



Cisco SD-WAN マルチテナント機能

- [Cisco SD-WAN マルチテナント機能の概要 \(1 ページ\)](#)
- [サポートされているデバイスとコントローラの仕様 \(6 ページ\)](#)
- [機能制限 \(8 ページ\)](#)
- [マルチテナント機能の初期設定 \(9 ページ\)](#)
- [マルチテナント展開を拡張してテナントとテナントデバイスのサポート数を追加 \(18 ページ\)](#)
- [テナントの管理 \(22 ページ\)](#)
- [マルチテナント機能の Cisco vManage ダッシュボード \(27 ページ\)](#)
- [テナント WAN エッジデバイスの管理 \(32 ページ\)](#)
- [Cisco vSmart コントローラのテナント固有のポリシー \(33 ページ\)](#)
- [テナントデータの管理 \(34 ページ\)](#)
- [Cisco vSmart コントローラでのテナントごとの OMP 統計表示 \(38 ページ\)](#)
- [Cisco vSmart コントローラに関連付けられたテナントの表示 \(39 ページ\)](#)
- [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 \(39 ページ\)](#)
- [マルチテナント Cisco SD-WAN オーバーレイの移行 \(43 ページ\)](#)
- [Cisco SD-WAN コントローラおよびエッジデバイスソフトウェアのアップグレード \(46 ページ\)](#)
- [マルチテナント Cisco vManage : ディザスタリカバリ \(47 ページ\)](#)
- [マルチテナント Cisco vManage : 仮想ルータを使用したオーバーレイネットワークでのディザスタリカバリ \(53 ページ\)](#)
- [マルチテナント Cisco vManage : 障害が発生したデータセンターが稼働状態になった後のディザスタリカバリ \(60 ページ\)](#)
- [障害が発生した Cisco vSmart コントローラの交換 \(65 ページ\)](#)

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、基盤となる Cisco SD-WAN コントローラと同じセット (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) を共有します。テナントデータは、これらの共有コントローラ上で論理的に分離されます。

サービスプロバイダーは、Cisco vManage クラスターの IP アドレスにマッピングされたドメイン名を使用して Cisco vManage にアクセスし、マルチテナント展開を管理します。各テナントには、テナント固有の Cisco vManage ビューにアクセスしてテナントの展開を管理するためのサブドメインが提供されます。たとえば、ドメイン名 managed-sp.com を使用するサービスプロバイダーは、テナント Customer1 と Customer2 にサブドメイン customer1.managed-sp.com と customer2.managed-sp.com を割り当て、各顧客に専用の Cisco SD-WAN コントローラセットを備えたシングルテナントのセットアップを提供する代わりに、それらを同じ Cisco SD-WAN コントローラセットで管理することができます。

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
- マルチテナント Cisco vBond オーケストレーション
- マルチテナント Cisco vSmart コントローラ
- テナント固有の WAN エッジデバイス
- 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 ESXi 6.7 以降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、Cisco CloudOps によって Amazon Web Services (AWS) サーバー上でホストすることもできます。
- テナント固有の Cisco vAnalytics : Cisco vAnalytics は、アプリケーションのパフォーマンスと基盤となる SD-WAN ネットワーク インフラストラクチャに関するインサイトを提供するクラウドベースのサービスです。各テナントは、テナント固有の Cisco vAnalytics インスタンスを要求し、Cisco vManage でのデータ収集を有効にすることで、オーバーレイネットワークに関する Cisco vAnalytics のインサイトを取得できます。サービスプロバイダーは、テナント オーバーレイ ネットワークの Cisco vAnalytics インスタンスのオンボーディングを促進するために、プロバイダービューで Cisco vManage のクラウドサービスを有効にする必要があります。

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。

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。

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。

- 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。

- テナントにサービスを提供するために複数の Cisco vSmart コントローラのペアを使用できる場合、Cisco vManage は、最も少ない数の予測デバイスに接続されている Cisco vSmart コントローラのペアをテナントに割り当てます。Cisco vSmart コントローラの 2 つのペアが同じ数のデバイスに接続されている場合、Cisco vManage は、テナントの数が最も少ない Cisco vSmart コントローラのペアをテナントに割り当てます。
- Cisco vManage リリース 20.9.1 以降では、テナントをマルチテナント展開にオンボーディングするときに、テナントにサービスを提供するマルチテナント Cisco vSmart コントローラのペアを選択できます。テナントのオンボーディング後、必要に応じて、テナントをマルチテナント Cisco vSmart コントローラの別のペアに移行できます。詳細については、「[マルチテナント Cisco vSmart コントローラでの柔軟なテナント配置](#)」を参照してください。
- 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。

テナント固有の 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。

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。

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://managed-sp.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 WAN エッジ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、プロバイダーに次の 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 Orchestrator、および Cisco vSmart Controller をプロビジョニングおよび管理します。
- テナントを追加、変更、または削除します。
- 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://managed-sp.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.managed-sp.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。



ヒント 専用テナント URL にアクセスできない場合は、ローカルマシンの `/etc/hosts` ファイルでサブドメインの詳細を更新します。または、外部 DNS サーバーを使用する場合は、テナントサブドメインの DNS エントリを追加します。

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。

サポートされているデバイスとコントローラの仕様

次の Cisco SD-WAN エッジデバイスはマルチテナント機能をサポートしています。

表 1: サポートされるデバイス

Platform	デバイス 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 8200 シリーズ エッジプラットフォーム • 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 • Cisco ENCS プラットフォーム

マルチテナント機能では、次のハイパーバイザがサポートされています。

- VMware ESXi 6.7 以降
- KVM
- AWS (クラウドホスト型、Cisco CloudOps による管理)

Cisco vManage リリース 20.6.1 以降、マルチテナント Cisco vManage インスタンスは、次の3つのいずれかのペルソナを使用できます。ペルソナにより、Cisco vManage インスタンスで事前定義された一連のサービスが有効になります。

表 2: Cisco vManage のペルソナ

ペルソナ	サービス
コンピューティング + データ	クラスタ Oracle、サービスプロキシ、メッセージングサービス、調整サービス、設定データベース、Data Collection Agent、統計データベース、およびアプリケーションサーバー
データ	クラスタ Oracle、サービスプロキシ、アプリケーションサーバー、Data Collection Agent、および統計データベース

ペルソナ	サービス
コンピューティング	クラスタ Oracle、サービスプロキシ、メッセージングサービス、調整サービス、設定データベース、およびアプリケーションサーバー

Cisco vBond Orchestrator、Cisco vManage、および Cisco vSmart Controller でサポートされるハードウェア仕様は次のとおりです。

50 テナントと 1000 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、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の詳細については、『[Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources](#)』を参照してください。

75 テナントと 2500 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、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の詳細については、『[Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources](#)』を参照してください。

100 テナントと 5000 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、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の詳細については、『[Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources](#)』を参照してください。

150 テナントと 7500 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、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の詳細については、『[Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources](#)』を参照してください。

機能制限

- 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。代わりに、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。

vmanage_system インターフェイスの IP アドレスを見つけるには、次のいずれかの方法を使用します。

- 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。
- **show interface description** コマンドを実行し、コマンド出力から vmanage_system IP アドレスを見つけます。

- 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。
- 以前に無効にしてオーバーレイネットワークから削除した WAN エッジデバイスを追加する場合は、デバイスの追加後にデバイスソフトウェアをリセットする必要があります。Cisco IOS XE SD-WAN デバイスのソフトウェアをリセットするには、**request platform software sdwan software reset** コマンドを使用します。

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 3: Cisco SD-WAN マルチテナント機能の最小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 20.6.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.6.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.6.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.6.1a

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。

- このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションにある推奨ハードウェア仕様に従ってください。
- 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. Cisco vManage クラスタを作成します。

1. 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、[3 ノードの Cisco vManage クラスタの作成](#)。
 2. 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、[6 ノードの Cisco vManage クラスタの作成](#)。
 3. Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、すべてのテナントで 150 のテナントと 7500 のデバイスをサポートするには、[6 ノードの Cisco vManage クラスタの作成](#)。
2. 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`
 3. 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、10 の Cisco vSmart コントローラを展開します。
 - Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、すべてのテナントで 150 のテナントと 7500 のデバイスをサポートするには、16 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。
 4. 新しいテナントを導入準備します。[新規テナントの追加 \(23 ページ\)](#) を参照してください。

3 ノードの Cisco vManage クラスタの作成

1. [Cisco Software Download](#) から、Cisco vManage リリース 20.6.1 以降のソフトウェアイメージをダウンロードします。
2. ダウンロードしたソフトウェアイメージファイルをインストールして、3 つの Cisco vManage インスタンス (vManage1、vManage2、および vManage3 など) を作成します。「[Deploy Cisco vManage](#)」を参照してください。

**重要**

- このドキュメントの「*Supported Devices and Controller Specifications*」セクションの「*Hardware Specifications to Support 50 Tenants and 1000 Devices*」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。
- Cisco vManage インスタンスごとに [Compute+Data] ペルソナを選択します。

3. vManage1 で次の操作を実行します。**1. CLI を使用して以下を設定します。**

- システム IP アドレス
- サイト ID
- サービスプロバイダーの組織名 (sp-organization-name)
- 組織名
- vBond IP アドレス
- VPN 0 トランスポート/トンネルインターフェイス
- VPN 0 アウトオブバンド (OOB) インターフェイス : このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
- VPN 512 管理インターフェイス



(注) VPN 0 にデフォルトルートをもつだけ設定します。

2. [Cisco vManage でのマルチテナント機能の有効化 \(16 ページ\)](#)。
3. (オプション) CLI を使用して、vManage1 のルート CA 証明書をインストールします。



(注) Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

4. Cisco vManage GUI を使用して以下を実行します。
 1. [証明書署名要求を生成します](#)
 2. Symantec またはエンタープライズルート CA が証明書に署名した後、[署名された証明書をインストール](#)します。
5. [Cisco vManage サーバーのクラスタ IP アドレスを設定](#)します。

次のステップに進む前に、**[Administration]>[Cluster Management]** ページの [vManage IP Address] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

4. vManage2 および vManage 3 で次の操作を実行します。



重要 vManage2 および vManage3 でマルチテナント機能を有効にしないでください。

1. CLI を使用して以下を設定します。
 - システム IP アドレス
 - サイト ID
 - サービスプロバイダーの組織名 (sp-organization-name)
 - 組織名
 - vBond IP アドレス
 - VPN 0 トランスポート/トンネルインターフェイス
 - VPN 0 アウトオブバンド (OOB) インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
 - VPN 512 管理インターフェイス
2. (オプション) CLI を使用して、vManage1 のルート CA 証明書をインストールします。



(注) Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

3. Cisco vManage GUI を使用して以下を実行します。
 1. [証明書署名要求を生成します](#)
 2. Symantec またはエンタープライズルート CA が証明書に署名した後、[署名付き証明書をインストールします](#)。
4. [Cisco vManage Web アプリケーションサーバーにログインします](#)。
5. 他の2つの Cisco vManage インスタンスの OOB インターフェイスに ping を送信し、到達可能であることを確認します。
6. [Cisco vManage サーバーのクラスタ IP アドレスを設定します](#)。

次のステップに進む前に、**[Administration] > [Cluster Management]** ページの **[vManage IP Address]** フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

5. vManage1 GUI にログインし、**vManage2 をクラスタに追加します。**

vManage2 は、クラスタに追加される前に再起動します。

vManage2 がクラスタに追加されている間、**[Administration] > [Cluster Management]** ページで、vManage2 の **[Configure Status]** には **[Pending]** と表示されます。**[System Generated ClusterSync]** トランザクションを監視すると、クラスタへの vManage2 の追加の進行状況を確認できます。

操作が完了すると、**[Administration] > [Cluster Management]** ページで、vManage1 と vManage2 の両方、およびそれらのノードペルソナを表示できます。

6. ステップ 5 を繰り返し、vManage3 をクラスタに追加します。



- (注) 再起動後、CLI からペルソナ（非クラウドセットアップ）を選択する必要があるため、サービスは選択したペルソナに従ってノードで実行を開始します。

6 ノードの Cisco vManage クラスタの作成

1. [Cisco Software Download](#) から、Cisco vManage リリース 20.6.1 以降のソフトウェアイメージをダウンロードします。
2. ダウンロードしたソフトウェアイメージファイルをインストールして、6 つの Cisco vManage インスタンスを作成します。「[Deploy Cisco vManage](#)」を参照してください。



重要

- すべてのテナントで 100 テナントと 5000 デバイスをサポートするには、このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションの「100 テナントと 5000 デバイスをサポートするハードウェア仕様」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。

Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、すべてのテナントで 150 テナントと 7500 デバイスをサポートするには、このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションの「150 テナントと 7500 デバイスをサポートするハードウェア仕様」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。

- 3 つの Cisco vManage インスタンス（vManage1、vManage2、および vManage 3 など）には、**[Compute+Data]** ペルソナを選択します。他の 3 つの Cisco vManage インスタンス（vManage4、vManage5、および vManage6 など）には、**[Data]** ペルソナを選択します。

3. vManage1 で次の操作を実行します。
 1. CLI を使用して以下を設定します。
 - システム IP アドレス
 - サイト ID
 - サービスプロバイダーの組織名 (sp-organization-name)
 - 組織名
 - vBond IP アドレス
 - VPN 0 トランスポート/トンネルインターフェイス
 - VPN 0 アウトオブバンド (OOB) インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
 - VPN 512 管理インターフェイス



(注) VPN 0 にデフォルトルートをもつだけ設定します。

2. [Cisco vManage でのマルチテナント機能の有効化 \(16 ページ\)](#)。
3. (オプション) CLI を使用して、vManage1 のルート CA 証明書をインストールします。



(注) Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

4. Cisco vManage GUI を使用して以下を実行します。
 1. [証明書署名要求を生成します](#)。
 2. Symantec またはエンタープライズルート CA が証明書を署名した後、[署名された証明書をインストールします](#)。
5. [Cisco vManage サーバーのクラスタ IP アドレスを設定します](#)。

次のステップに進む前に、[Administration]>[Cluster Management] ページの [vManage IP Address] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

4. vManage2 から vManage6 で次の操作を実行します。



重要 vManage2 から vManage6 でマルチテナント機能を有効にしないでください。

1. CLI を使用して以下を設定します。
 - システム IP アドレス
 - サイト ID
 - サービスプロバイダーの組織名 (sp-organization-name)
 - 組織名
 - vBond IP アドレス
 - VPN 0 トランスポート/トンネルインターフェイス
 - VPN 0 アウトオブバンド (OOB) インターフェイス : このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
 - VPN 512 管理インターフェイス
2. (オプション) CLI を使用して、vManage1 のルート CA 証明書をインストールします。



(注) Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

3. Cisco vManage GUI を使用して以下を実行します。
 1. 証明書署名要求を生成します。
 2. Symantec またはエンタープライズルート CA が証明書に署名した後、署名された証明書をインストールします。
 4. Cisco vManage Web アプリケーションサーバーにログインします。
 5. 他の Cisco vManage インスタンスの OOB インターフェイスに ping して、到達可能であることを確認します。
 6. Cisco vManage サーバーのクラスタ IP アドレスを設定します。

次のステップに進む前に、[Administration]>[Cluster Management] ページの [vManage IPAddress] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。
5. vManage1 GUI にログインし、vManage2 をクラスタに追加します。

vManage2 は、クラスタに追加される前に再起動します。

vManage2 がクラスタに追加されている間、**[Administration]** > **[Cluster Management]** ページで、vManage2 の **[Configure Status]** には **[Pending]** と表示されます。**[System Generated Cluster Sync]** トランザクションを監視すると、クラスタへの vManage2 の追加の進行状況を確認できます。

操作が完了すると、**[Administration]** > **[Cluster Management]** ページで、vManage1 と vManage2 の両方、およびそれらのノードペルソナを表示できます。

6. ステップ 5 を繰り返し、vManage3 から vManage6 をクラスタに追加します。

Cisco vManage でのマルチテナント機能の有効化

前提条件

既存の Cisco vManage からすべてのデバイスを無効にするか削除した場合でも、既存のシングルテナント Cisco vManage 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、Cisco vManage リリース 20.6.1 またはそれ以降のリリースの新しい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) Cisco vManage でマルチテナンシーを有効にした後、シングルテナントモードに戻すことはできません。

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、`managed-sp.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。



- (注) ステップ 5 および 6 で作成された [Domain] と [Cluster Id] の値は、プロバイダー FQDN として機能します。これらの値が現在の DNS 命名規則に準拠していることを確認してください。設定の保存後にこれらの値を変更することはできません。これらの値を変更するには、新しい Cisco vManage クラスタを展開する必要があります。プロバイダーとテナントの DNS 要件の詳細については、「[新規テナントの追加](#)」のステップ 3.d を参照してください。

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。

マルチテナント展開を拡張してテナントとテナントデバイスのサポート数を追加

サービスプロバイダーは、50 のテナントと 1000 のデバイスをサポートする Cisco SD-WAN マルチテナントオーバーレイを展開したとします。より多くのテナントまたはデバイスをサポートする必要がある場合は、Cisco vManage クラスタを拡張し、Cisco vSmart コントローラをオー

オーバーレイに追加して、最大 100 のテナントと 5000 のデバイスをサポートできます。Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、Cisco vManage クラスタを拡張し、Cisco vSmart コントローラをオーバーレイに追加して、最大 150 のテナントと 7500 のデバイスをサポートできます。

前提条件

最大 50 のテナントと 1000 のデバイスをサポートするマルチテナント Cisco SD-WAN オーバーレイ（このドキュメントの「マルチテナント機能の初期設定」セクションの手順に従って展開します）。

1. 3 ノードクラスタから 6 ノードクラスタへの拡張

- 最大 100 のテナントと 5000 のデバイスをサポートするには、オーバーレイに 10 の Cisco vSmart コントローラが必要です。したがって、オーバーレイ内の 6 つの既存の Cisco vSmart コントローラに加えて、4 つの Cisco vSmart コントローラを展開します。

最大 150 のテナントと 7500 のデバイスをサポートするには、オーバーレイに 16 の Cisco vSmart コントローラが必要です。したがって、オーバーレイ内の 6 つの既存の Cisco vSmart コントローラに加えて、10 の Cisco vSmart コントローラを展開します。

- 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。
- 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。

テナントを追加するか、既存のテナントで関連する制限に従ってデバイスを追加できるようになりました。

3 ノードクラスタから 6 ノードクラスタへの拡張



(注) 3 ノードの Cisco vManage クラスタは、6 ノードの Cisco vManage クラスタにのみ拡張できません。3 ノードクラスタを他のクラスタサイズに拡張することはサポートされていません。

- 100 のテナントと 5000 のデバイスをサポートするには、既存の 3 ノードクラスタ内の 3 つの Cisco vManage サーバーを、このドキュメントの「*Supported Devices and Controller Specifications*」セクションの「*Hardware Specifications to Support 100 Tenants and 5000 Devices*」の表のハードウェア仕様にアップグレードします。

Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降で、150 のテナントと 7500 のデバイスをサポートするには、既存の 3 ノードクラスタ内の 3 つの Cisco vManage サーバーを、このドキュメントの「*Supported Devices and Controller Specifications*」セクションにある表「*Hardware Specifications to Support 150 Tenants and 7500 Devices*」のハードウェア仕様にアップグレードします。

2. [Cisco Software Download](#) から、Cisco vManage リリース 20.6.1 以降のリリースのソフトウェアイメージをダウンロードします。
3. ダウンロードしたソフトウェアイメージファイルをインストールして、3つのCisco vManage インスタンス (vManage1、vManage2、および vManage3 など) を作成します。「[Deploy Cisco vManage](#)」を参照してください。

**重要**

- このドキュメントの「*Supported Devices and Controller Specifications*」セクションの「*Hardware Specifications to Support 100 Tenants and 5000 Devices*」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。

Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、150 テナントと 7500 デバイスをサポートするには、このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションの「150 テナントと 7500 デバイスをサポートするハードウェア仕様」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。

- Cisco vManage インスタンスごとに [Data] ペルソナを選択します。

4. vManage1 から vManage3 で次の操作を実行します。

**重要**

vManage1 から vManage3 でマルチテナント機能を有効にしないでください。

1. CLI を使用して以下を設定します。

- システム IP アドレス
- サイト ID
- サービスプロバイダーの組織名 (sp-organization-name)
- 組織名
- vBond IP アドレス
- VPN 0 トランスポート/トンネルインターフェイス
- VPN 0 アウトオブバンド (OOB) インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
- VPN 512 管理インターフェイス



(注) VPN 0 にデフォルトルートをもつだけ設定します。

2. (オプション) CLI を使用して、vManage1 のルート CA 証明書をインストールします。



(注) Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

3. Cisco vManage GUI を使用して以下を実行します。
 1. 証明書署名要求を生成します
 2. Symantec またはエンタープライズルート CA が証明書に署名した後、署名された証明書をインストールします。
4. Cisco vManage Web アプリケーションサーバーにログインします。
5. 他の Cisco vManage インスタンスの OOB インターフェイスに ping して、到達可能であることを確認します。
6. Cisco vManage サーバーのクラスタ IP アドレスを設定します。

次のステップに進む前に、**[Administration] > [Cluster Management]** ページの **[vManage IP Address]** フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

5. 既存の 3 ノード Cisco vManage クラスタの GUI にログインし、vManage1 をクラスタに追加します。

vManage1 は、クラスタに追加される前に再起動します。

vManage1 がクラスタに追加されている間、**[Administration] > [Cluster Management]** ページで、vManage1 の **[Configure Status]** には **[Pending]** と表示されます。**[System Generated Cluster Sync]** トランザクションを監視すると、クラスタへの vManage1 の追加の進行状況を確認できます。

操作が完了すると、**[Administration] > [Cluster Management]** ページで、元の 3 ノードクラスタの一部であった 3 つの Cisco vManage インスタンスとともにリストされた vManage1 とそのノードペルソナを表示できます。

6. ステップ 4 を繰り返し、vManage2 と vManage3 をクラスタに追加します。

テナントの管理

表 4:機能の履歴

機能名	リリース情報	説明
テナントデバイスの予測	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、サービスプロバイダーは、テナントがオーバーレイネットワークに追加できる WAN エッジデバイスの数を制御できます。これを行うと、プロバイダーは Cisco SD-WAN コントローラリソースを効率的に利用できます。

テナントデバイスの予測

マルチテナント Cisco SD-WAN 展開に新しいテナントを追加する際、サービスプロバイダーは、テナントがオーバーレイネットワークに展開できる WAN エッジデバイスの数を予測できます。Cisco vManage は、この予測制限を適用します。テナントがこの制限を超えてデバイスを追加しようとする、Cisco vManage は該当するエラーメッセージで応答し、デバイスの追加は失敗します。

マルチテナント展開では、テナントは最大で 1000 台のデバイスをオーバーレイネットワークに追加できます。



(注) Cisco IOS XE リリース 17.6.2、Cisco vManage リリース 20.6.2 以降では、テナントの追加後にテナントのデバイス予測を変更できます。この変更は、Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1 ではサポートされていません。

利点：

- サービスプロバイダーは、Cisco SD-WAN コントローラリソースがより効率的に使用されるようにすることができます。
- 設定によっては、マルチテナント展開では、すべてのテナントで固定数の WAN エッジデバイスをサポートできます。テナントが追加できるデバイスの数を予測することにより、サービスプロバイダーは、展開でサポートできるエッジデバイスのプール全体から各テナントにクォータを割り当てることができます。

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 のテナントと最大 1000 のテナントデバイスに対応できます。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的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 5: 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。
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** 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、**managed-sp.com** サービスプロバイダーの場合、有効なドメイン名は **customer1.managed-sp.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、**[Administration]** > **[Settings]** > **[Tenancy Mode]** 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。
- **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、Cisco 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. [Number of Devices] フィールドに、テナントが展開できる WAN エッジデバイスの数を入力します。

テナントがこの数を超える WAN エッジデバイスを追加しようとするすると、Cisco vManage はエラーを報告し、デバイスの追加は失敗します。

6. [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は、以下を変更できます。
 - [Description]：説明の最大長は 256 文字で、英数字のみを使用できます。
 - [Forecasted Device]：テナントが展開できる WAN エッジデバイスの数。
テナントは、最大 1000 台のデバイスを追加できます。



(注) このオプションは、Cisco IOS XE リリース 17.6.2、Cisco vManage リリース 20.6.2 から利用できます。

テナントが展開できるデバイスの数を増やす場合は、必要な数のデバイスライセンスを [Cisco Software Central](#) の **Plug and Play Connect** のテナントバーチャルアカウントに追加する必要があります。

テナントが展開できるデバイスの数を増やす前に、テナントに割り当てられた Cisco vSmart コントローラペアがこの増加した数をサポートできることを確認してください。Cisco vSmart コントローラのペアは、これらのすべてのテナントで最大 24 のテナントと 1000 のデバイスをサポートできます。

• [URL Subdomain Name]：テナントの完全修飾サブ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 \(33 ページ\)](#) 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、**[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 Orchestrator、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 Controller 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、ページの上部にある [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] > [Network] 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。

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] タブをクリックします。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 コントローラ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]> [Network]画面から [Device Dashboard] または [Real Time] ビューにアクセスします。

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]** > **[Network]** 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。

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 WAN エッジデバイス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、正常な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] > [Network]**画面から **[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] タブをクリックします。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。


DPI を表示 WAN エッジデバイスのフロー情報

[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



(注) 以前に無効にしてオーバーレイネットワークから削除した WAN エッジデバイスを追加する場合は、デバイスの追加後にデバイスソフトウェアをリセットする必要があります。Cisco IOS XE SD-WAN デバイスのソフトウェアをリセットするには、**request platform software sdwan software reset** コマンドを使用します。

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、**admin** 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、テナントとしてのプロバイダービューを表示します。

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、ポリシー設定をプルするように Cisco vSmart コントローラに通知します。
3. Cisco vSmart コントローラは、ポリシー設定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。

- [構成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 に保存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で、またはプロバイダー管理者がテナントとしてのプロバイダービューで実行できます。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 \(4 ページ\)](#) 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に、操作の進行中にネットワーク上で大きな変更を行わないでください。
- 複数のテナントが並行してバックアップと復元の操作を実行できます。

- 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、同一の Cisco vManage ソフトウェアバージョンを実行している Cisco vManage インスタンスでバックアップおよび復元操作を実行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。

構成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.managed-sp.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.managed-sp.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d>

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.managed-sp.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz

例：<https://customer1.managed-sp.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 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

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。
 - シングルテナントオーバーレイからマルチテナント展開への移行は、オンプレミスに展開された Cisco SD-WAN コントローラでのみサポートされます。クラウドホスト型の Cisco SD-WAN コントローラでは、移行はまだサポートされていません。
 - 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 20.6.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.6.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.6.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.6.1a

- 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 20.6.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.6.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.6.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.6.1a

- Cisco SD-WAN コントローラと WAN エッジデバイスのソフトウェアバージョンは、シングルテナント展開とマルチテナント展開の両方で同一である必要があります。
- 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、managed-sp.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.managed-sp.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。

- 手順 3 の API 呼び出しに応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。

- 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。

マルチテナント Cisco SD-WAN オーバーレイの移行

表 6: 機能の履歴

機能名	リリース情報	説明
マルチテナント Cisco SD-WAN オーバーレイの移行	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、共有 Cisco vManage インスタンスと Cisco vBond Orchestrator で構成されるマルチテナント Cisco SD-WAN オーバーレイ、およびテナント固有の Cisco vSmart コントローラを、共有 Cisco vManage インスタンス、Cisco vBond Orchestrator、および Cisco vSmart コントローラで構成されるマルチテナントオーバーレイに移行できます。

前提条件

移行するマルチテナントオーバーレイ内の Cisco SD-WAN コントローラおよび WAN エッジデバイス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 20.3.3
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.3.3

デバイス	ソフトウェアバージョン
Cisco vSmart Controller	Cisco SD-WAN リリース 20.3.3
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.3.3

制約事項

- この移行手順は、オンプレミスに展開された Cisco SD-WAN コントローラにのみ適用されます。
- マルチテナントオーバーレイは、Cisco vManage インスタンスが Cisco vManage リリース 20.6.1 ソフトウェアを実行し、Cisco SD-WAN コントローラが Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行するセットアップにのみ移行できます。
- この移行手順を使用して、複数のマルチテナントオーバーレイをマージすることはできません。新しいセットアップに一度に移行できるマルチテナントオーバーレイは1つだけです。

移行手順

1. クラスタ内の3つの Cisco vManage インスタンスのソフトウェアを Cisco vManage リリース 20.6.1 にアップグレードします。詳細については、「[Upgrade Cisco vManage Cluster](#)」を参照してください。



(注) いずれかの Cisco vManage インスタンスのみで、**request nms configuration-db upgrade** コマンドを実行します。

2. Cisco vManage ソフトウェアが Cisco vManage リリース 20.6.1 にアップグレードされたら、Cisco vManage GUI にログインします。
新しいパスワードの設定を求めるメッセージが表示されます。
 1. パスワードガイドラインに準拠した新しいパスワードを入力します。
3. Cisco SD-WAN リリース 20.6.1 ソフトウェアを Cisco vManage にアップロードします。詳細については、「[Add an Image to the Software Repository](#)」を参照してください。
4. Cisco vBond Orchestrator ソフトウェアを Cisco SD-WAN リリース 20.6.1 にアップグレードします。詳細については、「[Upgrade the Software Image on a Device](#)」を参照してください。
5. Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行する2つの 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。



(注) 2つの Cisco vSmart コントローラインスタンスで、最大 24 のテナントをサポートできます。最大 50 のテナントをサポートする場合は、6つの Cisco vSmart コントローラインスタンスを作成します。

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。

[Provider Dashboard] には、Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行している新しい Cisco vSmart コントローラが表示されます。[Tenant Dashboard] には、Cisco SD-WAN リリース 20.3.3 ソフトウェアを実行している古い Cisco vSmart コントローラが表示されます。

6. Cisco vManage でメンテナンスウィンドウを有効にします。詳細については、「[Configure or Cancel vManage Server Maintenance Window](#)」を参照してください。
3～4 時間のメンテナンスウィンドウをお勧めします。
7. Cisco SD-WAN リリース 20.3.3 ソフトウェアを実行している古いテナント固有の Cisco vSmart コントローラから、Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行している新しい共有 Cisco vSmart コントローラにテナント設定を移行します。

メソッド	POST
URL	https://<vmanageip>:<port>
エンドポイント	dataservice/tenant/vsmart-mt/migrate
許可	プロバイダーの admin ユーザーログイン情報。
本文	必須 フォーマット : Raw JSON {
応答	フォーマット : JSON { "processId": <vManage_process_ID>, }

Cisco vManage で、API 応答の `processId` を使用して、移行タスクのステータスを確認します。移行タスク中に、次の変更が反映されます。

1. 古い Cisco vSmart コントローラは無効化され、オーバーレイネットワークから削除されます。
2. テナントビューでは、古い Cisco vSmart コントローラが [Tenant Dashboard] および、[Devices] と [Certificates] のページから削除されます。
3. テナント WAN エッジデバイスは、新しい Cisco vSmart コントローラに接続されます。

8. (オプション) Cisco IOS XE SD-WAN デバイスソフトウェアを Cisco IOS XE リリース 17.6.1a にアップグレードします。詳細については、「[Upgrade the Software Image on a Device](#)」および「[Activate a New Software Image](#)」を参照してください。



ヒント マルチテナントオーバーレイを移行するのと同じメンテナンスウィンドウで、テナント WAN エッジデバイスソフトウェアをアップグレードする必要はありません。ただし、移行から数週間以内にテナント WAN エッジデバイスソフトウェアをアップグレードすることをお勧めします。

移行の確認

1. プロバイダービューで、次のチェックを実行します。
 1. [Main Dashboard] ページで、テナント WAN エッジデバイスが新しいマルチテナント Cisco vSmart コントローラに接続されているかどうかを確認します。
 2. [Cisco vSmart コントローラに関連付けられたテナントの表示 \(39 ページ\)](#)。
 3. Cisco vSmart コントローラ CLI で、**show control connections** コマンドを実行します。コマンド出力で、Cisco vSmart コントローラとテナント WAN エッジデバイスの間に制御接続が確立されていることを確認します。
2. テナントとしてのプロバイダービューで、マルチテナント Cisco vSmart コントローラが [Tenant Dashboard] に表示されるかどうかを確認します。

Cisco SD-WAN コントローラおよびエッジデバイスソフトウェアのアップグレード

前提条件

Cisco SD-WAN コントローラおよび WAN エッジデバイス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 20.4.1 以降
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.4.1 以降
Cisco vSmart Controller	Cisco SD-WAN リリース 20.4.1 以降
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.4.1 以降

アップグレード手順

1. クラスタ内の3つの Cisco vManage インスタンスのソフトウェアを Cisco vManage リリース 20.6.1 またはそれ以降のリリースにアップグレードします。詳細については、「[Upgrade Cisco vManage Cluster](#)」を参照してください。



(注) **request nms configuration-db upgrade** コマンドを使用して configuration-db サービスをアップグレードする手順をスキップします。

2. Cisco vManage ソフトウェアを Cisco vManage リリース 20.6.1 またはそれ以降のリリースにアップグレードしたら、Cisco vManage GUI にログインします。
3. Cisco SD-WAN リリース 20.6.1 またはそれ以降のリリースおよび Cisco IOS XE リリース 17.6.1a またはそれ以降のリリースのソフトウェアを Cisco vManage にアップロードします。詳細については、「[Add an Image to the Software Repository](#)」を参照してください。
4. Cisco vBond Orchestrator ソフトウェアを Cisco SD-WAN リリース 20.6.1 またはそれ以降のリリースにアップグレードします。詳細については、「[Upgrade the Software Image on a Device](#)」および「[Activate a New Software Image](#)」を参照してください。
5. Cisco vManage でメンテナンスウィンドウを有効にします。詳細については、「[Configure or Cancel vManage Server Maintenance Window](#)」を参照してください。
6. Cisco vSmart コントローソフトウェアを Cisco SD-WAN リリース 20.6.1 またはそれ以降のリリースにアップグレードします。詳細については、「[Upgrade the Software Image on a Device](#)」および「[Activate a New Software Image](#)」を参照してください。
7. Cisco IOS XE SD-WAN デバイスソフトウェアを Cisco IOS XE リリース 17.6.1a またはそれ以降のリリースにアップグレードします。詳細については、「[Upgrade the Software Image on a Device](#)」および「[Activate a New Software Image](#)」を参照してください。



ヒント 同じメンテナンスウィンドウ内で WAN エッジデバイスソフトウェアをアップグレードすることをお勧めします。OMP グレースフル リスタート ウィンドウ内で WAN エッジデバイスソフトウェアがアップグレードされない場合、トラフィックが失われる可能性があります。

マルチテナント Cisco vManage : ディザスタリカバリ

マルチテナント Cisco vManage クラスタ、またはクラスタ内の Cisco vManage ノードをホストするデータセンターに障害が発生した場合、スタンバイ Cisco vManage クラスタをアクティブ化することで障害から回復できます。ディザスタリカバリは次のように実行できます。

1. スタンバイ Cisco vManage クラスタを展開して設定します。

スタンバイ Cisco vManage クラスタはオーバーレイネットワークの一部ではなく、アクティブではありません。

2. アクティブな Cisco vManage クラスタの設定データベースを定期的にバックアップします。
設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、設定データベースをバックアップします。
3. アクティブな Cisco vManage クラスタに障害が発生した場合は、スタンバイ Cisco vManage クラスタで最新の設定データベースを復元し、スタンバイ Cisco vManage クラスタをアクティブにして、以前にアクティブだった Cisco vManage クラスタをオーバーレイネットワークから削除します。

設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、以前にアクティブだった Cisco vManage クラスタからバックアップした設定データベースを復元します。

デザスタリカバリをテストするには、アクティブな Cisco vManage クラスタに障害が発生するシナリオをシミュレートします。このような障害をシミュレートする1つの方法は、このドキュメントで説明されているようにトンネルインターフェイスを無効にすることです。

前提条件

- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードの数は同じである必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、同じ Cisco vManage ソフトウェアリリースを実行する必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、オーバーレイネットワーク内の Cisco vBond Orchestrator の WAN トランスポート IP アドレスに接続できる必要があります。
- 最初に、スタンバイクラスタの Cisco vManage ノードのトンネルインターフェイスを無効にする必要があります。
- スタンバイクラスタの Cisco vManage ノードは認定されている必要があります。
- スタンバイクラスタのすべての Cisco vManage ノードのクロックは、オーバーレイネットワーク内の Cisco SD-WAN コントローラおよび WAN エッジデバイスのクロックと同期されている必要があります。オーバーレイで NTP が設定されている場合は、スタンバイ Cisco vManage ノードでも同様に設定します。
- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードは、同一の neo4j ログイン情報を使用する必要があります。

制約事項

- 設定データベースのバックアップ中は、アクティブなプロセスを中断しないでください。

- SD-AVC を有効にする場合は、スタンバイ Cisco vManage ノードで設定データベースを復元する前に行う必要があります。

スタンバイ Cisco vManage クラスタの設定

1. アクティブな Cisco vManage ノードと同様の実行中の設定でスタンバイ Cisco vManage ノードを設定します。スタンバイ Cisco vManage ノードにローカル証明書をインストールします。



(注) スタンバイ Cisco vManage の実行コンフィギュレーションは、通常、アクティブな Cisco vManage ノードの実行コンフィギュレーションと同じです。ただし、システム IP アドレスやトンネルインターフェイス IP アドレスなどの設定が一意であることは確認する必要があります。

2. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスをシャットダウンします。CLI で、トランスポート インターフェイス設定に **shutdown** コマンドを含めます。
3. スタンバイ Cisco vManage ノードを使用してスタンバイクラスタを作成します。

この方法で設定されたスタンバイ Cisco vManage ノードでは、オーバーレイネットワークはスタンバイ Cisco vManage クラスタを認識しません。

アクティブな Cisco vManage クラスタ設定のバックアップ

アクティブな Cisco vManage クラスタの完全な設定データベースを定期的にバックアップします。また、アクティブな Cisco vManage 仮想マシンのスナップショットを作成します。

1. 設定データベースサービスをホストするアクティブな Cisco vManage ノードを選択し、設定データベースのバックアップをエクスポートします。Cisco vManage ノードの CLI で、次のコマンドを実行します。 **request nms configuration-db backup path file-path**

このコマンドは、設定データベースを .tar.gz ファイルにバックアップし、そのファイルを指定された *file-path* に保存します。

次の例では、データベースは、/home/admin/ ディレクトリの db_backup.tar.gz という名前のファイルにバックアップされます。

```
Active-vManage# request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

2. 設定データベースサービスをホストするスタンバイ Cisco vManage ノードを選択し、設定データベースのバックアップをこのノードにコピーします。

次の例では、db_backup.tar.gz がアクティブな Cisco vManage ノードからスタンバイ Cisco vManage ノードの /home/admin/ ディレクトリにコピーされます。

```
Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHv1rBUxWzNjd8mUz819gPf51MeopsgDlAc.
```

```

Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5

admin@10.126.93.92's password:
db_backup.tar.gz                               100% 399KB 4.4MB/s 00:00

```

設定データベースのバックアップを使用した Cisco vManage クラスタの復元

このバックアップをコピーしたスタンバイ Cisco vManage ノードで、アクティブな Cisco vManage クラスタからの設定データベースの最新バックアップを復元します。



- (注)
- 復元操作では、設定データベースに含まれるすべての情報が復元されるわけではありません。ユーザーやリポジトリなどの Cisco vManage 設定は、バックアップを使用して設定データベースを復元した後、スタンバイ Cisco vManage ノードで設定する必要があります。
 - 次の手順を完了すると、以前にアクティブだった Cisco vManage ノードは再利用できなくなります。ノードを再利用するには、このドキュメントの範囲を超える追加手順を実行する必要があります。

1. スタンバイ Cisco vManage ノードの CLI で、次のコマンドを実行します。 **request nms configuration-db restore path *file-path***

次の例では、バックアップファイル `db_backup.tar.gz` を使用して設定データベースを復元します。

```

Standby-vManage# request nms configuration-db restore path
/home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database

```

2. 適切なサービスがスタンバイ Cisco vManage ノードで実行されていることを確認します。各スタンバイ Cisco vManage ノードの CLI で、**request nms all status** コマンドを実行します。コマンド出力から、ノードで実行されているサービスを確認します。
3. すべてのスタンバイ Cisco vManage ノードに、アクティブおよびスタンバイ Cisco vManage ノードの全リストがあることを確認します。
 1. Cisco vManage のメニューから、**[Configuration] > [Devices] > [Controllers]** を選択します。
 2. ページにすべてのアクティブおよびスタンバイ Cisco vManage ノードが表示されていることを確認します。
4. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスを有効にします。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスを有効にします。各スタンバイ Cisco vManage ノードの CLI で、**no shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

- VPN 0 のトンネルインターフェイスをアクティブにします。各スタンバイ Cisco vManage ノードの CLI で、**tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

- 各スタンバイ Cisco vManage ノードをオーバーレイネットワークに追加します。
 - Cisco vManage のメニューから、**[Configuration] > [Devices]** の順に選択します。
 - [Controllers]** をクリックします。
 - Cisco vBond Orchestrator で、**[...]** をクリックし、**[Edit]** をクリックします。
 - [Edit]** ダイアログボックスで、Cisco vBond Orchestrator の詳細 (WAN トランスポート IP アドレス、ユーザー名、およびパスワード) を入力します。
 - すべての Cisco vBond Orchestrator について、**ステップ 5c** と **ステップ 5d** を繰り返します。
- アクティブな Cisco vManage ノードをオーバーレイネットワークから接続解除します。



- (注) 災害シナリオをシミュレートするラボ環境では、このステップを実行できます。しかし、実際の災害シナリオで Cisco vManage インスタンスに到達できない場合、このステップは実行できない可能性があり、省略できます。

次の 2 つの方法のいずれかを使用します。

- VPN 0 のトランスポート インターフェイスをシャットダウンします。アクティブな各 Cisco vManage ノードの CLI で、**shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

- VPN 0 のトンネルインターフェイスを非アクティブにします。アクティブな各 Cisco vManage ノードの CLI で、**no tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

- スタンバイ Cisco vManage から、更新されたコントローラとデバイスのリストを Cisco vBond Orchestrator に送信します。

コントローラのリストの送信 :

1. [Cisco vManage] メニューから、[**Configuration**] > [**Certificates**] を選択します。
2. [Controllers] をクリックします。
3. [Send to vBond] をクリックします。

設定タスクが完了するまで待ちます。タスクが完了すると、次のようになります。

- スタンバイ Cisco vManage ノードがアクティブな Cisco vManage ノードになります。
 - 以前にアクティブだった Cisco vManage ノードはオーバーレイネットワークの一部ではなくなります。
 - アクティブな Cisco vManage ノードの設定は、最新の設定データベースバックアップからの設定になります。
 - すべてのコントローラがネットワーク内の他のコントローラとの接続を確立します。
4. [WAN Edge List] をクリックします。
 5. [Send to Controllers] をクリックします。
8. 以下が失われていないことを確認します。
- ポリシー
 - テンプレート (Templates)
 - コントローラと WAN エッジデバイスのリスト
9. 有効な Cisco vManage ノードを確認します。
1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。
コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。
 2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。
コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。
10. 以前にアクティブだった Cisco vManage ノードを無効にします。



(注) Cisco vManage ノードを無効にした後は、このドキュメントの範囲を超える追加手順を実行しない限り、ノードを再利用することはできません。

1. [Cisco vManage] メニューから、[Configuration] > [Certificates] を選択します。
 2. [Controllers] をクリックします。
 3. 以前にアクティブだった Cisco vManage ノードごとに、[...] をクリックし、[Invalidate] をクリックします。
11. 有効な Cisco vManage ノードを確認します。
1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。
コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。
 2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。
コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

当初はスタンバイクラスタであった Cisco vManage クラスタが、アクティブな Cisco vManage クラスタになりました。

マルチテナント Cisco vManage : 仮想ルータを使用したオーバーレイネットワークでのディザスタリカバリ

マルチテナント Cisco vManage クラスタ、またはクラスタ内の Cisco vManage ノードをホストするデータセンターに障害が発生した場合、スタンバイ Cisco vManage クラスタをアクティブ化することで障害から回復できます。ディザスタリカバリは次のように実行できます。

1. スタンバイ Cisco vManage クラスタを展開して設定します。
スタンバイ Cisco vManage クラスタはオーバーレイネットワークの一部ではなく、アクティブではありません。
2. アクティブな Cisco vManage クラスタの設定データベースを定期的にバックアップします。
設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、設定データベースをバックアップします。

3. アクティブな Cisco vManage クラスタに障害が発生した場合は、スタンバイ Cisco vManage クラスタで最新の設定データベースを復元し、スタンバイ Cisco vManage クラスタをアクティブにして、以前にアクティブだった Cisco vManage クラスタをオーバーレイネットワークから削除します。

設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、以前にアクティブだった Cisco vManage クラスタからバックアップした設定データベースを復元します。

ディザスタリカバリをテストするには、アクティブな Cisco vManage クラスタに障害が発生するシナリオをシミュレートします。このような障害をシミュレートする1つの方法は、このドキュメントで説明されているようにトンネルインターフェイスを無効にすることです。

次のディザスタリカバリ手順は、Cisco vEdge Cloud ルータがブランチロケーションに導入されているオーバーレイネットワークに適用されます。

前提条件

- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードの数は同じである必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、同じ Cisco vManage ソフトウェアリリースを実行する必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、オーバーレイネットワーク内の Cisco vBond Orchestrator の WAN トランスポート IP アドレスに接続できる必要があります。
- 最初に、スタンバイクラスタの Cisco vManage ノードのトンネルインターフェイスを無効にする必要があります。
- スタンバイクラスタの Cisco vManage ノードは認定されている必要があります。
- スタンバイクラスタのすべての Cisco vManage ノードのクロックは、オーバーレイネットワーク内の Cisco SD-WAN コントローラおよび WAN エッジデバイスのクロックと同期されている必要があります。オーバーレイでNTPが設定されている場合は、スタンバイ Cisco vManage ノードでも同様に設定します。
- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードは、同一の neo4j ログイン情報を使用する必要があります。

制約事項

- 設定データベースのバックアップ中は、アクティブなプロセスを中断しないでください。
- SD-AVC を有効にする場合は、スタンバイ Cisco vManage ノードで設定データベースを復元する前に行う必要があります。

スタンバイ Cisco vManage クラスタの設定

1. アクティブな Cisco vManage ノードと同様の実行中の設定でスタンバイ Cisco vManage ノードを設定します。スタンバイ Cisco vManage ノードにローカル証明書を実インストールします。



(注) スタンバイ Cisco vManage の実行中の設定は、通常、アクティブな Cisco vManage ノードの実行中の設定と同じです。ただし、システム IP アドレスやトンネルインターフェイス IP アドレスなどの設定が一意であることは確認する必要があります。

2. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスをシャットダウンします。CLI で、トランスポート インターフェイス設定に **shutdown** コマンドを含めます。
3. スタンバイ Cisco vManage ノードを使用してスタンバイクラスタを作成します。

この方法で設定されたスタンバイ Cisco vManage ノードでは、オーバーレイネットワークはスタンバイ Cisco vManage クラスタを認識しません。

アクティブな Cisco vManage クラスタ設定のバックアップ

アクティブな Cisco vManage クラスタの完全な設定データベースを定期的にバックアップします。また、アクティブな Cisco vManage 仮想マシンのスナップショットを作成します。

1. 設定データベースサービスをホストするアクティブな Cisco vManage ノードを選択し、設定データベースのバックアップをエクスポートします。Cisco vManage ノードの CLI で、次のコマンドを実行します。 **request nms configuration-db backup path file-path**

このコマンドは、設定データベースを .tar.gz ファイルにバックアップし、そのファイルを指定された *file-path* に保存します。

次の例では、データベースは、/home/admin/ ディレクトリの db_backup.tar.gz という名前のファイルにバックアップされます。

```
Active-vManage# request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

2. 設定データベースサービスをホストするスタンバイ Cisco vManage ノードを選択し、設定データベースのバックアップをこのノードにコピーします。

次の例では、db_backup.tar.gz がアクティブな Cisco vManage ノードからスタンバイ Cisco vManage ノードの /home/admin/ ディレクトリにコピーされます。

```
Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHv1rBUxWzNjd8mUz819gPf51MeopsgDlAc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5
```

```
admin@10.126.93.92's password:
db_backup.tar.gz 100% 399KB 4.4MB/s 00:00
```

設定データベースのバックアップを使用した Cisco vManage クラスタの復元

このバックアップをコピーしたスタンバイ Cisco vManage ノードで、アクティブな Cisco vManage クラスタからの設定データベースの最新バックアップを復元します。



- (注)
- 復元操作では、設定データベースに含まれるすべての情報が復元されるわけではありません。ユーザーやリポジトリなどの Cisco vManage 設定は、バックアップを使用して設定データベースを復元した後、スタンバイ Cisco vManage ノードで設定する必要があります。
 - 次の手順を完了すると、以前にアクティブだった Cisco vManage ノードは再利用できなくなります。ノードを再利用するには、このドキュメントの範囲を超える追加手順を実行する必要があります。

1. スタンバイ Cisco vManage ノードの CLI で、次のコマンドを実行します。 **request nms configuration-db restore path file-path**

次の例では、バックアップファイル db_backup.tar.gz を使用して設定データベースを復元します。

```
Standby-vManage# request nms configuration-db restore path
/home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

2. 適切なサービスがスタンバイ Cisco vManage ノードで実行されていることを確認します。各スタンバイ Cisco vManage ノードの CLI で、**request nms all status** コマンドを実行します。コマンド出力から、ノードで実行されているサービスを確認します。
3. すべてのスタンバイ Cisco vManage ノードに、アクティブおよびスタンバイ Cisco vManage ノードの全リストがあることを確認します。
 1. Cisco vManage のメニューから、**[Configuration] > [Devices] > [Controllers]** を選択します。
 2. ページにすべてのアクティブおよびスタンバイ Cisco vManage ノードが表示されていることを確認します。
4. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャージ番号がリストされていることを確認します。
5. Cisco vEdge Cloud ルータの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーン番号がリストされていることを確認します。

6. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスを有効にします。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスを有効にします。各スタンバイ Cisco vManage ノードの CLI で、**no shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

2. VPN 0 のトンネルインターフェイスをアクティブにします。各スタンバイ Cisco vManage ノードの CLI で、**tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

7. 各スタンバイ Cisco vManage ノードをオーバーレイネットワークに追加します。
 1. Cisco vManage のメニューから、**[Configuration] > [Devices]** の順に選択します。
 2. **[Controllers]** をクリックします。
 3. Cisco vBond Orchestrator で、**[...]** をクリックし、**[Edit]** をクリックします。
 4. **[Edit]** ダイアログボックスで、Cisco vBond Orchestrator の詳細（WAN トランスポート IP アドレス、ユーザー名、およびパスワード）を入力します。
 5. すべての Cisco vBond Orchestrator について、**ステップ 7c** と **ステップ 7d** を繰り返します。
8. アクティブな Cisco vManage ノードをオーバーレイネットワークから接続解除します。



- (注) 災害シナリオをシミュレートするラボ環境では、このステップを実行できます。しかし、実際の災害シナリオで Cisco vManage インスタンスに到達できない場合、このステップは実行できない可能性があり、省略できます。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスをシャットダウンします。アクティブな各 Cisco vManage ノードの CLI で、**shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

- VPN0 のトンネルインターフェイスを非アクティブにします。アクティブな各 Cisco vManage ノードの CLI で、**no tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage (config)# vpn 0 interface interface-name
Active-vManage (config-interface)# no tunnel-interface
Active-vManage (config-interface)# commit and-quit
```

- スタンバイ Cisco vManage から、更新されたコントローラとデバイスのリストを Cisco vBond Orchestrator に送信します。

コントローラのリストの送信 :

- [Cisco vManage] メニューから、**[Configuration] > [Certificates]** を選択します。
- [Controllers]** をクリックします。
- [Send to vBond]** をクリックします。

設定タスクが完了するまで待ちます。タスクが完了すると、次のようになります。

- スタンバイ Cisco vManage ノードがアクティブな Cisco vManage ノードになります。
 - 以前にアクティブだった Cisco vManage ノードはオーバーレイネットワークの一部ではなくなります。
 - アクティブな Cisco vManage ノードの設定は、最新の設定データベースバックアップからの設定になります。
 - すべてのコントローラがネットワーク内の他のコントローラとの接続を確立します。
- [WAN Edge List]** をクリックします。
 - [Send to Controllers]** をクリックします。
- 以下が失われていないことを確認します。
 - ポリシー
 - テンプレート (Templates)
 - コントローラと WAN エッジデバイスのリスト
 - 有効な Cisco vManage ノードを確認します。
 - 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。
 コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。
 - Cisco vEdge Cloud ルータの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

12. 以前にアクティブだった Cisco vManage ノードを無効にします。

以前にアクティブだった Cisco vManage は、クラウド WAN エッジデバイスの証明書発行者です。アクティブな Cisco vManage は、以前にアクティブだった Cisco vManage ノードが無効化された後にも、クラウド WAN エッジデバイスに証明書を発行します。



(注)

- Cisco vManage ノードを無効にした後は、このドキュメントの範囲を超える追加手順を実行しない限り、ノードを再利用することはできません。
- 以前にアクティブだった Cisco vManage ノードを無効にすると、Cisco vManage はノードを無効としてマークし、すべてのコントローラに更新を送信します。ただし、以前にアクティブだった Cisco vManage はクラウド WAN エッジデバイスの CA であるため、Cisco vManage は有効な Cisco vManage UUID の更新されたリストを Cisco vBond Orchestrator にすぐには送信しません。したがって、Cisco vBond Orchestrator での **show orchestrator valid-vmanage-id** コマンドの出力には、無効化された Cisco vManage ノードの UUID が含まれます。

Cisco vManage には、24 時間ごとに実行されるスケジュールされたタスクがあり、すべてのクラウド WAN エッジがアクティブな Cisco vManage に移動されたかどうかを確認します。Cisco vManage は、クラウド WAN エッジデバイスがアクティブな Cisco vManage に移動された後にも、有効な Cisco vManage UUID の更新されたリストを Cisco vBond Orchestrator に送信します。このリストを受信した後、Cisco vBond Orchestrator での **show orchestrator valid-vmanage-id** コマンドの出力には、無効化された Cisco vManage ノードの UUID は含まれません。

1. [Cisco vManage] メニューから、[**Configuration**] > [**Certificates**] を選択します。
 2. [Controllers] をクリックします。
 3. 以前にアクティブだった Cisco vManage ノードごとに、[...] をクリックし、[Invalidate] をクリックします。
13. 24 時間後に有効な Cisco vManage ノードを確認します。
1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。
 コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。
 2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

当初はスタンバイクラスタであった Cisco vManage クラスタが、アクティブな Cisco vManage クラスタになりました。

マルチテナント Cisco vManage : 障害が発生したデータセンターが稼働状態になった後のディザスタリカバリ

マルチテナント Cisco vManage クラスタ、またはクラスタ内の Cisco vManage ノードをホストするデータセンターに障害が発生した場合、スタンバイ Cisco vManage クラスタをアクティブ化することで障害から回復できます。ディザスタリカバリは次のように実行できます。

1. スタンバイ Cisco vManage クラスタを展開して設定します。

スタンバイ Cisco vManage クラスタはオーバーレイネットワークの一部ではなく、アクティブではありません。

2. アクティブな Cisco vManage クラスタの設定データベースを定期的にバックアップします。

設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、設定データベースをバックアップします。

3. アクティブな Cisco vManage クラスタに障害が発生した場合は、スタンバイ Cisco vManage クラスタで最新の設定データベースを復元し、スタンバイ Cisco vManage クラスタをアクティブにして、以前にアクティブだった Cisco vManage クラスタをオーバーレイネットワークから削除します。

設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、以前にアクティブだった Cisco vManage クラスタからバックアップした設定データベースを復元します。

ディザスタリカバリをテストするには、アクティブな Cisco vManage クラスタに障害が発生するシナリオをシミュレートします。このような障害をシミュレートする1つの方法は、このドキュメントで説明されているようにトンネルインターフェイスを無効にすることです。

次の手順は、最初にアクティブだった Cisco vManage クラスタ、またはクラスタをホストするデータセンターに障害が発生し、スタンバイ Cisco vManage クラスタがアクティブな Cisco vManage クラスタになるように設定されているシナリオに適用されます。最初にアクティブだったクラスタが再び動作可能になると、スタンバイクラスタとして機能します。以下の手順を完了することで、このスタンバイクラスタをアクティブクラスタに変えることができます。

スタンバイ vManage NMS の設定の確認

1. スタンバイ Cisco vManage ノードの実行中の設定がアクティブな Cisco vManage ノードの実行中の設定と同様かどうかを確認します。ローカル証明書は、スタンバイ Cisco vManage ノードにインストールされている必要があります。



(注) スタンバイ Cisco vManage の実行中の設定は、通常、アクティブな Cisco vManage ノードの実行中の設定と同じです。ただし、システム IP アドレスやトンネルインターフェイス IP アドレスなどの設定が一意であることは確認する必要があります。

2. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスをシャットダウンします。CLI で、トランスポート インターフェイス設定に **shutdown** コマンドを含めます。

この方法で設定されたスタンバイ Cisco vManage ノードでは、オーバーレイネットワークはスタンバイ Cisco vManage クラスタを認識しません。

アクティブな Cisco vManage クラスタ設定のバックアップ

アクティブな Cisco vManage クラスタの完全な設定データベースを定期的にバックアップします。また、アクティブな Cisco vManage 仮想マシンのスナップショットを作成します。

1. 設定データベースサービスをホストするアクティブな Cisco vManage ノードを選択し、設定データベースのバックアップをエクスポートします。Cisco vManage ノードの CLI で、次のコマンドを実行します。 **request nms configuration-db backup path file-path**

このコマンドは、設定データベースを **.tar.gz** ファイルにバックアップし、そのファイルを指定された **file-path** に保存します。

次の例では、データベースは、**/home/admin/** ディレクトリの **db_backup.tar.gz** という名前のファイルにバックアップされます。

```
Active-vManage# request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

2. 設定データベースサービスをホストするスタンバイ Cisco vManage ノードを選択し、設定データベースのバックアップをこのノードにコピーします。

次の例では、**db_backup.tar.gz** がアクティブな Cisco vManage ノードからスタンバイ Cisco vManage ノードの **/home/admin/** ディレクトリにコピーされます。

```
Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHv1rBUxWzNjd8mUz819gPf51MeopsgDlAc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5

admin@10.126.93.92's password:
db_backup.tar.gz                               100% 399KB 4.4MB/s 00:00
```

設定データベースのバックアップを使用した Cisco vManage クラスタの復元

このバックアップをコピーしたスタンバイ Cisco vManage ノードで、アクティブな Cisco vManage クラスタからの設定データベースの最新バックアップを復元します。



- (注)
- 復元操作では、設定データベースに含まれるすべての情報が復元されるわけではありません。ユーザーやリポジトリなどの Cisco vManage 設定は、バックアップを使用して設定データベースを復元した後、スタンバイ Cisco vManage ノードで設定する必要があります。
 - 次の手順を完了すると、以前にアクティブだった Cisco vManage ノードは再利用できなくなります。ノードを再利用するには、このドキュメントの範囲を超える追加手順を実行する必要があります。

- スタンバイ Cisco vManage ノードの CLI で、次のコマンドを実行します。 **request nms configuration-db restore path file-path**

次の例では、バックアップファイル db_backup.tar.gz を使用して設定データベースを復元します。

```
Standby-vManage# request nms configuration-db restore path
/home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

- 適切なサービスがスタンバイ Cisco vManage ノードで実行されていることを確認します。各スタンバイ Cisco vManage ノードの CLI で、**request nms all status** コマンドを実行します。コマンド出力から、ノードで実行されているサービスを確認します。
- すべてのスタンバイ Cisco vManage ノードに、アクティブおよびスタンバイ Cisco vManage ノードの全リストがあることを確認します。
 - Cisco vManage のメニューから、**[Configuration] > [Devices] > [Controllers]** を選択します。
 - ページにすべてのアクティブおよびスタンバイ Cisco vManage ノードが表示されていることを確認します。
- スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスを有効にします。

次の 2 つの方法のいずれかを使用します。

- VPN 0 のトランスポート インターフェイスを有効にします。各スタンバイ Cisco vManage ノードの CLI で、**no shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

- VPN 0 のトンネルインターフェイスをアクティブにします。各スタンバイ Cisco vManage ノードの CLI で、**tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

5. 各スタンバイ Cisco vManage ノードをオーバーレイネットワークに追加します。
 1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
 2. **[Controllers]** をクリックします。
 3. Cisco vBond Orchestrator で、**[...]** をクリックし、**[Edit]** をクリックします。
 4. **[Edit]** ダイアログボックスで、Cisco vBond Orchestrator の詳細（WAN トランスポート IP アドレス、ユーザー名、およびパスワード）を入力します。
 5. すべての Cisco vBond Orchestrator について、**ステップ 5c** と **ステップ 5d** を繰り返します。
6. アクティブな Cisco vManage ノードをオーバーレイネットワークから接続解除します。



- (注) 災害シナリオをシミュレートするラボ環境では、このステップを実行できます。しかし、実際の災害シナリオで Cisco vManage インスタンスに到達できない場合、このステップは実行できない可能性があり、省略できます。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスをシャットダウンします。アクティブな各 Cisco vManage ノードの CLI で、**shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

2. VPN0 のトンネルインターフェイスを非アクティブにします。アクティブな各 Cisco vManage ノードの CLI で、**no tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

7. スタンバイ Cisco vManage から、更新されたコントローラとデバイスのリストを Cisco vBond Orchestrator に送信します。

コントローラのリストの送信 :

1. **[Cisco vManage]** メニューから、**[Configuration]** > **[Certificates]** を選択します。
2. **[Controllers]** をクリックします。
3. **[Send to vBond]** をクリックします。

設定タスクが完了するまで待ちます。タスクが完了すると、次のようになります。

- スタンバイ Cisco vManage ノードがアクティブな Cisco vManage ノードになります。
- 以前にアクティブだった Cisco vManage ノードはオーバーレイネットワークの一部ではなくなります。
- アクティブな Cisco vManage ノードの設定は、最新の設定データベースバックアップからの設定になります。
- すべてのコントローラがネットワーク内の他のコントローラとの接続を確立します。

4. [WAN Edge List] をクリックします。

5. [Send to Controllers] をクリックします。

8. 以下が失われていないことを確認します。

- ポリシー
- テンプレート (Templates)
- コントローラと WAN エッジデバイスのリスト

9. 有効な Cisco vManage ノードを確認します。

1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。

2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

10. 以前にアクティブだった Cisco vManage ノードを無効にします。



(注) Cisco vManage ノードを無効にした後は、このドキュメントの範囲を超える追加手順を実行しない限り、ノードを再利用することはできません。

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

2. [Controllers] をクリックします。

3. 以前にアクティブだった Cisco vManage ノードごとに、[...]をクリックし、[Invalidate] をクリックします。
11. 有効な Cisco vManage ノードを確認します。
 1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。
 2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

当初はスタンバイクラスタであった Cisco vManage クラスタが、アクティブな Cisco vManage クラスタになりました。

障害が発生した Cisco vSmart コントローラの交換

障害のある Cisco vSmart コントローラを新しいインスタンスで置き換えるには、次の手順に従います。

1. 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。
2. オーバーレイネットワークに [Cisco vSmart コントローラの追加](#)。
3. Cisco vManage のメニューから、**[Configuration] > [Devices]** の順に選択します。
4. **[Controllers]** をクリックします。
5. 障害のある Cisco vSmart コントローラに対して、[...]をクリックし、**[Invalidate]** をクリックします。

[Invalidate] ダイアログボックスが表示されます。



(注) 障害のある Cisco vSmart コントローラを置き換えることができる新しい Cisco vSmart コントローラを追加していない場合、Cisco vManage はエラーメッセージを通じてこのことを示します。[Invalidate] ダイアログボックスで **[Cancel]** をクリックし、新しい Cisco vSmart コントローラを追加してから、障害のあるインスタンスを無効化します。

6. [Invalidate] ダイアログボックスで、次の操作を行います。
 1. **[Replace vSmart]** チェックボックスをオンにします。

2. [Select vSmart] ドロップダウンリストから、障害のあるインスタンスを置き換える新しい Cisco vSmart コントローラを選択します。
3. [Invalidate] をクリックします。

Cisco vManage で、[Invalidate Device] および [Push CLI Template Configuration] タスクが起動します。これらのタスクが完了すると、障害のある Cisco vSmart コントローラが無効化され、オーバーレイネットワークから削除されます。障害のある Cisco vSmart コントローラがサービスを提供していたテナントは、置き換えとして選択した新しい Cisco vSmart コントローラが対応するようになりました。

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。