に、両方のスイッチの設定を消去する必要があります。クラスタ構成を消去するには、次の手順を実行します。

Action:

1. **show switch** コマンドを使用して、スイッチ番号とスイッチスタックにプロビジョニングされたスイッチが存在するかどうかを特定します。スイッチ番号が 2 の場合は、 **switch 2 renumber 1** コマンドを使用します。



(注) スイッチの再番号付けは、SVL スタックモードに不可欠です。

2. スイッチのスタートアップ構成を消去して初期状態に戻すには、**write erase** コマンドを使用します。
3. 新しい構成でスイッチをリロードするには、特権 EXEC モードで次のコマンドを使用し、変更した構成を保存しない場合は **n** を入力します。

```
switch(config)#reload
```

4. 最初のスイッチでスイッチスタックのリロードが完了したら、2 番目のスイッチデバイスで手順 2 と 3 を実行します。

Cisco Colo Manager からのスイッチデバイスの追加を確認するには、次の手順を実行します。

1. Cisco Colo Manager にログインし、**show pnp list** コマンドを使用します。

2 つのスイッチデバイスが表示されます。PNP は、Day-0 構成をプッシュし、スイッチデバイスを Cisco Colo Manager デバイスツリーに追加し、デバイス構成を Cisco Colo Manager と同期します。いずれかのスイッチデバイスを表示できない場合は、見つからないスイッチデバイスの PNP が正しく構成されていないか、ネットワークがダウンしている可能性があります。

スイッチにプッシュされた SVL 構成は、リポート後にスイッチにリポートコマンドを発行します。両方のスイッチデバイスが起動し、1 つのスタックになります。

2. Cisco Colo Manager で、約 14 分のタイマーをトリガーして、プライマリデバイスで別の同期を実行します。
3. デバイス構成と現在のステータスを表示するには、**show cluster cluster-name** コマンドを使用します。

ステータスが「GREY」と表示されている場合、スイッチデバイスはまだ Cisco Colo Manager のデバイスリストに追加されていません。ステータスが「RED」と表示されている場合、スイッチデバイスに到達できません。ステータスが「GREEN」と表示されている場合、デバイスは現在接続されています。また、プライマリスイッチデバイスを表示することもできます。

4. コロケーション内のデバイスステータスを表示するには、**show colo-config-status** コマンドを使用します。ステータスが「In-progress」の場合、スイッチデバイスはまだ同期されておらず、Cisco vManage はそれ以上の構成を送信できません。Cisco Colo Manager の状態遷移の詳細については、[Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのモニタリング \(127 ページ\)](#) の章を参照してください。

タイマーがその時間（たとえば、14 分）に達すると、Cisco Colo Manager は、プライマリ Catalyst 9500 デバイスとの再同期を試みます。

2 回目の同期が完了すると、Cisco Colo Manager の状態が「SUCCESS」と表示されます。

QoS ポリシー適用後のスイッチの構成

QoS ポリシーが適用されている場合、サービスチェーンの帯域幅を設定して展開すると、次の構成がスイッチデバイスに表示されます。

```
class ASAvOnly_chain1_VLAN_210police 2000000000class ASAvOnly_chain1_VLAN_310police
2000000000policy-map
service-chain-qosclass ASAvOnly_chain1_VLAN_210police 2000000000class
ASAvOnly_chain1_VLAN_310police 2000000000
```

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

ここでは、一般的なクラウドサービスプラットフォーム（CSP）の問題とそのトラブルシューティング方法について説明します。

Cisco CSP デバイスの RMA

Cisco vManage から CSP デバイスの **admin tech** コマンドを使用し、**[Tools] > [Operational Commands]**画面でデバイスのログ情報を収集します。次のログファイルを確認します。

- `nfvis_config.log` : デバイス構成関連のログを表示します
- `escmanager.log` : VM 展開関連のログを表示します。
- `Tech-support-output` : CSP デバイスから利用できる次の `show` コマンドを使用します。
 - `cat/proc/mounts` : マウント情報を表示します
 - `show hostaction backup status` : CSP デバイスで実行された最新の 5 つのバックアップのステータスを表示します
 - `show hostaction restore-status` : 全体的な復元プロセスと、デバイス、イメージとフレージャー、VM などの各コンポーネントのステータスを表示します
 - `show vm_lifecycle deployments` : 展開名と VM グループ名を表示します。

次に、NFS サーバーでのマウント操作の例を示します。

```
nfvis# show running-config mount
mount nfs-mount storage sujathast/
storagetype nfs
storage_space_total_gb 5000.0
server_ip 192.168.0.1
server_path /NFS/colobackup
```

次に、最新の 5 つのバックアップ操作の操作ステータス出力と、最新のバックアップに関する Cisco vManage の通知の例を示します。

```
eventTime 2021-02-02T04:02:25.577705+00:00
viptela
severity-level minor
host-name nfvis
```

```

system-ip 10.0.0.1
user_id admin
config_change false
transaction_id 0
status SUCCESS
status_code 0
status_message Backup configuration-only to nfs:test_storage/test_config_only.bkup
completed successfully with operational status: BACKUP-COMPLETED-PARTIALLY
details NA
event_type BACKUP_SUCCESS
severity INFO
host_name nfvis
!
```

次の例は、`show hostaction restore-status` コマンドを使用した後のデバイスのステータスを示しています。

```

nfvis# show hostaction restore-status
hostaction restore-status 2021-03-19T20:53:15-00:00
source nfs:sujathast/WZP22160NC7_2021_03_19T19_10_04.bkup
status RESTORE-ERROR
components NFVIS
status RESTORE-ERROR
last update 2021-03-19T21:02:11-00:00
details "Unable to load configuration Editing of storage definitions is not allowed"
components nfs:sujathast/WZP22160NC7_2021_03_19T19_10_04.bkup
status VERIFICATION-SUCCESS
```

VNIC および PNIC のステータスのクリア

1. PNIC 統計を表示するには、`show pnice stats` コマンドを使用します。
2. VNIC 統計を表示するには、次のいずれかのコマンドを使用します。

- すべての VM に対して `show vm_lifecycle vnic_stats`
- 単一の VM に対して `show vm_lifecycle vnic_stats vm-name`

3. 1 つ以上の VM の統計をクリアするには、次のコマンドを実行します。

```

clear counters vm all
clear counters vm vm-name vnic vnic-id
clear counters vm vm-name vnic all
```

4. すべての PNIC および VNIC の統計をクリアするには、`clear counters all` コマンドを使用します。

CSP をリブートすると、すべての PNIC および VNIC のカウンタが消去され、カウンタがクリアされます。VNIC と PNIC の統計が表示されない場合は、次のコマンドを使用して統計を表示できます。

```

show pnice-clear-counter
show vm_lifecycle tx_rx_clear_counters
```

Cisco CSP デバイスのオンボーディングの問題

1. デバイスが SD-WAN コントローラとのセキュアな制御接続を確立したことを確認するには、`show control connections` コマンドを使用します。

2. デバイスの認証に使用されるデバイスプロパティを確認するには、**show control local-properties** コマンドを使用します。

表示された出力から、次のことを確認します。

- システムパラメータは、**organization-name** と **site-id** を含むように設定されている
- **certificate-status** および **root-ca-chain-status** がインストールされている
- **certificate-validity** が [Valid] になっている
- **dns-name** が vBond IP アドレスまたは DNS を指している
- **system-ip** が構成され、**chassis-num/unique-id** および **serial-num/token** がデバイスで使用可能

3. デバイスが Cisco SD-WAN コントローラとの接続を確立できない場合、失敗の理由を表示するには、**show control connections-history** コマンドを使用します。[LOCAL ERROR] および [REMOTE ERROR] 列を表示して、エラーの詳細を収集します。

Cisco CSP デバイスが Cisco SD-WAN コントローラとの制御接続を確立できない理由は次のとおりです。

- **CRTVERFL** : エラー状態は、デバイスと Cisco SD-WAN コントローラ間のルート CA 証明書の不一致が原因で、デバイスの認証が失敗したことを示します。Cisco CSP デバイスで **show certificate root-ca-cert** を使用して、デバイスと Cisco SD-WAN コントローラに同じ証明書がインストールされていることを確認します。
- **CTORGNMMIS** : エラー状態は、Cisco SD-WAN コントローラで設定された組織名と比較して、組織名が一致しないためにデバイスの認証が失敗したことを示します。CSP デバイスで **show sdwan control local-properties** を使用して、すべての SD-WAN コンポーネントが同じ組織名で構成されていることを確認します。
- **NOVMCFG** : エラーステータスは、デバイスが Cisco vManage のデバイステンプレートにアタッチされていないことを示します。このステータスは、自動展開オプション (PnP) を使用してデバイスをオンボーディングするときに表示されます。
- **VB_TMO**、**VM_TMO**、**VP_TMO**、**VS_TMO** : このエラーは、デバイスが Cisco SD-WAN コントローラに到達できないことを示します。

クラスタのアクティブ化の失敗

CCM で、CCM 通知ステータスを表示して、スイッチの SVL 形成が完了し、デバイスがオンボードされているかどうかを確認します。

1. すべての SR-IOV および OVS ポートが Catalyst 9500 スイッチに正しくケーブル接続されていて、インターフェイスがリンクアップ状態になっていることを確認します。
2. CSP デバイスで **show lldp neighbors** コマンドを使用し、CSP デバイスと Catalyst 9500 スイッチ間の配線を確認して、SR-IOV および OVS ポートを特定します。

show lldp neighbors コマンドで 8 つのポートすべてに電源が入っていることが表示され、ネイバーについて報告されることを確認します。

3. Catalyst 9500 スイッチが SVL モードであり、インターフェイスに「SVL Complete」という説明があることを確認します。

証明書のインストールの失敗

show control connections-history コマンドを使用して、証明書のインストールの失敗を判別します。

図 39: 証明書のインストールの失敗

```

LB-CSP6444 show control connections-history
Legend For Errors:
ACRSM2 - Challenge rejected by peer.
NOVMCFG - No cfg in vmanage for device.
SERVREFL - Board ID signature verify failure.
NOZTPIN - No/Bad chassis-number entry in ZTP.
RDNTPM - Board ID not initialized.
OPSDOWN - Interface went peer down.
RDNTPWD - Peer Board ID Cert not verified.
OPTRNO - Server's peer timed out.
RDNTPID - Board ID signing failure.
RMGSPB - Remove Global saved peer.
CERTERR - Certificate expired.
RXTXTRM - Received heartbeat.
CERTUSER - Challenge response rejected by peer.
ROSIGPRB - Read Signature from Board ID failed.
CNTVERFL - Fail to verify Peer Certificate.
SERNTPRES - Serial Number not present.
COTCONMIS - Certificate Org name mismatch.
SSLNFIEL - Failure to create new SSL context.
DCONFAIL - DTLS connection failure.
STMOCLETD - Peerdown extra vBond in STUN server mode.
DEVALC - Device memory Alloc failure.
SYSIPCHNG - System IP changed.
DSTTMO - DTLS Handshake Timeout.
SYSPCHNG - System property changed.
DISCVBO - Disconnect vBond after register reply.
TMRMALC - Timer Object Memory failure.
DSTTLOC - TLS Disabled.
TMRMLOC - Timer Object Memory failure.
DUPSLVBO - Read a Dup Client Hello, Reset GI Peer.
TMOCDROB - Failed to read challenge to boardID.
DUPSER - Duplicate Serial Number.
UNMSGDORG - Unknown Message Type or Bad Register msg.
DUPSRIPSEL - Duplicate System IP.
UNMUTHEL - Read Hello from Unauthorized peer.
NAFAIL - SSL Handshake failure.
VDMEST - vDmson process terminated.
IP_TOS - Socket Options failure.
VECERTREV - vEdge Certificate revoked.
DUPSRIPSEL - Duplicate System IP.
VDCERTREV - vSmart Certificate revoked.
LISNERR - Listening socket IO error.
VR_TMO - Peer vBond Timed out.
MORTLCKD - Migration blocked, Wait for local TMO.
VM_TMO - Peer vManage Timed out.
RDMALCFL - Memory Allocation failure.
IP_TMO - Peer vEdge Timed out.
NOACTIV - No Active vBond found to connect.
VS_TMO - Peer vSmart Timed out.
NOERR - No Error.
KTMTRMOR - Peerdown extra vManage.
NOULPRCET - Unable to get peer's certificate.
KTVSTROM - Peerdown extra vSmart.
NOVNDONMIS - New vBond with no vmg connections.
KTVSTROM - Peerdown extra vSmart.
NTPRNMINT - Not preferred interface to vmanage.
STENTRY - Delete same tloc state entry.
VMBONDFAIL - Emberg check failed

```

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	LOCAL COLOR	STATE	LOCAL ERROR	REMOTE ERROR	REPEAT COUNT	DOMTIME
vBond	dtls	0.0.0.0	0	0	172.23.191.87	12344	172.23.191.87	12344	default	tear_down	DISCVBO	NOERR	0	2018-12-20T03:13:20+0000
vBond	dtls	0.0.0.0	0	0	172.23.191.87	12344	172.23.191.87	12344	default	up	RXTXTRM	VECERTREV	0	2018-12-20T03:12:44+0000
vmanage	dtls	172.16.255.200	100	0	172.23.191.86	12444	172.23.191.86	12444	default	up	RXTXTRM	VECERTREV	0	2018-12-20T03:12:44+0000
vmanage	dtls	172.16.255.200	100	0	172.23.191.86	12444	172.23.191.86	12444	default	tear_down	SYSIPCHNG	NOERR	0	2018-12-20T03:12:30+0000
vBond	dtls	0.0.0.0	0	0	172.23.191.87	12344	172.23.191.87	12344	default	tear_down	SYSIPCHNG	NOERR	0	2018-12-20T03:12:30+0000

Action:

発生する可能性のあるエラーに基づいて実行できる検証は次のとおりです。

- vBond with error SERNTPRES : このエラーは、デバイスのシリアルまたはトークンが vBond のシリアルまたはトークンと一致しない場合に発生します。vManage をチェックして、デバイスが「有効」な状態であり、適切にデコミッションされたことを確認します。
- Cisco vManage with error NOVMCFG : このエラーは、テンプレートがデバイスに接続されていない場合に発生します。クラスタをアクティブ化すると、この問題が解決します。
- vBond で、**show orchestrator valid-vedges** コマンドがデバイスを正しく表示することを確認します。これは、使用したトークンと同じトークンでデバイスが有効であることを意味します。
- Cisco vManage および CSP デバイスのクロックが同期していることを確認します。

制御接続の失敗

show control connections-history で DCONFAIL が表示されます。ファイアウォールを開いて、開く必要があるポートを表示します。

図 40: 制御接続の失敗、*DCONFAIL*

INSTANCE	PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	STATE	ORGANIZATION NAME	UPTIME
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12346	209.165.201.1	12346	default	up	JamesLo_honeywell	- 3853220:00:00:03
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12446	209.165.201.1	12446	default	up	JamesLo_honeywell	- 3853220:00:00:03
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12546	209.165.201.1	12546	default	up	JamesLo_honeywell	- 3853220:00:00:02
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12646	209.165.201.1	12646	default	up	JamesLo_honeywell	- 3853220:00:00:02
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12746	209.165.201.1	12746	default	up	JamesLo_honeywell	- 3853220:00:00:03

Action:

次のポートが開いている必要があります。

表 45: 開く UDS および TCP ポート

コア番号	DTLS (UDP) のポート	TLS (TCP) のポート
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

CSP に DHCP IP アドレスがない

CSP デバイスは、接続されたデバイスとして Cisco vManage に表示されません。

Action:

1. CIMC インターフェイスを使用して CSP に接続します。
2. Cloud OnRamp for Colocation 管理ポートで **show system:system settings** コマンドを実行して、CSP に IP アドレスがあるかどうかを確認します。
3. DHCP サーバーに IP アドレスがあるかどうかを確認します。静的 IP アドレスを割り当てて DHCP スティック IP を設定するには、[DHCP IP アドレス割り当て \(182 ページ\)](#) を参照してください。
4. ping を使用して、PNP サーバーに到達可能であることを確認します。
5. PNP サーバーから、CSP デバイスに接続して要求できるかどうか、またはリダイレクトが成功するかどうかを確認します。PNP ポータルで、デバイスの保留中のリダイレクトが表示されている場合は、シリアル番号が CSP デバイスと同じかどうかを確認します。
6. CSP で **show platform-details** コマンドを使用して、シリアル番号を確認します。
7. PNP ポータルで、接続済みと表示されているかどうかを確認します。

CSP が Cisco vManage との接続を確立していない

CSP デバイスは、接続されたデバイスとして Cisco vManage に表示されません。

Action:

1. **show certificate installed** および **show certificate root-ca-cert** を使用して、CSP デバイスに PNP からインストールされたルート CA があるかどうかを確認します。
2. CSP が vBond IP アドレスに ping できるかどうかを確認します。次に、**show running-config viptela-system:system** を使用して vBond IP を取得します
3. vBond への ping が失敗した場合は、管理インターフェイスでネットワーク接続を確認します。
4. vBond への ping が通る場合は、**running-config vpn 0** を使用して、制御接続の構成を表示します。
5. 制御接続構成が存在する場合は、Cisco vManage 設定を確認します。
6. Cisco vManage で、**show control connections** および **show control local-properties** コマンドを使用して、クラスタがアクティブ化され、デバイスの OTP 情報が含まれているかどうかを確認します。
7. **request vedge-cloud activate chassi-number token-number** コマンドを使用して、CSP トークン番号が手動で入力されているかどうかを確認します。正しい OTP を使用してコマンドを再実行します。

CSP デバイスの工場出荷時設定へのリセット

CSP デバイスを工場出荷時のデフォルトにリセットするには、次のコマンドを使用します。

CSPxx# factory-default-reset all

このコマンドは、VM とボリューム、ログ、通知、イメージ、証明書などのファイルを削除します。すべての設定を削除します。接続が切断され、管理者パスワードが工場出荷時のデフォルトパスワードに変更されます。リセット後、システムは自動的にリブートします。出荷時設定へのリセットが進行中の 15～20 分間は、何も操作を実行しないでください。工場出荷時設定へのリセットプロセスを続行するように求められたら、続行できます。

ストレージディスクが不良な CSP

制御接続が確立され、クラスタがアクティブ化されます。Cisco vManage モニタリング画面には、使用可能な 8 つの CSP ディスクすべてと、障害のあるディスクの 1 つが表示されます。

Action:

不良ディスクを交換します。

CSP デバイスのメモリまたは CPU が少ない

制御接続が確立され、クラスタがアクティブ化されます。Cisco vManage モニタリング画面に、メモリのしきい値に達したことが表示されます。

Action:

最小要件に一致する特定の CSP デバイスをアップグレードします。

CSP デバイスの I/O カードが間違っただスロットにある

Action:

CIMC インベントリからスロットの詳細を確認します。

Colo Manager が CSP デバイスで正常でない

Action:

1. Cisco Colo Manager の状態を確認するには、次の手順を実行します。
 1. **show container ColoMgr** コマンドを使用して、コンテナの正常性を確認します。
『[Cisco Colo Manager の問題のトラブルシューティング \(183 ページ\)](#)』を参照してください。
 2. **show notification stream viptela** コマンドを使用して、Viptela デバイスからのイベントに関する通知を表示します
2. Cisco Colo Manager にアクセスするには、Cisco Colo Manager が有効になっている CSP デバイスで **ccm console** コマンドを実行します。
このアクションにより、Cisco Colo Manager CLI に移動します。**show running-config cluster cluster name** コマンドを実行します。
3. **admin-tech** コマンドを使用して、Cisco vManage からログを取得します。または、デバイスから直接ログを取得することもできます。『[CSP からのログ収集 \(188 ページ\)](#)』を参照してください。

CSP への Day-0 構成プッシュが失敗する

この障害は、CSP に適切なハードウェアがないか、VNF の Day-0 構成に間違っただ入力があることが原因である可能性があります。

Action:

1. CSP のハードウェア構成を確認し、サポートされている構成であることを確認します。
2. サービスチェーンの Day-0 構成を確認してから、構成プッシュを再度トリガーします。

CSP がクラスタに追加されない

[vManage] > [Configuration] > [Cloud OnRamp for Colocation] のインターフェイスのクラスタ状態は、「FAILED」を示します。追加された CSP は、Cloud OnRamp for Colocation のグラフィック表示で「RED」として示されます。

Action:

1. CSP のハードウェア構成を確認し、サポートされていることを確認します。
2. クラスタのアクティブ化を再試行します

CSP との IP 接続を維持できない

CSP デバイスが DHCP IP を更新すると、CSP への IP 接続を維持できません。

Action:

DHCP IP アドレスの割り当てについては、DHCP サーバーが常に CSP デバイスと同じサブネット上にあることを確認してください。

CSP デバイスが Cisco vManage に到達できない

Action:

次の操作を行ってください。

1. KVM コンソールを使用して、CSP デバイスに Cisco NFVIS をインストールします。NFVIS のインストールについては、『[Cisco Enterprise NFV Infrastructure Software Configuration Guide](#)』を参照してください。
2. NFVIS システムにログインし、ゲートウェイに ping を送信します

ping を送信していないまたは到達可能でない場合は、スイッチに接続されている OOB スイッチポートのポートチャネル構成が完了していることを確認します。

1. スイッチのポートチャネル構成がない場合は、`nfvis# support ovs appctl bond-show mgmt-bond` コマンドを実行します。出力は次のとおりです。

```
--- mgmt-bond ----
bond_mode: balance-slb
bond may use recirculation: no, Recirc-ID : -1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
next rebalance: 3479 ms
lacp_status: configured
active slave mac: 00:00:00:00:00:00 (none)
slave eth0-1: disabled
    may_enable: false
slave eth0-2: disabled
    may_enable: false
```

2. スイッチのポートチャネルは構成されているが、`eth0-2` がスイッチに接続されていない場合は、`nfvis# support ovs appctl bond-show mgmt-bond` コマンドを実行します。次の出力は、`eth0-2` がスイッチに接続されていないことを示しています。

```

---- mgmt-bond ----
bond_mode: balance-slb
bond may use recirculation: no, Recirc-ID : -1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
next rebalance: 4938 ms
lACP_status: off
active slave mac: 50:2f:a8:c7:64:c2 (eth0-1)

slave eth0-1: enabled
active slave
may_enable: true
hash 195: 2 kB load

slave eth0-2: disabled
may_enable: false

```



(注) Cisco vManage は CSP デバイスを管理するため、NETCONF または REST API または CLI を介した OOB 構成により、デバイスが Cisco vManage と同期しなくなります。Cisco vManage は、次の構成がそこからプッシュされるときに、この構成を削除します。トラブルシューティングの場合、Cisco CSP または NFVIS を構成するには、共有モードまたは NETCONF ターゲット候補でのみ構成を使用してからコミットします。この構成は、ConfD データベースのように必要であり、CDB は Cisco SD-WAN Cloud onRamp for Colocation ソリューションの Cisco NFVIS で候補モードになっています。**config t** CLI モードまたは NETCONF ターゲットの実行が使用されている場合、CDB データベースが同期されていない可能性があり、CSP デバイスで異常な動作が発生し、クラスタが使用できなくなります。

DHCP IP アドレス割り当て

静的 IP アドレスを構成するには、次の手順を実行します。

1. DHCP サーバーのクリーンインストール後、**confd cli** を実行します。
2. **nfvis# show running-config vm_lifecycle** コマンドを使用して、既存の構成を確認します。

次に例を示します。

```
nfvis# show running-config vm_lifecycle networks
```

```
vm_lifecycle networks network int-mgmt-net
!
```

3. **nfvis# config shared** コマンドを使用して、静的 IPv4 アドレスを設定します。

次に例を示します。

```
nfvis# config shared
```

```
Entering configuration mode terminal
nfvis(config)# vm_lifecycle networks network int-mgmt-net subnet int-mgmt-net-subnet
address <host-ip> gateway <host-ip-gateway> netmask <your-host-ip-netmask> dhcp
false
nfvis(config-ip-receive-acl-0.0.0.0/0)# commit
Commit complete.
nfvis(config-ip-receive-acl-0.0.0.0/0)# end
nfvis#
```

DHCP スティック IP の構成

スティック DHCP IP の場合は、DHCP サーバーを構成します。デバイスのシリアル番号をすぐに利用できることを確認してください。

1. CentOS 7.4 を DHCP サーバーとして使用する場合は、`/etc/dhcp/dhcpd.conf` に次の同様の構成があることを確認します。

```
host abcxxxx175 {
option dhcp-client-identifier <serial number>;
}
```

2. IOS を DHCP サーバーとして使用する場合は、IOS DHCP サーバーまたはプールに次の同様の構成があることを確認してください。

```
ip dhcp pool P_112
host 209.165.201.12 255.255.255.0
client-identifier 4643.4832.3xxx.3256.3xxx.48
```

この例では、IP アドレス 209.165.201.12 は、識別子が 4643.4832.3xxx.3256.3xxx.48 のクライアントの DHCP スティック IP です。次に、クライアント識別子を見つけることができます。

3. クライアント識別子を見つけるには、IOS DHCP サーバーで `debug ip dhcp server packet` をオンにします。

デバッグコンソールの出力から、SD-WAN Cloud OnRamp for Colocation デバイスの DHCP クライアント識別子を表示できます。

Cisco Colo Manager の問題のトラブルシューティング

ここでは、一般的な Cisco Colo Manager の問題とそのトラブルシューティング方法について説明します。

一般的な Cisco Colo Manager の問題

SVL の形成に失敗した場合のポート接続の確認

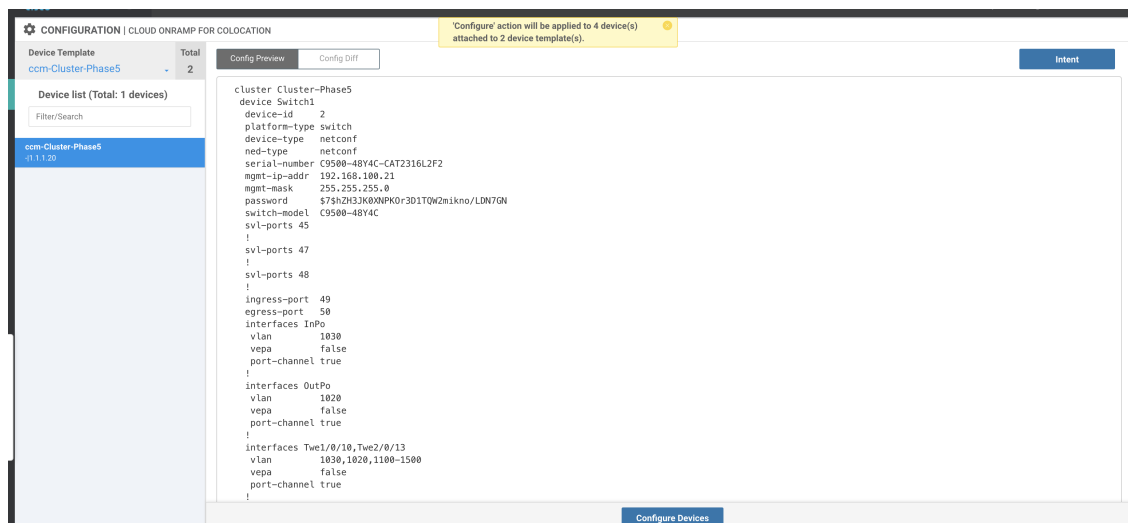
クラスタをアクティブ化した後、CCM からの SVL およびアップリンクポートを確認するには、次の手順を実行します。

1. Cisco vManage で、**[Configuration]** > **[Cloud OnRamp for Colocation]** をクリックします。

2. クラスタのポート接続を確認するには、テーブルからクラスタを選択し、行の右側にある [More Actions] アイコンをクリックしてから、[Sync] を選択します。
3. [Device Template] で、コロケーションクラスタをクリックし、ドロップダウンリストから CCM クラスタを選択します。
4. CCM 構成を表示するには、CCM クラスタをクリックします。

クラスタ内の両方のスイッチデバイスのポート接続の詳細を表示し、接続の問題を特定できるようにしました。

図 41: SVL およびアップリンクポートの検証



Cisco Catalyst 9500 SVL 形成の失敗

1. 管理者ユーザーとして Cisco NFVIS との SSH セッションを確立します。 **ccm-console** コマンドを使用して Cisco Colo Manager にログインし、 **show colo-config-status** コマンドを実行します。

```
admin@ncs# show colo-config-status
```

推奨されるアクションを表示します。

```
colo-config-status status failure
colo-config-status description "Step 4 of 7:
Device c9500-2 : 192.168.6.252 (CAT2324L42L)
SVL ports specified by vmanage does not match with
actual cabled svl ports. Recommended action: Correct
the configured svl ports specified in cluster
configuration by vmanage in accordance with switch
SVL port cabling" colo-config-status severity critical
```

2. Cisco vManage の SVL 用に選択したポート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、およびそれらが Cisco Catalyst 9500 スイッチによって検出されることを確認してください。

Day-0のクラスタをアクティブにしているときに **Cisco Colo Manager** が異常であるか、**Cisco Colo Manager** の実行中に **Cisco CSP** が削除されます。また、新しく追加された **Cisco CSP** デバイスの新しい **Cisco Colo Manager** がインスタンス化に失敗するか、異常になります

ここで、Cisco Colo Manager はホスト側で異常な状態にあり、Cisco Colo Manager の内部状態は「FAILURE」を示しています。Cisco vManage モニタリングでも、Cisco Colo Manager が「UNHEALTHY」状態で表示されます。

Action:

1. **show container ColoMgr** コマンドを実行して、新しく追加された Cisco CSP デバイスの Cisco Colo Manager の状態を確認します。

```
CSP1# show container ColoMgr
container ColoMgr
  uuid          57b9b8646ff1066ba24707415b5449111d915664629f56221e141c1171ee283d
  ip-address    172.31.232.182
  netmask       24
  default-gw    172.31.232.2
  bridge        int-mgmt-net-br
  state         healthy
  error
CSP1#
```

2. 前の手順で示したエラーフィールドを調べて、Cisco Colo Manager が異常な状態になっている理由を確認します。
3. ゲートウェイへの ping に関連する障害の場合は、IP アドレス、マスク、ゲートウェイ IP アドレスなどの Cisco Colo Manager パラメータが有効であることを確認します。また、ゲートウェイへの物理接続の到達可能性を確認します。
4. いずれかのパラメータが正しくない場合は、Cisco vManage からそれらを修正してから、クラスタのアクティブ化または同期を再試行します。
5. Cisco Colo Manager が正常でない理由がパッケージエラーである場合は、テクニカルサポートに連絡してください。

サービスチェーンの問題のトラブルシューティング

ここでは、一般的なサービスチェーンの問題とそのトラブルシューティング方法について説明します。

一般的なサービスチェーンの問題

サービスグループへのサービスチェーンの追加または削除が失敗する

• Action:

- Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は、構成プッシュに対して「FAILURE」を示しています。構成プッシュが失敗し、Cisco Colo Manager が「FAILURE」状態になり、クラスタが「FAILURE」状態になります。

Action:

1. Cisco Colo Manager にアクセスするには、Cisco Colo Manager が有効になっている CSP デバイスで **ccm console** コマンドを実行します。

このアクションにより、Cisco Colo Manager の CLI に移動します。次のコマンドを実行します。

1. **show colo-config-status**

このアクションにより、説明に失敗の理由を表示できます。

2. 障害をデバッグするためにさらに情報が必要な場合は、Cisco Colo Manager をホストしている CSP で **admin-tech** コマンドを使用してログを収集します。または、デバイスから直接ログを取得することもできます。『[CSP からのログ収集 \(188 ページ\)](#)』を参照してください。

2. VNF サービスチェーンの Day-0 構成を確認します。

3. VNF サービスチェーンを再度プロビジョニングします。



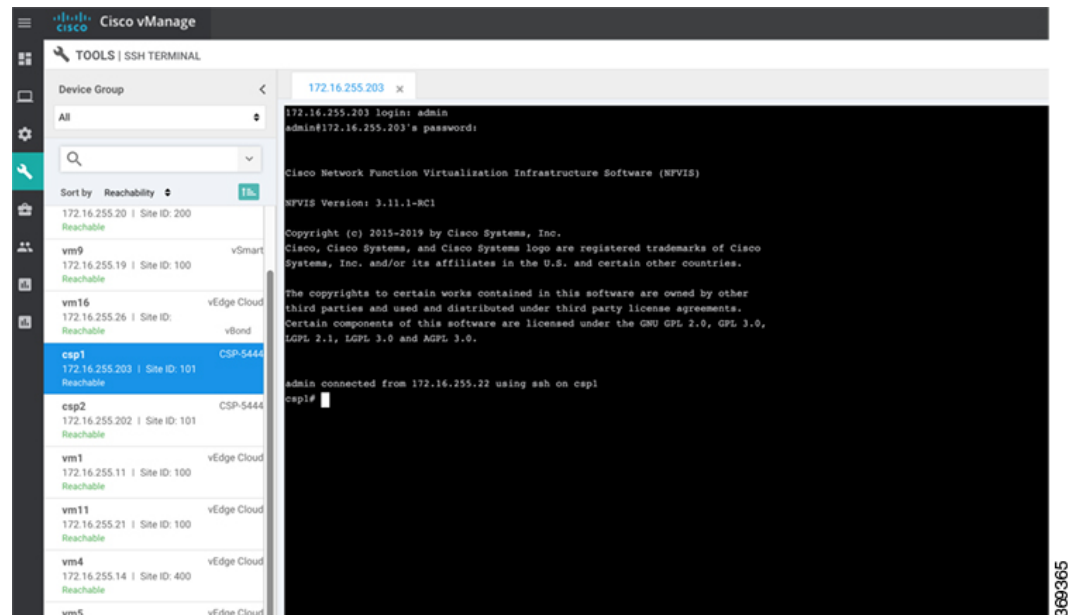
(注) サービスチェーンの追加または削除によって Cisco Colo Manager で障害が発生した場合は、同期するオプションがあります。

サービスチェーンの追加中に、VNF がエラー状態になる

VNF が Cisco vManage でダウンとして表示されます。

Action:

1. VNF の Day-0 構成を確認します。
2. Cisco vManage から SSH を使用して、VNF をホストしている CSP に移動します。



3. 次のコマンドを実行します。

```
nfvis# show system:system deployments
```

```
nfvis# get the VNF ID
```

次に例を示します。

```
NAME ID STATE
```

```
-----
```

```
Firewall2_SG-3 40 running
```

```
nfvis# support show config-drive content 40
```

すべての変数がキーと値のペアで適切に置き換えられていることを確認してください。

物理ネットワーク機能管理の問題のトラブルシューティング

PNF デバイスの共有の問題を解決するには、次の点を考慮してください。

1. Catalyst 9500 への PNF デバイスのケーブル接続が正しく、VLAN 構成は Catalyst 9500 の正しいポートにあること。
2. LLDP の有効化を確認すること。デフォルトでは、LLDP は Catalyst 9500 で有効になっています。PNF で LLDP が有効になっていることを確認し、LLDP ネイバーとネイバーインターフェイスをチェックして接続を確認します。
3. PNF で欠落している構成を確認すること。

CSP からのログ収集

Cisco vManage から CSP に到達できず、デバッグのためにログを収集する必要がある場合は、CSP から **tech-support** コマンドを使用します。

次に、tech-support コマンドの使用例を示します。

```
nfvis# tech-support
nfvis# show system:system file-list
system:system file-list disk local 1
  name          nfvis_scp.log
  path          /data/intdatastore/logs
  size          2.1K
  typ
```

Cisco NFVIS から外部システムへ、または外部システムから Cisco NFVIS へのログファイルのコピーを保護するには、管理ユーザーは特権 EXEC モードで **scp** コマンドを使用できます。次の例は、**scp techsupport** コマンドを示しています。

```
nfvis# scp techsupport:NFVIS_nfvis_2019-04-11T15-33-09.tar.gz
cisco@172.31.232.182:/home/cisco/.
```

Cisco vManage の問題のトラブルシューティング

次の場所を使用して、Cisco vManage の問題をトラブルシューティングします。

[SD-WAN Techzone ナレッジベース](#)



第 11 章

共有 VNF のカスタムパッケージの詳細

- [Cisco vEdge ルータ変数リスト \(189 ページ\)](#)
- [Cisco CSR1000V 変数リスト \(193 ページ\)](#)
- [ASAv 変数リスト \(197 ページ\)](#)

Cisco vEdge ルータ変数リスト

次の Cisco vEdge ルータ変数リストでは、同じ変数名をサービスチェーン 5 と 6 にそれぞれ使用でき、サービスチェーンについて説明したように適切な番号を付け直すことができます。

Cisco vEdge ルータ変数リスト

Cisco vEdge ルータがスタンドアロンモードで、ネイバーが **HA** モード

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。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数。
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_PRIM	ORG_NAME	
INSIDE_DATA_MASK_LEN	BGP_NO	
INSIDE_PEER_DATA_IP_PRIM	SYSTEM_IP	
INSIDE_AS	MGMT_PRIM	
LOCAL_INSIDE_AS	MGMT_MASK_LEN	
INSIDE_GW	MGMT_GW	

ユーザ変数	システム変数	
SERVICE_VPN	RCC	
SERVICE_VPN_2	VM_INSTANCE_NAME	
SERVICE_VPN_3	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_4	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MASK_LEN_3
	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_IP_SEC_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MASK_LEN_4
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_IP_SEC_4

Cisco vEdge ルータ変数リスト

Cisco vEdge ルータがスタンドアロンモードで、ネイバーがスタンドアロンモード

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。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数。
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_PRIM	ORG_NAME	
INSIDE_DATA_MASK_LEN	BGP_NO	
INSIDE_PEER_DATA_IP_PRIM	SYSTEM_IP	
INSIDE_AS	MGMT_PRIM	
LOCAL_INSIDE_AS	MGMT_MASK_LEN	

ユーザ変数	システム変数	
INSIDE_GW	MGMT_GW	
SERVICE_VPN	RCC	
SERVICE_VPN_2	VM_INSTANCE_NAME	
SERVICE_VPN_3	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_4	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MASK_LEN_3
	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MASK_LEN_4
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4

Cisco vEdge ルータ変数リスト

Cisco vEdge ルータがスタンドアロンモードで、ネイバーがスタンドアロンモード
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。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_VLAN1	ORG_NAME	
INSIDE_PRIM_SUBNET1_IP	BGP_NO	
INSIDE_DATA_MASK_LEN1	SYSTEM_IP	
INSIDE_VLAN2	MGMT_PRIM	
INSIDE_PRIM_SUBNET2_IP	MGMT_MASK_LEN	
INSIDE_DATA_MASK_LEN2	MGMT_GW	

ユーザ変数	システム変数	
INSIDE_GW1	RCC	
INSIDE_GW2	VM_INSTANCE_NAME	
SERVICE_VPN	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_2	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MASK_LEN_3
SERVICE_VPN_3	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
SERVICE_VPN_4	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MASK_LEN_4
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4

Cisco vEdge ルータ変数リスト

Cisco vEdge ルータがスタンドアロンモードで、ネイバーが HA モード

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。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数。
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_VLAN1	ORG_NAME	
INSIDE_PRIM_SUBNET1_IP	BGP_NO	
INSIDE_DATA_MASK_LEN1	SYSTEM_IP	
INSIDE_VLAN2	MGMT_PRIM	
INSIDE_PRIM_SUBNET2_IP	MGMT_MASK_LEN	
INSIDE_DATA_MASK_LEN2	MGMT_GW	
INSIDE_GW1	RCC	

ユーザ変数	システム変数	
INSIDE_GW2	VM_INSTANCE_NAME	
SERVICE_VPN	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_2	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MASK_LEN_3
SERVICE_VPN_3	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
SERVICE_VPN_4	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_IP_SEC_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MASK_LEN_4
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_IP_SEC_4

Cisco CSR1000V 変数リスト

Cisco CSR1000V 変数リスト

最後の Cisco CSR1000V VNF が HA モードで、ネイバーがスタンドアロンモード
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（ASA
ファイアウォール）はスタンドアロンモードです。

ユーザ変数	システム変数	
	必須変数	オプションの変数
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	

ユーザ変数	システム変数	
THROUGHPUT_IN_MB	MGMT_GW	
TOKEN_VALUE	MGMT_SEC	
PASS	INSIDE_VLAN_1	INSIDE_VLAN_3
OUTSIDE_PRIM	INSIDE_PRIM	INSIDE_PRIM_3
OUTSIDE_DATA_MASK	INSIDE_DATA_MASK	INSIDE_DATA_MASK_3
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM_3
OUTSIDE_AS	INSIDE_AS	INSIDE_AS_3
LOCAL_OUTSIDE_AS	INSIDE_VLAN_2	INSIDE_VLAN_4
OUTSIDE_PEER_DATA_IP_SEC	INSIDE_PRIM_2	INSIDE_PRIM_4
OUTSIDE_SEC	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK_4
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA_IP_PRIM_4
	INSIDE_AS_2	INSIDE_AS_4

Cisco CSR1000V 変数リスト

最後の Cisco CSR1000V VNF がスタンドアロンモードで、ネイバーがスタンドアロンモード最後の 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。

ユーザ変数	システム変数	
	必須変数	オプションの変数
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	
THROUGHPUT_IN_MB	MGMT_GW	
TOKEN_VALUE	INSIDE_VLAN_1	INSIDE_VLAN_3
PASS	INSIDE_PRIM	INSIDE_PRIM_3

ユーザ変数	システム変数	
OUTSIDE_PRIM	INSIDE_DATA_MASK	INSIDE_DATA_MASK_3
OUTSIDE_DATA_MASK	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM_3
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_AS	INSIDE_AS_3
OUTSIDE_AS	INSIDE_PEER_DATA_IP_SEC	INSIDE_PEER_DATA_IP_SEC_3
LOCAL_OUTSIDE_AS	VIP_IP_ADDRESS	VIP_IP_ADDRESS_3
	INSIDE_SEC	INSIDE_SEC_3
	INSIDE_VLAN_2	INSIDE_VLAN_4
	INSIDE_PRIM_2	INSIDE_PRIM_4
	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK_4
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA_IP_PRIM_4
	INSIDE_AS_2	INSIDE_AS_4
	INSIDE_PEER_DATA_IP_SEC_2	INSIDE_PEER_DATA_IP_SEC_4
	VIP_IP_ADDRESS_2	VIP_IP_ADDRESS_4
	INSIDE_SEC_2	INSIDE_SEC_4

Cisco CSR1000V 変数リスト

最後の Cisco CSR1000V VNF がスタンドアロンモードで、ネイバーが HA モード

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 HA モードです。

ユーザ変数	システム変数	
	必須変数	オプションの変数
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	
THROUGHPUT_IN_MB	MGMT_GW	

ユーザ変数	システム変数	
TOKEN_VALUE	INSIDE_VLAN_1	INSIDE_VLAN_3
PASS	INSIDE_PRIM	INSIDE_PRIM_3
OUTSIDE_PRIM	INSIDE_DATA_MASK	INSIDE_DATA_MASK_3
OUTSIDE_DATA_MASK	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM_3
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_AS	INSIDE_AS_3
OUTSIDE_AS	INSIDE_VLAN_2	INSIDE_VLAN_4
LOCAL_OUTSIDE_AS	INSIDE_PRIM_2	INSIDE_PRIM_4
	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK_4
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA_IP_PRIM_4
	INSIDE_AS_2	INSIDE_AS_4

Cisco CSR1000V 変数リスト

最後の Cisco CSR1000V VNF が HA モードで、ネイバーが HA モード

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 HA モードです。

ユーザ変数	システム変数	
	必須変数	オプションの変数
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	
THROUGHPUT_IN_MB	MGMT_GW	
TOKEN_VALUE	MGMT_SEC	
PASS	INSIDE_VLAN_1	INSIDE_VLAN_3
OUTSIDE_PRIM	INSIDE_PRIM	INSIDE_PRIM_3
OUTSIDE_DATA_MASK	INSIDE_DATA_MASK	INSIDE_DATA_MASK_3

ユーザ変数	システム変数	
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM_3
OUTSIDE_AS	INSIDE_AS	INSIDE_AS_3
LOCAL_OUTSIDE_AS	INSIDE_PEER_DATA_IP_SEC	INSIDE_PEER_DATA_IP_SEC_3
OUTSIDE_PEER_DATA_IP_SEC	VIP_IP_ADDRESS	VIP_IP_ADDRESS_3
OUTSIDE_SEC	INSIDE_SEC	INSIDE_SEC_3
	INSIDE_VLAN_2	INSIDE_VLAN_4
	INSIDE_PRIM_2	INSIDE_PRIM_4
	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK_4
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA_IP_PRIM_4
	INSIDE_AS_2	INSIDE_AS_4
	INSIDE_PEER_DATA_IP_SEC_2	INSIDE_PEER_DATA_IP_SEC_4
	VIP_IP_ADDRESS_2	VIP_IP_ADDRESS_4

ASAv 変数リスト



- (注) 次の ASAv 変数リストでは、同じ変数名をサービスチェーン 5 と 6 にそれぞれ使用でき、サービスチェーンについて説明したように適切な番号を付け直すことができます。

ASAv 変数リスト

最初の ASAv VNF が HA モードで、ネイバーが HA モード

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 HA モードです。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数。
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	

ユーザ変数	システム変数	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	
ID_TOKEN	VM_INSTANCE_NAME	
PASS	TNAME	
TIMEZONE	HA_PRIM_IP	
INSIDE_PRIM	HA_SEC_IP	
INSIDE_SEC	HA_MASK	
INSIDE_DATA_MASK	MGMT_PRIM	
INSIDE_PEER_DATA_IP_PRIM	MGMT_MASK	
INSIDE_PEER_DATA_IP_SEC	MGMT_GW	
INSIDE_AS	MGMT_SEC	
LOCAL_INSIDE_AS	OUTSIDE_PRIM	OUTSIDE_PRIM_3
	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MASK_3
	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_IP_SEC_3
	OUTSIDE_SEC	OUTSIDE_SEC_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MASK_4
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_IP_SEC_4
	OUTSIDE_SEC_2	OUTSIDE_SEC_4

ASAv 変数リスト

最初の ASAv VNF がスタンドアロンモードで、ネイバーがスタンドアロンモード
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。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数。
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	
ID_TOKEN	VM_INSTANCE_NAME	
PASS	TNAME	
TIMEZONE	MGMT_PRIM	
INSIDE_PRIM	MGMT_MASK	
INSIDE_DATA_MASK	MGMT_GW	
INSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PRIM	OUTSIDE_PRIM_3
INSIDE_AS	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MASK_3
LOCAL_INSIDE_AS	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MASK_4
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4

ASAv 変数リスト

最初の ASAv VNF がスタンドアロンモードで、ネイバーが HA モード

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 HA モードです。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数。
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	
ID_TOKEN	VM_INSTANCE_NAME	
PASS	TNAME	
TIMEZONE	MGMT_PRIM	
INSIDE_PRIM	MGMT_MASK	
INSIDE_DATA_MASK	MGMT_GW	
INSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PRIM	OUTSIDE_PRIM_3
INSIDE_AS	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MASK_3
LOCAL_INSIDE_AS	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_IP_SEC_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MASK_4
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_IP_SEC_4

ASAv 変数リスト

最初の ASAv VNF が HA モードで、ネイバーが HA モード

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。

ユーザ変数	システム変数	
	サービスチェーン 1 と 2 が共有されている場合の必須変数。	サービスチェーン 3 および 4 が共有されている場合のオプション変数。
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	
ID_TOKEN	VM_INSTANCE_NAME	
PASS	TNAME	
TIMEZONE	HA_PRIM_IP	
INSIDE_PRIM_SUBNET1_IP	HA_SEC_IP	
INSIDE_PEER_DATA_IP_PRIM1	HA_MASK	
INSIDE_AS1	MGMT_PRIM	
LOCAL_INSIDE_AS1	MGMT_MASK	
INSIDE_VLAN1	MGMT_GW	
INSIDE_DATA_MASK_SUBNET1	MGMT_GW	
INSIDE_PRIM_SUBNET2_IP	OUTSIDE_PRIM	OUTSIDE_PRIM_3
INSIDE_PEER_DATA_IP_PRIM2	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MASK_3
INSIDE_AS2	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_IP_PRIM_3
LOCAL_INSIDE_AS2	OUTSIDE_AS	OUTSIDE_AS_3
INSIDE_VLAN2	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
INSIDE_DATA_MASK_SUBNET2	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_IP_SEC_3
INSIDE_PRIM_SUBNET3_IP	OUTSIDE_SEC	OUTSIDE_SEC_3
INSIDE_PEER_DATA_IP_PRIM3	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4

ユーザ変数	システム変数	
INSIDE_AS3	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MASK_4
LOCAL_INSIDE_AS3	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_IP_PRIM_4
INSIDE_VLAN3	OUTSIDE_AS_2	OUTSIDE_AS_4
INSIDE_DATA_MASK_SUBNET3	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
INSIDE_PRIM_SUBNET4_IP	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_IP_SEC_4
INSIDE_PEER_DATA_IP_PRIM4	OUTSIDE_SEC_2	OUTSIDE_SEC_4
INSIDE_AS4		
LOCAL_INSIDE_AS4		
INSIDE_VLAN4		
INSIDE_DATA_MASK_SUBNET4		

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。