



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

表 1: 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 \(1 ページ\)](#)
- [マルチテナント環境での役割と機能 \(3 ページ\)](#)
- [マルチテナント環境での推奨仕様 \(4 ページ\)](#)
- [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 \(5 ページ\)](#)
- [サービスプロバイダー機能 \(6 ページ\)](#)
- [テナント コロケーション クラスタの管理 \(9 ページ\)](#)
- [c-tenant-functionalities \(10 ページ\)](#)
- [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 \(11 ページ\)](#)

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 \(11 ページ\)](#)』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 \(11 ページ\)](#)』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 2: 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](#)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](#)』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](#)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。

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。