



Cisco SD-WAN マルチテナント機能 (Cisco IOS XE リリース 17.4.x および 17.5.x)

表 1: 機能の履歴

機能名	リリース情報	機能説明
Cisco SD-WAN マルチテナント機能	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	Cisco SD-WAN マルチテナント機能を使用すると、サービスプロバイダーは、Cisco vManage からテナントと呼ばれる複数の顧客を管理できます。マルチテナント Cisco SD-WAN 展開では、テナントは Cisco vManage インスタンス、Cisco vBond オーケストレーション、および Cisco vSmart コントローラを共有します。テナントデータは、これらの共有リソース上で論理的に分離されます。

- [Cisco SD-WAN マルチテナント機能の概要 \(2 ページ\)](#)
- [マルチテナント環境でのユーザーロール \(5 ページ\)](#)
- [ハードウェアのサポートと仕様 \(7 ページ\)](#)
- [マルチテナント機能の初期設定 \(8 ページ\)](#)
- [テナントの管理 \(12 ページ\)](#)
- [マルチテナント機能の Cisco vManage ダッシュボード \(16 ページ\)](#)
- [テナント WAN エッジデバイスの管理 \(21 ページ\)](#)
- [Cisco vSmart コントローラでのテナント固有のポリシー \(22 ページ\)](#)
- [テナントデータの管理 \(23 ページ\)](#)
- [Cisco vSmart コントローラでのテナントごとの OMP 統計表示 \(27 ページ\)](#)
- [Cisco vSmart コントローラに関連付けられたテナントの表示 \(28 ページ\)](#)
- [シングルテナント Cisco SD-WAN オーバーレイからマルチテナント Cisco SD-WAN 展開への移行 \(28 ページ\)](#)

Cisco SD-WAN マルチテナント機能の概要

Cisco SD-WAN マルチテナント機能を使用すると、サービスプロバイダーは、Cisco vManage からテナントと呼ばれる複数の顧客を管理できます。テナントは、Cisco vManage インスタンス、Cisco vBond オーケストレーション、およびCisco vSmart コントローラを共有します。サービスプロバイダーのドメイン名には、テナントごとにサブドメインがあります。たとえば、multitenancy.com サービスプロバイダーは、テナント Customer1 (Customer1.multitenancy.com) と Customer2 (Customer2.multitenancy.com) を管理できます。

Cisco SD-WAN マルチテナント機能の主な機能は次のとおりです。

- 完全なエンタープライズ マルチテナント機能：Cisco SD-WAN はマルチテナント機能をサポートし、企業はサービスプロバイダーやテナントなどの役割を柔軟に分離することができます。サービスプロバイダーは、マルチテナント機能を使用して顧客に Cisco SD-WAN サービスを提供できます。
- マルチテナント Cisco vManage：
 - Cisco vManage はサービスプロバイダーによって展開および設定されます。プロバイダーは、マルチテナント機能を有効にし、テナントにサービスを提供する Cisco vManage クラスタを作成します。SSH 端末を介して Cisco vManage インスタンスにアクセスできるのはプロバイダーのみです。



(注) SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力から見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から `vmanage_system` の IP アドレスを見つけることもできます。

- Cisco vManage は、サービスプロバイダーに SD-WAN マルチテナント展開の全体像を提供し、プロバイダーが共有 Cisco vBond オーケストレーションデバイスと Cisco vSmart コントローラデバイスを管理できるようにします。また、Cisco vManage により、サービスプロバイダーは各テナントの展開を監視および管理できます。
- Cisco vManage により、テナントは展開を監視および管理できます。Cisco vManage により、テナントは WAN エッジデバイスを展開および設定できます。テナントは、割り当てられた Cisco vSmart コントローラでカスタムポリシーを設定することもできます。

- マルチテナント Cisco vBond オーケストレーション :

- Cisco vBond オーケストレーション は、サービスプロバイダーによって展開および設定されます。SSH 端末を介して Cisco vBond オーケストレーション にアクセスできるのはプロバイダーのみです。



(注) SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力からを見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から `vmanage_system` の IP アドレスを見つけることもできます。

- Cisco vBond オーケストレーション は、デバイスがオーバーレイネットワークに追加されると、複数のテナントの WAN エッジデバイスにサービスを提供します。

- マルチテナント Cisco vSmart コントローラ :

- Cisco vSmart コントローラは、サービスプロバイダーによって展開されます。デバイスおよび機能テンプレートを作成して Cisco vSmart コントローラに接続できるのはプロバイダーのみで、SSH 端末を介して Cisco vSmart コントローラにアクセスできます。



(注) SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力からを見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から `vmanage_system` の IP アドレスを見つけることもできます。

- テナントが作成されると、Cisco vManage はテナントに 2 つの Cisco vSmart コントローラを割り当てます。Cisco vSmart コントローラは、アクティブ/アクティブクラスタを形成します。

各テナントには2つの Cisco vSmart コントローラのみが割り当てられます。テナントを作成する前に、テナントにサービスを提供するために2つの Cisco vSmart コントローラを使用できる必要があります。

- Cisco vSmart コントローラの各ペアは、最大 24 のテナントに対応できます。
- テナントは、割り当てられた Cisco vSmart コントローラでカスタムポリシーを設定できます。Cisco vManage はポリシーテンプレートをプルするように Cisco vSmart コントローラに通知します。Cisco vSmart コントローラはテンプレートをプルし、特定のテナントのポリシー設定を展開します。
- Cisco vManage で Cisco vSmart コントローラのイベント、監査ログ、および OMP アラームを表示できるのは、プロバイダーのみです。
- WAN エッジデバイス：
 - テナントまたはテナントに代わって機能するプロバイダーは、WAN エッジデバイスをテナントネットワークに追加したり、デバイスを設定したり、テナントネットワークからデバイスを削除したり、SSH 端末を介してデバイスにアクセスしたりできます。



- (注) SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力から見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から `vmanage_system` の IP アドレスを見つけることもできます。

- プロバイダーは、**テナントとしてのプロバイダー**ビューからのみ WAN エッジデバイスを管理できます。**プロバイダー**ビューでは、Cisco vManage は WAN エッジデバイスの情報を表示しません。
- Cisco vManage は、WAN エッジデバイスのイベント、ログ、およびアラームを、**テナントロール**ビューおよびテナントとしてのプロバイダービューでのみレポートします。
- VPN 番号の重複：特定の VPN または共通の VPN のセットは、独自の設定および監視ダッシュボード環境を使用して、特定のテナントに割り当てられます。これらの VPN 番号は、他のテナントが使用する場所で重複する可能性があります。
- オンプレミスおよびクラウド展開モデル：Cisco SD-WAN コントローラは、VMware vSphere ESXi またはカーネルベースの仮想マシン (KVM) ハイパーバイザを実行しているサーバー

上の組織のデータセンターに展開できます。Cisco SD-WAN コントローラは、Amazon Web Services (AWS) サーバー上のクラウドに展開することもできます。

マルチテナント環境でのユーザーロール

マルチテナント環境には、サービスプロバイダーとテナントのロールが含まれます。各ロールには、個別の権限、ビュー、および機能があります。

プロバイダーロール

プロバイダーロールは、システム全体の管理者権限を付与します。プロバイダーロールを持つユーザーは、デフォルトのユーザー名 **admin** を持っています。プロバイダーユーザーは、サービスプロバイダーのドメイン名または Cisco vManage IP アドレスを使用して Cisco vManage にアクセスできます。ドメイン名を使用する場合、ドメイン名の形式は `https://multitenancy.com` です。

admin ユーザーは、ユーザーグループ **netadmin** の一部です。このグループのユーザーは、テナントのコントローラと Cisco SD-WAN デバイスに対するすべての操作を実行することが許可されます。**netadmin** グループにユーザーを追加できます。

netadmin グループの権限は変更できません。Cisco vManage では、**[Administration] > [Manage Users] > [User Groups]** ページからユーザーグループの権限を表示できます。



- (注) **netadmin** ユーザーを含む新しいプロバイダーユーザーを Cisco vManage で作成すると、デフォルトでは、ユーザーは Cisco vManage VM への SSH アクセスを許可されません。SSH アクセスを有効にするには、AAA テンプレートを使用して SSH 認証を設定し、Cisco vManage へテンプレートをプッシュします。SSH 認証の有効化の詳細については、「[SSH Authentication using vManage on Cisco IOS XE SD-WAN Devices](#)」を参照してください。

ユーザーとユーザーグループの構成の詳細については、「[Configure User Access and Authentication](#)」を参照してください。

Cisco vManage は、プロバイダーに 2 つのビューを提供します。

• プロバイダービュー

プロバイダーユーザーが **admin** または別の **netadmin** ユーザーとしてマルチテナント Cisco vManage にログインすると、Cisco vManage にプロバイダービューが表示され、プロバイダーダッシュボードが表示されます。

プロバイダービューから次の機能を実行できます。

- Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラのプロビジョニングと管理。
- テナントの追加、変更、または削除。

- オーバーレイネットワークのモニタリング。
- テナントとしてのプロバイダービュー

プロバイダーユーザーがプロバイダーダッシュボードの上部にある [Select Tenant] ドロップダウンリストから特定のテナントを選択すると、Cisco vManage にテナントとしてのプロバイダービューが表示され、選択したテナントのテナントダッシュボードが表示されます。プロバイダーユーザーは、**tenantadmin** としてログインしたときのテナントユーザーと同じ Cisco vManage のビューを持ちます。プロバイダーは、このビューから、テナントに代わってテナントの展開を管理できます。

プロバイダーダッシュボードでは、テナントのテーブルに各テナントのステータスの概要が表示されます。プロバイダーユーザーは、このテーブルのテナント名をクリックして、テナントとしてのプロバイダービューを起動することもできます。

テナントロール

テナントロールは、テナント管理権限を付与します。テナントロールを持つユーザーは、デフォルトのユーザー名 **tenantadmin** を持っています。デフォルトのパスワードは **Cisco#123@Viptela** です。最初のログイン時にデフォルトのパスワードを変更することをお勧めします。デフォルトのパスワードの変更については、「[Hardware and Software Installation](#)」を参照してください。

tenantadmin ユーザーは、ユーザーグループ **tenantadmin** の一部です。このグループのユーザーは、テナントの WAN エッジデバイスですべての操作を実行できます。**tenantadmin** グループにユーザーを追加できます。

tenantadmin グループの権限は変更できません。Cisco vManage では、**[Administration]>[Manage Users]>[User Groups]** ページからユーザーグループの権限を表示できます。

ユーザーとユーザーグループの構成の詳細については、「[Configure User Access and Authentication](#)」を参照してください。

テナントユーザーは、専用の URL とデフォルトのユーザー名 **tenantadmin** を使用して Cisco vManage にログインできます。たとえば、ドメイン名 <https://multitenancy.com> を使用するプロバイダーの場合、テナントの専用 URL は <https://Customer1.multitenancy.com> になる可能性があります。ユーザーがログインすると、Cisco vManage にテナントビューが表示され、テナントダッシュボードが表示されます。

管理者権限を持つテナントユーザーは、次の機能を実行できます。

- テナントルータのプロビジョニングと管理
- テナントのオーバーレイネットワークのモニタリング
- 割り当てられた Cisco vSmart コントローラにカスタムポリシーを作成
- テナントルータのソフトウェアをアップグレード。

ハードウェアのサポートと仕様

次のプラットフォームはマルチテナント機能をサポートしています。

表 2: ルータモデル

Platform	ルータモデル
Cisco IOS XE SD-WAN デバイス	<ul style="list-style-type: none"> • Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco ISR 1000 シリーズ サービス統合型 ルータ • Cisco ISR 4000 シリーズ サービス統合型 ルータ • Cisco Catalyst 8300 シリーズ エッジプラットフォーム • Cisco Catalyst 8500 シリーズ エッジプラットフォーム • Cisco Catalyst 8000V Edge ソフトウェア

マルチテナント機能では、次のハイパーバイザと展開モデルがサポートされています。

表 3: 展開モデル

仕様	Description
サポートされるハイパーバイザ	VMware、KVM、AWS (シスコがクラウドホスト)
Cisco vManage 展開モデル	クラスタ、各インスタンスがすべての NMS サービスを実行する 3 つの vManage インスタンス。

Cisco vBond オーケストレーション、Cisco vManage および Cisco vSmart コントローラ でサポートされるハードウェア仕様は次のとおりです。

表 4: オンプレミス展開

サーバー	Cisco vManage	Cisco vBond オーケストレーション	Cisco vSmart コントローラ
デプロイメントモデル	クラスタ	該当なし	非コンテナ化
インスタンス数	3	2	24 テナントあたり 2

CPU	32 vCPU	4 vCPU	8 vCPU
DRAM	72 GB	4 GB	16 GB
ハード ディスク	1 TB	10 GB	16 GB
NMS サービスの分散	一部のサービスは、クラスタ内の3つのCisco vManage インスタンスすべてで実行されますが、一部のサービスは、クラスタ内の3つのインスタンスのうち1つでのみ実行されます。したがって、CPU 負荷はインスタンス間で異なる場合があります。	該当なし	該当なし



(注) DPI が有効になっている場合、すべての Cisco vManage インスタンス全体で集約された DPI データが 1 日あたり 350 GB を超えないようにすることをお勧めします。

マルチテナント機能の初期設定

前提条件

- 次の表で推奨されているソフトウェアバージョンをダウンロードしてインストールします。

表 5: Cisco SD-WAN マルチテナント機能のソフトウェア前提条件

デバイス	ソフトウェアバージョン
Cisco vManage	Cisco vManage リリース 20.4.1
Cisco vBond オーケストレーション	Cisco SD-WAN リリース 20.4.1
Cisco vSmart コントローラ	Cisco SD-WAN リリース 20.4.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.4.1a

1 つまたは複数のコントローラまたは WAN エッジデバイスが、上記の表に示すものより前のソフトウェアバージョンを実行している構成はサポートされていません。

- 既存の Cisco vManage インスタンスにおいてデバイスをすべて無効化または削除した場合でも、既存のシングルテナント Cisco vManage インスタンスをマルチテナントモードに移行しないでください。代わりに、新しい Cisco vManage ソフトウェアイメージをダウンロードしてインストールします。



(注) マルチテナント機能用に Cisco vManage を有効にした後は、シングルテナントモードに戻すことはできません。

- プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。

1. 3つの Cisco vManage インスタンスと関連する設定テンプレートを作成します。「[Deploy Cisco vManage](#)」を参照してください。

1. Cisco vManage インスタンスを設定するときに、サービスプロバイダーの組織名 (sp-organization-name) と組織名 (organization-name) を設定します。

例 :

```
sp-organization-name multitenancy
organization-name multitenancy
```

2. マルチテナント機能をサポートするように Cisco vManage インスタンスの1つを設定します。[Cisco vManage でのマルチテナント機能の有効化 \(10 ページ\)](#) を参照してください。
3. 3つの Cisco vManage インスタンスで構成される Cisco vManage クラスタを作成します。「[Cluster Management](#)」を参照してください。

- Cisco vManage クラスタには3つの Cisco vManage インスタンスが必要です。インスタンスが4つ以上または3つ未満のクラスタは、Cisco SD-WAN マルチテナント機能でサポートされる構成ではありません。
- Cisco vManage クラスタの作成時は、マルチテナント機能をサポートするように設定した Cisco vManage インスタンスを追加してから、他の2つの Cisco vManage インスタンスを追加します。

4. Cisco vManage のすべてのインスタンスを認可します。「[Generate vManage NMS Certificate](#)」を参照してください。

5. Cisco vBond Orchestrator インスタンスを作成して設定します。「[Deploy Cisco vBond Orchestrator](#)」を参照してください。

Cisco vBond Orchestrator インスタンスを設定するときに、サービスプロバイダーの組織名 (sp-organization-name) と組織名 (organization-name) を設定します。「[Configure Organization Name in Cisco vBond Orchestrator](#)」を参照してください。

```
sp-organization-name multitenancy
organization-name multitenancy
```

6. Cisco vSmart コントローラインスタンスを作成します。「[Deploy the Cisco vSmart Controller](#)」を参照してください。

すべてのテナントで 50 のテナントと 1000 のデバイスをサポートするには、6 つの Cisco vSmart Controller インスタンスを展開します。すべてのテナントで 100 のテナントと 5000 のデバイスをサポートするには、12 の Cisco vSmart コントローラを展開します。

1. オーバーレイネットワークに [Cisco vSmart コントローラの追加](#) します。
7. 新しいテナントを導入準備します。「[新規テナントの追加](#)」を参照してください。

Cisco vManage でのマルチテナント機能の有効化

1. URL `https://vmanage-ip-address:port` を使用して Cisco vManage を起動します。プロバイダーの **admin** ユーザーとしてログインします。
2. Cisco vManage のメニューから **[Administration]** > **[Settings]** の順に選択します。
3. テナンシーモードバーで、**[Edit]** をクリックします。
4. **[Tenancy]** フィールドで、**[Multitenant]** をクリックします。
5. **[Domain]** フィールドに、サービスプロバイダーのドメイン名 (たとえば、`multitenancy.com`) を入力します。
6. クラスタ ID (たとえば、`cluster-1` または `123456`) を入力します。
7. **[Save]** をクリックします。
8. **[Proceed]** をクリックして、テナンシーモードを変更することを確認します。

Cisco vManage はマルチテナントモードで再起動し、プロバイダーユーザーが Cisco vManage にログインすると、プロバイダーダッシュボードが表示されます。

Cisco vSmart コントローラの追加

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
3. **[Controllers]** をクリックします。
4. **[Add Controller]** をクリックし、**[vSmart]** をクリックします。
5. **[Add vSmart]** ダイアログボックスで、次を実行します。
 1. **[vSmart Management IP Address]** フィールドに、Cisco vSmart コントローラのシステム IP アドレスを入力します。
 2. Cisco vSmart コントローラへのアクセスに必要な **[Username]** と **[Password]** を入力します。
 3. コントロールプレーン接続に使用するプロトコルを選択します。デフォルトは **[DTLS]** です。

[TLS] を選択した場合は、TLS 接続に使用するポート番号を入力します。デフォルトは 23456 です。

4. 証明書署名要求を作成するには、Cisco vManage の [Generate CSR] チェックボックスをオンにします。
5. [Add] をクリックします。
6. [Cisco vManage] メニューから、[Configuration] > [Certificates] を選択します。
Cisco vSmart コントローラを新規に追加した場合、[Operation Status] には「CSR Generated」と表示されます。
 1. Cisco vSmart コントローラを新規に追加した場合、[More Options] アイコンをクリックし、[View CSR] をクリックします。
 2. CSR を認証局 (CA) に提出して、署名付き証明書を取得します。
7. [Cisco vManage] メニューから、[Configuration] > [Certificates] を選択します。
8. [Install Certificate] をクリックします。
9. [Install Certificate] ダイアログボックスで証明書を [Certificate Text] に貼り付けるか、[Select a File] をクリックして証明書ファイルをアップロードします。[Install] をクリックします。

Cisco vManage により、証明書が Cisco vSmart コントローラにインストールされます。Cisco vManage により、証明書のシリアル番号が他のコントローラにも送信されます。

[Configuration] > [Certificates] ページで、新しく追加された Cisco vSmart コントローラの [Operation Status] には、「vBond Updated」と表示されます。

[Configuration] > [Devices] ページで、新しいコントローラがコントローラテーブルに表示されます。このテーブルにはコントローラタイプ、コントローラのホスト名、IP アドレス、サイト ID、およびその他の詳細も表示されます。[Mode] は [CLI] に設定されています。

10. テンプレートをデバイスにアタッチして、新しく追加された Cisco vSmart コントローラのモードを [vManage] に変更します。
 1. [Cisco vManage] メニューから、[Configuration] > [Templates] を選択します。
 2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. Cisco vSmart コントローラにアタッチするテンプレートを見つけます。
4. [...] をクリックして、[Attach Devices] をクリックします。

5. [Attach Devices] ダイアログボックスで、新しいコントローラを [Selected Device] リストに移動し、[Attach] をクリックします。
6. [Config Preview] を確認し、[Configure Devices] をクリックします。

Cisco vManage は、テンプレートの設定を新しいコントローラにプッシュします。

[Configuration] > [Devices] ページでは、Cisco vSmart コントローラの [Mode] に [vManage] と表示されます。新しい Cisco vSmart コントローラをマルチテナント展開で使用する準備ができました。

テナントの管理

新規テナントの追加

前提条件

- 新しいテナントを追加する前に、少なくとも 2 つの Cisco vSmart コントローラが動作し、vManage モードになっている必要があります。
テンプレートを Cisco vManage からコントローラにプッシュすると、Cisco vSmart コントローラは vManage モードに入ります。CLI モードの Cisco vSmart コントローラは、複数のテナントに対応できません。
- Cisco vSmart コントローラの各ペアは、最大 24 のテナントに対応できます。新しいテナントに対応できる Cisco vSmart コントローラが少なくとも 2 つあることを確認します。展開内の Cisco vSmart コントローラのペアが新しいテナントに対応できない場合は、2 つの Cisco vSmart コントローラを追加して、それらのモードを vManage に変更します。
- テナントを追加した直後に 2 番目のテナントを追加すると、Cisco vManage はそれらを並行してではなく順番に追加します。
- 各テナントには、Cisco Software Central のプラグアンドプレイコネクトに一意のバーチャルアカウント (VA) が必要です。テナント VA は、プロバイダー VA と同じスマートアカウント (SA) に属している必要があります。
- オンプレミス展開の場合、プラグアンドプレイコネクトでテナント用の Cisco vBond Orchestrator コントローラプロファイルを作成します。次の表のフィールドは必須です。

表 6: コントローラ プロファイル フィールド

フィールド	説明/値
プロファイル名	コントローラプロファイル名を入力します
マルチテナント機能	ドロップダウンリストから、[Yes] を選択します。

フィールド	説明/値
SP Organization Name	プロバイダー組織名を入力します。
組織名	テナント組織名を <SP Org Name>-<Tenant Org Name> の形式で入力します。 (注) 組織名には最大 64 文字を使用できません。
プライマリコントローラ (Primary Controller)	プライマリ Cisco vBond Orchestrator のホストの詳細を入力します。

クラウド展開の場合、テナント作成プロセスの一部として Cisco vBond Orchestrator コントローラプロファイルが自動的に作成されます。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから **[Administration] > [Tenant Management]** の順に選択します。
3. **[Add Tenant]** をクリックします。 **[Add Tenant]** ダイアログボックスで、次の手順を実行します。
 1. テナントの名前を入力します。
クラウド展開の場合、テナント名はプラグアンドプレイコネクットのテナント VA 名と同じである必要があります。
 2. テナントの説明を入力します。
説明の最大長は 256 文字で、英数字のみを使用できます。
 3. 組織の名前を入力します。
組織名では、大文字と小文字が区別されます。各テナントまたは顧客には、一意の組織名が必要です。
組織名を次の形式で入力します。
<SP Org Name>-<Tenant Org Name>
たとえば、プロバイダーの組織名が「multitenancy」でテナントの組織名が「Customer1」の場合、テナントを追加するときに、組織名を **multitenancy-Customer1** として入力します。



(注) 組織名には最大 64 文字を使用できます。

4. **[URL Subdomain Name]** フィールドに、テナントの完全修飾サブドメイン名を入力します。

- サブドメイン名には、サービスプロバイダーのドメイン名が含まれている必要があります。たとえば、multitenancy.com サービスプロバイダーの場合、有効なドメイン名は Customer1.multitenancy.com です。



(注) サービスプロバイダー名はすべてのテナントで共有されます。したがって、URL 命名規則が、Cisco vManage の[**Administration**] > [**Settings**] > [**Tenancy Mode**]の GUI ナビゲーションパスからマルチテナンシーを有効にするときに提供されたものと同じドメイン名規則に従っていることを確認してください。

- オンプレミス展開の場合、テナントの完全修飾サブドメイン名を DNS に追加します。完全修飾サブドメイン名を、Cisco vManage クラスタ内の 3 つの Cisco vManage インスタンスの IP アドレスにマッピングします。

完全修飾ドメイン名 (FQDN) を作成する場合、次の DNS エントリが必要です。

- **プロバイダーレベル** : DNS A レコードを作成し、Cisco vManage クラスタで実行されている Cisco vManage インスタンスの IP アドレスにマップします。A レコードは、「[Enable Multitenancy on Cisco vManage](#)」の手順 5 と 6 で作成されたドメインとクラスタ ID から派生しています。たとえば、ドメインが **sdwan.cisco.com** でクラスタ ID が **vmanage123** の場合、A レコードは **vmanage123.sdwan.cisco.com** として設定する必要があります。



(注) DNS エントリの更新に失敗すると、vManage へのログイン時に認証エラーが発生します。**nslookup vmanage123.sdwan.cisco.com** を実行して、DNS が正しく設定されていることを確認します。

- **テナントレベル** : 作成された各テナントの DNS CNAME レコードを作成し、プロバイダーレベルで作成された FQDN にマップします。たとえば、ドメインが **sdwan.cisco.com** でテナント名が **customer1** の場合、CNAME レコードは **customer1.sdwan.cisco.com** として設定する必要があります。



(注) CNAME レコードにはクラスタ ID は必要ありません。**nslookup customer1.sdwan.cisco.com** を実行して、DNS が正しく設定されていることを確認します。

クラウド展開の場合、テナントの完全修飾サブドメイン名は、テナント作成プロセスの一部として DNS に自動的に追加されます。テナントを追加した後、テナントの完全修飾サブドメイン名が DNS によって解決されるまでに最大 1 時間かかる場合があります。

5. [Save] をクリックします。

[Create Tenant] 画面が表示され、テナント作成の [Status] が [In progress] と表示されます。テナントの作成に関連するステータスメッセージを表示するには、ステータスの左側にある [>] ボタンをクリックします。

Cisco vManage は次のことを行います。

- テナントを作成します
- テナントにサービスを提供する 2 つの Cisco vSmart コントローラを割り当て、CLI テンプレートをこれらのコントローラにプッシュしてテナント情報を設定します
- テナントと Cisco vSmart コントローラの情報を Cisco vBond Orchestrator に送信します。

次に行う作業：

[Status] 列が [Success] に変わったら、[Administration] > [Tenant Management] ページでテナント情報を表示できます。

テナント情報の変更

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから [Administration] > [Tenant Management] の順に選択します。
3. 左ペインで、テナントの名前をクリックします。
右側のペインにテナント情報が表示されます。
4. テナントデータを変更するには、次のようにします。
 1. 右側のペインで、鉛筆アイコンをクリックします。
 2. [Edit Tenant] ダイアログボックスで、テナント名、説明、またはドメイン名を変更します。
 3. [Save (保存)] をクリックします。

テナントの削除

テナントを削除する前に、すべてのテナント WAN エッジデバイスを削除します。[テナントネットワークからの WAN エッジデバイスの削除 \(22 ページ\)](#) を参照してください。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから [Administration] > [Tenant Management] の順に選択します。
3. 左ペインで、テナントの名前をクリックします。

右ペインにテナント情報が表示されます。

4. テナントを削除するには、次のようにします。
 1. 右側のペインで、ごみ箱アイコンをクリックします。
 2. [Delete Tenant] ダイアログボックスで、プロバイダーの [admin] のパスワードを入力し、[Save] をクリックします。

マルチテナント機能の Cisco vManage ダッシュボード

マルチテナント機能について Cisco vManage を有効にした場合、Cisco vManage にログインすると、マルチテナントダッシュボードを表示できます。Cisco vManage マルチテナントダッシュボードは、プロバイダーまたはテナントが基盤となるシステムを表示およびプロビジョニングできるポータルです。

すべての Cisco vManage マルチテナント画面の上部にあるバーには、スムーズなナビゲーションを可能にするアイコンがあります。

テナントアクティビティ、デバイス、およびネットワーク情報の表示

マルチテナント Cisco vManage に管理者としてログインすると、プロバイダーダッシュボードに次のコンポーネントが表示されます。他の Cisco vManage 画面からプロバイダーダッシュボードに戻るには、左側のバーにある [Dashboard] をクリックします。

- デバイスペイン：マルチテナントダッシュボード画面の上部に表示されます。デバイスペインには、アクティブな Cisco vSmart コントローラ、Cisco vBond オーケストレーション、および Cisco vManage インスタンスの数、デバイスの接続ステータス、および期限切れまたは期限切れ間近の証明書に関する情報が表示されます。
- テナントペイン：テナントの総数と、すべてのテナントの制御ステータス、サイトの正常性、ルータの正常性、および Cisco vSmart コントローラステータスの概要が表示されます。
- オーバーレイネットワーク内のテナントのテーブル：各テナントの制御ステータス、サイトの正常性、WAN エッジデバイスの正常性、および Cisco vSmart コントローラステータスに関する個別の情報を含む、個々のテナントのリストです。

テナント固有のステータスの概要情報を表示するには、次の手順を実行します。

1. テナントリストからテナント名をクリックします。
画面の右側にダイアログボックスが開き、テナントのステータスに関する追加情報が提供されます。
2. 選択したテナントのテナントダッシュボードにアクセスするには、[<Tenant name> Dashboard] をクリックします。

Cisco vManage に、テナントとしてのプロバイダービューが表示され、テナントダッシュボードが表示されます。プロバイダービューに戻るには、ページの上にある [Provider] をクリックします。

3. ダイアログボックスを閉じるには、テナントリストからテナント名をクリックします。

テナント設定の詳細情報の表示

Cisco vManage は、次の場合にテナント展開に関する情報を提供するテナントダッシュボードを表示します。

- プロバイダーの **admin** ユーザーがプロバイダーダッシュボードの [Select Tenant] ドロップダウンリストから特定のテナントを選択する。このビューは、テナントとしてのプロバイダービューと呼ばれます。
- **tenantadmin** ユーザーが Cisco vManage にログインする。このビューはテナントビューと呼ばれます。

テナントオーバーレイ ネットワークのすべてのネットワーク接続を表示する

[Device] ペインは、テナントダッシュボードの上部に表示され、テナントのオーバーレイネットワーク内の Cisco vManage から Cisco vSmart コントローラおよびルータへの制御接続の数を表示します。WAN エッジデバイスごとに、[Device] ペインに次の情報が表示されます。

- Cisco vSmart コントローラと WAN エッジデバイス間の制御接続の総数
- Cisco vSmart コントローラと WAN エッジデバイス間の有効な制御接続の数
- Cisco vSmart コントローラと WAN エッジデバイス間の無効な制御接続の数

接続番号をクリックするか、上矢印または下矢印をクリックして、各接続に関する詳細情報を示す表を表示します。各テーブル行の右側にある [More Actions] アイコンをクリックして、[Monitor] > [Devices] 画面から [Device Dashboard] または [Real Time] ビューにアクセスするか、または [Tools] > [SSH Terminal] 画面にアクセスします。



- (注) Cisco vManage リリース 20.6.x 以前のリリースでは、[Real Time] ビューは [Monitor] > [Network] 画面の一部です。

デバイスの再起動に関する情報の表示

[Reboot] ペインには、ネットワーク内のすべてのデバイスについて、過去 24 時間の再起動の合計数が表示されます。これには、ソフト再起動とコールド再起動、およびデバイスの電源再投入の結果として発生した再起動が含まれます。再起動ごとに、次の情報が表示されます。

- 再起動したデバイスのシステム IP およびホスト名。

- デバイスが再起動された時刻。
- デバイスの再起動の理由

同じデバイスが 2 回以上再起動すると、各再起動オプションが個別に報告されます。

[Reboot] ペインをクリックして、[Reboot] ダイアログボックスを開きます。[Reboot] ダイアログボックスで、[Crashes] をクリックします。すべてのデバイスクラッシュについて、次の情報が表示されます。

- クラッシュが発生したデバイスのシステム IP およびホスト名。
- デバイスのクラッシュインデックス
- デバイスがクラッシュしたコアタイム。
- デバイスクラッシュログのファイル名

ネットワーク接続の表示

[Control Status] ペインには、Cisco vSmart コントローラと WAN エッジデバイスが接続されているかどうかが表示されます。各 Cisco vSmart コントローラは、ネットワーク内の他のすべての Cisco vSmart コントローラに接続する必要があります。各 WAN エッジデバイスは、設定された最大数の Cisco vSmart コントローラに接続する必要があります。[Control Status] ペインには、3 つのネットワーク接続数が表示されます。

- [Control Up] : 必要な数の動作可能なコントロールプレーンが Cisco vSmart Controller に接続されているデバイスの総数。
- [Partial] : 動作可能なコントロールプレーンの一部 (すべてではない) が Cisco vSmart コントローラに接続されているデバイスの総数。
- [Control Down] : Cisco vSmart コントローラにコントロールプレーンが接続されていないデバイスの総数

デバイスの詳細を含むテーブルを表示するには、[Control Status] ダイアログボックスの行をクリックします。各テーブル行の右側にある [More Actions] アイコンをクリックして、[Monitor] > [Devices] 画面から [Device Dashboard] または [Real Time] ビューにアクセスします。



(注) Cisco vManage リリース 20.6.x 以前のリリースでは、[Real Time] ビューは [Monitor] > [Network] 画面の一部です。

サイトのデータ接続の状態の表示

[Site Health] ペインには、サイトのデータ接続の状態が表示されます。サイトに複数の WAN エッジデバイスがある場合、このペインには、個々のデバイスではなくサイト全体の状態が表示されます。[Site Health] ペインには、次の 3 つの接続状態が表示されます。

- **[Full WAN Connectivity]** : すべてのルータ上のすべての BFD セッションが稼働状態にあるサイトの総数。
- **[Partial WAN Connectivity]** : トンネルおよびすべてのルータ上のすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトでは、データプレーン接続が制限されています。
- **[No WAN Connectivity]** : すべてのルータ上のすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトにはデータプレーン接続がありません。

各サイト、ノード、またはトンネルに関する詳細情報を含むテーブルを表示するには、**[Site Health]** ダイアログボックスの行をクリックします。テーブルの各行の右側にある **[More Actions]** アイコンをクリックして、**[Monitor]** > **[Devices]** 画面から **[Device Dashboard]** または **[Real Time]** ビューにアクセスするか、または **[Tools]** > **[SSH Terminal]** 画面にアクセスします。



(注) Cisco vManage リリース 20.6.x 以前のリリースでは、**[Real Time]** ビューは **[Monitor]** > **[Network]** 画面の一部です。

WAN エッジインターフェイスのインターフェイス使用状況の表示

[Transport Interface Distribution] ペインには、VPN 0 のすべての WAN エッジインターフェイスにおける過去 24 時間のインターフェイスの使用状況が表示されます。これには、すべての TLOC インターフェイスが含まれます。ペインをクリックして、**[Transport Interface Distribution]** ダイアログボックスにインターフェイスの使用状況の詳細を表示します。

WAN エッジデバイス数の表示

[WAN Edge Inventory] ペインには、次の 4 つのカウントが表示されます。

- **[Total]** : Cisco vManage にアップロードされた WAN エッジデバイスの認証済みシリアル番号の総数。シリアル番号は **[Configuration]** > **[Devices]** 画面でアップロードします。
- **[Authorized]** : オーバーレイネットワーク内の認証済み WAN エッジデバイスの総数。これらの WAN エッジデバイスは、**[Configuration]** > **[Certificates]** > **[WAN Edge List]** 画面で **[Valid]** としてマークされています。
- **[Deployed]** : 導入されている WAN エッジデバイスの総数。これらは、**[Valid]** とマークされ、現在ネットワークで動作している WAN エッジデバイスです。
- **[Staging]** : オーバーレイネットワークの一部になる前に、ステージングサイトで構成する WAN エッジデバイスの総数。これらのルータは、ルーティングの決定には関与せず、Cisco vManage によるネットワークモニタリングに影響を与えることもありません。

ペインをクリックして、**[WAN Edge Inventory]** ダイアログボックスから各ルータのホスト名、システム IP、サイト ID、およびその他の詳細を表示します。

WAN エッジデバイスの集約状態の表示

[WAN Edge Health] ペインは、各状態のデバイス数のカウントを表示することで、WAN エッジデバイスの状態を集約したビューを提供し、ハードウェアノードの正常性を示します。3 つの WAN エッジデバイスの状態は次のとおりです。

- **Normal** : メモリ、ハードウェア、CPU が正常な状態の WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 70% 未満の場合は、normal 状態に分類されます。
- **Warning** : メモリ、ハードウェア、または CPU が注意状態にある WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 70% ~ 90% の場合は、注意状態に分類されます。
- **Error** : メモリ、ハードウェア、または CPU がエラー状態にある WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 90% を超える場合は、エラー状態に分類されます。


数値または WAN エッジデバイスの状態をクリックすると、過去 12 時間または 24 時間のメモリ使用量、CPU 使用率、およびハードウェア関連のアラーム（温度、電源、PIM モジュールなど）のテーブルが表示されます。テーブルの各行の右側にある [More Actions] アイコンをクリックして、以下にアクセスします。


- **ハードウェア環境**
- **[Monitor] > [Devices]**画面の [Real Time] ビュー
Cisco vManage リリース 20.6.x 以前のリリース : **[Monitor] > [Network]** 画面の [Real Time] ビュー
- **[Tools] > [SSH Terminal]**画面。

WAN エッジデバイスの損失、遅延、ジッターの表示

[Transport Health] ペインには、すべてのリンクとすべてのカラーの組み合わせ（すべての LTE-to-LTE リンク、すべての LTE-to-3G リンクなど）の集約された平均損失、遅延、およびジッターが表示されます。

[Type] ドロップダウン矢印から、損失、遅延、またはジッターを選択します。

 アイコンをクリックして、トランスポートの正常性を表示する期間を選択します。

 アイコンをクリックして、[Transport Health] ダイアログボックスを開きます。このダイアログボックスには、より詳細なビューが表示されます。情報を表形式で表示するには、[Details] をクリックします。表示される正常性のタイプと期間を変更することを選択できます。

WAN エッジデバイスの DPI フロー情報の表示

[Top Applications] ペインには、オーバーレイネットワーク内のルータを通過するトラフィックの DPI フロー情報が表示されます。



(注) DPI フロー情報は、過去 24 時間のみ表示されます。過去 24 時間より前の DPI フロー情報を表示するには、特定のデバイスの情報を確認する必要があります。

☰アイコンをクリックして、データを表示する期間を選択します。[VPN] ドロップダウンリストから VPN を選択して、その VPN 内のすべてのフローの DPI 情報を表示します。


☒アイコンをクリックして、[Top Applications] ダイアログボックスを開きます。このダイアログボックスには、同じ情報のより詳細なビューが表示されます。VPN と期間を変更できます。

トンネルデータの表示

[Application-Aware Routing] ペインでは、[Type] ドロップダウン矢印から次のトンネル基準を選択できます。

- 損失
- 遅延
- Jitter

トンネル基準に基づいて、ペインに下位 10 件のトンネルが表示されます。たとえば、損失を選択した場合、ペインには、過去 24 時間の平均損失が最も大きい 10 のトンネルが表示されます。

行に対して  アイコンをクリックすると、データがグラフィック形式で表示されます。データを表示する期間を選択するか、[Custom] をクリックして、カスタム期間を指定するためのドロップダウン矢印を表示します。

☒アイコンをクリックして、[Application-Aware Routing] ダイアログボックスを開きます。このダイアログボックスには、[Type] ドロップダウン矢印から選択した基準（損失、遅延、およびジッター）に基づいて下位 25 件のトンネルが表示されます。

テナント WAN エッジデバイスの管理

テナントネットワークへの WAN エッジデバイスの追加

1. Cisco vManage にログインします。

プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

テナントユーザーの場合は、tenantadmin としてログインします。

2. デバイスのシリアル番号ファイルを Cisco vManage にアップロードします。
3. デバイスを検証し、詳細をコントローラに送信します。

4. デバイスの設定テンプレートを作成し、デバイスをテンプレートにアタッチします。

デバイスの設定中に、次の例のようにサービスプロバイダーの組織名とテナントの組織名を設定します。

```
sp-organization-name multitenancy
organization-name multitenancy-Customer1
```



(注) organization-name は <SP Org Name>-<Tenant Org Name> の形式で入力します。

5. Cisco vManage によって生成されたブートストラップ設定を使用してデバイスをブートストラップするか、デバイスで初期設定を手動で作成します。
6. エンタープライズ証明書を使用してデバイスを認証する場合は、CSR を Cisco vManage からダウンロードし、エンタープライズ CA によって署名された CSR を取得します。Cisco vManage に証明書をインストールします。

テナントネットワークからの WAN エッジデバイスの削除

1. Cisco vManage にログインします。

プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

テナントユーザーの場合は、tenantadmin としてログインします。

2. 構成テンプレートからデバイスを切り離します。
3. [WAN エッジルータ](#)を削除します。

Cisco vSmart コントローラ でのテナント固有のポリシー

プロバイダーの admin ユーザー (Cisco vManage のテナントとしてのプロバイダービューから) または tenantadmin ユーザー (Cisco vManage のテナントビューから) は、テナントにサービスを提供する Cisco vSmart コントローラ でテナント固有のポリシーを作成および展開できます。ユーザーは、CLI ポリシーを設定するか、UI ポリシー構成ウィザードを使用してポリシーを作成できます。

ポリシーをアクティブ化または非アクティブ化すると、次のようになります。

1. Cisco vManage は、テナントにサービスを提供する Cisco vSmart コントローラ を識別します。
2. Cisco vManage は、ポリシー構成をプルするように Cisco vSmart コントローラ に通知します。

3. Cisco vSmart コントローラ は、ポリシー構成をプルして展開します。
4. Cisco vManage は、Cisco vSmart コントローラ によるポリシープルのステータスを報告します。

テナントデータの管理

テナントデータのバックアップ

Cisco vManage マルチテナント機能のテナントデータバックアップソリューションは、次の機能を提供します。

- [設定データのバックアップファイルの作成、抽出、および表示](#)。
- 後で復元するオプションを使用して、特定のテナントの設定データベースをバックアップします。「[テナントデータのバックアップファイルの復元と削除](#)」を参照してください。
- Cisco vManage に格納されているテナントのバックアップファイルを削除します。テナントデータバックアップファイルの削除については、「[テナントデータのバックアップファイルの復元と削除](#)」をご覧ください。

データ バックアップ ソリューションを使用する場合、次の要因が適用されます。

- テナントデータのバックアップソリューションの操作は、テナント管理者がテナントビューを介し、プロバイダーとして実行できます。さまざまなビューからテナントダッシュボードにアクセスする方法については、[マルチテナント環境でのユーザーロール \(5 ページ\)](#)を参照してください。
- テナントは、特定の時間に次のバックアップ操作を実行でき、1つの操作を完了してから新しい操作を開始する必要があります。
 - 単一の設定データベースのバックアップ
 - バックアップファイルのダウンロード
 - バックアップファイルの復元またはインポート
 - バックアップファイルの削除
 - バックアップファイルの一覧表示
- テナントのバックアップファイルの形式は次のとおりです。
`Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz`
- テナントデータのバックアップ操作は、設定データベースに対する読み取り専用操作です。ただし、データの整合性を確保し、データの損失を防ぐため、ネットワーク上で大きな変更は実行しないでください。

- 特定のテナントのバックアップまたは復元操作が進行中のとき、他のテナントはバックアップおよび復元操作をスムーズに実行できます。
- テナントデータベースの復元操作が進行中の場合、テナントは他のバックアップ操作を実行できません。したがって、テナントは単一のバックアップ操作を実行でき、この操作が進行中の場合、すべての新しいバックアップ操作要求は拒否されます。
残りのテナントは、バックアップ操作を続行できます。
- テナントは、バックアップの生成および復元操作に対して、同じ Cisco vManage バージョンを使用する必要があります。
- テナントは最大 3 つのバックアップファイルを Cisco vManage に保存でき、ダウンロードして Cisco vManage リポジトリの外部に保存できます。テナントにすでに 3 つのバックアップファイルがある場合、後続のバックアップ操作により、最も古いバックアップファイルが削除され、新しいバックアップファイルが生成されます。
- バックアップファイルと、テナントが復元操作を要求したセットアップの両方で、次のパラメータ値が一致していることを確認します。
 - テナントID (Tenant Id)
 - 組織名
 - SP Organization Name
- テナントデータのバックアップソリューションは、Cisco vManage のテナントビューにタスクを作成します。そのため、テナントはテナントダッシュボードのタスクビューから操作の進行状況を監視できます。
- プロバイダーは、このソリューションを使用してプロバイダーデータをバックアップすることはできません。したがって、プロバイダーは、CLI を使用してすべてのテナント設定データベースをバックアップすることにより、すべてのテナント情報を一度にバックアップできます。

設定データのバックアップファイルの作成、抽出、および表示

1. Cisco vManage にログインします。

プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

テナントユーザーの場合は、tenantadmin としてログインします。

2. アドレスバーで、REST API 接続の dataservice を使用して URL パスを変更します。

例 : `https://<tenant_URL>/dataservice`

3. 次の API を使用して構成バックアップファイルを作成します。

`https://<tenant_URL>/dataservice/tenantbackup/export.`

- 構成バックアップファイルが正常に作成されると、Cisco vManage タスクビューにバックアップファイルが生成されたことが示されます。作成されたプロセスまたはタスクのプロセス識別子を表示できます。

例：

```
{
  "processId": "72d69805-b987-436f-9b7a-afef2f3f9061",
  "status": "in-progress"
}
```

- 取得したプロセス識別子でタスクの状態を確認します。

例：

```
https://<tenant_URL>/dataservice/device/action/status/72d69805-b987-436f-9b7a-afef2f3f9061
```

検証により、タスクの詳細が JSON ファイル形式で生成されます。

- タスクが完了したら、JSON タスクファイルの [data] セクションにあるバックアップファイルを抽出またはダウンロードします。

例：バックアップファイルを抽出またはダウンロードするには、次の API を使用します。

```
https://<tenant_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz
```

- 次の API を使用して、Cisco vManage に保存されているバックアップファイルを一覧表示します。

例：https://<tenant_URL>/dataservice/tenantbackup/list

テナントデータのバックアップファイルの復元と削除

始める前に

テナントデータ バックアップ ファイルの復元および削除 API を実行するには、Postman ツールまたは http アプリケーションとサービスをテストするための他の代替ツールをダウンロードしてインストールします。このドキュメントでは、Postman ツールを使用してテナントデータのバックアップファイルを復元および削除する手順を説明しました。Postman は、API 開発環境として使用されるソフトウェアツールです。このツールは、Postman の Web サイトからダウンロードできます。

- Google Chrome または別のブラウザを開き、開発者モードを有効にします。
- Cisco vManage にログインします。

プロバイダー ユーザーの場合は、管理者としてログインします。プロバイダー ダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

テナント ユーザーの場合は、tenantadmin としてログインします。

- 復元 API のヘッダー情報を取得するには、次のようにします。

- 画面の右側で、[Network] タブをクリックして、ネットワーク キャプチャ ビューを表示します。

2. ネットワーク キャプチャ ビューで、[Name] 列をクリックして、リストされている項目を並べ替えます。
 3. index.html を検索してクリックします。
 4. [Headers] タブをクリックし、[Request Headers] を展開します。
 5. Request Headers の下のすべてのテキストを選択し、クリップボードにコピーします。
4. Postman UI を使用してバックアップファイルをインポートします。
 1. Postman UI を開きます。
 2. SSL 証明書の検証を無効にするには、[Postman] > [Preferences] > [General] > [Request] をクリックします。[SSL Certificate Verification] をオフにします。
 3. Postman UI で、新しいタブを作成します。
 4. [Request Headers] をクリックし、[Bulk Edit] をクリックします。
 5. [Request Headers] ブロックからステップ 3 でコピーしたテキストを、編集可能なフォームに貼り付けます。
 6. [GET] メソッド ドロップダウン リストから、[POST] を選択します。
 7. [Paste request URL] フィールドに、テナントの専用 URL を貼り付け、dataservice/tenantbackup/import を含めます。
例 : `https://Customer1.multitenancy.com/dataservice/tenantbackup/import`
 8. [Body] タブをクリックし、[form-data] を選択します。
 9. [KEY] 列に `bakup.tar.gz` と入力します。
 10. [VALUE] 列で、[Select Files] をクリックし、インポートするバックアップファイルを選択します。
 11. API を実行するには、[Send] をクリックします。
Postman UI の [Response] セクションで、復元されたファイルを示す JSON 情報を表示できます。

5. 次のいずれかの方法で、バックアップファイルの復元を監視します。

1. バックアップファイルが正常にインポートされたかどうかを示す Cisco vManage タスクビューを使用します。作成されたプロセスまたはタスクのプロセス識別子を表示できます。

例 :

```
{
  "processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
  "status": "Import Successfully Submitted for tenant 1579026919487"
}
```

2. 次の URL を使用してステータスを取得します。 `https://<tenant_URL>/dataservice/device/action/status/<processId>`

例 :

<https://Customer1.multitenancy.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96cd1d>

6. Postman UI を使用してテナントデータのバックアップファイルを削除します。
 1. Postman UI で、新しいタブを作成します。
 2. [Request Headers] をクリックし、[Bulk Edit] をクリックします。
 3. [Request Headers] ブロックからステップ3でコピーしたテキストを、編集可能なフォームに貼り付けます。
 4. [GET] メソッド ドロップダウン リストから [DELETE] を選択します。
 5. [Paste request URL] フィールドに、テナントの専用 URL を貼り付け、`dataservice/tenantbackup/delete?fileName='filename'` を含めます。ファイル名には、バックアップファイルの名前または `all` を指定できます。

例 :

https://Customer1.multitenancy.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz

例 : <https://Customer1.multitenancy.com/dataservice/tenantbackup/delete?fileName=all>

6. API を実行するには、[Send] をクリックします。

Postman UI の [Response] セクションで、削除されたファイルを示す JSON 情報を表示できます。

例 :

```
{
  "Deleted": [
    "bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz"
  ]
}
```

Cisco vSmart コントローラでのテナントごとの OMP 統計表示

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. 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 のメニューから [Monitor] > [Network] の順に選択します。
3. デバイスのテーブルで、Cisco vSmart コントローラのホスト名をクリックします。
4. 左側のペインで、[Real Time] をクリックします。
5. [Device Options] フィールドに [OMP] と入力し、表示する OMP 統計を選択します。

6. [Select Filters] ダイアログボックスで [Show Filters] をクリックします。
7. [Tenant Name] を入力し、[Search] をクリックします。

Cisco vManage は、特定のテナントの選択された OMP 統計を表示します。

Cisco vSmart コントローラに関連付けられたテナントの表示

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. **vSmart** 接続番号をクリックし、各接続に関する詳細情報を示す表を表示します。
Cisco vManage は、Cisco vSmart コントローラとその接続の概要を示す表を表示します。
3. Cisco vSmart コントローラの場合は、[...] をクリックし、[Tenant List] をクリックします。
Cisco vManage は、Cisco vSmart コントローラに関連付けられたテナントの概要を表示します。

シングルテナント Cisco SD-WAN オーバーレイからマルチテナント Cisco SD-WAN 展開への移行

表 7: 機能の履歴

機能名	リリース情報	説明
シングルテナント Cisco SD-WAN オーバーレイからマルチテナント Cisco SD-WAN 展開への移行	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、一連の Cisco vManage API 呼び出しを使用して、シングルテナントの Cisco SD-WAN オーバーレイをマルチテナント展開に移行できます。

はじめる前に

- 移行を開始する前に、次の手順を実行します。
 - シングルテナント展開のエッジデバイスがマルチテナント展開の Cisco vBond Orchestrator に到達できることを確認します
 - エッジデバイスのテンプレート、ルーティング、およびポリシー構成が Cisco vManage の現在の構成と同期していることを確認します

- この手順を実行する前に、シングルテナントオーバーレイのメンテナンスウィンドウを構成します。「[Configure or Cancel vManage Server Maintenance Window](#)」を参照してください。

- 移行するシングルテナントオーバーレイの最小ソフトウェア要件

デバイス	ソフトウェアバージョン
Cisco vManage	Cisco vManage リリース 20.5.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.5.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.5.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.4.1a

- シングルテナントオーバーレイの移行先となるマルチテナント展開の最小ソフトウェア要件

デバイス	ソフトウェアバージョン
Cisco vManage	Cisco vManage リリース 20.5.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.5.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.5.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.5.1a

- API 呼び出しを実行するには、カスタムスクリプトまたは Postman などのサードパーティアプリケーションを使用することをお勧めします。

移行手順

1. オーバーレイを制御する Cisco vManage インスタンスからシングルテナントの展開および構成データをエクスポートします。

メソッド	POST
URL	<code>https://ST-vManage-IP-address</code>
エンドポイント	<code>/dataservice/tenantmigration/export</code>
許可	管理者ユーザーログイン情報。

本文	<p>必須</p> <p>フォーマット : Raw JSON</p> <pre>{ "desc": <tenant_description>, "name": <tenant_name>, "subdomain": <tenant_name>.<domain>, "orgName": <tenant_orgname > }</pre> <p>Field Description:</p> <ul style="list-style-type: none"> • desc : テナントの説明。説明の最大長は 256 文字で、英数字のみを使用できます。 • name : マルチテナント展開のテナントの一意の名前。 • subdomain : テナントの完全修飾サブドメイン名。サブドメイン名には、サービスプロバイダーのドメイン名が含まれている必要があります。たとえば、multitenancy.com がサービスプロバイダーのドメイン名であり、テナント名が Customer1 である場合、テナントのサブドメイン名は Customer1.multitenancy.com になります。 • orgName : テナント組織の名前。組織名では、大文字と小文字が区別されます。
応答	<p>フォーマット : JSON</p> <pre>{ "processId": <vManage_process_ID>, }</pre>

データのエクスポート中に、Cisco vManage は、マルチテナント展開への移行に備えて、エッジデバイスから CLI テンプレートを切り離そうとします。Cisco vManage によってプロンプトが表示された場合は、CLI テンプレートをエッジデバイスから切り離し、エクスポート API 呼び出しを再度実行します。

2. Cisco vManage でデータエクスポートタスクのステータスを確認します。タスクが成功したら、URL
<https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz> を使用してデータをダウンロードします
3. マルチテナント Cisco vManage インスタンスで、シングルテナント オーバーレイからエクスポートされたデータをインポートします。

メソッド	POST
URL	https://MT-vManage-IP-address
エンドポイント	/dataservice/tenantmigration/import
許可	プロバイダー管理者ユーザーログイン情報。

本文	必須 フォーマット：フォームデータ キータイプ：ファイル 値：default.tar.gz
応答	フォーマット：JSON <pre>{ "processId": <vManage_process_ID>, "migrationTokenURL": <token_URL>, }</pre>

タスクが成功すると、マルチテナント Cisco vManage で、シングルテナント オーバーレイからインポートされたデバイス、テンプレート、およびポリシーを表示できます。

4. 手順 3 の API 呼び出しに回答して取得したトークン URL を使用して、移行トークンを取得します。

方法	GET
URL	https://MT-vManage-IP-address
エンドポイント	手順 3 で取得した migrationTokenURL。
許可	プロバイダー管理者ユーザーログイン情報。
応答	エンコードされたテキストの大きな BLOB としての移行トークン。

5. シングルテナント Cisco vManage インスタンスで、マルチテナント展開へのオーバーレイの移行を開始します。

メソッド	POST
URL	https://ST-vManage-IP-address
エンドポイント	dataservice/tenantmigration/networkMigration
許可	管理者ユーザーログイン情報。
本文	必須 フォーマット：生のテキスト 内容：手順 4 で取得した移行トークン。
応答	フォーマット：JSON <pre>{ "processId": <vManage_process_ID>, }</pre>

Cisco vManage で、移行タスクのステータスを確認します。移行タスクの一部として、マルチテナント vBond Orchestrator のアドレス、サービスプロバイダーおよびテナントの組織名が、シングルテナントオーバーレイの WAN エッジデバイスにプッシュされます。タス

クが成功すると、WAN エッジデバイスはマルチテナント展開のコントローラへの制御接続を形成します。WAN エッジデバイスは、シングルテナントオーバーレイのコントローラに接続されなくなります。

マルチテナント展開への移行後に、(手順1で) エッジデバイスから切り離された CLI テンプレートを接続します。テンプレートを接続する前に、マルチテナント展開の構成と一致するように Cisco vBond Orchestrator の IP アドレスと組織名を更新します。



-
- (注) シングルテナント展開では、Cisco vManage 署名付き証明書がクラウドベースの WAN エッジデバイスにインストールされている場合、デバイスがマルチテナント展開に移行されるときに証明書がクリアされます。マルチテナント Cisco vManage でデバイスを再認証する必要があります。エンタープライズ証明書がクラウドベースの WAN エッジデバイスにインストールされている場合、証明書は移行の影響を受けません。詳細については、「[Enterprise Certificates](#)」を参照してください。
-

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。