Cisco ACI with VMware vRealize

この章は、次の内容で構成されています。

- Cisco ACI with VMware vRealize について （1 ページ）
- Cisco ACI with VMware vRealize の開始 （6 ページ）
- Cisco ACI with VMware vRealize アップグレード ワークフロー （14 ページ）
- Cisco ACI with VMware vRealize ダウングレードのワークフロー （16 ページ）
- 管理者とテナント エクスペリエンスのユース ケース シナリオ （17 ページ）
- トラブルシューティング （112 ページ）
- APIC プラグインの削除 （113 ページ）
- プラグインの概要 （114 ページ）
- vRealize Orchestrator におけるテナント用 vRA ホストの設定 （114 ページ）
- vRealize Orchestrator における IaaS ホストの設定 （115 ページ）

Cisco ACI with VMware vRealize について

Cisco Application Centric Infrastructure（ACI）は、VMware vCenter との統合に加えて、VMware の製品 vRealize Automation （vRA） および vRealize Orchestrator （vRO） と統合されます。vRA と vRO は、マルチベンダー ハイブリッド クラウド環境を構築して管理する VMware vRealize スイートに含まれています。

Cisco APIC リリース 3.1(1) 以降、vRA および vRO は、VMware DVS に加えて Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge（Cisco ACI Virtual Edge）をサポートします。

この章では、vRealize Automation リリース 7.x について説明します。Cisco ACI と VMware vRealize Automation、リリース 8.x の統合の詳細については、Cisco ACI vRealize 8 プラグイン ガイドを参照してください。

（注） Cisco Application Policy Infrastructure Controller（APIC）リリース 5.0(1) 以降、Cisco Application Virtual Switch（AVS）はサポートされません。 シスコの AVS を使用して Cisco APIC リリース 5.0(1) にアップグレードする場合、問題が発生した際にファブリックはサポートされません。また、シスコの AVS ドメインに障害が発生します。

Cisco ACI with VMware vRealize ソリューションの概要

vRA の統合は、vRA にインポートされた一連のサービス ブループリントを通じて提供されます。サービス ブループリントでは vRO Application Policy Infrastructure Controller (APIC) ワークフローを活用して、テナントがネットワーキング コンポーネントを作成、管理および削除できるように、セルフサービス ポータルにカタログ項目を提供します。ACI ワークフローを持つ複数のマシンは、次の機能を使用できます。

- 自動作成テナント エンドポイント グループ (EPG)
- APIC で必要なポリシー
- vCenter での VM とポートグループの作成
- 各ポート グループへの VM の自動配置
- APIC による作成
- アクセス リストを使用するセキュリティ ポリシーの作成
- L4-L7 サービスの設定および外部接続の提供

この消費モデルにより、ユーザはワンクリックで、事前定義されたカスタマイズ可能なコンピューティングおよびネットワーク ポリシーで、単一および複数層アプリケーション ワークロードを展開できます。カタログ項目がインフラストラクチャ管理者によって発行され、それにより詳細な権限をテナントごとに追加または削除できます。

統合では、2 つのモードのネットワーキングが提供されます。

モード	説明
共有	共有モードは、使用する IP アドレス空間の好みがなく、共有コンテキスト (VRF) を持つ共有アドレス空間がテナント間で使用されるテナント向けです。ACI エンドポイント グループ (EPG) を使用して分離が提供され、ホワイト リスト メソッドを使用して EPG 間での接続が有効化されます。

モード	説明
仮想プライベート クラウド (VPC)	VPC モードでは独自のアドレス空間アーキテクチャが使用され、ネットワーク接続はテナントごとに一意のコンテキスト (VRF) を介して分離され、共通共有 L3 出力を介して外部接続が提供されます。

物理トポロジと論理トポロジ

ここでは、vRealize ACI 統合の論理モデルと、共有サービス プランと仮想プライベート クラウド プランの比較を示します。

図 *1 : vRealize ACI* 統合の論理モデル図

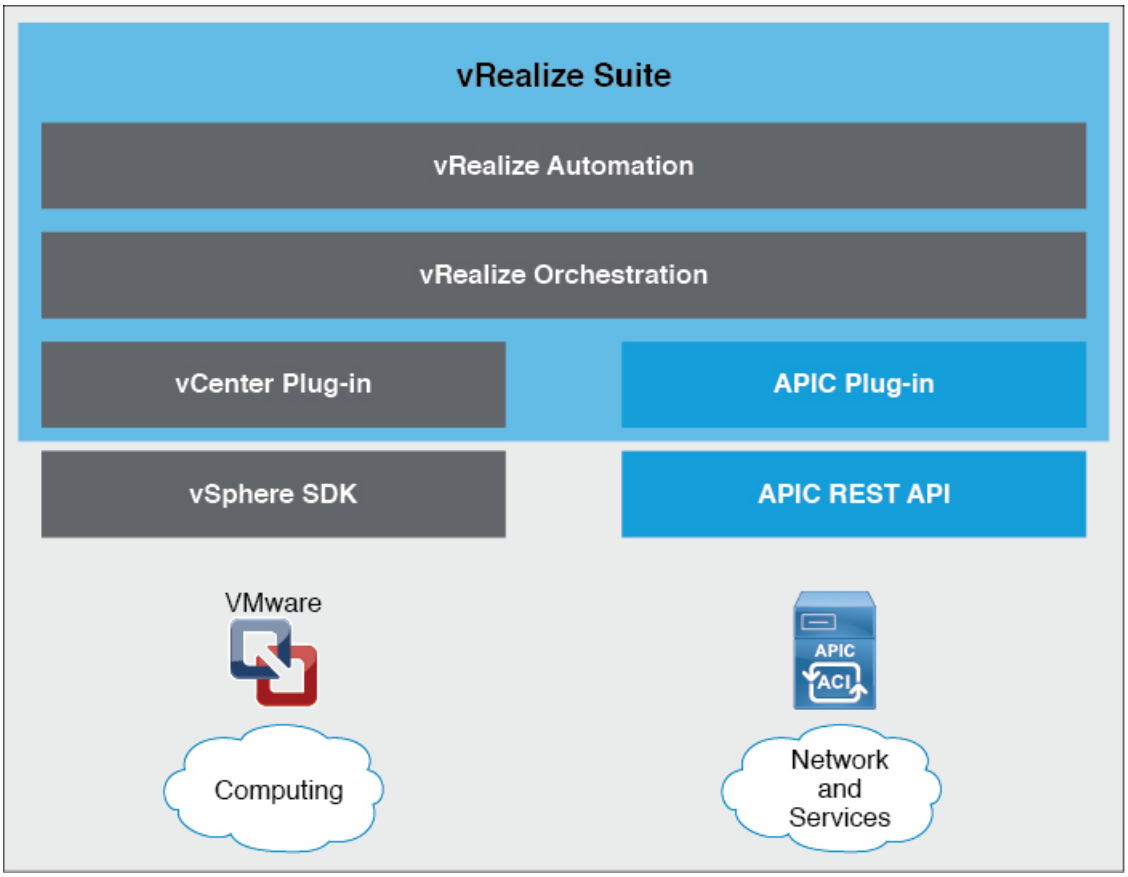
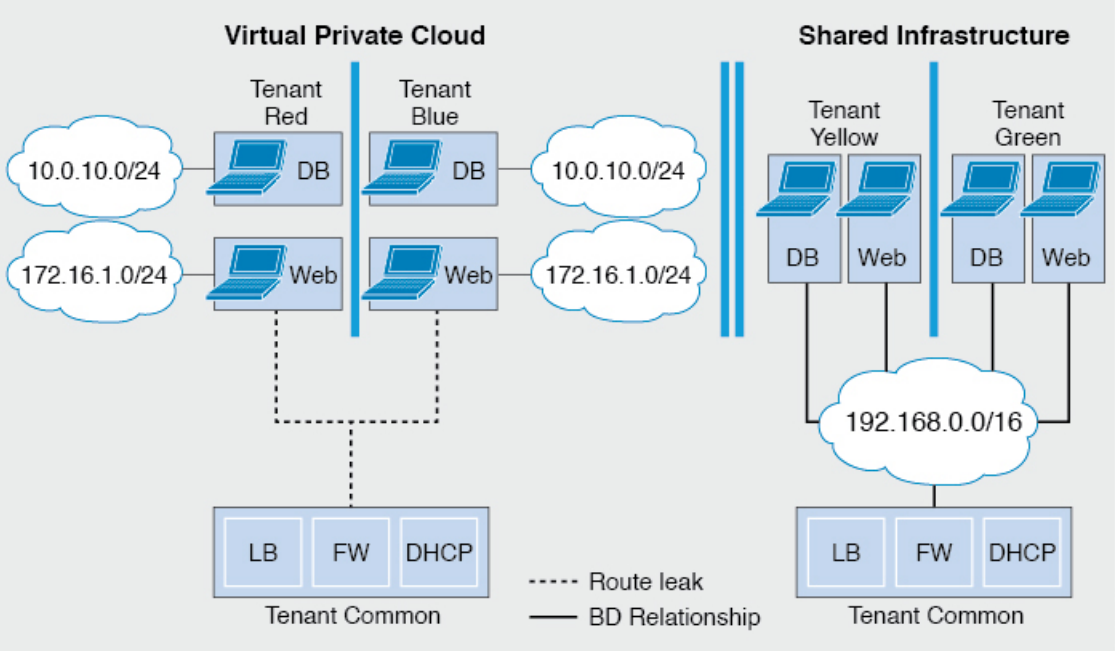


図 *2:* 共有サービス プランと仮想プライベート クラウド プランの比較図



詳細については、「*Cisco APIC* ベーシック コンフィギュレーション ガイド」を参照してください。

VMware vRealize における ACI 構造のマッピングについて

次の表に、Cisco ACI ポリシーと vRealize ポリシーの機能間の対応を示します。

Cisco ACI	VMware vRealize
テナント	テナント
EPG	Networks
レイヤ 3 外部接続	外部ルーテッド ネットワーク
コントラクト	セキュリティ ポリシー
フィルタ	ルール エントリ リスト
L4-L7 サービス デバイス	共有ロード バランサまたはファイアウォール

このリストは、次の機能に関する詳細を示します。

- テナント：テナントには、組織内の従業員、事業部門、アプリケーション所有者、またはアプリケーションを指定できます。サービス プロバイダーの場合は、ホスティング カスタマー（IT サービスを受けるために支払を行う個人または組織）を指定できます。

- ネットワーク：Cisco ACI では、「ネットワーク」はアプリケーションをネットワークにマッピングするための新しいモデルを提供するEPGのことを指します。アドレスやVLANなどの転送構造を使用して接続やポリシーを適用する代わりに、EPGではアプリケーションエンドポイントのグループ化を使用します。EPGは、vRealizeポータルでネットワークにマッピングされます。分離されたネットワークはアプリケーション、アプリケーションコンポーネントおよび層のコレクションのコンテナとして機能し、転送・ポリシーロジックを適用するために使用できます。ネットワーク ポリシー、セキュリティおよび転送をアドレッシングから分離し、代わりにこれらを論理アプリケーション境界に適用します。vRealize でネットワークが作成される際、バックエンドでは vCenter のポート グループとして作成されます。vRealize テナントは、vCenter を使用してコンピューティング リソースを管理し、仮想マシンを適切なネットワークに接続できます。

- レイヤ 3 外部接続：Cisco ACI ファブリックはレイヤ 3 外部ネットワークを介して外部に接続します。これらの構造をvRealizeテナントで使用して、データセンター内、データセンター間、またはインターネット上の他のサービスにアクセスすることもできます。

- セキュリティ ポリシー：Cisco ACI はセキュリティが強化されたモデルの上に構築されており、ポリシー契約によって明示的に許可された場合を除き、EPG（分離されたネットワーク）間のトラフィックは拒否されます。Cisco ACI契約は、vRealizeポータルでセキュリティ ポリシーにマッピングされます。セキュリティ ポリシーは、サービスを提供および使用するネットワーク（EPG）を記述します。セキュリティ ポリシーには、1 つ以上のルール エントリ リスト（フィルタ）、さまざまなアプリケーション間の通信を定義する一連のレイヤ 4 TCP またはユーザ データグラム プロトコル（UDP）ポート番号を記述するステートレス ファイアウォール ルールが含まれます。

- 共有ロード バランサおよびファイアウォール：Cisco ACI は、サービスをアプリケーションの一体要素として扱います。必要なサービスはすべて、Application Policy Infrastructure Controller（APIC）でインスタンス化されるサービス グラフとして管理されます。ユーザはアプリケーションのサービスを定義し、サービス グラフはアプリケーションで必要な一連のネットワークおよびサービス機能を識別します。Cisco ACI には、そのサービスが Cisco ACI とネイティブに統合される L4-7 サービス ベンダーのオープン エコシステムがあります。この統合は、ベンダーによって記述され所有されるデバイス パッケージを介して実現します。APICはネットワーク サービスを管理し、Cisco ACIポリシー モデルに従ってサービスを実装します。vRealize 向けに、Cisco ACI は仮想および物理フォーム ファクタの両方で、F5 および Citrix ロード バランサおよび Cisco ASA ファイアウォールを提供しており、これらは Cisco ACI ファブリックに接続され、さまざまな vRealize テナントで共有されます。デバイスが Cisco ACI に統合されたら、vRealize 管理者はデバイスをプレミアム サービスとして追加し、プランをアップセルすることを選択できます。vRealize管理者は共有デバイスの仮想IPアドレス範囲を管理して、vRealizeテナントのワークフローを簡易化します。

- VPC プラン：VPC プランでは、vRealize テナントは独自のアドレス空間を定義し、DHCP サーバを再起動して、アドレス空間をネットワークにマッピングできます。VPCテナントは、共有サービス プランからロード バランシングなどのサービスを受けることもできます。このシナリオでは、デバイスに複数の仮想 NIC（vNIC）が存在します。1 つの vNIC はプライベート アドレス空間に接続し、もう 1 つは共有サービス インフラストラクチャに接続します。共有サービス インフラストラクチャに接続する vNIC には、インフラスト

ラクチャによって割り当てられたアドレスがあり、インフラストラクチャが所有する共有ロード バランサを消費します。

イベント ブローカー VM のカスタマイズ

vRealize Automation イベント ブローカーはユーザーが設定した事前定義の条件の下で、vRealize Orchestrator からワークフローを呼び出す、vRealize Automation ワークフロー サブスクリプション サービスです。これは、Cisco APIC 3.0 (1) 以降でサポートされています。

単一または階層アプリケーションの展開はイベントブローカーに自動的に登録されます。マシン上の作成や削除など vRA で設定されている任意のマシンの操作は、イベント ブローカーをトリガします。これは、単一または多層アプリケーションに関連付けられているプロパティ グループによって定義されている Cisco APIC で事前設定された操作を起動します。

Cisco APIC ワークフロー サブスクリプションを追加するには、VMware vRealize Automation アプライアンスを ACI 向けに設定 （11 ページ） 次の手順を実行します。ワークフロー サブスクリプションしは自動的に追加されます。

Cisco ACI with VMware vRealize の開始

ここでは、Cisco ACI with VMware vRealize を使い始める方法について説明します。

Cisco ACI with VMware vRealize をインストールする前に、2.2(1) リリースの Cisco ACI と VMware vRealize ファイルをダウンロードして解凍します。

手順

ステップ 1 シスコの Application Policy Infrastructure Controller（APIC）Web サイトにアクセスします。

http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

ステップ 2 [All Downloads for this Product] を選択します。

ステップ 3 リリース バージョンと **apic-vrealize-2.2.1x.tgz** ファイルを選択します。

ステップ 4 [Download] をクリックします。

ステップ 5 **Apic-vrealize-2.2.1x.tgz** ファイルを解凍します。

（注）
Cisco ACI with VMware vRealize は ASCII 文字のみをサポートします。非 ASCII 文字はサポートしていません。

Cisco ACI with VMware vRealize を開始するための前提条件

開始する前に、vRealize のコンピューティング環境が以下の前提条件を満たしていることを確認します。

- vRealize Automation (vRA) リリース 7.0-7.4 がインストールされている必要があります

  Vmware の vRealize マニュアルを参照してください。

  vRA 8.x を使用することを強く推奨します。Cisco ACI との vRA 8.x 統合の詳細については、Cisco ACI vRealize 8 プラグイン ガイドを参照してください。

- vRealize ACI プラグインのバージョンと Cisco APIC のバージョンは一致する必要があります。

- テナントは vRealize Automation で設定し、ID ストアに関連付けます。テナントで「インフラ管理者」、「テナント管理者」、および「テナントユーザ」の役割を持つユーザを 1 人以上設定する必要があります。

  Vmware の vRealize マニュアルを参照してください。

- テナントで「ビジネス グループ」を 1 つ以上設定する必要があります。

  Vmware の vRealize マニュアルを参照してください。

- エンドポイントとして vRealize Orchestrator を設定します。

  Vmware の vRealize マニュアルを参照してください。

- エンドポイントとして vCenter を設定します。

  Vmware の vRealize マニュアルを参照してください。

- vCenter コンピューティング リソースを使用して「予約」を設定します。

  Vmware の vRealize マニュアルを参照してください。

- vRealize アプライアンスを設定します。

  Vmware の vRealize マニュアルを参照してください。

- レイヤ 3（L3）出力ポリシーがテナントによって消費される場合は、BGP ルート リフレクタを設定する必要があります。

  基本 GUI を使用して MP-BGP ルート リフレクタを設定する方法や、MP-BGP ルート リフレクタを設定する方法については、*Cisco APIC* ベーシック コンフィギュレーション ガイドを参照してください。

- vRO で vRA ハンドルを設定します。

  これは、ACI サービス カタログ ワークフローをインストールするために使用します。

- vRO で IAAS ハンドルを設定します。

  これは、ACI サービス カタログ ワークフローをインストールするために使用します。

  vRealize Orchestrator における IaaS ハンドルの設定 （8 ページ）を参照してください。

- vCO/vRO の vCAC/vRA カスタム プロパティ ツールキットをインストールします。このパッケージは次の URL からダウンロードできます。

  https://communities.vmware.com/docs/DOC-26693

- vRA の組み込み vRO にはデフォルトでインストールされる vCAC vRO プラグインがあります。スタンドアロンの vRO を使用する場合は、vCAC vRO プラグインをインストールする必要があります。このプラグインは次の URL からダウンロードできます:

  https://solutionexchange.vmware.com/store/products/vmware-vrealize-orchestrator-plug-in-for-vra-6-2-0

vRealize Orchestrator における IaaS ハンドルの設定

ここでは、vRealize Orchestrator（vRO）で Infrastructure as a Service（IaaS）ハンドルを設定する方法を説明します。

手順

ステップ 1 VMware vRealize Orchestrator に管理者としてログインします。

ステップ 2 VMware vRealize Ochestrator GUI が表示されたら、メニュー バーのドロップダウン リストから [Run] を選択します。

ステップ 3 [Navigation] ペインで、[Workflows] アイコンを選択します。

ステップ 4 **Adminstrator@*vra_name*** > **Library** > **vRealize Automation** > **Configuration** > **Add the IaaS host of a vRA host** を選択します。

ステップ 5 **Add the IaaS host of a vRA host** を右クリックして、**Start Workflow** を選択します。

ステップ 6 [Start Workflow: Add the IaaS host of a vRA host] ダイアログボックスで、次の操作を実行します。

a) **vRA host** フィールドに、vRealize ハンドルを入力します。
b) [Next] をクリックします。

ステップ 7 次の画面で、次の操作を実行します。

a) [Host Name] フィールドに、名前を入力します。
b) [Host URL] フィールドに、IaaS ホストの URL を入力します。
c) 残りのフィールドはデフォルト値を使用します。
d) [Next] をクリックします。

ステップ 8 次の画面で、次の操作を実行します。

a) [Session mode] ドロップダウン リストで、[Shared Session] を選択します。
b) [Authentication user name] フィールドに、認証ユーザ名を入力します。
c) [Authentication password] フィールドに、パスワードを入力します。
d) [Next] をクリックします。

ステップ 9 次の画面で、次の操作を実行します。

a) [Workstation for NTLM authentication] フィールドに、NTLM 認証に使用するワークステーションの名前を入力します。
b) [Domain for NTLM authentication] フィールドに、IaaS ホスト URL で使用するドメインを入力します。
c) [Submit] をクリックします。

Cisco ACI with VMware vRealize のインストール ワークフロー

ここでは、Cisco ACI with VMware vRealize のインストール ワークフローを説明します。

手順

ステップ 1 vRealize Orchestrator（vRO）に APIC プラグインをインストールします。

詳細については、vRealize オーケストレータでの APIC プラグインのインストール （9 ページ）を参照してください。

ステップ 2 VMware vRealize Automation アプライアンスを ACI 向けに設定します。

詳細については、「VMware vRealize Automation アプライアンスを ACI 向けに設定 （11 ページ）」を参照してください。

vRealize オーケストレータでの APIC プラグインのインストール

ここでは、vRealize オーケストレータに APIC プラグインをインストールする方法を説明します。

手順

ステップ 1 パッケージを展開したら、既知のディレクトリに **aci-vra-plugin-3.0.1000.N.dar** ファイルを保存します。

ステップ 2 SSH を使用して vRA アプライアンスに root としてログインし、以下を入力します。

```
$ ssh root@<vra_ip>
```

ステップ 3 コンフィギュレータを起動してコンフィギュレータ サービス Web インターフェイスを有効にし、次のコマンドを入力します。

```
# service vco-configurator start
.
.
.
Tomcat started.
```

```
Status:          Running as PID=15178
```

ステータスが実行中であることを確認します。

ステップ 4 Firefox ブラウザを使用して VMware アプライアンスにログインし、以下を入力します。

https://*applicance_address***:8283/vco-controlcenter**

（注）
Firefox ブラウザを使用することが推奨されます。

初回は、Internet Explorer や Chrome ブラウザを使用しないでください。デフォルトのユーザ名とパスワードを使用するときの既知の問題があります。適切にログインできません。

詳細については、https://communities.vmware.com/thread/491785を参照してください。

a) VMware vRealize Orchestrator Configuration GUI で、デフォルトのユーザ名とパスワード（vmware と vmware）を入力します。パスワードの変更を求められます。

ステップ 5 **Plug-Ins** セクションで、**Manage Plug-Ins** をクリックします。

ステップ 6 [Install plug-in] で、[Browse...] ボタンをクリックして、次の手順に従います:

a) aci-vra-plugin-3.0.1000.N.dar ファイルを保存した場所を検索して、aci-vra-plugin-3.0.1000.N.dar ファイルを選択します。

b) 右側の **Install** をクリックし、[Cisco APIC Plug-in] が表示されたら、**Install** をもう一度クリックします。

- プラグインがインストール中であることがメッセージが緑色でハイライト表示されます。
- 「The Orchestrator server must be restarted for the changes to take effect. The restart can be performed from the Startup Options page」というメッセージが黄色でハイライト表示されます。

ステップ 7 **Startup Options** をクリックします。

Startup Options ページにリダイレクトされます。

ステップ 8 **Restart** をクリックしてサーバを再起動します。[Current Status] に [RUNNING] と表示されるまで待ちます。

ステップ 9 **Manage Plug-Ins** ページに左上の **Home** をクリックして戻り、**Manage Plug-Ins** を **Plug-Ins** セクションでクリックします。

ステップ 10 Cisco APIC プラグインがインストール済みであるかどうかを **Plug-Ins** で確認します。

プラグインは最初の箇所に、Cisco のアイコンとともに表示されます。

VMware vRealize Automation アプライアンスを ACI 向けに設定

ここでは、VMware vRealize Automation アプライアンスを Cisco ACI 向けに設定する方法について説明しますCisco。

手順

ステップ 1 ブラウザを使用し、テナント ポータルを介して VMware vRealize Automation アプライアンスに管理者としてログインします。

https://*applicance_address***/vcac/org/***tenant_id*

例：

https://192.168.0.10/vcac/org/tenant1

管理者のユーザ名とパスワードを入力します。

ステップ 2 VMware vRealize Automation アプライアンス GUI で、次の操作を実行します。

a) **[Administration]** > **[Users & Groups]** > **[Custom Groups]** の順に選択します。
b) [Custom Group] ペインで [Add] をクリックして、カスタム グループを追加します。
c) カスタム グループの名前を入力します。（サービス アーキテクト）
d) [Roles to this group] フィールドで、前の手順で作成したカスタム グループを選択します。（サービス アーキテクト）
e) [Member] ペインを選択し、ユーザ名を入力して選択します。
f) [Add] をクリックします。
これにより、カスタム グループとメンバーが作成されます。
g) [Custom Group] ペインで、作成したカスタム グループを選択します。（サービス アーキテクト）
h) [Edit Group] ペインでは、[Members] ペインでメンバーを確認できます。

ステップ 3 ブラウザで、VMware vRealize Automation アプライアンスを入力します。

https://*applicance_address*

次に例を示します。

https://vra3-app.ascisco.net

a) [vRealize Orchestrator Client] を選択して client.jnlp ファイルをダウンロードします。
b) [Downloads] ダイアログボックスが表示され、**client.jnlp** ファイルが起動します。

ステップ 4 VMware vRealize Orchestrator に管理者としてログインします。

ステップ 5 VMware vRealize オーケストレータ GUI が表示されたら、メニュー バーのドロップダウン リストから **Run** を選択します。

ステップ 6 [Navigation] ウィンドウで、[Workflows] アイコンを選択します。

ステップ 7 **[Adminstrator@vra3-app.ascisco.net]** > **[Cisco APIC Workflows]** > **[Utils]** > **[Install ACI Service Catalog]** の順に選択します。

ステップ 8 [Install ACI Service Catalog] を右クリックして [Start Workflow] を選択します。

ステップ 9 [Start Workflow - Install ACI Service Catalog] ダイアログボックスで、次の操作を実行します。

a) **APIC Hostname/IP Address** フィールドに、APIC のホスト名または IP アドレスを入力します。

b) **APIC Admin Password** フィールドに、APIC の admin パスワードを入力します。

c) **vRealize Automation IP Address** フィールドに、vRA の IP アドレスを入力します。

d) **vRealize Automation handle** フィールドで、**Not set** をクリックして、アプライアンスの vRealize 自動化ハンドルを選択します。

e) **Business group** フィールドで、**Not set** をクリックして、ビジネス グループを選択します。

（注）
vRealize 7.0 を実行している場合には、**Business Group** を **Business Group から選択します (これは廃止されました)**。

（注）
ユーザ名には、ドメイン名を含める必要があります。たとえば admin1@vsphere.local のようにします。

f) **Admin User** フィールドに、テナントの管理者ユーザを入力します。

g) **vRealize Automation Admin Password** フィールドに、 vRA 管理者のパスワードを入力します。

h) **End users** フィールドで、**Not set** をクリックして、権限を有効にするユーザ名を入力します。

（注）
ユーザ名はコピー アンド ペーストではなく、直接入力してください。

i) **JSON File containing vRealize Properties** フィールドで、**Not set** をクリックして、vRealize プロパティを含む JSON ファイルに移動して選択します。(aci-vra-properties-3.0.1000.x.json)

（注）
ユーザ名には、ドメイン名を含める必要があります。たとえば admin1@vsphere.local のようにします。

j) **Zip file containing the service blueprints** フィールドで、**Not set** をクリックして、サービス ブループリントを含む zip ファイルに移動して選択します。(aci-vra-asd-3.0.1000.x.zip)

k) [Submit] をクリックします。

ステップ 10 インストールが成功した場合、**Navigation** ウィンドウで、**Install ACI Service Catalog** の横に緑色のチェックマークが表示されます。

ステップ 11 [Navigation] ウィンドウで、[Workflows] アイコンを選択します。

ステップ 12 **Install ACI Property Definitions** を右クリックして、**Start Workflow** を選択します。

ステップ 13 **Start Workflow - Install ACI Property Definitions** ダイアログボックスで、**Net set** をクリックし、IaaS ホストに移動して選択します。

a) [Submit] をクリックします。

インストールが成功した場合、**Navigation** ウィンドウの [Install ACI Property Definitions] の横に緑色のチェックマークが表示されます。

ステップ 14 テナントとして確認するには、vRealize Automation アプライアンスにテナントとしてログインして、**Catalog** を選択します。サービスが表示されます。

ステップ 15 管理者として確認するには、vRealize Automation アプライアンスに管理者としてログインして、**Catalog** を選択します。サービスが表示されます。

a) **Infrastructure** > **Blueprints** > **Property Definitions** を選択します。プロパティが表示されます。

ACI の初回操作

ここでは、ACI の初回操作について説明します。

始める前に

- ファブリックの起動

  ファブリックを開くとすべてのトポロジがサポートされます。

- アクセス ポリシー
  - アタッチ エンティティ ポリシー（AEP）
  - リーフ スイッチと ESXi ホスト間のアクセス ポリシーを設定し、リーフとホスト間で CDP および LLDP を有効にします。
- レイヤ 3（L3）out 設定
  - 消費されるユーザ テナントにする共通テナントで L3 Out 設定を作成します。
  - L3 ポリシーには任意の名前を選択できます。
  - 外部 EPG は、「[L3OutName|InstP]」という名前にする必要があります。
  - 2 つのポリシーを作成します。

    共有プランには「default」を指定し、VPC プランには「vpcDefault」を指定します。

    詳細については、L3 外部接続について （44 ページ）を参照してください。
- サービス グラフ テンプレートとデバイス

  共通テナントでサービス グラフ デバイスを作成します。

  詳細については、XML POST を使用した APIC でのサービスの設定 （41 ページ）を参照してください。
- セキュリティ ドメインとテナント ユーザ
  - vRealize プラグインには、2 つのユーザ アカウントが必要です。

    最初のアカウントには管理者権限が必要です。このアカウントでは、テナント共通、アクセス ポリシー、VMM ドメインでオブジェクトを作成、読み取り、更新、および廃棄できます。

2番目のアカウントには、制限されたテナント権限が必要です。このアカウントでは、共通テナントおよびVMMドメインの読み取りのみ行うことができます。ただし、独自のテナントではオブジェクトを作成、読み取り、更新、および廃棄できます。

- ロールベース アクセス コントロール （RBAC） ルールは、プラグインではなく、APIC によって実施されます。

手順

詳細については、*Cisco APIC* ベーシック コンフィギュレーション ガイドを参照してください。

VMware VMM ドメインと AEP の関連付け

このセクションでは、接続可能エンティティ プロファイル（AEP）を VMware VMM ドメインに関連付ける方法について説明します。

（注） ドメイン タイプが Cisco AVS の場合は、この手順を実行する必要はありません。

手順

ステップ 1 APIC GUI にログインし、**Fabric** > **Access Policies** を選択します。

ステップ 2 ナビゲーション ウィンドウで、**Policies** > **Global** > **Attachable Access Entity Profiles**を展開し、***profile*** をクリックします。

ステップ 3 作業ウィンドウで、次の操作を実行します:

a) **Domains (VMM, Physical or External) Associated to Interfaces** フィールドで、**+** をクリックして展開します。

b) **unformed** フィールドで、VMM ドメインを選択し、**Update** をクリックします。

Cisco ACI with VMware vRealize アップグレード ワークフロー

ここでは、Cisco ACI with VMware vRealize のアップグレード ワークフローを説明します。

手順

ステップ 1 APIC イメージをアップグレードします。

ステップ 2 vRealize Orchestrator（vRO）で APIC プラグインをアップグレードします。

詳細については、vRealize Orchestrator での APIC プラグインのアップグレード （15 ページ）を参照してください。

ステップ 3 VMware vRealize Automation アプライアンスを ACI 向けに設定します。

詳細については、VMware vRealize Automation アプライアンスを ACI 向けに設定 （11 ページ）を参照してください。

ステップ 4 APIC と vRealize 間の接続を確認します。

詳細については、「APIC と vRealize 間の接続の確認 （15 ページ）」を参照してください。

vRealize Orchestrator での APIC プラグインのアップグレード

このセクションでは、vRealize Orchestrator で APIC プラグイン証明書をアップグレードする方法について説明します。

手順

ステップ 1 アップグレードするには、 vRealize オーケストレータでの APIC プラグインのインストール （9 ページ） の指示に従ってください。

ステップ 2 サービス ブループリント、サービス カテゴリおよびエンタイトルメントをアップグレードします。VMware vRealize Automation アプライアンスを ACI 向けに設定 （11 ページ）を参照してください。

APIC と vRealize 間の接続の確認

Application Policy Infrastructure Controller（APIC）コントローラとスイッチ ソフトウェアをアップグレードしたら、vRealize Orchestrator から APIC への接続を確認する必要があります。

始める前に

- APIC コントローラとスイッチ ソフトウェアがアップグレードされていることを確認します。

  詳細については、『*Cisco ACI Firmware Management Guide*』を参照してください。

手順

ステップ 1 vRealize Orchestrator に管理者としてログインします。

ステップ 2 [Navigation] ペインで、[Inventory] アイコンを選択します。

ステップ 3 [Cisco APIC Plugin] を展開して APIC を選択し、以下を確認します。

a) [General] ペインで、[Name] フィールドにコントローラが表示されているかどうかを確認します

b) APIC の下でネストされた階層を制御できるかどうかを確認します。これにより、APIC と通信していることを確認できます。

vRO から APIC への接続が確立されていない場合、APIC 名の横に文字列 **down** が表示され、接続がダウンしていることが示されます。

Cisco ACI with VMware vRealize ダウングレードのワークフロー

ここでは、Cisco ACI with VMware vRealize のダウングレード ワークフローを説明します。

手順

ステップ 1 APIC イメージをダウングレードします。

ステップ 2 APIC プラグイン パッケージとすべての APIC のワークフローを削除します。

詳細については、パッケージとワークフローの削除 （17 ページ）を参照してください。

ステップ 3 vRealize Orchestrator (vRO) に APIC プラグインをインストールします。

詳細については、vRealize Orchestrator での APIC プラグインのアップグレード （15 ページ）を参照してください。

ステップ 4 VMware vRealize Automation アプライアンスを ACI 向けにセットアップします。

詳細については、VMware vRealize Automation アプライアンスを ACI 向けに設定 （11 ページ）を参照してください。

ステップ 5 APIC と vRealize 間の接続を確認します。

詳細については、「APIC と vRealize 間の接続の確認 （15 ページ）」を参照してください。

パッケージとワークフローの削除

ここでは、パッケージとワークフローの削除方法について説明します。

手順

ステップ 1 管理者として vRO クライアントにログインします。

ステップ 2 [Design] ロールを選択します。

ステップ 3 [Packages] タブを選択します。

ステップ 4 [com.cisco.apic.package] を右クリックし、[Delete element with content] を選択します。

ステップ 5 ポップアップ ウィンドウで [Keep Shared] を選択します。

ステップ 6 [Workflows] タブを選択します。

ステップ 7 「Cisco APIC workflows」フォルダとサブフォルダ内のすべてのワークフローが削除されたことを確認します。

ワークフローを削除するには、そのワークフローを選択し、右クリックして、[Delete] を選択します。

管理者とテナント エクスペリエンスのユース ケース シナリオ

ここでは、管理者とテナントエクスペリエンスのユース ケース シナリオについて説明します。

層アプリケーション導入の概要

ここでは、3 層アプリケーション導入の概要を説明します。

プロパティ グループを使用した単一層アプリケーションの導入	構成プロファイルを使用した単一層アプリケーションの導入（17 ページ）を参照してください。
複数マシン ブループリントを使用した 3 層アプリケーションの導入	「マルチマシン ブループリントを使用した 3 層 アプリケーションの導入 （20 ページ）」を参照してください。

構成プロファイルを使用した単一層アプリケーションの導入

ここでは、プロパティ グループを使用して単一階層アプリケーションを導入する方法を説明します。

手順

ステップ 1 次の URL をブラウザに入力して、vRealize Automation アプライアンスに接続します。

`https://appliance_address/vcac/org/tenant_id`

ステップ 2 テナント管理者のユーザ名とパスワードを入力します。

ステップ 3 [Catalog] を選択します。

ステップ 4 **Configure Property Group** をクリックします。

データベース層を設定します。

ステップ 5 [Request] をクリックします。

ステップ 6 [Request Information] タブで、要求の説明を入力します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Common] タブで、次の操作を実行します。

a) [IaaS Host for vRealize] フィールドで [Add] をクリックします。

b) 必要な IaaS ホストの横のボックスにチェックマークを付けます。

c) [Submit] をクリックします。

d) [APIC Tenant] フィールドで [Add] をクリックします。

e) ***apic_name*** > **Tenants** の順に展開します。

f) 必要なテナント名の横のボックスにチェックマークを付けます。

例：

```
green
```

g) [Submit] をクリックします。

h) [Property Group Name] フィールドに、新しいグループの名前を入力します。

例：

```
green-app-bp
```

i) **Plan Type (Shared or VPC)** フィールドで **Shared** をクリックします。

j) [VMM Domain/DVS] フィールドで [Add] をクリックします。

k) ***[apic_name]*** > **[Vcenters]** > ***[vcenter_name]*** の順に展開します。

l) 必要な vCenter 名の横のボックスにチェックマークを付けます。

例：

```
green
```

m) [Submit] をクリックします。

ステップ 9 [Next] をクリックします。

ステップ 10 [VM Networking] タブで、すべてのフィールドをデフォルト値のままにします。

ステップ 11 [Next] をクリックします。

ステップ 12 [Security] タブで、次の操作を実行します。

a) **Configure Security Policy**ドロップダウン リストで **No** を選択します。

ステップ 13 **Load Balancer** タブで、ドロップダウン リストから **No** を選択します。

ステップ 14 **Firewall** タブで、ドロップダウン リストから **No** を選択します。

ステップ 15 [送信（Submit）] をクリックします。

ステップ 16 [OK] をクリックします。

ステップ 17 要求を確認するには、[Requests] タブを選択します。

a) 送信した要求を選択し、[view details] をクリックします。ステータスが [Succesful] であることを確認します。

ステップ 18 （オプション）ビルド プロファイルでブループリントを編集するには、**Infrastructure** > **Blueprints** > **Property Groups** の順に選択します。

a) **Property Group**ペインで、作成したビルドプロファイル（green-app-bp）を選択して、**edit** をクリックします。

b) **Edit Property Group**ペインで、編集するビルドプロファイルを選択し、鉛筆アイコンをクリックして特定のブループリントを編集します。

c) 編集が完了したら、[OK] をクリックします。

ステップ 19 ビルド プロファイルを VM にアタッチして、**Infrastructure** > **Blueprints** の順に選択します。

ステップ 20 **Blueprints** ペインで、ドロップダウン リストから **New Blueprint** をクリックして、**Virtual** > **vSphere (vCenter)** の順に選択します。

ステップ 21 [New Blueprint vSphere (vCenter)] ペインで、次の操作を実行します。

a) [Blueprint Information] タブで、ブループリントを作成するための情報を入力して [OK] をクリックします。マシン ブループリントを作成する方法の詳細については、VMware のドキュメントを参照してください。

b) **Build Information** タブで、ビルドプロファイルを作成するための情報を入力して **OK** をクリックします。マシン ブループリントを作成する方法の詳細については、VMware のドキュメントを参照してください。

ステップ 22 **Properties** タブで、次の操作を実行します。

a) **Property Group**フィールドで、作成したプロパティ グループ（green-app-bp）を選択して、**OK**をクリックします。

b) 新しく作成したプロパティ グループ（green-app-bp）の虫眼鏡アイコンをクリックします。

c) **Property Group Custom Properties**ダイアログボックスで、プロパティがビルドプロファイルと一致することを確認します。これにより、VM および ACI ネットワークとの接続が作成されます。

d) **New Blueprint vSphere (vCenter)** ペインで **OK** をクリックします。

ステップ 23 **Blueprints** ペインで、次の操作を実行します。

a) 作成したビルドプロファイル（green-app-bp）を選択し、カーソルを当てて **Publish** を選択します。

b) [OK] をクリックします。

c) **Aministration** > **Catalog Management** > **Catalog Items** の順に選択します。

ステップ 24 **Catalog Items** ペインで、次の操作を実行します。

a) 作成したブループリント（green-app-bp）を探して選択します。

ステップ 25 **Configure Catalog Item** ペインで、次の操作を実行します。

a) **Details** タブの **Service** フィールドで **VM Services**を選択します。

b) **New and noteworthy** チェックボックスをオンにします。

c) [Update] をクリックします。

これで、プロパティ グループを使用して単一階層アプリケーションが導入されました。

ステップ 26 単一階層アプリケーションの導入を確認するには、管理者セッションをログアウトして、テナントとしてログインし直します。

a) **Catalog** タブをクリックします。

b) **navigation** ペインで **VM Services** を選択します。

c) **Work** ペインで、作成したブループリントを選択します。

d) **Catalog Item Details**ペインで、ブループリントのプロパティを確認して **Request** をクリックします。

e) **New Request**ペインで **Submit**をクリックしてから **OK**をクリックします。

これにより、新しい仮想マシンである ACI ネットワークがプロビジョニングされ、両者が接続されます。

マルチマシン ブループリントを使用した 3 層 アプリケーションの導入

VMware vRealize マルチマシン ブループリントは、同時に導入する 1 台以上のマシン ブループリントが属するグループです。一般的な使用例は、Web 層、アプリケーション層、データベース層が一緒に導入される 3 層型 Web アプリケーションです。ネットワークの観点から、アプリケーション ポリシーを Cisco Application Centric Infrastructure（ACI）にプッシュして、通信する必要がある層間で安全な通信を有効にする必要があります。これは、セキュリティ ポリシーを作成し、展開時に関連するマシンを動的に関連付けることによって実現されます。

マルチマシン ブループリントで使用されるブループリントを設定する際には、セキュリティ ポリシーを作成する必要があります。作成プロセスで、消費側と提供側を指定する必要があります。提供側には、構築中のマシンを必ず指定します。消費側には他のマシンやネットワークを指定できます。

例として、ポート 3306 でサービスを提供する MySQL データベース マシン ブループリントがあるとします。アプリケーション層のマシンはこのデータベースにアクセスする必要がありますが、Web 層のマシンはその必要はありません。**Configure Property Group**ワークフローの **Security Policy**セクションで、「アプリケーション」層を消費側とするポリシーを作成し、ポート 3306 を許容（デフォルトでは、他のすべてが拒否される）としてリストすると、ブループリントは自動的に「db」層をプロバイダーとして配置します。

「アプリケーション」層はサービスも提供する必要があります。この例では、サーバはポート 8000 でリッスンします。このサービスは、Web 層が消費します。セキュリティ ポリシーは、「アプリ」層のビルド プロファイルで指定する必要があります。

（注） マシンプレフィクスにより、導入される各仮想マシンに一意の名前が生成されます。「Green」というテナントのプレフィクス例は、「green-web-」にマシンごとの 3 つの固有の数字を加えたものです。シーケンスは「green-web-001」、「green-web-002」、「green-web-003」のようになります。Application Policy Infrastructure Controller（APIC）プラグインが消費側エンドポイント グループ名を正確に予測できるように、マシン プレフィクスと同様のスキームに従うことが重要です。また、各マシンは同じプレフィックス番号である必要があります。たとえば、3 層アプリケーションの名前は、green-db-001、green-app-001、green-web-001 である必要があります。いずれかの層が整合していない場合、セキュリティ ポリシーは正確な関係を形成しません。vRealize では兄弟階層の名前が提供されず、プラグインは独自の名前に基づいて兄弟の名前を推測する必要があるため、これは必要条件です。

ビルド プロファイルでセキュリティ ポリシーを設定するときは、コンシューマ名がマシン プレフィクスの第 2 文字である必要があります。プレフィクス例の「green-web-」では、コンシューマ名は「web」です。

ここでは、マルチマシン ブループリントを使用して 3 層 アプリケーションを導入する方法を説明します。

手順

ステップ 1 次の URL をブラウザに入力して、vRealize Automation アプライアンスに接続します。

`https://appliance_address/vcac/org/tenant_id`

ステップ 2 テナント管理者のユーザ名とパスワードを入力します。

ステップ 3 [Catalog] を選択します。

ステップ 4 [Configure Property Group] をクリックします。

データベース層を設定します。

ステップ 5 [Request] をクリックします。

ステップ 6 [Request Information] タブで、要求の説明を入力します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Common] タブで、次の操作を実行します。

a) [IaaS Host for vRealize] フィールドで [Add] をクリックします。
b) 必要な IaaS ホストの横のボックスにチェックマークを付けます。
c) [Submit] をクリックします。
d) [APIC Tenant] フィールドで [Add] をクリックします。
e) ***apic_name*** > **Tenants** の順に展開します。
f) 必要なテナント名の横のボックスにチェックマークを付けます。

例：

`green`

g) [Submit] をクリックします。
h) [Property Group Name] フィールドに、新しいグループの名前を入力します。

例：

```
green-db-mm
```

i) [VMM Domain/DVS] フィールドで [Add] をクリックします。
j) ***[apic_name]*** > **[Vcenters]** > ***[vcenter_name]*** の順に展開します。
k) 必要な vCenter 名の横のボックスにチェックマークを付けます。

例：

```
green
```

l) [Submit] をクリックします。

ステップ 9 [Next] をクリックします。
ステップ 10 [VM Networking] タブで、すべてのフィールドをデフォルト値のままにします。
ステップ 11 [Next] をクリックします。
ステップ 12 [Security] タブで、次の操作を実行します。

a) [Configure Security Policy] ドロップダウン リストで [Yes] を選択します。
b) [Consumer Network/EPG Name of Security Policy] フィールドに、完全なマシン プレフィクスなしでコンシューマ ネットワークの名前を入力します。

例：

```
app
```

データベース層には、消費側としてアプリケーション層が必要です。

c) [Starting Port Number in Security Policy] フィールドに、開始ポート番号を入力します。

例：

```
3306
```

d) [Ending Port Number in Security Policy] フィールドに、終了ポート番号を入力します。

例：

```
3306
```

e) 他のフィールドについては、値をデフォルトのままにします。

ステップ 13 [Next] をクリックします。
ステップ 14 [Load Balancer] タブで、フィールドをデフォルト値のままにします。
ステップ 15 [Next] をクリックします。
ステップ 16 [Firewall] タブで、フィールドをデフォルト値のままにします。
ステップ 17 [送信（Submit）] をクリックします。
ステップ 18 [OK] をクリックします。
ステップ 19 [Configure Property Group] をクリックします。

今回は、アプリケーション層を設定します。

ステップ 20 [Request] をクリックします。

ステップ 21 [Request Information] タブで、要求の説明を入力します。

ステップ 22 [Next] をクリックします。

ステップ 23 [Common] タブで、次の操作を実行します。

a) [IaaS Host for vRealize] フィールドで [Add] をクリックします。
b) 必要な IaaS ホストの横のボックスにチェックマークを付けます。
c) [Submit] をクリックします。
d) [APIC Tenant] フィールドで [Add] をクリックします。
e) ***apic_name*** > **Tenants** の順に展開します。
f) 必要なテナント名の横のボックスにチェックマークを付けます。

例：

```
green
```

g) [Submit] をクリックします。
h) [Property Group Name] フィールドに、新しいグループの名前を入力します。

例：

```
green-app-mm
```

i) [VMM Domain/DVS] フィールドで [Add] をクリックします。
j) ***[apic_name]*** > **[Vcenters]** > ***[vcenter_name]*** の順に展開します。
k) 必要な vCenter 名の横のボックスにチェックマークを付けます。

例：

```
green
```

l) [Submit] をクリックします。

ステップ 24 [Next] をクリックします。

ステップ 25 [VM Networking] タブで、すべてのフィールドをデフォルト値のままにします。

ステップ 26 [Next] をクリックします。

ステップ 27 [Security] タブで、次の操作を実行します。

a) [Configure Security Policy] ドロップダウン リストで [Yes] を選択します。
b) [Consumer Network/EPG Name of Security Policy] フィールドに、完全なマシン プレフィクスなしでコンシューマ ネットワークの名前を入力します。

例：

```
web
```

アプリケーション層には、消費側として Web 層が必要です。

c) [Starting Port Number in Security Policy] フィールドに、開始ポート番号を入力します。

例：

```
8000
```

d) [Ending Port Number in Security Policy] フィールドに、終了ポート番号を入力します。

例：

```
8000
```

e) 他のフィールドについては、値をデフォルトのままにします。

ステップ 28 [Next] をクリックします。

ステップ 29 [Load Balancer] タブで、フィールドをデフォルト値のままにします。

ステップ 30 [Next] をクリックします。

ステップ 31 [Firewall] タブで、フィールドをデフォルト値のままにします。

ステップ 32 [送信（Submit）] をクリックします。

ステップ 33 [OK] をクリックします。

ステップ 34 [Configure Property Group] をクリックします。

Web 層を設定します。

ステップ 35 [Request] をクリックします。

ステップ 36 [Request Information] タブで、要求の説明を入力します。

ステップ 37 [Next] をクリックします。

ステップ 38 [Common] タブで、次の操作を実行します。

a) [IaaS Host for vRealize] フィールドで [Add] をクリックします。
b) 必要な IaaS ホストの横のボックスにチェックマークを付けます。
c) [Submit] をクリックします。
d) [APIC Tenant] フィールドで [Add] をクリックします。
e) ***apic_name*** > **Tenants** の順に展開します。
f) 必要なテナント名の横のボックスにチェックマークを付けます。

例：

```
green
```

g) [Submit] をクリックします。
h) [Property Group Name] フィールドに、新しいグループの名前を入力します。

例：

```
green-web-mm
```

i) [VMM Domain/DVS] フィールドで [Add] をクリックします。
j) ***[apic_name]*** > **[Vcenters]** > ***[vcenter_name]*** の順に展開します。
k) 必要な vCenter 名の横のボックスにチェックマークを付けます。

例：

```
green
```

l) [Submit] をクリックします。

ステップ 39 [Next] をクリックします。

ステップ 40 [VM Networking] タブで、すべてのフィールドをデフォルト値のままにします。

ステップ 41 [Next] をクリックします。

ステップ 42 **Security** タブで、フィールドをデフォルト値のままにします。

これは消費側ポリシーであるため、セキュリティ ポリシーを設定する必要はありません。

ステップ 43 [Next] をクリックします。

ステップ 44 [Load Balancer] タブで、フィールドをデフォルト値のままにします。

ステップ 45 [Next] をクリックします。

ステップ 46 [Firewall] タブで、フィールドをデフォルト値のままにします。

ステップ 47 [送信（Submit）] をクリックします。

ステップ 48 **[OK]** をクリックします。

プラン タイプについて

管理者は独自の価値観でプランを作成します。プラン タイプは次のとおりです。

	共有インフラストラクチャ	仮想プライベート クラウド（VPC）
分離ネットワーク	はい	○
ファイアウォール	はい	○
プロバイダー DHCP	はい	○
共有ロード バランサ	はい	○
パブリック インターネット アクセス	はい	○
テナント間共有サービス	はい	○
独自のアドレス空間（プライベート アドレス空間）と DHCP サーバの保持	いいえ	はい

vRealize サービスのカテゴリとカタログ項目について

ここでは、vRealize サービスのカテゴリとカタログ項目について説明します。すべての項目のリストは各サービスにグループ化され、各サービスにエンタイトルメントが割り当てられています。ACI エンタイトルメントは特定のユーザに割り当てられます。

詳細については、 vRealize の ACI 管理者サービス （28 ページ）を参照してください。

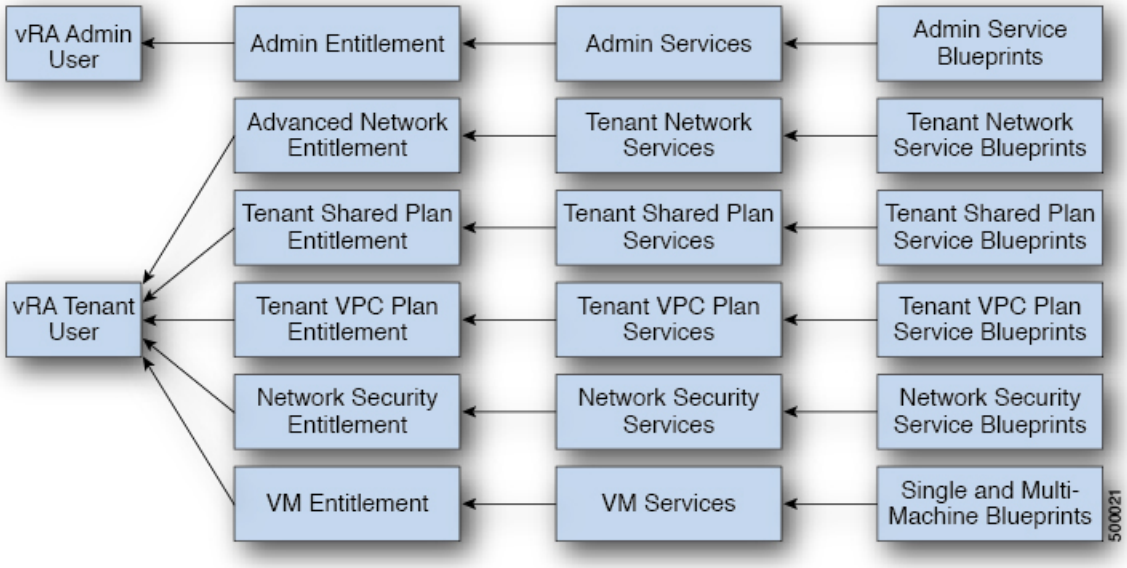
詳細については、vRealize の ACI テナント サービス （31 ページ）を参照してください。

詳細については、 vRealize における ACI カタログ項目向けエンタイトルメント （37 ページ）を参照してください。

ACI プラン タイプと vRealize サービス カテゴリのマッピング

ここでは、Cisco ACI プラン タイプと vRealize サービス カテゴリのマッピングを示します。

図 *3: vRA* - ユーザ、エンタイトルメント、サービス、およびブループリント



vRA カタログ カテゴリ	ブループリント一覧
管理サービス ブループリント	Add APIC with Admin credentials Add APIC with Tenant credentials Add Provider for Shared Service (Contract) Add or Update Tenant Add VIP Pool Add VMM Domain, AVS Local Switching with Vlan Encap Add VMM Domain, AVS Local Switching with Vxlan Encap Add VMM Domain, AVS No Local Switching Add VMM Domain, AVE Local Switching with Vlan Encap Add VMM Domain, AVE Local Switching with Vxlan Encap Add VMM Domain, AVE No Local Switching Add VMM Domain, DVS and Vlan Pool Add or Delete Bridge Domain in Tenant-common Add or Delete Consumer for Shared Service (Contract) Add or Delete L3 context (VRF) in Tenant-common Add or Delete Router Id Add or Delete Subnets in Bridge Domain for Tenant-Common Update FW Policy (DFW) association to AVS or AVE VMM Domain Configure Property Group Create FW Policy (DFW) and Associate to AVS or AVE VMM Domain Delete APIC Delete FW Policy (DFW) Delete Provider Shared Service (Contract) Delete Tenant Delete VIP Pool Delete VMM Domain, AVS or AVE, and VLAN, Multicast Pool Delete VMM Domain, DVS and Vlan Pool Generate and Add Certificate to APIC Rest API Update FW Policy (DFW) AVS or AVE Update Vlan Pool, AVS or AVE Update Multicast Pool, AVS Update VMM Domain DVS security domain mapping Update AVS or AVE VMM Domain Security Domain Mapping
テナント共有プラン サービス ブループリント	Add a Useg Network - Shared Plan Add FW and LB to Tenant Network - Shared Plan Add FW to Tenant Network - Shared Plan Add Loadbalancer to Tenant Network - Shared plan Add Tenant Network - Shared plan Delete a Useg Network - Shared Plan Delete FW and LB from Tenant Network - Shared Plan Delete FW from Tenant Network - Shared Plan Delete Loadbalancer from Tenant Network - Shared Plan Delete Tenant Network - Shared plan
テナントVPCプランサービス ブループリント	Add a Useg Network - VPC Plan Add FW and LB to Tenant Network - VPC Plan Add FW to Tenant Network - VPC Plan Add Loadbalancer to Tenant Network - VPC plan Add Tenant Network - VPC plan Delete a Useg Network - VPC Plan Delete FW and LB from Tenant Network - VPC Plan Delete Loadbalancer from Tenant Network - VPC Plan Delete Tenant Network - VPC plan
ネットワーク セキュリティ サービス ブループリント	Add Security Policy (Contracts) Delete Security Policy (Contracts) Update Access List Security Rules

vRA カタログ カテゴリ	ブループリント一覧
テナント ネットワーク サービス ブループリント	Add or Delete Bridge domain in Tenant Add or Delete L3 Context (VRF) in Tenant Add or Delete Subnets in Bridge domain Add or Delete Useg Attribute Attach or Detach L3 external connectivity to Network Update Tenant Network

vRealize の ACI 管理者サービス

ここでは、vRealize の ACI 管理者サービスについて説明します。

ACI 管理者サービス向けの管理者サービス カタログ項目の一覧

ここでは、ACI 管理者サービスの管理者サービス カタログ項目の一覧を示します。

カタログ項目	説明
テナント クレデンシャルでの APIC の追加	テナント クレデンシャルで Application Policy Infrastructure Controller（APIC）ハンドルを作成します。
管理者クレデンシャルでの APIC の追加	管理者クレデンシャルで APIC ハンドルを作成します。
テナント共通のブリッジ ドメインの追加または削除	テナント共通のブリッジ ドメインを追加または削除します。
共有サービス（契約）のコンシューマの追加または削除	共有サービス（契約）のコンシューマを追加または削除します。
テナント共通の L3 コンテキスト（VRF）の追加または削除	テナント共通のレイヤ 3 コンテキスト（VRF）を追加または削除します。
テナント共通のブリッジ ドメインのサブセットの追加または削除	テナント共通のブリッジ ドメインのサブセットを追加または削除します。
共有サービス（契約）のプロバイダーの追加	共有サービス（契約）のプロバイダーを追加します。
ルータ ID の追加または削除	ルータ ID を追加または削除します。

カタログ項目	説明
テナントの追加または更新	これにより、テナントを追加または更新します。 テナントが EPG の間のファイアウォールを使用する場合は、[Enable inter-EPG Firewall] を **Yes** に設定します。アプリケーション層の階層数も設定する必要があります。一般的な 3 層 web、アプリ、db アプリケーションを使用する場合には、階層数は **3** に設定します。
VIP プールの追加	仮想 IP プールを追加します。
プロパティ グループの設定	これによりプロパティグループを設定します。
[削除（Delete）]APIC	APIC を削除します。
プロバイダー共有サービス（契約）の削除	プロバイダー共有サービス（契約）を削除します。
テナントの削除	テナントを削除します。
VIP プールの削除	仮想 IP プールを削除します。
証明書を生成して APIC に追加します。	このブループリントは、特定のユーザの証明書を生成するために使用できます。その後、この証明書は、APIC への証明書ベースのアクセスで使用できます。
REST API	REST API です。

ここでは、VMM ドメイン タイプが DVS の ACI 管理者サービスの管理者サービス カタログ項目のリストを示します。

カタログ項目	説明
VMM ドメイン、DVS および VLAN プールの追加	VMM ドメイン、DVS および VLAN プールを追加します。 APIC で vCenter に DVS が作成された、データセンター内のすべてのホストに、少なくとも 1 つの物理 NIC が接続されていること確認します。これにより、DVS のポート グループが仮想NIC の配置に使用できるようになります。
VMM ドメイン、DVS および VLAN プールの削除	VMM ドメイン、DVS および VLAN プールを削除します。

カタログ項目	説明
VLAN プール（encap ブロック）の更新	VLAN プール（encap ブロック）を更新します。
VMM ドメイン DVS セキュリティ ドメイン マッピングの更新	VMM ドメイン DVS セキュリティ ドメイン マッピングを更新します。

このセクションには、VMM ドメインタイプ Cisco AVS または Cisco ACI Virtual Edge (AVE) 向けの ACI 管理者サービス用の、管理者サービス カタログ項目のリストを示します。

カタログ項目	説明
Add VMM Domain, AVS or AVE Local Switching with Vlan Encap	これは、デフォルトのカプセル化モードを VLAN とする VMM ドメインを Cisco APIC 内に作成します。また、VLAN プールと (混合モード時の) マルチキャスト アドレス プールを作成します。この項目はまた、vCenter 内のローカル スイッチングと関連付けられている Cisco AVS または Cisco ACI Virtual Edge も作成します。
Add VMM Domain, AVS or AVE Local Switching with Vxlan Encap	これは、デフォルトのカプセル化モードを VXLAN とする VMM ドメインを Cisco APIC 内に作成します。また、マルチキャスト アドレス プールと (混合モード時の) VLAN プールを作成します。この項目はまた、vCenter 内のローカル スイッチングと関連付けられている Cisco AVS または Cisco ACI Virtual Edge も作成します。
Add VMM Domain, AVS or AVE No Local Switching	これは、Cisco APIC 内に VMM ドメイン、マルチキャスト アドレス プールを追加し、vCenter のローカル スイッチングに関連付けられていない Cisco AVS または Cisco ACI Virtual Edge を作成します。
Update Multicast Pool, AVS or AVE	これは、Cisco AVS または Cisco ACI Virtual Edge VMM ドメインのマルチキャスト プールを更新します。
Update VLAN Pool, AVS or AVE	これは、Cisco AVS または Cisco ACI Virtual Edge VMM ドメインの VLAN プールを更新します。
Update AVS or AVE VMM Domain Security Domain Mapping	これは、Cisco AVS または Cisco ACI Virtual Edge VMM ドメインのセキュリティドメイン マッピングを更新します。

カタログ項目	説明
Delete VMM Domain AVS or AVE, Vlan, Multicast Pool	これは、Cisco APIC の Cisco AVS または Cisco ACI Virtual Edge VMM ドメインおよび VLAN プール およびマルチキャスト プールを削除し、vCenter の関連付けられている Cisco AVS または Cisco ACI Virtual Edge を削除します。
Create FW Policy (DFW) and Associate to AVS or AVE VMM Domain	これは、分散型ファイアウォール ポリシーを作成し、Cisco AVS または Cisco ACI Virtual Edge VMM ドメインに関連付けます。
Update FW Policy (DFW) association to AVS or AVE VMM Domain	これは、既存の分散ファイアウォールポリシーを Cisco AVS または Cisco ACI Virtual Edge VMM ドメインに関連付けます。または関連づけを解除します。
Update FW Policy (DFW)	既存の分散ファイアウォール ポリシーを更新します。
Delete FW Policy (DFW)	既存の分散ファイアウォール ポリシーを削除します。

要求を送信するには、次の手順を実行します。

1. 管理者として vRealize Automation にログインし、**[カタログ（Catalog）]**>**[会管理サービス（Admin Services）]**を選択します。
2. 要求を選択し、フィールドに情報を入力して、**Submit** をクリックします。

要求を表示するには、次の手順を実行します。

1. vRealize Automation の GUI で [Requests] を選択します。
2. 送信した要求を選択し、[view details] をクリックします。

vRealize の ACI テナント サービス

ここでは、vRealize の ACI テナント サービスについて説明します。

ACI テナント サービス向けネットワーク セキュリティ カタログ項目一覧

ここでは、ACI テナント サービスのネットワーク セキュリティ カタログ項目の一覧を示します。

カタログ項目	説明
セキュリティ ポリシーの追加（契約）	テナント ネットワーク間のセキュリティ ポリシーを作成します。例：コンシューマ EPG とプロバイダー EPG 間の APIC 契約。
セキュリティ ポリシーの削除（契約）	テナント ネットワーク間のセキュリティ ポリシーを削除します。例：コンシューマ EPG とプロバイダー EPG 間の APIC 契約。
アクセス リストのセキュリティ ルールの更新	（セキュリティ ポリシーの追加（契約）を使用して）APIC で作成されたセキュリティ ポリシー フィルタに関連付けられているアクセス リスト ルールを追加または削除します。アクセス リスト ルールの形式は、<送信元ポート、宛先ポート、プロトコル、EtherType> です。 （注） 送信元および宛先ポートは、arp、icmp、icmpv6 ルールでは使用できません。ポートは TCP および UDP プロトコルでのみ有効です。アクセス リスト ルールは ACI ファブリックで導入および適用され、本質的にはステートレスです。 また、このブループリントには、入力として提供されている特定のサービス グラフのために、Cisco ASA などのファイアウォール アプライアンスでステートフル ファイアウォール ルールを更新するオプションがあります。

要求を送信するには、次の手順を実行します。

1. vRealize Automation に管理者としてログインし、**[Catalog]** > **[Network Security]** の順に選択します。
2. 要求を選択し、フィールドに情報を入力して、**Submit** をクリックします。

要求を表示するには、次の手順を実行します。

1. vRealize Automation の GUI で [Requests] を選択します。
2. 送信した要求を選択し、[view details] をクリックします。

ACI テナント サービス向けテナント ネットワーク サービス カタログ項目一覧

次の表に、ACI テナント サービスのテナント ネットワーク サービスのカタログ項目のリストを示します。テナント ネットワーク サービスのカタログ項目を実行するには、テナントの管理者権限でテナント ポータルにログインする必要があります。

カタログ項目	説明
テナントのブリッジ ドメインの追加または削除	テナントのブリッジ ドメインを追加または削除します。
テナントのL3コンテキスト（VRF）の追加または削除	テナントのレイヤ 3 コンテキスト（VRF）を追加または削除します。
ブリッジ ドメインのサブネットの追加または削除	ブリッジ ドメインのサブネットを追加または削除します。
ネットワークへのL3外部接続の接続または切断	ネットワークへのレイヤ 3 外部接続を接続または切断します。
テナント ネットワークの更新	テナント ネットワークを更新します。

次の表には、タイプが Cisco AVS および Cisco ACI Virtual Edge のみである VMM ドメインのテナント ネットワーク サービスのカタログ項目のリストを示します。テナント ネットワーク サービスのカタログ項目を実行するには、テナントの管理者権限でテナント ポータルにログインする必要があります。

カタログ項目	説明
uSeg 属性の追加または削除	マイクロセグメント EPGの属性を追加または削除します。

要求を送信するには、次の手順を実行します。

1. テナント管理者として vRealize Automation にログインし、**[カタログ（Catalog）]**>**[テナント ネットワーク サービス（Tenant Network Services）]**を選択します。
2. 要求を選択し、フィールドに情報を入力して、**Submit** をクリックします。

要求を表示するには、次の手順を実行します。

1. vRealize Automation の GUI で [Requests] を選択します。
2. 送信した要求を選択し、[view details] をクリックします。

ACI テナント サービス向けテナント共有プラン カタログ項目一覧

次の表に、ACIテナント サービスのテナント共有プランのカタログ項目のリストを示します。テナント共有プランのカタログ項目を実行するには、テナントの管理者権限でテナント ポータルにログインする必要があります。

カタログ項目	説明
テナント ネットワークの追加	共有プランのテナント ネットワークを追加します。

カタログ項目	説明
テナント ネットワークへの FW および LB の追加 - 共有プラン	共有プランのテナント ネットワークにファイアウォールとロード バランサを追加します。
テナント ネットワークへの FW の追加 - 共有プラン	共有プランのテナント ネットワークにファイアウォールを追加します。
テナントネットワークへのロードバランサの追加 - 共有プラン	共有プランのテナント ネットワークにロードバランサを追加します。
テナント ネットワークからの FW および LB の削除 - 共有プラン	共有プランのテナント ネットワークからファイアウォールとロードバランサを削除します。
テナント ネットワークからの FW の削除 - 共有プラン	共有プランのテナント ネットワークからファイアウォールを削除します。
テナントネットワークからのロードバランサの削除 - 共有プラン	共有プランのテナント ネットワークからロード バランサを削除します。
テナント ネットワークの削除 - 共有プラン	共有プランのテナント ネットワークを削除します。

次の表に、Cisco AVS のタイプのみの VMM ドメインのテナント共有プランのカタログ項目のリストを示します。テナント共有プランのカタログ項目を実行するには、テナントの管理者権限でテナント ポータルにログインする必要があります。

カタログ項目	説明
uSeg ネットワークの追加 - 共有プラン	共有プランにマイクロセグメント EPG を追加します。
uSeg ネットワークの削除 - 共有プラン	共有プランのマイクロセグメント EPG を削除します。

要求を送信するには、次の手順を実行します。

1. 管理者として vRealize Automation にログインし、**[カタログ（Catalog）]**>**[テナント共有プラン（Tenant Shared Plan）]**を選択します。
2. 要求を選択し、フィールドに情報を入力して、**Submit** をクリックします。

要求を表示するには、次の手順を実行します。

1. vRealize Automation の GUI で [Requests] を選択します。
2. 送信した要求を選択し、[view details] をクリックします。

（注） 症状：vRealize Automation（vRA）のワークフローによってサービス グラフを削除中にVMware vCenter のエラーが表示されることがあります。

条件：VPX や F5 などのサービス デバイスを設定する前にポート グループを削除した場合、サービス グラフの削除中にこのようなエラーが表示されます。このシーケンスは vRA からは制御できません。

回避策：回避策はありません。これらは一時的なエラーなので、サービスデバイスの再構成が完了すると表示されなくなります。

ACI テナント サービス向けテナント VPC プラン カタログ項目一覧

次の表に、ACI テナント サービスのテナント仮想プライベート クラウド（VPC）プランのカタログ項目のリストを示します。テナント VPC プランのカタログ項目を実行するには、テナントの管理者権限でテナント ポータルにログインする必要があります。

カタログ項目	説明
テナント ネットワークの追加 - VPC プラン	VPC プランのテナント ネットワークを追加します。
テナント ネットワークへの FW および LB の追加 - VPC プラン	VPC プランのテナント ネットワークにファイアウォールとロード バランサを追加します。
テナント ネットワークへの FW の追加 - VPC プラン	これは VPCプランのテナント ネットワークにファイアウォールを追加します。
テナントネットワークへのロードバランサの追加 - VPC プラン	VPC プランのテナント ネットワークにロードバランサを追加します。
テナント ネットワークからの FW および LB の削除 - VPC プラン	VPC プランのテナント ネットワークからファイアウォールとロードバランサを削除します。
テナントネットワークからのロードバランサの削除 - VPC プラン	VPC プランのテナント ネットワークからロード バランサを削除します。
テナント ネットワークの削除 - VPC プラン	VPC プランのテナント ネットワークを削除します。

次の表には、タイプが Cisco AVS および Cisco ACI Virtual Edge のみである VMM ドメインのテナント VPC プランのカタログ項目のリストを示します。テナント VPC プランのカタログ項目を実行するには、テナントの管理者権限でテナントポータルにログインする必要があります。

カタログ項目	説明
uSeg ネットワークの追加 - VPC プラン	VPC プランにマイクロセグメント EPG を追加します。

カタログ項目	説明
uSeg ネットワークの削除 - VPC プラン	VPC プランからマイクロセグメント EPG を削除します。

要求を送信するには、次の手順を実行します。

1. 管理者として vRealize Automation にログインし、**[カタログ（Catalog）] > [テナント VPC プラン（Tenant VPC Plan）]**を選択します。
2. 要求を選択し、フィールドに情報を入力して、**Submit** をクリックします。

要求を表示するには、次の手順を実行します。

1. vRealize Automation の GUI で [Requests] を選択します。
2. 送信した要求を選択し、[view details] をクリックします。

ACI テナント サービス向け VM サービス カタログ項目一覧

ここでは、ACI テナント サービスの VM サービスのカタログ項目の一覧を示します。

このサービス カテゴリには、単一マシンと複数マシンのブループリントに基づくテナント カタログ項目があります。たとえば、一般的な 3 層アプリケーションには、「Web」、「アプリケーション」、単一マシン ブループリントを使用する「Db」の 3 つのカタログ項目と、複数マシン ブループリントを使用するカタログ項目「Web アプリケーション Db」 1 つが含まれます。

カタログ項目	説明
アプリケーション	アプリケーション VM です。
Db	データベース VM です。
Test	プロパティ グループ テスト用の単一マシン VM ブループリントです。
Web	Web VM です。
Web Db アプリケーション	この複数マシン ブループリントは 3 層アプリケーション、Web 層に接続されたロード バランサ、およびセキュリティ ポリシー設定を作成します。

要求を送信するには、次の手順を実行します。

1. vRealize Automation に管理者としてログインし、**[Catalog] > [VM Services]** の順に選択します。
2. 要求を選択し、フィールドに情報を入力して、**Submit** をクリックします。

要求を表示するには、次の手順を実行します。

1. vRealize Automation の GUI で [Requests] を選択します。
2. 送信した要求を選択し、[view details] をクリックします。

vRealize における ACI カタログ項目向けエンタイトルメント

ここでは、vRealize における ACI カタログ項目向けエンタイトルメントについて説明します。各サービス カテゴリにはエンタイトルメントが必要です。エンタイトルメントによって、ユーザがカタログ項目を使用できるようになります。

エンタイトルメントを作成および管理して、カタログ項目、操作へのアクセスを制御し、カタログ要求に適用する承認ポリシーを指定できます。エンタイトルメントの優先度を更新して、特定の要求に適用する承認ポリシーを指定できます。

ACI カタログ項目向けエンタイトルメント一覧

ここでは、ACI カタログ項目向けエンタイトルメント一覧を示します。

名前
VM エンタイトルメント
管理者エンタイトルメント
テナント共有プラン エンタイトルメント
テナント VPC プラン エンタイトルメント
共通ネットワーク サービス エンタイトルメント
テナント ネットワーク サービス エンタイトルメント
テナント共通ネットワーク サービス
ネットワーク セキュリティ エンタイトルメント

エンタイトルメントを編集するには、次の手順を実行します。

1. 管理者として vRealize Automation にログインし、**[管理（Administration）] > [カタログ管理（Catalog Management）] > [資格（Entitlements）]**を選択します。
2. 編集するエンタイトルメントを選択し、フィールドに情報を入力して、[Update] をクリックします。

vRealize オーケストレータの ACI プラグイン

サービス カテゴリとカタログ項目をワークフローにマップします。

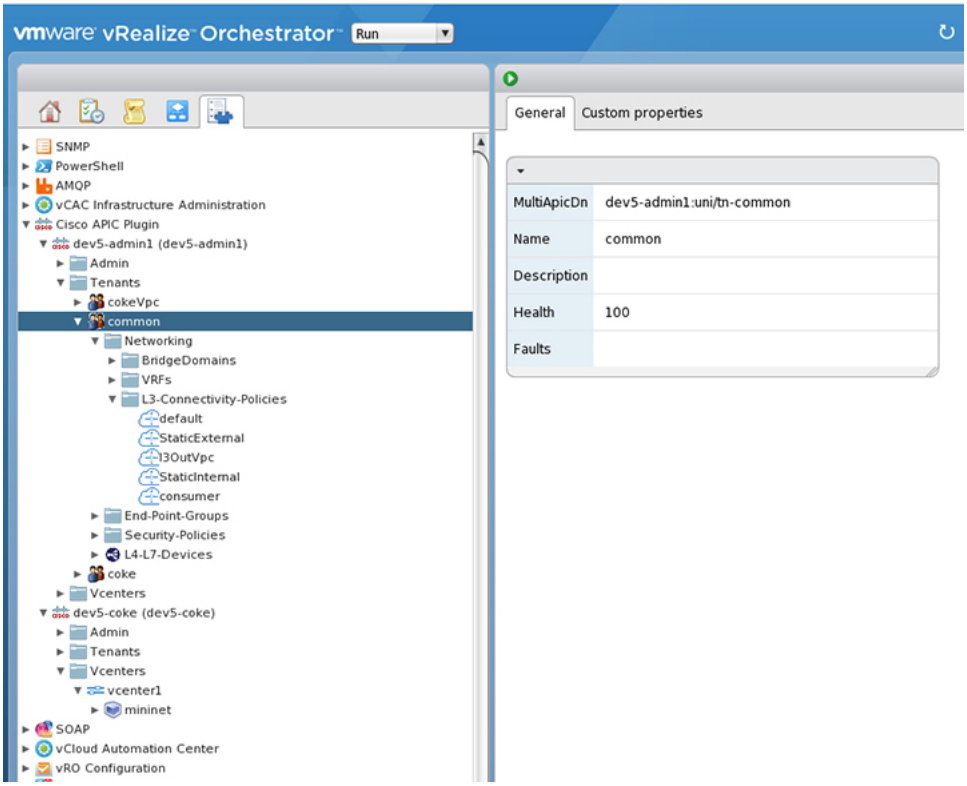
APIC のワークフロー

以下は、サービス カテゴリおよびカタログ項目であり、各カタログ項目は vRealize Orchestrator のワークフローとして実装され、カタログ項目のパラメータはワークフローパラメータと正確に同じです。

サービス カテゴリ	説明
管理サービス	グローバル管理者によって実行される管理カタログ項目
ネットワーク セキュリティ	セキュリティ ポリシーを設定するためのカタログ項目
テナント ネットワーク サービス	ネットワーク サービスの設定用（ブリッジ ドメイン、サブネット）
テナント共有プラン	共有モードでロード バランサ、およびファイアウォール サービスを使用する EPG/ネットワーク、マイクロセグメント EPG の設定用
テナント VPC プラン	VPC モードでロードバランサ、およびファイアウォール サービスを使用する EPG/ネットワーク、マイクロセグメント EPG の設定用
VM サービス	ACI のプロパティ グループで設定された、単一マシンおよび複数マシンのブループリント

APIC のインベントリ ビュー

vRealize Orchestrator GUI のインベントリ ビューでは、Cisco APIC プラグインは読み取り専用ビューです。vRealize Orchestrator の Cisco APIC プラグインは APIC にマッピングされます。たとえば、vRealize Orchestrator GUI でオブジェクトを表示すると、Cisco APIC GUI の MultiApicDn が表示されます。



ロード バランシングおよびファイアウォール サービスについて

VLAN、Virtual Routing and Forwarding（VRF）スティッチングは従来のサービス挿入モデルによってサポートされ、Application Policy Infrastructure Controller（APIC）はポリシー制御の中心点として機能する一方でサービス挿入を自動化できます。APIC ポリシーは、ネットワーク ファブリックとサービス アプライアンスの両方を管理します。APIC は、トラフィックがサービスを通って流れるように、ネットワークを自動的に設定できます。APICは、アプリケーション要件に従ってサービスを自動的に設定することもでき、それにより組織はサービス挿入を自動化し、従来のサービス挿入の複雑な技術の管理に伴う課題を排除できます。

境界ファイアウォールは通常、アプリケーションへのすべての着信外部トラフィックに、ステートフル ファイアウォール サービスを提供するために使用されます。トラフィックがファイアウォールを通過した後に実装されるもう1つの一般的なサービスは、ロードバランシングです。外部トラフィックは仮想IPに向かって送信されます。ロードバランサはこのトラフィックを終了させて、ロードバランサの背後にある使用可能なサーバ間で着信トラフィック（Web サーバなど）のロード バランスを行います。

詳しくは、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』を参照してください。

APIC vRealize プラグインを使用して新しい複数層アプリケーションを作成したり（それらの間のトラフィックにロード バランサとファイアウォール サービスを実装しつつ）、既存のアプリケーションのエンドポイント グループ間のトラフィックにファイアウォールとロード バランサ サービスを実装したりすることができます。複数層アプリケーションと L4-7 サービスを作成するには、[Admin Services] の [Configure Property Group] カタログ項目を使用して、プロ

パティ グループを作成する必要があります。「テナント共有サービス」項目から適切なカタログ項目を選択して、既存のアプリケーションのエンドポイント グループ間に L4-7 サービスを追加することができます。

（注） このリリースでは、ロード バランサおよびファイアウォール サービスに対して、共有プランのサポートのみがサポートされます。

サービスを有効にするための条件

ここでは、サービスを有効にするための条件について説明します。

APIC vRealize プラグインを使用してレイヤ 4 ～ レイヤ 7 のサービスを導入するには、次のタスクを実行する必要があります:

- APIC 管理者によって、ロード バランサのデバイス パッケージがアップロードされる必要があります。

  リンクを使用して、必要な Citrix、F5 および Cisco ASA デバイス パッケージをダウンロードします。

  http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-734587.html

  デバイス パッケージのバージョンが、使用している APIC リリースで認定されていることを確認します。

- APIC 管理者によってテナント「共通」でロード バランサのデバイス クラスタ、ファイアウォールが作成される必要があります。Citrix および F5 は、ロード バランサでサポートされているベンダーです。Cisco ASA は、ファイアウォールでサポートされているベンダーです。

- スタンドアロン ファイアウォールまたはロード バランサ サービスに、単一ノードのサービス グラフ テンプレートを設定する必要があります。ファイアウォールおよびロード バランサ サービスに、2 つのノードのサービス グラフ テンプレートを設定する必要があります。

- 抽出サービス グラフでは、ファイアウォール ノード（vnsAbsNode）に **FW** という名前を付け、ロード バランサ ノードに **SLB** という名前を付ける必要があります。

- ロード バランサのみの抽象サービス グラフ名（vnsAbsGraph）は、ロード バランサ デバイス クラスタ（vnsLdevVip）と同じである必要があります。

- ロードバランサのみのサービスでは、テナント共通の「デフォルト」VRF で、コンシューマ L3 接続ポリシーを設定する必要があります。

- ファイアウォールには、テナント共通の別個の VRF（「外部」）で、コンシューマ L3 接続ポリシーを設定する必要があります。

- ファイアウォール デバイスは、ルーテッド モードで導入する必要があります。ファイアウォール デバイス接続用に、2 つの追加の L3 接続ポリシーを設定する必要があります。

1つは「外部」VRFで設定する必要があり、ファイアウォールデバイスへの外部接続として使用されます。もう1つは「デフォルト」VRFで設定する必要があり、ファイアウォールデバイスへの内部接続として使用されます。ファイアウォールに接続されているこれら2つのL3接続ポリシーにより、ファイアウォールはVRFスティッチングを実行し、VRF間でトラフィックを適切にリダイレクトできます。管理者は、L3外部接続ポリシーのもとで、正しいインポートおよびエクスポートフラグが付いた適切なプレフィクスが設定されていることを確認する必要があります。

- L3接続ポリシーの設定時には、次の規則を使用する必要があります。L3接続ポリシーには ***L3ExtName*** という名前を付ける必要があり、子L3インスタンスには ***L3ExtName*****Inst** という名前を付ける必要があります。
- ファイアウォールとロードバランサデバイスで使用されるインターフェイスIPアドレスを、抽象グラフで設定する必要があります。
- 2ノード抽象グラフの場合、ファイアウォールノードに、すべてのトラフィックを許可するアクセスリストを設定する必要があります。

XML POST を使用した APIC でのサービスの設定

管理者のみがXML POSTを設定して送信できます。テンプレートPOSTは、`services`ディレクトリの`apic-vrealize`パッケージにあります。

始める前に

- Application Policy Infrastructure Controller（APIC）でデバイスパッケージファイルをアップロードしておく必要があります。

  詳細については、『*Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*』を参照してください。

- テナント共通には、「default」および「vpcDefault」という2つのブリッジドメインが必要です。ロードバランサを利用するテナントで使用されるサブネットが、これらのブリッジドメインに追加されていることを確認します。通常、vRealizeテナントにDHCPインフラストラクチャを設定する際に、これらのブリッジドメインとサブネットを作成します。
- 非仮想プライベートクラウド（VPC）プランでは、ロードバランサのバックエンドインターフェイスは、上で作成したテナント共通下のデフォルトEPGに配置する必要があります。VPCプランでは、EPGは「vpcDefault」です。
- VIPサブネットがL3にリンクされていることを確認します。EPGあたり1つのVIPが、テナントに関連するVIPプールから割り当てられます。
- サービス スクリプトの条件：
  - Python 2.7
  - Python ライブラリ：
    - jinja2

- yaml
- glob
- json
- 要求
- xml
- re

手順

ステップ 1 次のリンクを使用して、必要なデバイス パッケージ Citrix、F5 および ASA をダウンロードします。デバイス パッケージのバージョンが、使用している APIC リリースで認定されていることを確認します。次のディレクトリに、デバイス パッケージ zip ファイルを保存します。

http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-734587.html

ステップ 2 `shared.cfg` ファイルまたは `vpc.cfg` ファイルの `VENDOR-DEVICE-PACKAGE.zip` のエントリを正しいデバイス パッケージ ファイルに置き換えます。

ステップ 3 `setup.yaml` ファイルを編集し、設定に応じて変数を変更します。

`setup.yaml` ファイルのテンプレート変数は次のとおりです。

```
TEMPLATE_VARS:
    VCENTER: "vcenter1"
    ASA_IP: "1.1.1.1"
    ASA_CLUSTER: "AsaCluster1"
    ASA_VM: "asav-service5"
    OUTSIDE_CTX: "outside"
    INSIDE_CTX: "default"
    FW_GRAPH: "FWOnlyGraph"
    FW_SLB_GRAPH: "FWAndSLBGraph"
    BD_WEB: "default"
    CITRIX_MGMT_IP: "1.1.1.1"
    FW_NODE: "FW"
    SLB_NODE: "SLB"
    CITRIX_GRAPH: "CitrixCluster1_L3"
    CITRIX_CLUSTER: "CitrixCluster1_L3"
    CITRIX_GRAPH: "CitrixCluster1_L3"
    CITRIX_VM: "NS-service4"
    F5_BD: "F5Cluster1_L3"
    F5_EPG: "F5Cluster1_L3"
    F5_CLUSTER: "F5Cluster1_L3"
    F5_MGMT_IP: "1.1.1.1"
    F5_GRAPH: "F5Cluster1_L3"
    F5_ABS_NODE: "SLB"
    # Use deleted to generate the "deleted" version of the posts
    # STATUS: "deleted"
    STATUS: ""
```

ステップ 4 次のコマンドを入力します。

共有プランの場合：

例：

```
../jinja.py setup.yaml tn-common-template.xml > tn-common.xml
../jinja.py setup.yaml Shared-Plan-Citrix-graph-template.xml > Shared-Plan-Citrix-graph.xml
../jinja.py setup.yaml Shared-Plan-F5-graph-template.xml > Shared-Plan-F5-graph.xml
```

VPC プランの場合：

例：

```
../jinja.py setup.yaml VPC-tn-common-template.xml > VPC-tn-common.xml
../jinja.py setup.yaml VPC-Plan-Citrix-LB-graph-template.xml > VPC-Plan-Citrix-LB-graph.xml
../jinja.py setup.yaml VPC-Plan-F5-LB-graph-template.xml > VPC-Plan-F5-LB-graph.xml
```

Python エラーが表示されたら、前提条件の Python ライブラリがシステムにインストールされていることを確認します。

ステップ 5 shared.cfg ファイルまたは vpc.cfg ファイルを編集して hosts: <YOUR_APIC_IP> と passwd: <YOUR_APIC_ADMIN_PASSWD> に値を設定します。

shared.cfg ファイルの例：

例：

```
host:   <YOUR_APIC_IP>:443
name:   admin
passwd: <YOUR_APIC_ADMIN_PASSWD>
tests:
    - type: file
      path: /ppi/node/mo/.xml
#      file: asa-device-pkg-1.2.2.1.zip
#      Replace actual ASA Device package file in the line below
      file: ASA-DEVICE-PACKAGE.zip
      wait: 2
    - type: file
      path: /ppi/node/mo/.xml
#      file: CitrixNetscalerPackage.zip
#      Replace actual Citrix Device package file in the line below
      file: CITRIX-DEVICE-PACKAGE.zip
      wait: 2
    - type: file
      path: /ppi/node/mo/.xml
#      file: CitrixNetscalerPackage.zip
#      Replace actual F5 Device package file in the line below
      file: F5-DEVICE-PACKAGE.zip
      wait: 2
    - type: xml
      path:  /api/node/mo/.xml
      file: tn-common.xml
      wait: 0
    - type: xml
      path:  /api/node/mo/.xml
      file: Shared-Plan-Citrix-graph.xml
      wait: 0
    - type: xml
      path:  /api/node/mo/.xml
      file: Shared-Plan-F5-graph.xml
      wait: 0
```

ステップ 6 テンプレートをポストします。

共有プランの場合は、次のコマンドを入力します。

例：

```
../request.py shared.cfg
```

VPC プランの場合は、次のコマンドを入力します。

例：

```
../request.py vpc.cfg
```

サービス設定の削除

ここでは、サービス設定の削除方法について説明します。管理者のみが XML POST を設定して送信できます。テンプレート POST は、`services` ディレクトリの `apic-vrealize` パッケージにあります。

手順

ステップ 1 `shared.cfg` ファイルを編集し、`hosts: <YOUR_APIC_IP>` および `passwd: <YOUR_APIC_ADMIN_PASSWD>` の値を設定します。

ステップ 2 `setup.yaml` ファイルを編集して `STATUS` 変数を `deleted` に設定し、削除されたバージョンのポストを生成します。

ステップ 3 次のコマンドを実行します。

```
./jinja.py setup.yaml tn-common-template.xml > tn-common-del.xml
./jinja.py setup.yaml Shared-Plan-Citrix-graph-template.xml >
Shared-Plan-Citrix-graph-del.xml
./jinja.py setup.yaml Shared-Plan-F5-graph-template.xml > Shared-Plan-F5-graph-del.xml
```

ステップ 4 テンプレートをポストします。

```
./request.py shared_del.cfg
```

L3 外部接続について

レイヤ 3（L3）外部接続は、スタティック ルーティング、OSPF、EIGRP、BGP などの L3 ルーティング プロトコルによって、外部ネットワークに ACI ファブリックを接続する Cisco Application Centric Infrastructure（ACI）機能です。vRealize に L3 外部接続を設定することで、テナント ネットワークはファブリック外部への発信トラフィックを開始し、外部からのトラフィックを引き付けることができます。この機能の前提は、テナント仮想マシンの IP アドレ

スが、NAT を使用しないファブリック外部に表示され、ACI L3 外部接続に NAT が含まれないことです。

vRealize に L3 外部接続を設定するため条件

vRealize にレイヤ 3（L3）外部接続を設定するには、次の条件を満たす必要があります。

- Application Policy Infrastructure Controller（APIC）GUI にログインし、メニュー バーで **[テナント（TENANT）]** > **[共通（common）]**を選択します。
  - 「default」という l3ExtOut を作成し、BD「default」を参照します。
  - l3ExtOut の下に名前が「defaultInstP」の l3extInstP を作成します。これは、共有サービスのテナントで使用されます。

  L3 外部接続の設定については、『*Cisco APIC* ベーシック コンフィギュレーション ガイド』を参照してください。
- APIC GUI にログインし、メニュー バーで **[テナント（TENANT）]** > **[共通（common）]** を選択します。
  - 「vpcDefault」という l3ExtOut を作成し、BD「vpcDefault」を参照します。
  - この l3ExtOut の下に名前が「vpcDefaultInstP」の l3extInstP を作成します。

    これは、VPC テナントで使用されます。

  テナントの外部接続の設定については、『*Cisco APIC* ベーシック コンフィギュレーション ガイド』を参照してください。

  vRealize は、上述した命名規則以外の特別な要件なしで、共通の l3ExtOut 設定を活用します。

管理者のエクスペリエンス

Cisco ACI と Cisco AVS またはCisco ACI Virtual Edge

Cisco Application Virtual Switch (AVS) または Cisco ACI Virtual Edge の一般情報については、次のマニュアルを参照してください:

- Cisco AVS: Cisco.com の 『Cisco ACI Virtualization Guide』、または 『Cisco AVS guides』の最新バージョンの「Cisco ACI with Cisco AVS」の章を参照してください。
- Cisco ACI Virtual Edge: Cisco.com の 『Cisco ACI Virtual Edge documentation』を参照してください。

Cisco AVS または Cisco ACI Virtual Edge VMM ドメインの作成

Cisco AVS または Cisco ACI Virtual Edge 用の VMM ドメインは、VLAN または VXLAN カプセル化を使用し、またはローカル スイッチングを使用せずに作成することができます。

Cisco APIC リリース 2.1(1) 以降では、カプセル化モードを混在させることができます。つまり、VLAN または VXLAN を使用するように VMM ドメインを構成した場合でも、後ほどドメインのデフォルトのカプセル化を上書きする EPG を追加することができます。詳細については、『Cisco Application Virtual Switch Configuration Guide』の「Mixed-Mode Encapsulation Configuration」のセクション、または『Cisco ACI Virtual Edge Configuration Guide』の「Mixed-Mode Encapsulation」の章を参照してください。

また、ローカル スイッチングを使用しない Cisco AVS または Cisco ACI Virtual Edge VMM ドメインを作成することもできます。ローカルスイッチング モードでは、リーフはすべてのトラフィックを転送します。許可されるカプセル化のタイプは VXLAN だけです。『Cisco Application Virtual Switch Installation Guide』または『Cisco ACI Virtual Edge Installation Guide』を参照してください。

Cisco AVS または Cisco ACI Virtual Edge VMM ドメインを作成した後に、ドメインのカプセル化プールを更新して、Cisco AVS または Cisco ACI Virtual Edge および VMM ドメインを削除することができます。

Cisco AV または Cisco ACI Virtual Edge VMM ドメインの作成

このセクションでは、Cisco AVS または Cisco ACI Virtual Edgeカプセル化なし、VLAN、または VXLAN カプセル化をサポートしていない VMM ドメインを作成する方法を示します。仮想スイッチ(**Cisco AV** または **Cisco AVE**) およびスイッチング基本設定 (**Local Switching** または **No Local Switching**)を選択すると、vRealize GUI は必須または任意のフィールド入力を表示または非表示に設定します。

始める前に

Cisco ACI の 0 日目の一部として、アタッチ可能なアクセス エンティティ プロファイル (AAEP) を作成することをお勧めします。

手順

ステップ 1 vRealize Automation に管理者としてログインして **Catalog**を選択します。

ステップ 2 **Add VMM Domain** および **AVS** または **AVE** を選択します。

ステップ 3 [New Request] ダイアログボックスで、次のステップを実行します。

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) [Request Information] ペインで説明を追加して [Next] をクリックします。

c) **Domain name** フィールドに、VMM ドメイン名を入力します。

d) **Virtual Switch** セレクターに対しては、**Cisco AVS** または **Cisco AVE** を選択します。

e) **Switching Preference** セレクターに対して、**Lo Local Switching** または **Local Switching** を選択します。

f) **Local Switching**を選択した場合、**Encap mode**セレクターに対して、**VLAN** または **VXLAN** を選択します。

Encap mode は、 **Local Switching** にのみ適用可能です。

g) **AAEP Name** フィールドに、接続可能アクセス エンティティ プロファイル（AEP）名を入力して、それを VMM ドメインに関連付けます。

AAEP が入力されていない場合は、それが作成されます。

h) 割り当てられる **VLAN Ranges** の場合、**Not set** をクリックし、値を追加して VLAN を作成します。

Encap_Block_Role の場合、**external** または **internal** を指定します。

i) (オプション)**AVS Fabric-wide Multicast Address** または **AVE Fabric-wide Multicast Address** フィールドで、マルチキャスト アドレス ブロック範囲に対して 224.0.0.0 から 239.255.255.255 まで(両端を含む)の有効なマルチキャスト アドレスを入力します。

j) (オプション)**Multicast Address Start** フィールドで、ルチキャスト アドレス ブロック範囲に対して 224.0.0.0 から 239.255.255.255 まで(両端を含む)の有効なマルチキャスト アドレスを入力します。

k) (オプション) **Multicast Address End** フィールドで、ルチキャスト アドレス ブロック範囲に対して 224.0.0.0 から 239.255.255.255 まで(両端を含む)の有効なマルチキャスト アドレスを入力します。

l) **AAA ドメイン** エリアで、緑色の十字をクリックし、セキュリティ ドメインを選択し、**Next** をクリックします。

m) **Vcenter IP (または Hostname)**フィールドに、ホスト名または IP アドレスを入力します。

ホスト名を使用する場合、Cisco APIC で DNS ポリシーをすでに設定してあることが必要です。DNS ポリシーを設定していない場合は、vCenter Server の IP アドレスを入力します。

n) **DVS Version** ドロップダウンリストから、DVS バージョンを選択します。

o) **Username** フィールドに、vCenter にログインするためのユーザー名を入力します。

p) **Password** フィールドに、vCenter へのログインに対してパスワードを入力します。

q) **vCenter Datacenter** フィールドに、データ センター名を入力します。

（注）
入力するデータ センターの名前は vCenter での名前と正確に一致する必要があります。名前では、大文字と小文字が区別されます。

vCenter での Cisco AVS または Cisco ACI Virtual Edge の作成の確認

（注） Cisco APIC リリース 5.0（1）以降、Cisco Application Virtual Switch（AVS）はサポートされなくなりました。Cisco AVS を使用して Cisco APIC リリース 5.0(1) にアップグレードする場合、問題が発生した際にファブリックはサポートされません。また、Cisco AVS ドメインの障害が発生します。

Cisco AVS を使用する場合は、Cisco ACI Virtual Edge に移行することを推奨します。ポリシーについては、『*Cisco ACI Virtual Edge Installation Guide*』を参照してください。

手順

ステップ 1 vSphere クライアントで vCenter サーバへの接続を開きます。

ステップ 2 vCenter で **Home** > **Inventory** > **Networking** ビューを選択します。

ステップ 3 データセンターを選択します。

ステップ 4 データセンターの下で、Cisco AVS または Cisco ACI Virtual Edge およびそのフォルダが作成されたことを確認します。

Cisco APIC で Cisco AVS または Cisco ACI Virtual Edge VMM ドメインの作成の確認

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[仮想ネットワーキング（Virtual Networking）]** > **[インベントリ（Inventory）]**を選択します。

ステップ 3 **[インベントリ（Inventory）]**ナビゲーションペインで、**[VMM ドメイン（VMM Domains）]** > **[VMware]**を選択します。

ステップ 4 作業ウィンドウの、**Properties** の下、**vCenter Domains** フィールドで、新しく作成された VMM ドメインがリストに表示されていることを確認します。

Cisco AVS または Cisco ACI Virtual Edge VMM ドメイン カプセル化プールの更新

Cisco AVS VMM または Cisco ACI Virtual Edge ドメインを作成した後、VLAN またはマルチキャスト アドレス プールを更新できます。それから更新を確認してください。

Cisco AVS または Cisco ACI Virtual Edge VMM ドメインの VLAN プールの更新

（注） Cisco APIC リリース 5.0（1）以降、Cisco Application Virtual Switch（AVS）はサポートされなくなりました。Cisco AVS を使用して Cisco APIC リリース 5.0(1) にアップグレードする場合、問題が発生した際にファブリックはサポートされません。また、Cisco AVS ドメインの障害が発生します。

Cisco AVS を使用する場合は、Cisco ACI Virtual Edge に移行することを推奨します。ポリシーについては、『*Cisco ACI Virtual Edge Installation Guide*』を参照してください。

手順

ステップ 1 vRealize Automation に管理者としてログインして **Catalog** を選択します。

ステップ 2 [Update Vlan Pool, AVS] または [Update Vlan Pool, AVE] を選択します。

（注）
この更新操作はダイナミック VLAN プールでのみサポートされます。静的 VLAN プールはサポートされません。

ステップ 3 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

ステップ 4 [New Request] ダイアログボックスで、次のステップを実行します。

a) 説明を追加し、[Next] をクリックします。
b) [Vlan Pool Name] フィールドに、既存の VLAN プールの名前を入力します。
c) [List of encap blocks] 領域で、[New] の横の緑色の十字形をクリックします。
d) 各 Encap ブロックの、**VlanStart** 列で、開始 VLAN を入力します。
e) **VlanEnd** 列に 終了 VLAN を入力します。
f) **encapRole** で、**external** または **internal** を指定します。
g) **IsAddoperation** のチェック ボックスをオンにして、Encap ブロックを VLAN プールに追加します。

入力した Encap ブロックを VLAN プールに入れない場合には、チェック ボックスをオフのままにします。

h) [Submit] をクリックします。

次のタスク

Cisco APIC の Cisco AVS または Cisco ACI Virtual Edge の VLAN プールの更新を確認する （49 ページ）の手順を完了します。

Cisco APIC の Cisco AVS または Cisco ACI Virtual Edge の VLAN プールの更新を確認する

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]**を選択します。

ステップ 3 **Policies** ナビゲーション ウインドウで **Pools** フォルダを展開します。

ステップ 4 **VLAN** フォルダを展開します。

ステップ 5 VLAN プールを選択します。

ステップ 6 作業ウィンドウで VLAN プールが更新されたことを確認します。

Cisco AVS または Cisco ACI Virtual Edge VMM ドメインのマルチキャスト アドレス プールの更新

手順

ステップ 1 vRealize Automation に管理者としてログインして **Catalog** を選択します。

ステップ 2 **Update Multicast Pool, AVS or AVE** を選択します。

ステップ 3 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

ステップ 4 [New Request] ダイアログボックスで、次のステップを実行します。

a) [Multicast Pool Name] フィールドに、既存のマルチキャスト アドレス プールの名前を入力します。

b) [List of Multicast Address Range] 領域で、[New] の横の緑色の十字形をクリックします。

c) マルチキャスト アドレス ブロックごとに、開始マルチキャスト アドレスとして 224.0.0.0 から 239.255.255.255 までの値 (最初値と最大値も含みます) を **MulticastAddressStart** 列に入力します。

d) **MulticastAddressEnd** 列に、終了マルチキャスト アドレスとして 224.0.0.0 から 239.255.255.255 までの値 (最初値と最大値も含みます) を

e) マルチキャスト アドレス ブロックをマルチキャスト アドレス プールに追加するには、**IsAddOperation** 列のチェック ボックスをオンにします。

入力したマルチキャスト アドレス ブロックをマルチキャスト アドレス プールから削除するには、このチェック ボックスをオフのままにします。

f) [Submit] をクリックします。

次のタスク

Cisco APIC でマルチキャスト アドレス プールを更新する （50 ページ）の手順を完了します。

Cisco APIC でマルチキャスト アドレス プールを更新する

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 3 **Policies** ナビゲーション ウィンドウで、**Pools** フォルダを展開します。

ステップ 4 **Multicast Address** フォルダを展開します。

ステップ 5 マルチキャスト アドレス プールを選択します。

ステップ 6 作業ウィンドウで、マルチキャスト アドレス プールが更新されたことを確認します。

Cisco AVS または Cisco ACI Virtual Edge と VMM ドメインの削除

Cisco AVS または Cisco ACI Virtual Edge と VMM ドメインは削除することができます。その後、削除を確認する必要があります。

Cisco AVS または Cisco ACI Virtual Edge と VMM ドメインの削除

手順

ステップ 1 vRealize Automation に管理者としてログインして **Catalog** を選択します。

ステップ 2 **Delete VMM Domain, AVS or AVE** を選択します。

ステップ 3 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

ステップ 4 [New Request] ダイアログボックスで、次のステップを実行します。

a) 説明を追加し、[Next] をクリックします。

b) **Domain name** フィールドで、削除する VMM ドメインの名前を入力します。

（注）
VMM ドメインに、関連付けられているマルチキャスト アドレス プール (*Domain/AVS or AVE name_mcastpool*) または VLAN プール (*Domain/AVS or AVE name_vlanpool*) がある場合には、それも削除されます。

c) [Submit] をクリックします。

次のタスク

次の手順を実行します。

- vCenter で Cisco AVS または Cisco ACI Virtual Edge の削除を確認する （51 ページ）
- Cisco APIC の VMM ドメインの削除の確認 （52 ページ）
- Cisco APIC で VLAN プールの削除を確認する （52 ページ）
- Cisco APIC でマルチ キャスト アドレス プールの削除の確認 （52 ページ）

vCenter で Cisco AVS または Cisco ACI Virtual Edge の削除を確認する

手順

ステップ 1 vSphere クライアントで vCenter サーバーへの接続を開きます。

ステップ 2 vCenter では、**[ホーム（Home）]** > **[インベントリ（Inventory）]** > **[ネットワーキング（Networking）]**ビューを選択します。

ステップ 3 データセンターを選択します。

ステップ 4 データセンターの下で、Cisco AVS または Cisco ACI Virtual Edge とそのフォルダが削除されたことを確認します。

Cisco APIC の VMM ドメインの削除の確認

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **仮想ネットワーク** > **インベントリ**を選択します。

ステップ 3 **インベントリ** ナビゲーション ウィンドウでは、**VMM Domains** フォルダーと **VMware** フォルダーを展開します。

ステップ 4 **Vmware** の下で、削除された VMM ドメインが存在しないことを確認します。

Cisco APIC で VLAN プールの削除を確認する

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **Fabric** > **Access Policies** を選択します。

ステップ 3 **Policies** ナビゲーション ウィンドウで、**Pools** フォルダを展開します。

ステップ 4 **VLAN** フォルダを選択します。

ステップ 5 作業ウィンドウの **Pools - VLAN** で、VLAN プール(*Domain/AVS name*_vlanpool) が削除されたことを確認します。

Cisco APIC でマルチ キャスト アドレス プールの削除の確認

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 3 [Policies] ナビゲーション ウィンドウで、[Pools] フォルダを展開します。

ステップ 4 選択、 **マルチキャスト アドレス** フォルダ。

ステップ 5 作業ウィンドウで [**プール、マルチ キャスト アドレス** 、マルチキャスト アドレス プールを確認します (ドメイン/*AV* または平均名 _mcastpool) が削除されます。

Cisco AV または Cisco ACI Virtual Edge VMM ドメインのセキュリティ ドメインのマッピング

Cisco AV のセキュリティ ドメインのマッピングを更新するまたは Cisco ACI Virtual Edge VMM ドメイン。

シスコ AVS または Cisco ACI Virtual Edge VMM ドメインのセキュリティ ドメイン マッピングの更新

手順

ステップ 1 vRealize Automation に管理者としてログインして [Catalog] を選択します。

ステップ 2 **Update AVS or AVE VMM Domain Security Domain Mapping** を選択し、次の手順を実行します:

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) [Request Information] ペインで説明を追加して [Next] をクリックします。

c) **AVS/VMM-domain name** フィールドに、VMM のドメイン名を入力します。

d) **AAA Domain list** テーブルで、**New** をクリックして、AAA ドメイン名を入力します。

エントリごとに、**aaaDomainName** 列で既存のセキュリティ ドメインを指定します。AVS または AVE VMM ドメインを AAA に追加するには、**IsAddOperation** 列のチェック ボックスをオンにします。オフの場合、AVS または AVE VMM ドメインは、AAA ドメインから削除されます。

e) [Submit] をクリックします。

次のタスク

Cisco AVS またはCisco ACI Virtual Edge VMM ドメインのセキュリティ ドメイン マッピングの確認 （53 ページ）の手順を完了します。

Cisco AVS または*Cisco ACI Virtual Edge VMM* ドメインのセキュリティ ドメイン マッピングの確認

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[仮想ネットワーキング（Virtual Networking）] > [インベントリ（Inventory）] > [VMM ドメイン（VMM Domains）] > [VMware]**を選択します。

ステップ 3 VMM ドメインを選択します。

ステップ 4 作業ウィンドウの **Properties** の下で、**Security Domains** フィールドが更新されていることを確認します。

分散ファイアウォール ポリシー

ユーザは分散ファイアウォール (DFW) のポリシーは作成、更新、および削除が可能で、DFW ポリシーと Cisco AVS または Cisco ACI Virtual Edge VMM ドメインの関連づけを更新できます。

分散ファイアウォールの詳細については、次のいずれかを参照してください:

- 『Cisco ACI AVS 構成ガイド』のセクション「分散ファイアウォール」
- 『Cisco ACI VirtualEdge Configuration Guide』の「Distributed Firewall」の章

分散ファイアウォール ポリシーの作成

このセクションでは、DFW ポリシーを作成し、Cisco AVS または Cisco ACI Virtual Edge VMM ドメインと関連付ける方法を説明します。

手順

ステップ 1 vRealize Automation に管理者としてログインして [Catalog] を選択します。

ステップ 2 **[FW ポリシーの作成（DFW）および AVS またはAVE VMM ドメインへの関連付け]** を選択して、次の手順を実行します:

a) 入力フィールドのサービスブループリント情報を表示して [Request] をクリックします。

b) **Request Information** ペインで説明を追加して、**Next** をクリックします。

c) **FW Policy Name** フィールドに、ポリシーの名前を入力します。

d) **[モード]** ドロップダウン リストから、**[ラーニング]**、**[有効]** または **[無効]** を選択します。

- 学習：Cisco AVS または Cisco AVS 仮想スイッチではmすべての TCP 通信をモニタし、フローテーブルにフローを作成しますが、ファイアウォールは適用しません。ラーニング モードは、トラフィックを失わずにファイアウォールを有効にする方法を提供します。
- 有効：分散ファイアウォールを適用します。分散ファイアウォールをサポートしていない以前のバージョンの Cisco AVS からのアップグレードで、Cisco AVS のみをアップグレードしている場合は、最初にすべての VMM ドメイン上の Cisco AVS ホストをアップグレードしてから、分散ファイアウォールを有効にする必要があります。
- 無効：分散型ファイアウォールは適用されず、Cisco AVS または Cisco ACI Virtual Edgeからすべてのフロー情報を削除します。このモードは、分散ファイアウォールを使用しないときにのみ選択します。

e) **[VMM 名]** フィールドで、DFW ポリシーに関連付ける既存の Cisco AV または Cisco ACI Virtual Edge VMM ドメインの名前を入力し、**[次へ]** をクリックします。

f) **[Syslog フォーム]** ページで、**[管理状態]** ドロップダウン リストから **[有効]** または **[無効]** を選択します。

g) Cisco AVS または Cisco ACI Virtual Edge は、分散ファイアウォールによって許可または拒否されたフローをシステム ログ（syslog）サーバに報告します。次の手順を実行します。

- Cisco AVS または Cisco ACI Virtual Edge が syslog サーバに許可されたフローを報告する場合、**[フローの許可]** ドロップダウン リストから、**[はい]** を選択します。Cisco AVS または Cisco ACI Virtual Edge が syslog サーバに許可されたフローを報告しない場合、**[いいえ]** を選択します。
- Cisco AVS または Cisco ACI Virtual Edge が syslog サーバに拒否されたフローを報告する場合、**[拒否されたフロー]** ドロップダウン リストから、**[はい]** を選択します。Cisco AVS または Cisco ACI Virtual Edge が syslog サーバーに拒否されたフローを報告しない場合、**[いいえ]** を選択します。

h) **[投票間隔（秒）]** エリアで、60 秒から 86,400 時間の間隔を入力します。

i) **[ログ レベル]** ドロップダウン リストから、syslog サーバに定義された重大度レベル以上のログ重大度レベルを選択します。

j) **[宛先グループ]** エリアで、既存の syslog モニタリング宛先グループを入力します。

k) [Submit] をクリックします。

次のタスク

Cisco APIC で分散ファイアウォール ポリシーの作成を確認する （55 ページ）の手順を完了します。

Cisco APIC で分散ファイアウォール ポリシーの作成を確認する

このセクションでは、Cisco APIC で分散ファイアウォール ポリシーの作成を確認する方法について説明します。

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 3 **Policies** ナビゲーション ウィンドウで、**Policies** > **Interface** > **Firewall** を選択します。

ステップ 4 作業ウィンドウの、**Interface - Firewall** の下で、対応するファイアウォール ポリシーが作成されていることを確認します。

ステップ 5 分散ファイアウォール ポリシーと VMM ドメインとの関連付けを表示するには、次の手順に従います:

a) **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** を選択します。

b) 対応する VMM ドメインをクリックします。

c) 作業ウィンドウで、**VSwitch Policy** をクリックし、作成した分散ファイアウォール ポリシーが **Firewall Policy** フィールドに設定されていることを確認します。

分散型ファイアウォール ポリシーの更新

このセクションでは、既存の DFW ポリシーの更新方法について説明します。

手順

ステップ 1 vRealize Automation に管理者としてログインして [Catalog] を選択します。

ステップ 2 選択 **更新 FW ポリシー (含めた** し、次の手順を実行します。

一部のドロップダウン リストにはサービス ブルー プリントで、 **<NO change="">** 設定されている値を変更しないかどうかを選択したオプションによって</NO>。

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) **Request Information** ペインで説明を追加して、**Next** をクリックします。

c) **FW Policy Name** フィールドに、更新後のポリシーの名前を入力します。

d) **モード** ドロップダウンリスト、選択 **ラーニング** 、 **Enabled** 、 **Disabled** 、または **<NO change="">** .</NO> [Next] をクリックします。

e) **Syslog フォーム** ページで、選択 **Disabled** 、 **Enabled** 、または **<NO change="">** から、 **Administrative State** ドロップダウンリスト</NO>。

f) **フローを許可** ドロップダウンリスト、選択 **はい** 、 **no** 、または **<NO change="">** .</NO>

g) **フロー拒否** ドロップダウンリスト、選択 **はい** 、 **no** 、または **<NO change="">** .</NO>

h) **ポーリング間隔 (秒)**] エリアで、60 ~ 86,400 秒から値を間隔を更新します。

（注）
間隔を指定しない場合は、更新は行われません。

i) **ログレベル** ドロップダウンリスト、syslog サーバに定義された重大度レベル以上であるログ重大度レベルを選択します。選択 **<NO change="">** ログ レベルを変更しないかどうか</NO>。

j) **Dest グループ**] エリアで、新規または既存の syslog が宛先グループのモニタリングを入力します。

（注）
新規または既存の syslog が宛先グループのモニタリングを入力しないと、更新は行われません。

k) [Submit] をクリックします。

Cisco APIC の分散ファイアウォール ポリシーの更新を確認する

このセクションでは、Cisco APIC で分散ファイアウォール ポリシーの更新を確認する方法について説明します。

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 3 **Policies** ナビゲーション ウィンドウで、**Policies** > **Interface** > **Firewall** を選択します。

ステップ 4 作業ウィンドウの **Interface - Firewall** の下で、対象のファイアウォール ポリシーをダブルクリックし、更新を確認します。

分散ファイアウォール ポリシーの削除

この項では、DFW ポリシーの作成方法について説明します。

手順

ステップ 1 vRealize Automation に管理者としてログインして [Catalog] を選択します。

ステップ 2 選択 **削除 FW ポリシー (含めた** し、次の手順を実行します。

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) **Request Information** ペインで説明を追加して、**Next** をクリックします。

c) **ポリシー name** フィールドで、削除する VMM BIOS ポリシー名前を入力します。

d) [Submit] をクリックします。

Cisco APIC の分散ファイアウォール ポリシーの削除を確認する

このセクションでは、Application Policy Infrastructure Controller での分散ファイアウォール ポリシーの削除を確認する方法について説明します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Fabric** > **Access Policies** を選択します。

ステップ 3 **Policies** ナビゲーション ウィンドウで、**Policies** > **Interface** > **Firewall** を選択します。

ステップ 4 作業ウインドウの **Interface - Firewall** の下で、削除したファイアウォール ポリシーがなくなったことを確認します。

Cisco AVS または Cisco ACI Virtual Edge VMM Domain での分散型ファイアウォール ポリシーの関連付けを更新する

このセクションでは、Cisco AVS または Cisco ACI Virtual Edge VMM ドメインに関連付けられている DFW ポリシーを更新する方法について説明します。

手順

ステップ 1 vRealize Automation に管理者としてログインして **Catalog** を選択します。

ステップ 2 **Update FW Policy (DFW) association to AVS or AVE VMM Domain** を選択して、次の手順を実行します:

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) **Request Information** ペインで説明を追加して、**Next** をクリックします。

c) **FW Policy Name** フィールドに、ポリシーの名前を入力します。

d) **VMM Domain name** フィールドに、既存の Cisco AVS または Cisco ACI Virtual Edge VMM ドメイン名を入力します。

e) **Operations** ドロップダウン リストから、次のいずれかのオプションを選択します:

- **add** — Cisco AVS の DFW ポリシーまたは Cisco ACI Virtual Edge VMM ドメインに関連付けます。
- **del** — Cisco AVS または Cisco ACI Virtual Edge VMM ドメイン から DFW ポリシーの関連付けを解除します。

f) [Submit] をクリックします。

次のタスク

APIC 上の Cisco AVS または Cisco ACI Virtual Edge VMM ドメインでのマイクロセグメント関連づけの更新を確認する （85 ページ） の手順を実行します。

分散ファイアウォール ポリシーと *Cisco AVS* または *Cisco ACI Virtual Edge APIC* との関連付けの確認

ここでは、Cisco APIC で分散ファイアウォール ポリシーと シスコの AVS または Cisco ACI Virtual Edge との関連付けを確認する方法について説明します。

手順

ステップ 1 Cisco APIC に管理者としてログインします。

ステップ 2 **[仮想ネットワーキング（Virtual Networking）] > [インベントリ（Inventory）] > [VMM ドメイン（VMM Domains）] > [VMware]**を選択します。

ステップ 3 必要な VMM ドメインをクリックします。

ステップ 4 **Work** ウィンドウの **Properties** の下で、分散ファイアウォール ポリシーが vSwitch ポリシーの **Firewall Policy** フィールドの VMM ドメインと関連付けられていることを確認します。

共有または仮想プライベート クラウド プランのテナント エクスペリエンス

共有プランでのネットワークの作成

ここでは、共有プランでネットワークを作成する方法を説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして [Catalog] を選択します。

ステップ 2 [Navigation] ペインで、[Tenant Shared Plan] を選択します。

ステップ 3 [Tenant Shared Plan] ペインで [Add Tenant Network - Shared Plan] を選択し、次の操作を実行します。

a) 入力フィールドのサービス ブループリント情報を表示し、[Request] をクリックします。

b) [Request Information] ペインで説明を追加して、[Next] をクリックします。

c) [Step] ペインで、次の操作を実行します。

d) [NetworkEPG name] フィールドに、新しい共有ネットワークの名前（new-shared-network）を入力します。

e) **Domain/DVS** フィールドで、**Add** をクリックし、***your_apic*** > **vCenters** > ***your_vcenter*** を展開し、DVS を選択します。

f) カプセル化モードとして、**encapMode** ドロップダウンリストから **Auto**、 **VLAN**、または **VXLAN** のいずれかを選択します。

（注）
EncapMode フィールドは VMM ドメイン タイプが Cisco AV または Cisco ACI Virtual Edge（ローカル スイッチング）の場合にのみ適用されます。VDS VMM ドメインで VLAN または VXLAN を選択すると、予期しない結果が生じる可能性があります。

g) **Application Tier Number** フィールドに、1 ～ 10 の数値を入力します。

h) **Intra EPG Deny** フィールドで、**Yes** または **No** のいずれかの値を選択します。

i) **許可"マイクロセグメンテーション"** フィールドで、いずれかの値を選択 **はい** または **No** 。

（注）
Allow Microsegmentation フィールドは VMM ドメイン タイプが VDS VMM ドメインである場合にのみ適用されます。

j) **Use Default BD?** フィールドでは、**Yes** または **No** のいずれかの値を選択します。

No を選択した場合、**Add** をクリックして、カスタム ブリッジ ドメインを選択します。

- ***your_apic_user*** > **Tenants** > ***your_tenant*** > **Networking** > **BridgeDomains** > ***your_bridgedomain*** を展開し、このブリッジ ドメインを選択します。

k) **スイッチング モード** セレクター、選択 **ネイティブ** または **平均** 。

ネイティブ オプションは、デフォルトのスイッチング; **平均** は Cisco ACI Virtual Edge スイッチング用です。

l) [Submit] をクリックします。

VMware vRealize と APIC で新しく作成されたネットワークの確認

この項では、VMware vRealize と Application Policy Infrastructure Controller（APIC）で新しく作成されたネットワークを確認する方法を説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインし、[Request] を選択して要求のステータスが正常であることを確認します。

ステップ 2 APIC GUI にテナントとしてログインし、[Tenants] を選択します。

ステップ 3 [Navigation] ペインで、**[Tenant *name]*** > **[Application Profiles]** > **[default]** > **[Application EPGs]** > **[EPG new-shared-network]** の順に展開します。

ステップ 4 [Properties] ペインで、[Received Bridge Domain] フィールドが共通/デフォルトであることを確認します。

ステップ 5 [Navigation] ペインで [Domains (VMs and Bare-Metals)] を選択し、VMware/*your_vmm_domain* にバインドされていることを確認します。

VPC プランでのブリッジ ドメインの作成

ここでは、VPC プランでブリッジ ドメインを作成する方法を説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして [Catalog] を選択します。

ステップ 2 [Navigation] ペインで、[Tenant Network Services] を選択します。

ステップ 3 [Tenant Network Services] ペインで [Add or Delete Bridge domain in Tenant] を選択し、次の操作を実行します。

a) 入力フィールドのサービス ブループリント情報を表示し、[Request] をクリックします。

b) [Request Information] ペインで説明を追加して、[Next] をクリックします。
c) [Step] ペインで、次の操作を実行します。
d) [Add a bridge domain] フィールドで、[Yes] を選択します。
e) [Bridge Domain name] フィールドに、ブリッジ ドメイン名（new-bd）を入力します。
f) [Enable ARP Flooding] フィールドで [No] を選択します。
g) [Enable flooding for L2 Unknown Unicast] フィールドで [hardware-proxy] を選択します。
h) [Enable flooding for L3 Unknown Multicast] フィールドで [flood] を選択します。
i) [L3 context (VRF)] フィールドで [Add] をクリックし、***[your_apic]*** > **[Tenants]** > ***[your_tenant]*** > **[Networking]** > **[VRFs]** の順に展開して、VRF（ctx1）を選択します。
j) [Submit] をクリックします。
k) [Operation] フィールドで [Add] を選択します。
l) [Submit] をクリックします。

APIC で新しく作成したブリッジ ドメインの確認

ここでは、Application Policy Infrastructure Controller（APIC）で新しく作成したブリッジ ドメインを確認する方法について説明します。

手順

ステップ 1 APIC GUI にテナントとしてログインし、[Tenants] を選択します。
ステップ 2 [Navigation] ペインで、**[Tenant *name]*** > **[Networking]** > **[Bridge Domain]** > ***[your_newly_created_bd]*** の順に展開します。
ステップ 3 [Properties] ウィンドウで、フィールドが VMware vRealize GUI と同じであることを確認します。

VPC プランでのネットワークの作成およびブリッジ ドメインへの関連付け

ここでは、VPC プランでネットワークを作成してブリッジ ドメインに関連付ける方法を説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして [Catalog] を選択します。
ステップ 2 [Navigation] ペインで、[Tenant VPC Plan] を選択します。
ステップ 3 [Tenant VPC Plan] ペインで [Add Tenant Network - VPC Plan] を選択し、次の操作を実行します。
a) 入力フィールドのサービス ブループリント情報を表示し、[Request] をクリックします。
b) [Request Information] ペインで説明を追加して、[Next] をクリックします。

c) [Step] ペインで、次の操作を実行します。
d) [NetworkEPG name] フィールドに、新しい共有ネットワークの名前（new-vpc-network）を入力します。
e) **Domain/DVS** フィールドで、**Add** をクリックし、***your_apic*** > **vCenters** > ***your_vcenter*** を展開し、DVS を選択します。
f) **encapMode** ドロップダウンリストで、**Auto**、**VLAN**、または **VXLAN** のいずれかをカプセル化モードとして選択します。

（注）
encapMode フィールドは、VMMdomain タイプが Cisco AVS の場合、または Cisco ACI Virtual Edge (ローカル スイッチング) の場合にのみ適用されます。VDS VMM ドメインで VLAN または VXLAN を選択すると、予期しない結果が生じる可能性があります。

g) **Application Tier Number** フィールドに、1 ～ 10 の数値を入力します。
h) **Intra EPG Deny** フィールドで、**Yes** または **No** のいずれかの値を選択します。
i) **Allow Microsegmentation** フィールドで、**Yes** または **No** のいずれかの値を選択します。

（注）
Allow Microsegmentation フィールドは VMMdomain タイプが VDS VMM ドメインである場合にのみ適用されます。

j) **Use Default BD?** フィールドでは、**Yes** または **No** のいずれかの値を選択します。

No を選択した場合、**Add** をクリックして、カスタム ブリッジ ドメインを選択します。

- ***your_apic_user*** > **Tenants** > ***your_tenant*** > **Networking** > **BridgeDomains** > ***your_bridgedomain*** を展開し、このブリッジ ドメインを選択します。

k) [Subnet Prefix] フィールドに、ゲートウェイ IP アドレスとサブネット マスクを入力します（10.1.1.1/24）。
l) [Submit] をクリックします。

APIC での VPC プランのネットワークとブリッジ ドメインへのアソシエーションの確認

ここでは、APIC で新しく作成したブリッジ ドメインを確認する方法について説明します。

手順

ステップ 1 APIC GUI にテナントとしてログインし、[Tenants] を選択します。
ステップ 2 [Navigation] ペインで、**[Tenant name]** > **[Application Profiles]** > **[default]** > **[Application EPGs]** > **[EPG new-vpc-network]** の順に展開します。
ステップ 3 [Properties] ペインで、ブリッジ ドメインが *your_tenant*/bd1 であることを確認します。
ステップ 4 [Navigation] ペインで [Domains (VMs and Bare-Metals)] を選択し、*your_vmm_domain* にバインドされていることを確認します。

ステップ 5 [Navigation] ペインで、**[Tenant *name*]** > **[Networking]** > **[Bridge Domain]** > ***[bd1]*** > **[Subnets]** の順に展開します。

ステップ 6 [Subnets] ペインで、ネットワークを作成して VPC プラン（10.1.1.1/24）のブリッジ ドメインに関連付けた際に入力したゲートウェイ IP アドレスとサブネット マスクを確認し、スコープがプライベートから VRF であることを確認します。

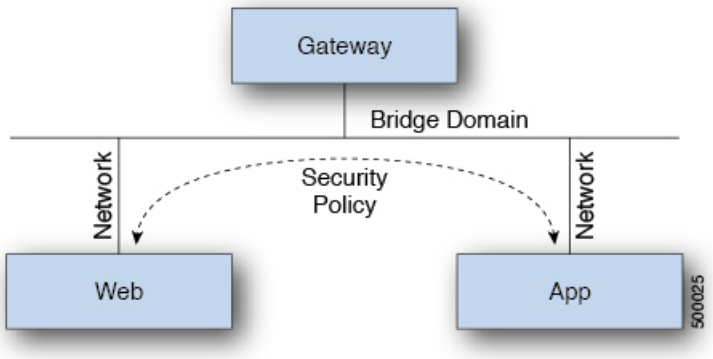
ステップ 7 メニュー バーで、[Virtual Networking] を選択します。

ステップ 8 [navigation] ペインで、**VMM Domains** > **VMware** > ***your_vmm_domain*** > **Controllers** > **vcenter1** > **DVS -** ***your_vmm_domain*** > **Portgroups** の順に展開し、ポート グループとテナント アプリケーション プロファイル EPG 名が表示されていることを確認します。

テナント内のセキュリティ ポリシーの作成

ここでは、テナント内のセキュリティ ポリシーを作成する方法を説明します。

次の図は、Web とアプリケーションは同じブリッジ ドメインにありますが、通信していないことを示しています。Web とアプリケーションは隔離されていますが、ゲートウェイとは通信できます。Web とアプリケーションが通信するには、セキュリティ ポリシーを作成する必要があります。



始める前に

2 つの仮想マシン（VM）を持つ 2 つの共有ネットワークが設定されていることを確認します。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Network Security]** の順に選択します。

ステップ 2 [Add Security Policy (Contracts)] を選択します。

ステップ 3 [Request] を選択します。

ステップ 4 [Request Information] タブで、要求の説明を入力します。

ステップ 5 [Next] を選択します。

ステップ 6 [Step] タブで、次の操作を実行します。

a) [Rule Entry List] フィールドに値を入力し、[Save] をクリックします。

次の表は、各ルール エントリの値を示しています。

ルール エントリ リスト	値
dstFormPort	• ブランク • 未指定 • 1 ～ 65535
dstToPort	• ブランク • 未指定 • 1 ～ 65535
protocol	• icmp • icmpv6 • tcp • udp • ブランク
etherType	• IP • 『ARP』

b) [Consumer Network/EPG name] フィールドで [Add] をクリックし、コンシューマのネットワーク/EPG を検索して選択します。（Web ホスト）

c) [Submit] をクリックします。

d) [Provider Network/EPG name] フィールドで [Add] をクリックし、プロバイダーのネットワーク/EPG を検索して選択します。（app-host）

e) [Submit] をクリックします。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 **[OK]** をクリックします。

APIC でのテナント内セキュリティ ポリシーの確認 APIC

ここでは、APIC でテナント内セキュリティ ポリシーを確認する方法を説明します。

手順

ステップ 1 Cisco APICにログインし、**TENANTS** を選択します。

ステップ 2 **[Navigation]** ペインで、**[Tenant *your_tenant*]** > **[Networking]** > **[Security Policies]** > **[Contracts]** の順に展開します。

a) **[Contracts]** の下にネストされている名前が、プロバイダーとコンシューマの名前であることを確認します。（app-host_ctrct_web-hosts）

ステップ 3 **[Navigation]** ペインで、**[Tenant *your_tenant*]** > **[Networking]** > **[Security Policies]** > **[Filters]** の順に展開します。

a) **[Filters]** の下にネストされている名前が、プロバイダーとコンシューマの名前であることを確認します。（app-host_flt_web-hosts）

ステップ 4 **[Navigation]** ペインで、**[Tenant *your_tenant*]** > **[Networking]** > **[Application Profiles]** > **[default]** > **[Application EPGs]** > **[EPG web-hosts]** > **[Contracts]** の順に展開します。

a) **[Work]** ペインで、コンシューマが **[Comsumed]** であることを確認します。

ステップ 5 **namigation** ペインで、**Tenant *your_tenant*** > **Networking** > **Application Profiles** > **default** > **Application EPGs** > **EPG app-hosts** > **Contracts** の順に展開します。

a) **[Work]** ペインで、プロバイダーが **[Provided]** であることを確認します。

テナント内のセキュリティ ポリシーの接続の確認

ここでは、テナント内のセキュリティ ポリシーの接続を確認する方法について説明します。

手順

ステップ 1 仮想マシン（Webホスト）にログインし、コマンドラインから他のVM（アプリケーションホスト）を ping します。

ステップ 2 仮想マシン（アプリケーションホスト）にログインし、コマンドラインから他のVM（Webホスト）を ping します。

これにより、VM が互いに通信していることが確認できます。

共通テナントでの共有サービスの消費

ここでは、共通テナントでの共有サービスの消費について説明します。

始める前に

ブリッジ ドメインと「共通/デフォルト」の関係にある共通テナントの EPG が必要です。

手順

ステップ 1 テナントとして vRealize Automation にログインし、**[Catalog]** > **[Network Security]** の順に選択します。

ステップ 2 [Add Security Policy (Contracts)] を選択します。

ステップ 3 [Request] を選択します。

ステップ 4 [Request Information] タブで、要求の説明を入力します。

ステップ 5 [Next] を選択します。

ステップ 6 [Step] タブで、次の操作を実行します。

a) [Rule Entry List] フィールドに値を入力し、[Save] をクリックします。

次の表は、各ルール エントリの値を示しています。

ルール エントリ リスト	値
dstFormPort	• ブランク • 未指定 • 1 ～ 65535
dstToPort	• ブランク • 未指定 • 1 ～ 65535
protocol	• icmp • icmpv6 • tcp • udp • ブランク
etherType	• IP • 『ARP』

b) [Consumer Network/EPG name] フィールドで [Add] をクリックし、コンシューマのネットワーク/EPG を検索して選択します。（Web ホスト）

c) [Submit] をクリックします。

d) [Provider Network/EPG name] フィールドで [Add] をクリックし、プロバイダーのネットワーク/EPG を検索して選択します。（SYSLOG-EPG）

e) [Submit] をクリックします。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 **[OK]** をクリックします。

テナント共通のセキュリティ ポリシーを確認する APIC

ここでは、APIC でテナント共通でのセキュリティ ポリシーを確認する方法を説明します。

手順

ステップ 1 Cisco APIC にテナントとしてログインし、**TENANTS** を選択します。

ステップ 2 **[Navigation]** ペインで、**[Tenant *your_tenant*]** > **[Networking]** > **[Security Policies]** > **[Contracts]** の順に展開します。

a) **[Contracts]** の下にネストされている名前が、プロバイダーとコンシューマの名前であることを確認します。(SYSLOG-EPG_ctrct_web-hosts)

ステップ 3 **[Navigation]** ペインで、**[Tenant *your_tenant*]** > **[Networking]** > **[Security Policies]** > **[Filters]** の順に展開します。

a) **[Filters]** の下にネストされている名前が、プロバイダーとコンシューマの名前であることを確認します。(SYSLOG-EPG_flt_web-hosts)

ステップ 4 **[Navigation]** ペインで、**[Tenant *your_tenant*]** > **[Networking]** > **[Application Profiles]** > **[default]** > **[Application EPGs]** > **[EPG web-hosts]** > **[Contracts]** の順に展開します。

a) **[Work]** ペインで、コンシューマが **[Comsumed]** であることを確認します。

ステップ 5 **[Navigation]** ペインで、**[Tenant *your_tenant*]** > **[Networking]** > **[Application Profiles]** > **[default]** > **[Application EPGs]** > **[EPG SYSLOG-EPG-hosts]** > **[Contracts]** の順に展開します。

a) **[Work]** ペインで、プロバイダーが **[Provided]** であることを確認します。

テナント共通でのセキュリティ ポリシーの接続の確認

ここでは、テナント共通でのセキュリティ ポリシーの接続を確認する方法について説明します。

手順

ステップ 1 仮想マシン（Web ホスト）にログインし、コマンドラインから他の VM（SYSLOG-EPG）を ping します。

ステップ 2 仮想マシン（SYSLOG-EPG）にログインし、コマンドラインから他の VM（Web ホスト）を ping します。

これにより、VM が互いに通信していることが確認できます。

セキュリティ ポリシー（アクセス コントロール リスト）の更新

ここでは、セキュリティ ポリシー（アクセス コントロール リスト）を更新する方法を説明します。

手順

ステップ 1 テナントとして vRealize Automation にログインし、**[Catalog]** > **[Network Security]** の順に選択します。

ステップ 2 [Update Security policies (Access Control Lists)] を選択します。

ステップ 3 [Request] を選択します。

ステップ 4 [Request Information] タブで、要求の説明を入力します。

ステップ 5 [Next] を選択します。

ステップ 6 [Step] タブで、次の操作を実行します。

a) [apic security filter name] フィールドで [Add] をクリックして、vRealize によってプッシュされたフィルタを見つけて選択します。

b) [Rule Entry List] フィールドに値を入力し、[Save] をクリックします。ルール エントリ リストを再作成する必要があります。

（注）
このセキュリティ ポリシー（アクセス コントロール リスト）の更新を行うと、新しいルールが追加され、同じ名前の既存ルールは上書きされます。

次の表は、各ルール エントリの値を示しています。

ルール エントリ リスト	値
dstFormPort	• ブランク • 未指定 • 1 ～ 65535
dstToPort	• ブランク • 未指定 • 1 ～ 65535

ルール エントリ リスト	値
protocol	• icmp • icmpv6 • tcp • udp • ブランク
etherType	• IP • 『ARP』

c) [Update firewall access-list] フィールドで、アクセス リストがファイアウォールで使用されている場合は [Yes] をクリックし、そうでない場合は [No] をクリックします。

d) [送信（Submit）] をクリックします。

ステップ 7 [OK] をクリックします。

ステップ 8 要求を確認するには、[Requests] タブを選択します。

a) 送信した要求を選択し、[view details] をクリックします。ステータスが [Succesful] であることを確認します。

セキュリティ ポリシー（アクセス コントロール リスト）の削除

ここでは、セキュリティ ポリシー（アクセス コントロール リスト）を削除する方法について説明します。

手順

ステップ 1 テナントとして vRealize Automation にログインし、**[Catalog]** > **[Network Security]** の順に選択します。

ステップ 2 [Delete Security policies (Access Control Lists)] を選択します。

ステップ 3 [Request] を選択します。

ステップ 4 [Request Information] タブで、要求の説明を入力します。

ステップ 5 [Next] を選択します。

ステップ 6 [Step] タブで、次の操作を実行します。

a) [Comsume Network/EPG name] フィールドで [Add] をクリックし、プロバイダーのネットワーク/EPG を検索して選択します。（Web ホスト）

b) [Provider Network/EPG name] フィールドで [Add] をクリックし、プロバイダーのネットワーク/EPG を検索して選択します。（app-host）

c) [送信（Submit）] をクリックします。

ステップ 7 [OK] をクリックします。

ステップ 8 要求を確認するには、[Requests] タブを選択します。

a) 送信した要求を選択し、[view details] をクリックします。ステータスが [Succesful] であることを確認します。

VPC プランでのネットワークの作成

ここでは、VPC プランでネットワークを作成する方法を説明します。

手順

ステップ 1 vRealize Automation アプライアンスにテナントとしてログインし、**[Catalog]** > **[Tenant VPC Plan]** > **[Add Tenant Network - VPC plan]** の順に選択して [Request] をクリックします。

ステップ 2 [Request Information] ペインで、次の操作を実行します。

a) [Description] フィールドに、説明を入力します。

b) [Next] をクリックします。

ステップ 3 [Step] ペインで、次の操作を実行します。

a) [Network/EPG name] フィールドに、ネットワーク/EPG 名を入力します。（web-hosts-vpc）

b) [Domain Type] フィールドでドロップダウン リストから、仮想マシンに接続する場合は [VmmDomain (Dynamic Binding)]、物理インフラストラクチャに接続する場合は [PhysDomain (Static Binding)] を選択します。Ciscoでは、vRealize プラグインの全機能を使用するには、**VmmDomain (Dynamic Binding)** を選択することを推奨します。

c) **Domain/DVS** フィールドで、**Add** をクリックし、***your_apic*** > **vCenters** > ***your_vcenter*** を展開し、DVS を選択します。

d) カプセル化モードとして、**encapMode** ドロップダウンリストから **Auto**、 **VLAN**、または **VXLAN** のいずれかを選択します。

（注）
encapMode フィールドは、VMM ドメイン タイプが Cisco AVS の場合、または Cisco ACI Virtual Edge (ローカル スイッチング) の場合にのみ適用されます。VDS VMM ドメインで VLAN または VXLAN を選択すると、予期しない結果が生じる可能性があります。

e) **Application Tier Number** フィールドに、1 ～ 10 の数値を入力します。

f) **Intra EPG Deny** フィールドで、**Yes** または **No** のいずれかの値を選択します。

g) **Allow Microsegmentation** フィールドで、**Yes** または **No** のいずれかの値を選択します。

（注）
Allow Microsegmentation フィールドは VMM ドメイン タイプが VDS VMM ドメインである場合にのみ適用されます。

h) **Use Default BD?** フィールドでは、**Yes** または **No** のいずれかの値を選択します。

No を選択した場合、**Add** をクリックして、カスタム ブリッジ ドメインを選択します。

- ***your_apic_user*** > **Tenants** > ***your_tenant*** > **Networking** > **BridgeDomains** > ***your_bridgedomain*** を展開し、このブリッジ ドメインを選択します。

i) [Subnet prefix] フィールドに、ゲートウェイ IP アドレスとサブネット マスクを入力します。（192.168.1.1/24）

サブネット プレフィクスは、この VPC で任意のホストに対して利用できるサブネットです。

j) [送信（Submit）] をクリックします。

k) [OK] をクリックします。

ステップ 4 [Requests] を選択します。

ステップ 5 送信した要求を選択し、[view details] をクリックします。

ステップ 6 要求のステータスが **Successful** であることを確認します。

APIC での VPC プランのネットワークの確認

ここでは、APIC で VPC プランのネットワークを確認する方法を説明します。

手順

ステップ 1 Cisco APICへテナントとしてログインして、 **Tenants** > ***your_tenant*** を選択します。

ステップ 2 [Navigation] ペインで、**[Tenant *your_tenant*] > [Application Profiles] > [default] > [Application EPGs] > [EPG web-hosts-vpc]** の順に選択します。

ステップ 3 [properties] ペインの [Bridge Domain] フィールドで、テナント名と bd1 があることを確認します。（green/bd1）

ステップ 4 [Navigation] ペインで、**[Tenant *your_tenant*] > [Application Profiles] > [default] > [Application EPGs] > [EPG web-hosts-vpc] > [Domains (VMs and Bare-Metals)]** の順に選択します。

ステップ 5 状態が作成され、ドメイン プロファイルが VMware/*vmmdomain_you_specified VMware/* であることを確認します。

ステップ 6 [Navigation] ペインで、**[Tenant *your_tenant*] > [Networking] > [Bridge Domains] > [bd1] > [Subnets]** の順に選択します。

ステップ 7 [Subnets] で、指定したサブネット プレフィクスが存在することを確認します。

vCenter での VPC プランのネットワークの確認

ここでは、vCenter で VPC プランのネットワークを確認する方法を説明します。

手順

ステップ 1 vSphere Web クライアント GUI にログインし、[Networking] アイコンを選択します。

ステップ 2 ナビゲーション ウィンドウで、***vCenter_IP/Host*** > **Datacenter** > ***green*** > ***distributed_virtual_switch*** > ***port_group*** を選択し、存在することを確認します。

port_group 名の形式は、テナント名|アプリケーション プロファイル名|アプリケーション EPG 名です。

VMM ドメインとのテナント ネットワークの関連付けを更新する

このセクションでは、VMM ドメインとテナント ネットワークの関連付けを更新する方法について説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして **[カタログ]** を選択します。

ステップ 2 **navigation** ウィンドウで、**Tenant Network services** を選択します。

ステップ 3 **[テナントネットワークの更新]** を選択し、次の操作を実行します。

a) 入力フィールドのサービス ブループリント情報を表示し、[Request] をクリックします。

b) [Request Information] ペインで説明を追加して、[Next] をクリックします。

c) **[テナント名]** フィールドで、該当するテナントの名前を入力します。

d) **ネットワーク/EPG** フィールドで、をクリックして **Add** 、展開 ***your_apic*** > **テナント** > ***your_tenant*** > **エンド小数点グループ** 、EPG を選択します。

e) **Domain Type** ドロップダウン リストから、ドメイン タイプを選択します。ドメイン タイプが VMware VDS または Cisco AVS または Cisco ACI Virtual Edge に対して **VmmDomain**（**ダイナミック バインディング**） です。

f) **[ドメイン/DVS フィールド]** で、**[追加]** をクリックし、***your_apic*** > **vCenters** > ***your_vcenter*** を展開して、VMM ドメインにテナント ネットワーク（EPG）を関連付ける DVS を選択します。

g) **encapMode** ドロップダウンリストから、**Auto**、 **VLAN**、または **VXLAN** をカプセル化モードとして選択します。

（注）
encapMode フィールドは、EPG を Cisco AVS の VMM ドメインまたは Cisco ACI Virtual Edge(ローカル スイッチング)タイプに関連付ける場合にのみ、適用されます。関連付けは次の手順で実行します。

h) **操作** ドロップダウン リストから、**[追加]** を選択して VMM ドメインと テナント ネットワークに関連付けるか、**[削除]** を選択して VMM ドメインからテナント ネットワークの関連付けを解除します。

i) **[スイッチング モード]** セレクタで、**[ネイティブ]** または **[AVE]** を選択します。

[ネイティブ] オプションはデフォルトのスイッチングであり、**[AVE]** は Cisco ACI Virtual Edge のためのものです。

j) [Submit] をクリックします。

APIC で VMM ドメインとテナント ネットワークの関連付けを確認する

このセクションでは、APIC 上の VMM ドメインとテナント ネットワークの関連づけを確認する方法について説明します。

手順

ステップ 1 APIC にテナントとしてログインし、 **Tenants** > **your_tenant** を選択します。

ステップ 2 **navigation** ウィンドウで、**Tenant** ***your_tenant*** > **Application Profiles** > **default** > **Application EPGs** > **your_tenant_network** > **Domains (VMs and Bare-Metals)** を選択します。

ステップ 3 VMM ドメインの関連付けが正しいことを確認します。

マイクロセグメンテーション

このセクションでは、共有されるマイクロセグメンテーションと VPC プランについて記し、ユーザに関連するサービス ブループリントについて説明します。

（注） Cisco APIC vRealize プラグイン 2.0(1) リリース以降では、マイクロセグメンテーションに関連するサービス ブループリントは、Cisco AVS VMM ドメインでのみサポートされるようになりました。

ACI でのマイクロセグメンテーション

Cisco ACI でマイクロセグメンテーションを使用すると、さまざまな属性に基づいて、エンドポイントをエンドポイント グループ (EPG) と呼ばれる論理セキュリティ ゾーンに自動的に割り当てることができます。

マイクロセグメンテーションの詳細については、「Microsegmentation with Cisco ACI」を参照してください『*Cisco ACI Virtualization Guide*』に含まれています。

共有プランのマイクロセグメンテーション

共有プランでは、マイクロセグメントの作成、更新、および削除を行うことができます。

共有プランでのマイクロセグメンテーションの作成

ここでは、共有プランでマイクロセグメントを作成する方法を説明します。

（注） Cisco APIC リリース 5.0（1）以降、Cisco Application Virtual Switch（AVS）はサポートされなくなりました。Cisco AVS を使用して Cisco APIC リリース 5.0(1) にアップグレードする場合、問題が発生した際にファブリックはサポートされません。また、Cisco AVS ドメインの障害が発生します。

Cisco AVS を使用する場合は、Cisco ACI Virtual Edge に移行することを推奨します。ポリシーについては、『*Cisco ACI Virtual Edge Installation Guide*』を参照してください。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして **Catalog**を選択します。

ステップ 2 **navigation** ウィンドウで、**Tenant Shared Plan** を選択します。

ステップ 3 **[Useg ネットワークの追加 - 共有プラン]** を選択し、次の手順を実行します。:

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) [Request Information] ペインで説明を追加して [Next] をクリックします。

c) **Tenant name** フィールドに、対応するテナントの名前を入力します。

d) **ネットワーク/EPG 名** フィールドを作成する microsegment (uSeg) の名前を入力します。

e) **Domain Type** ドロップダウン リストから、ドメイン タイプを選択します。Cisco AVS または Cisco ACI Virtual Edge VMM ドメインの場合、ドメイン タイプは **VmmDomain (Dynamic Binding)** です。

f) **[ドメイン/DVS]** フィールドで、**[追加]** をクリックし、***your_apic*** > **vCenters** > ***your_vcenter***, を展開し、DVS (Cisco AVS または Cisco ACI Virtual Edge VMM ドメイン) を選択して、uSeg をVMM ドメインに関連付けます。

g) **encapMode** ドロップダウンリストから、**Auto**、 **VLAN**、または **VXLAN** をカプセル化モードとして選択します。

（注）
encapMode フィールドは、**VMM ドメイン** タイプが Cisco AVS または Cisco ACI Virtual Edge (ローカル スイッチング) の場合にのみ適用されます。

h) **アプリケーション層番号** フィールドで、uSeg が所属する層の数を入力します。デフォルトの階層番号は 1 です。入力する階層番号は、サービス ブループリントの **[テナントの追加または更新]** オプションを介してテナントの作成の一部として作成されたアプリケーション階層の番号以下である必要があります。

たとえば、階層番号 2 を入力すると、uSeg が VRF（共通/デフォルト）の一部である BD（共通/cmnbd2）に配置されます。参考資料については、次の表を参照してください。

階層番号	BD	VRF
1	common/default	common/default
2	common/cmnbd2	common/default
3	common/cmnbd3	common/default

i) **内通 EPG 拒否** ドロップダウンリスト、選択 **はい** 内通 EPG の分離を適用します。選択 **No** 内通 EPG の分離を実施したくない場合。

AVS または Cisco ACI Virtual Edge VLAN モード、DVS-VXLAN モード、または Microsoft VMM ドメインでは、EPG 内分離はサポートされていません。これらのモードまたはドメインで EPG 内分離を適用すると、ポートがブロックされた状態に移行する可能性があります。

j) **Ip 条件** テーブルで、をクリックして **New** し、IP 条件 (または IP の属性) を入力します。エントリごとに、次の列が適用されます。

- **名前** : IP の条件 (または IP の属性) の名前。
- **Description**— IP 基準の説明です。
- **IP**— IP アドレスとして、アドレスまたはサブネットを指定します (たとえば 1.1.1.1 または 1.1.1.0/30)。

k) **Mac 条件** テーブルで、をクリックして **New** し、MAC 条件 (または MAC 属性) を入力します。エントリごとに、次の列が適用されます。

- **名前** : MAC 条件 (または MAC 属性) の名前。
- **Description**— MAC 基準の説明です。
- **MAC**— MAC アドレスとして、アドレスを指定します (たとえば 00:50:56:44:44:5D)。

l) **VM 条件** テーブルで、をクリックして **New** し、VM の条件 (または VM 属性) を入力します。エントリごとに、次の列が適用されます。

- **Name**— VM 基準 (または VM 属性) の名前です。
- **Type**— 次の表には、サポートされている属性タイプ、APIC でのそのマッピング、および例が示されています。(MAC 属性と IP の属性がある優先順位 1 および 2 は、それぞれ。)

vRealize でのタイプ	APIC でのタイプ (マッピング)	優先順位	例
vnic	VNic Dn	3	00:50:56:44:44:5 D

vRealize でのタイプ	APIC でのタイプ (マッピング)	優先順位	例
vm	VM ID	4	vm 821
vmName	VM Name	5	HR_VDI_VM1
hv	ハイパーバイザ ID	6	ホスト 43
domain	VMM ドメイン	7	AVS-SJC-DC1
datacenter	データセンター	8	DCI
正しい	カスタム属性	9	SG_DMZ
guestOS	オペレーティングシステム	10	Windows 2008。

- **演算子** ：次の表は、サポートされている演算子とそのマッピングで APIC 。

VRealize で演算子	[オペレータ APIC (マッピング)
equals	Equals
contains	Contains
startsWith	Starts With
endsWith	Ends With

- **AttributeName**— 属性名を入力します。VM の条件の表の **AttributeName** は、**customLabel** 属性タイプにのみ適用されます。
- **VmmDomain_vC_VmName**— VM の条件の表では、これは **vnic** タイプ、**equals** 演算子にのみ適用されます。入力形式は <VmmDomain>/<vC>/<VmName> で、ここで <VmmDomain> (AVS VMM ドメイン) と <vC> (vCenter) はコントローラのインスタンスに属します。例：vmmdomain1/vcenter1/VM1。
- **Value**— 属性タイプの値を入力します。各属性タイプの例は、上記のタイプの表に示されています。

m) [Submit] をクリックします。

次のタスク

APIC で共有プランでのマイクロセグメンテーションの作成を確認する （77 ページ）の手順を完了します。

APIC で共有プランでのマイクロセグメンテーションの作成を確認する

このセクションでは、 Application Policy Infrastructure Controller共有プランでのマイクロセグメンテーションの作成が成功したことを確認する方法について説明します 。

手順

ステップ 1 テナントに Cisco APIC としてログインし、**Tenants** > ***your_tenant*** を選択します。

ステップ 2 [Navigation] ペインで、**[Tenant]** ***[your_tenant]*** > **[Application Profiles]** > **[default]** > **[uSeg EPGs]** の順に選択します。

ステップ 3 **uSeg EPGs** ペインで、プロパティの表示が必要な uSeg をダブルクリックします。

ステップ 4 **[Properties]** ペインで、設定が正しいことを確認してください。

ステップ 5 [Navigation] ペインで、**[Tenant]** ***[your_tenant]*** > **[Application Profiles]** > **[default]** > **[uSeg EPGs]** > ***[your_useg]*** > **[Domains (VMs and Bare-Metals)]** の順に選択します。

ステップ 6 状態が形成され、ドメインプロファイルが Vmware/vmmdomain_you_specified*vmmdomain_you_specified* であることを確認します。

共有プランのマイクロセグメントの削除

このセクションでは、マイクロセグメントの削除方法について説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして **Catalog**を選択します。

ステップ 2 **navigation** ウィンドウで、**Tenant Shared Plan** を選択します。

ステップ 3 **Delete a Useg Network - Shared Plan** を選択して、次の操作を実行します:

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) [Request Information] ペインで説明を追加して [Next] をクリックします。

c) **Tenant name** フィールドで、テナント名が対応するテナントにハード コードされていることを確認します。

d) **Network/EPG** フィールドで、**Add** をクリックし、***priapic*** > **Tenants** > ***appurtenant*** > **Useg-End-Point-Groups**を展開し、マイクロセグメント EPG を選択します。

e) [Submit] をクリックします。

次のタスク

APIC で"マイクロセグメンテーション"削除の確認 （78 ページ）の手順を完了します。

APIC で"マイクロセグメンテーション"削除の確認

このセクションでは、Application Policy Infrastructure Controller でマイクロセグメントの削除を確認する方法について説明します。

手順

ステップ 1 テナントに Cisco APIC としてログインし、**Tenants** > ***your_tenant*** を選択します。

ステップ 2 [Navigation] ペインで、**[Tenant]** ***[your_tenant]*** > **[Application Profiles]** > **[default]** > **[uSeg EPGs]** の順に選択します。

ステップ 3 **USeg Epg**] ペインで、削除された uSeg が存在しないことを確認します。

VPC プランには、"マイクロセグメンテーション"

作成、更新、および VPC プランで、microsegment を削除することができます。

VPC プランでのマイクロセグメンテーションの作成

ここでは、VPC プランでネットワークを作成する方法を説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして **Catalog**を選択します。

ステップ 2 [Navigation] ペインで、[Tenant VPC Plan] を選択します。

ステップ 3 選択 **Useg ネットワーク - VPC プランを追加** し、次の手順を実行します。

a) 入力フィールドのサービスブループリント情報を表示して [Request] をクリックします。

b) [Request Information] ペインで説明を追加して [Next] をクリックします。

c) **Tenant name** フィールドに、対応するテナントの名前を入力します。

d) **ネットワーク/EPG 名** フィールドを作成する microsegment (uSeg) の名前を入力します。

e) **Domain Type** ドロップダウン リストから、ドメイン タイプを選択します。

f) **ドメイン/DVS** フィールドで、をクリックして **Add** 、展開 ***your_apic*** > **vCenters** > ***your_vcenter*** 、DVS を選択します (Cisco AV または Cisco ACI Virtual Edge VMM ドメイン) VMM に uSeg を関連付けるドメイン。

g) **EncapMode** ドロップダウンリスト、選択 **自動** 、 **VLAN** 、または **VXLAN** モード (mode) カプセル化します。

（注）
EncapMode フィールドは、VMM ドメイン タイプが Cisco AV 場合にのみ適用されます。 または Cisco ACI Virtual Edge (ローカル スイッチング)。

h) **Subnet** フィールドに、ゲートウェイ IP アドレスとサブネット マスクを入力します（1.1.1.1/24）。

i) **アプリケーション層番号** フィールドで、uSeg が所属する層の数を入力します。デフォルトの階層番号は1です。入力した階層番号はサービスブループリントを介してテナントの作成の一部として作成されたアプリケーション層の数以下である必要があります **追加または更新テナント** オプション。

たとえば、名前付きテナント コーク 、uSeg が VRF (コーク/ctx1) の一部である BD (コーク/bd2) に配置されます層番号2を入力するかどうか。参考資料については、次の表を参照してください。

階層番号	BD	VRF
1	コーク/bd1	コーク/ctx1
2	コーク/bd2	コーク/ctx1
3	コーク/bd3	コーク/ctx1

j) **内通 EPG 拒否** ドロップダウンリスト、選択 **はい** 内通 EPG の分離を適用します。選択 **No** 内通 EPG の分離を実施したくない場合。

Cisco AV で内通 EPG 分離はサポートされていませんまたは Cisco ACI Virtual Edge VLAN モード、DVS VXLAN モードまたは Microsoft VMM ドメイン。これらのモードまたはドメイン内 EPG の分離を強制する場合は、ポートがブロックされた状態に移動可能性があります。

k) **Ip 条件** テーブルで、をクリックして **New** し、IP 条件 (または IP の属性) を入力します。エントリごとに、次の列が適用されます。

- **名前** : IP の条件 (または IP の属性) の名前。
- **Description**— IP 基準の説明です。
- **IP**— IP アドレスとして、アドレスまたはサブネットを指定します (たとえば 1.1.1.1 または 1.1.1.0/30)。

l) **Mac 条件** テーブルで、をクリックして **New** し、MAC 条件 (または MAC 属性) を入力します。エントリごとに、次の列が適用されます。

- **名前** : MAC 条件 (または MAC 属性) の名前。
- **Description**— MAC 基準の説明です。
- **MAC**—MAC アドレスとして、アドレスを指定します (たとえば 00:50:56:44:44:5D)。

m) **VM 条件** テーブルで、をクリックして **New** し、VM の条件 (または VM 属性) を入力します。エントリごとに、次の列が適用されます。

- **Name**— VM 基準 (または VM 属性) の名前です。
- **Description**— VM 基準の説明です。

- **Type**— 次の表には、サポートされている属性タイプ、APIC でのそのマッピング、および例が示されています。(MAC 属性と IP の属性がある優先順位 1 および 2 は、それぞれ。)

vRealize でのタイプ	APIC でのタイプ (マッピング)	優先順位	例
vnic	VNic Dn	3	00:50:56:44:44:5 D
vm	VM ID	4	vm 821
vmName	VM Name	5	HR_VDI_VM1
hv	ハイパーバイザ ID	6	ホスト 43
domain	VMM ドメイン	7	AVS-SJC-DC1
datacenter	データセンター	8	DCI
正しい	カスタム属性	9	SG_DMZ
guestOS	オペレーティングシステム	10	Windows 2008。

- **演算子** : 次の表は、サポートされている演算子とそのマッピングで APIC 。

VRealize で演算子	[オペレータ APIC (マッピング)
equals	Equals
contains	Contains
startsWith	Starts With
endsWith	Ends With

- **AttributeName**— 属性名を入力します。VM の条件の表で、 **AttributeName** にのみ適用されます、 **正しい** 属性のタイプ。
- **VmmDomain_vC_VmName**]: タイプにのみ適用されますが、VM の条件でテーブル **vnic** 、オペレータ **と等しい** 。入力する形式は<VmmDomain>/<vC>/<VmName> where <VmmDomain>(AV VMM ドメイン) および<vC>(vCenter) コントローラ インスタンスに属して</vC></VmmDomain></VmName></vC></VmmDomain>。例: vmmdomain1/vcenter1/VM1。
- **Value**— 属性タイプの値を入力します。各属性タイプの例は、上記のタイプの表に示されています。

n) [Submit] をクリックします。

次のタスク

APIC 上の VPC プランでのマイクロセグメンテーション作成の確認 （81 ページ）の手順を完了します。

APIC 上の *VPC* プランでのマイクロセグメンテーション作成の確認

このセクションでは、Application Policy Infrastructure Controller の VPC プランでのマイクロセグメンテーション作成の検証方法について説明します。

手順

ステップ 1 テナントに Cisco APIC としてログインし、**Tenants** > ***your_tenant*** を選択します。

ステップ 2 [Navigation] ペインで、**[Tenant]** ***[your_tenant]*** > **[Application Profiles]** > **[default]** > **[uSeg EPGs]** の順に選択します。

ステップ 3 **uSeg EPGs** ペインで、プロパティの表示が必要な uSeg をダブルクリックします。

ステップ 4 **[Properties]** ペインで、設定が正しいことを確認してください。

ステップ 5 [Navigation] ペインで、**[Tenant]** ***[your_tenant]*** > **[Application Profiles]** > **[default]** > **[uSeg EPGs]** > ***[your_useg]*** > **[Domains (VMs and Bare-Metals)]** の順に選択します。

ステップ 6 状態が形成され、ドメインプロファイルが Vmware/vmmdomain_you_specified*vmmdomain_you_specified* であることを確認します。

ステップ 7 [Navigation] ペインで、**[Tenant]** ***[your_tenant]*** > **[Networking]** > **[Bridge Domains]** > ***[corresponding_bd]*** > **[Subnets]** の順に選択します。

ステップ 8 **[Subnets]** で、指定したサブネット プレフィクスが存在することを確認します。

VPC プランのマイクロセグメントの削除

このセクションでは、マイクロセグメントの削除方法について説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして **Catalog**を選択します。

ステップ 2 [Navigation] ペインで、[Tenant VPC Plan] を選択します。

ステップ 3 **Delete a Useg Network - VPC Plan** を選択して、次の手順に従います:

a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。

b) [Request Information] ペインで説明を追加して [Next] をクリックします。

c) **Tenant name** フィールドで、テナント名が対応するテナントにハード コードされていることを確認します。

d) **Network/EPG** フィールドで、**Add** をクリックし、***your_apic*** > **Tenants** > ***your_tenant*** > **Useg-End-Point-Groups** を展開し、uSeg EPG を選択します。

e) [Submit] をクリックします。

次のタスク

APIC で"マイクロセグメンテーション"削除の確認 （78 ページ）の手順を完了します。

マイクロセグメンテーション属性の更新

このセクションでは、既存のマイクロセグメンテーションを更新する方法について説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして **Catalog** を選択します。

ステップ 2 **navigation** ウィンドウで、**Tenant Network services** を選択します。

ステップ 3 **[Useg 属性の追加または削除]** を選択し、次の手順を実行します。

a) 入力フィールドのサービスブループリント情報を表示して [Request] をクリックします。

b) [Request Information] ペインで説明を追加して [Next] をクリックします。

c) **[ネットワーク/EPG]** フィールドで、**[追加]** をクリックし、***your_apic*** > **Tenants** > ***your_tenant*** > **Useg-End-Point-Groups** を展開して uSeg EPG を選択します。

d) **Tenant name** フィールドに、対応するテナントの名前を入力します。

e) IP 条件を追加する場合、**[Ip 条件の追加]** テーブルで、**[新規]** をクリックし、IP 条件（または IP の属性）を入力します。エントリごとに、次の列が適用されます。

- **名前** : IP の条件 (または IP の属性) の名前。
- **Description**— IP 基準の説明です。
- **IP**— IP アドレスとして、アドレスまたはサブネットを指定します (たとえば 1.1.1.1 または 1.1.1.0/30)。

f) MAC 条件を追加する場合、**[MAC 条件の追加]** テーブルで、**[新規]** をクリックし、MAC 条件（または MAC の属性）を入力します。エントリごとに、次の列が適用されます。

- **名前** : MAC 条件 (または MAC 属性) の名前。
- **Description**— MAC 基準の説明です。
- **MAC**—MAC アドレスとして、アドレスを指定します (たとえば 00:50:56:44:44:5D)。

g) VM 条件を追加する場合、**[VM 条件の追加]** テーブルで、**[新規]** をクリックし、VM 条件（または VM の属性）を入力します。エントリごとに、次の列が適用されます。

- **Name**— VM 基準 (または VM 属性) の名前です。

- **Type**— 次の表には、サポートされている属性タイプ、APIC でのそのマッピング、および例が示されています。(MAC 属性と IP の属性がある優先順位 1 および 2 は、それぞれ。)

vRealize でのタイプ	APIC でのタイプ (マッピング)	優先順位	例
vnic	VNic Dn	3	00:50:56:44:44:5 D
vm	VM ID	4	vm 821
vmName	VM Name	5	HR_VDI_VM1
hv	ハイパーバイザ ID	6	ホスト 43
domain	VMM ドメイン	7	AVS-SJC-DC1
datacenter	データセンター	8	DCI
正しい	カスタム属性	9	SG_DMZ
guestOS	オペレーティングシステム	10	Windows 2008。

- **演算子** : 次の表は、サポートされている演算子とそのマッピングで APIC 。

VRealize で演算子	[オペレータ APIC (マッピング)
equals	Equals
contains	Contains
startsWith	Starts With
endsWith	Ends With

- **AttributeName**— 属性名を入力します。VM の条件の表の **AttributeName** は、**customLabel** 属性タイプにのみ適用されます。
- **Value**— 属性タイプの値を入力します。各属性タイプの例は、上記のタイプの表に示されています。
- **VmmDomain_vC_VmName**— VM の条件の表では、これは **vnic** タイプ、**equals** 演算子にのみ適用されます。入力形式は <VmmDomain>/<vC>/<VmName> で、ここで <VmmDomain> (AVS VMM ドメイン) と <vC> (vCenter) はコントローラのインスタンスに属します。例：vmmdomain1/vcenter1/VM1。

h) 既存の IP 条件を追加する場合、**[IP 条件の削除]** テーブルで、**[新規]** をクリックし、削除する IP 条件（または IP の属性）の名前を入力します。

i) 既存の MAC 条件を削除する場合、**[MAC 条件の削除]** テーブルで、**[新規]** をクリックし、削除する MAC 条件（または MAC の属性）の名前を入力します。

j) 既存の VM 条件を削除する場合、**[VM 条件の削除]** テーブルで、**[新規]** をクリックし、削除する VM 条件（または VM 属性）の名前を入力します。
k) [Submit] をクリックします。

次のタスク

APIC でのマイクロセグメンテーション属性の更新を確認する （84 ページ）の手順を完了します。

APIC でのマイクロセグメンテーション属性の更新を確認する

このセクションでは、マイクロセグメンテーション属性が Application Policy Infrastructure Controller 上で更新されたことを確認する方法について説明します。

手順

ステップ 1 テナントに Cisco APIC としてログインし、**Tenants** > ***your_tenant*** を選択します。
ステップ 2 [Navigation] ペインで、**[Tenant]** ***[your_tenant]*** > **[Application Profiles]** > **[default]** > **[uSeg EPGs]** の順に選択します。
ステップ 3 **uSeg EPGs** ペインで、プロパティの表示が必要な uSeg をダブルクリックします。
ステップ 4 **Properties** ペインで、**uSeg Attributes** フィールドの属性が更新されたことを確認します。

Cisco AVS または Cisco ACI Virtual Edge VMM ドメインとマイクロセグメンテーションの関連付けを更新する

このセクションでは、Cisco AVS または Cisco ACI Virtual Edge VMM ドメインに関連付けられている マイクロセグメンテーションを更新する方法について説明します。

手順

ステップ 1 vRealize Automation にテナント管理者としてログインして **Catalog** を選択します。
ステップ 2 **navigation** ウィンドウで、**Tenant Network services** を選択します。
ステップ 3 **Update Tenant Network** を選択し、次の手順を実行します。
a) 入力フィールドのサービス ブループリント情報を表示して [Request] をクリックします。
b) **Request Information** ペインで説明を追加して、**Next** をクリックします。
c) **Tenant name** フィールドに、対応するテナントの名前を入力します。
d) **Network/EPG** フィールドで、**Add** を選択し、***your_apic*** > **Tenants** > ***your_tenant*** > **Useg-End-Point-Groups** を展開し、uSeg EPG を選択します。

e) **Domain Type** ドロップダウン リストから、ドメイン タイプを選択します。Cisco AVS または Cisco ACI Virtual Edge VMM ドメインの場合、ドメイン タイプは **VmmDomain (Dynamic Binding)** です。

f) **Domain/DVS** フィールドで、**Add** をクリックし、***your_apic*** > **vCenters** > ***your_vcenter*** を展開し、DVS (Cisco AVS または Cisco ACI Virtual Edge VMM ドメイン) を選択して、uSeg を VMM ドメインに関連付けます。

g) **encapMode** ドロップダウンリストから、**Auto**、**VLAN**、または **VXLAN** をカプセル化モードとして選択します。

（注）
encapMode フィールドは、EPG を Cisco AVS の VMM ドメインまたは Cisco ACI Virtual Edge (ローカル スイッチング) タイプに関連付ける場合にのみ、適用されます。関連付けは次の手順で実行します。

h) **Operation** ドロップダウンリストから **add** を選択して、マイクロセグメントを Cisco AVS または Cisco ACI Virtual Edge ドメインに関連付けます。**delete** を選択して、マイクロセグメントを Cisco AVS または Cisco ACI Virtual Edge VMM ドメインとの関連付けからを解除します。

i) [Submit] をクリックします。

次のタスク

APIC 上の Cisco AVS または Cisco ACI Virtual Edge VMM ドメインでのマイクロセグメント関連づけの更新を確認する （85 ページ）の手順を完了します。

APIC 上の Cisco AVS または Cisco ACI Virtual Edge VMM ドメインでのマイクロセグメント関連づけの更新を確認する

このセクションでは Cisco APIC 上での シスコの AVS または Cisco ACI Virtual Edge VMM ドメインとのマイクロセグメント関連付けの更新を確認する方法について説明します。

手順

ステップ 1 テナントとして Cisco APIC にログインし、**[テナント（Tenants）]** > ***[your_tenant]***を選択します。

ステップ 2 ナビゲーション ペインで、**[テナント（Tenant）]*[your_tenant]*** > **[アプリケーション プロファイル（Application Profiles）]** > **[デフォルト（default）]** > **[uSeg EPGs]** > ***[your_useg]*** > **[ドメイン（VM およびベアメタル（Domains (VMs and Bare-Metals)）]** を選択します。

ステップ 3 VMM ドメインの関連付けが正しいことを確認します。

マシン ブループリントを使用しない VM の作成とネットワークへの接続

ここでは、マシンブループリントを使用せずにマシン（VM）を作成しネットワークに接続する方法を説明します。

手順

ステップ 1 vSphere Web クライアント GUI にログインし、[Networking] アイコンを選択します。

ステップ 2 次に ウィンドウで、***[vCenter_IP/Host]*** > **[Datacenter]** > **[Unmanaged]** の順に選択し、ACI ネットワークを接続する仮想マシンを選択します。

ステップ 3 [Summary] ペインの [VM Hardware] セクションで、[Edit Settings] をクリックします。

ステップ 4 [Edit Settings] ダイアログボックスで、ACI ネットワークに接続するネットワーク アダプタを選択して、ドロップダウン リストから作成したポート グループを選択します。
（green|default|web-hosts-vpc (green)）

ステップ 5 [OK] をクリックします。
この VM で ACI ネットワーキングを利用できるようになりました。

ロード バランサのテナント ネットワークへの追加について

ここでは、ロード バランサ サービスをテナント ネットワーク（APIC の EPG）に追加する手順について説明します。このリリースでは、ロードバランサの共有プランのみをサポートします。今後のリリースでは、VPC プランがサポートされます。

このプランでは、ロードバランサを tn-common に導入することで、共有インフラストラクチャを使用して vRA および APIC テナントに消費モデルを提供します。

図 *4:* 共有プラン：ロード バランサの概要

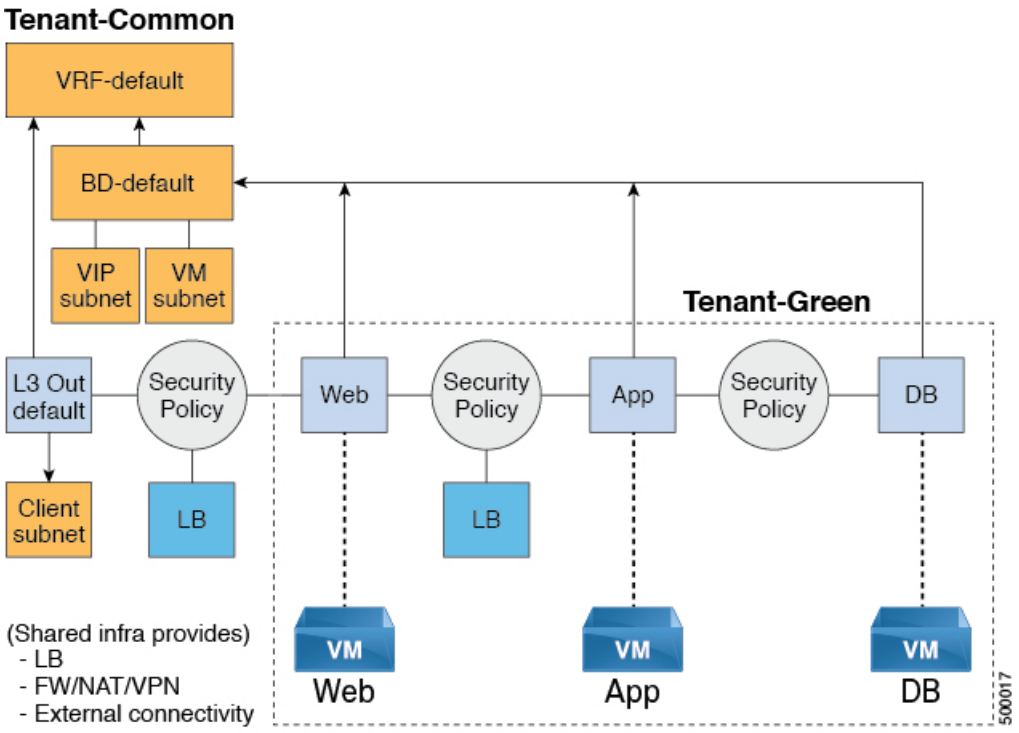
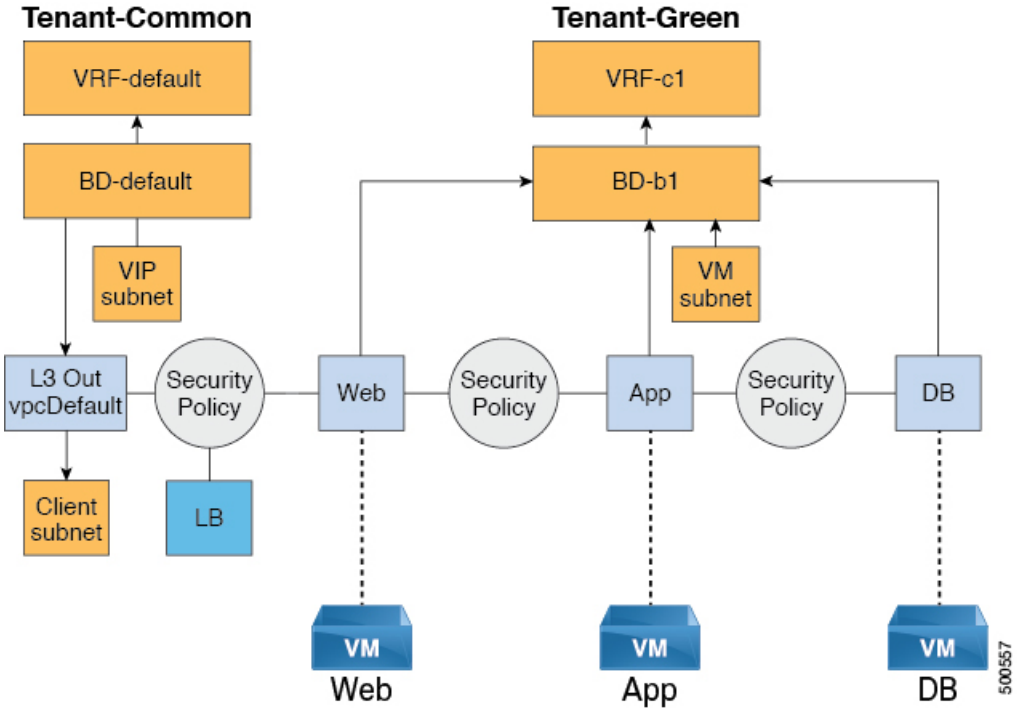


図 *5 : VPC* プラン：ロード バランサのみ



の設定要件 APIC

ここでは、APIC の設定要件について説明します。

- APIC 管理者によって、ロード バランサのデバイス パッケージがアップロードされる必要があります。
- ロード バランサのデバイス クラスタが、APIC 管理者によって tn-common（テナント「共通」）で作成される必要があります。Citrix および F5 は、ロード バランサでサポートされているベンダーです。
- Citrix および F5 の共有プランのロード バランサ サービス グラフ テンプレートが、APIC 管理者によって tn-common で作成される必要があります

VIP プールの追加

ここでは、VIP プールを追加する方法について説明します。

始める前に

vRA テナントが ロード バランサ サービスを利用するには、事前に vRA 管理者が管理者カタログの「VIP プールの追加」サービス ブループリントを使用して、vRA テナントごとに仮想 IP プールを作成する必要があります。

たとえば Tenant-Red の場合、VIP プールは 6.1.1.1 ～ 6.1.1.30 で、Tenant-Green の場合、VIP プールは 6.1.2.1 ～ 6.1.2.30 です。

（注） VIP プールは、テナント「共通」の BD「デフォルト」で定義されているサブネットの 1 つである必要があります。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Admin Services]** の順に選択します。

ステップ 2 **Add VIP Pool** を選択して、次の手順を実行します:

a) **Tenant** フィールドに、テナント名を入力します。
b) **VIP address start** フィールドに、VIP の開始アドレスを入力します。
c) **VIP Address End** フィールドに、VIP の終了アドレスを入力します。
d) **Internal VIP for Inter-EPG in VPC plan** フィールドで、[Yes] または [No] を選択します。
e) [Submit] をクリックします。

VIP プールの削除

ここでは、VIP プールの削除方法について説明します。

このブループリントでは、テナントで消費されるすべてのロード バランサ サービスを削除した後に、VIP プールの必要なクリーンアップを行います。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Admin Services]** の順に選択します。

ステップ 2 選択 **VIP プールの削除** 、次のアクション項目を実行します。

a) **テナント** フィールドで、をクリックして **Add** 、展開 ***your_apic*** > **テナント** し、テナントを選択します。
b) **VIP address start** フィールドに、VIP の開始アドレスを入力します。
c) **VIP Address End** フィールドに、VIP の終了アドレスを入力します。
d) **Internal VIP for Inter-EPG in VPC plan** フィールドで、[Yes] または [No] を選択します。
e) [Submit] をクリックします。

共有プランでのテナント ネットワークへのロード バランサの追加

vRA テナントはテナント ネットワークにロード バランサ（LB）を追加できます。必要なパラメータは、ネットワーク名、LB デバイス クラスタ、LB エンドポイント（プロトコル、ポー

ト）、ベンダー タイプ、およびコンシューマ EPG または L3out です。このワークフローの一部として、プロバイダーEPGとして選択したテナント ネットワークを持つすべての必要なサービス グラフ インスタンスと契約（セキュリティ ポリシー）が作成されます。このロード バランスが設定されたエンドポイントのコンシューマは、テナント共通の L3out であることも、テナントに属する別のテナント ネットワークであることもあります。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant Shared Plan]** の順に選択します。

ステップ 2 [Add Load Balancer to Tenant Network - Shared Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

VPC プランでのテナント ネットワークへのロード バランサの追加

ここでは、VPC プランでのテナント ネットワークへのロード バランサの追加方法について説明します。

（注） VPC プランでは、EPG 間のロード バランサはサポートされていません。リリース 1.2(2x) では、L3out と第 1 階層（Web）間のロード バランサのみをサポートしています。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant VPC Plan]** の順に選択します。

ステップ 2 [Add Load Balancer to Tenant Network - VPC Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

共有プランでのテナント ネットワークからのロード バランサの削除

既存のテナント ネットワークやエンドポイント グループからロードバランサ サービス（lb-port、lb-protocol）を削除できます。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant Shared Plan]** の順に選択します。

ステップ 2 [Delete Load Balancer to Tenant Network - Shared Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

VPC プランでのテナント ネットワークからのロード バランサの削除

既存のテナントネットワークやエンドポイントグループからロードバランサ サービス（lb-port、lb-protocol）を削除できます。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant VPC Plan]** の順に選択します。

ステップ 2 [Delete Load Balancer to Tenant Network - VPC Plan] を選択し、[Request] をクリックします。

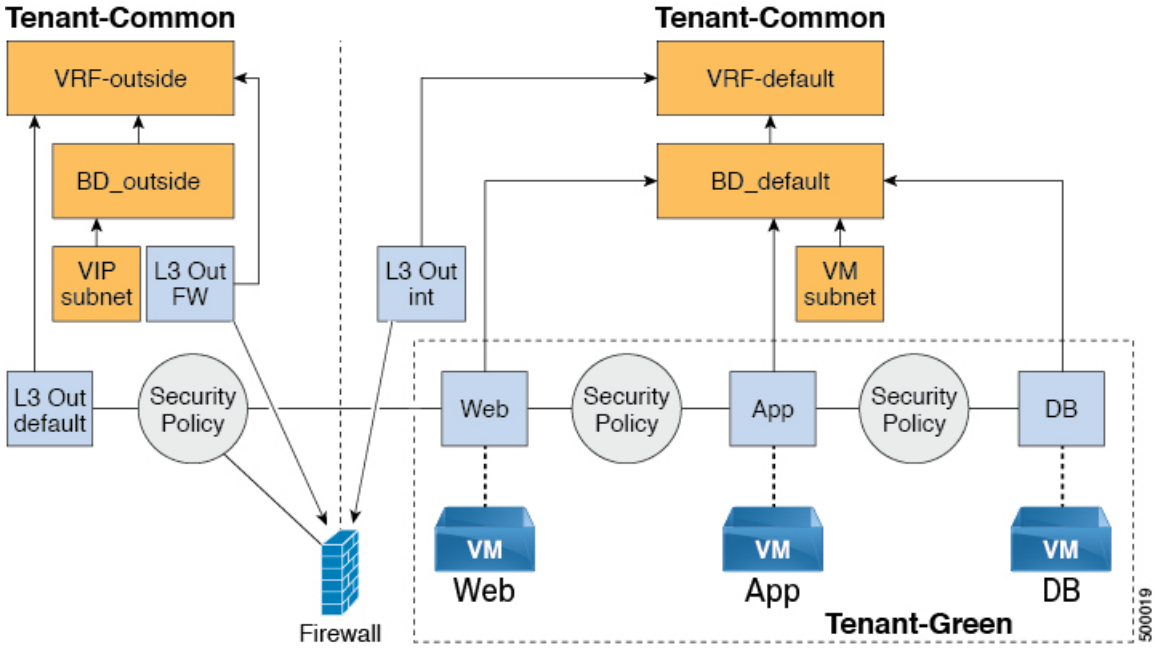
ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

ファイアウォールの設定

ここでは、テナント ネットワーク（Application Policy Infrastructure Controller のエンドポイントグループ）にファイアウォール サービスを追加する手順について説明します。

図 *6* : 共有プラン：境界ファイアウォールのみの概要



（注） VPC プランでは周辺ファイアウォール専用サービスはサポートされていません。VPC プランでは、EPG 間のファイアウォール サービスを設定することができます。

共有プランでのテナント ネットワークへのファイアウォールの追加

既存のテナント ネットワークまたはエンドポイント グループにファイアウォールを追加できます。ファイアウォールのコンシューマは、別の VRF（たとえば「外部」の VRF）でレイヤ 3 外部接続ポリシーを設定しておく必要があります。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant Shared Plan]** の順に選択します。

ステップ 2 [Add FW to Tenant Network - Shared Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

共有プランでのテナント ネットワークからのファイアウォールの削除

既存のテナント ネットワークやエンドポイント グループからファイアウォールを削除できます。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant Shared Plan]** の順に選択します。

ステップ 2 [Delete FW from Tenant Network - Shared Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

ファイアウォールとロード バランサの設定

ここでは、テナント ネットワーク（Application Policy Infrastructure Controller のエンドポイント グループ）にファイアウォールおよびロード バランサ サービスを追加する手順について説明します。

このプランでは、ファイアウォールとロード バランサ デバイスは「共通」テナントに導入され、共有インフラストラクチャを使用する vRealize Automation（vRA）および APIC テナントの消費モデルを提供します。

図 7: 共有プラン：ファイアウォールとロード バランサの概要

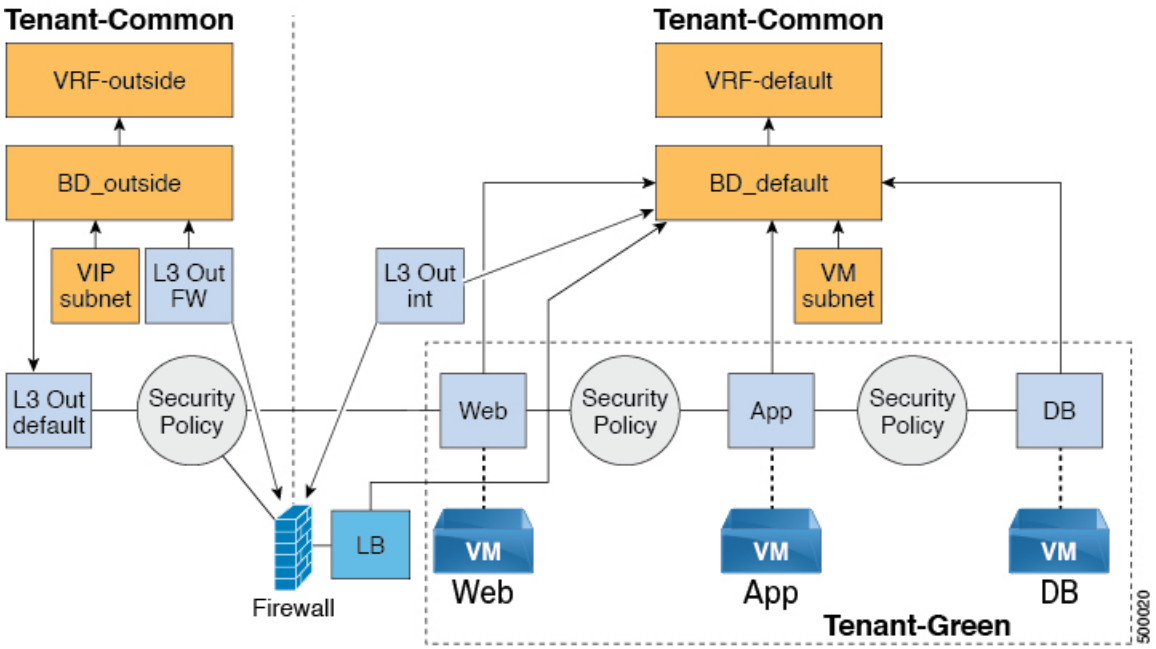
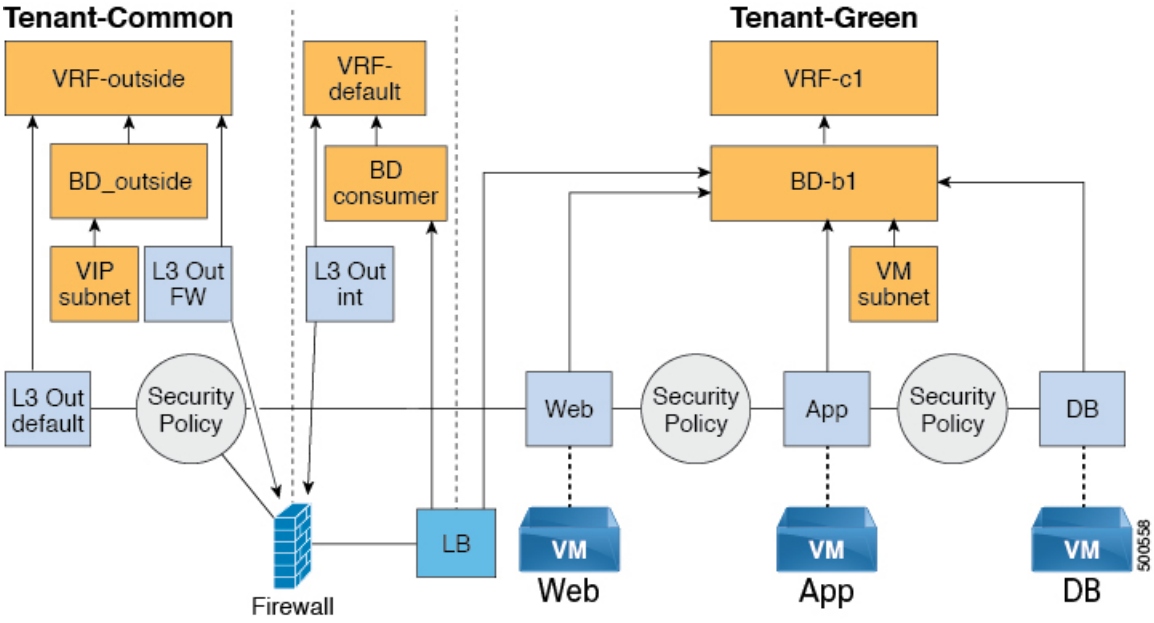


図 *8 : VPC* プラン：境界ファイアウォールとロード バランサ



共有プランでのテナント ネットワークへのファイアウォールとロード バランサの追加

ファイアウォールおよびロード バランサ サービスを使用する前に、仮想 IP アドレス プールをテナントに追加する必要があります。

VIP プールの追加 （87 ページ）を参照してください。

ファイアウォールとロード バランサは、既存のテナント ネットワークまたはエンドポイント グループに追加できます。ファイアウォールのコンシューマは、「外部」VRF で L3 out 接続ポリシーを設定する必要があります。

始める前に

ファイアウォールおよびロード バランサ サービスを導入するには、ファイアウォールとロード バランサの両方について、サービスのみが満たされている必要があります。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant Shared Plan]** の順に選択します。

ステップ 2 [Add FW and LB to Tenant Network - Shared Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

VPC プランでのテナント ネットワークへのファイアウォールとロード バランサの追加

ここでは、VPC プランのテナント ネットワークへのファイアウォールとロード バランサの追加方法について説明します。

（注） ファイアウォールとロードバランサ（LB）のワークフローを実行するたびに、LBの外部レッグは「default」のブリッジ ドメイン（BD）を指します。お客様は常に、tn-common の下にある「デフォルト」の BD 内にファイアウォールの内部レッグを配置する必要があります。これによって、ファイアウォールとロードバランサの両方が同じBDを指すようになり、トラフィックは中断されることなく流れるようになります。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant VPC Plan]** の順に選択します。

ステップ 2 [Add FW and LB to Tenant Network - VPC Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

共有プランでのテナント ネットワークからのファイアウォールとロード バランサの削除

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant Shared Plan]** の順に選択します。

ステップ 2 [Delete FW and LB from Tenant Network - Shared Plan] を選択し、[Request] をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

VPC プランでのテナント ネットワークからのファイアウォールとロード バランサの削除

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Tenant VPC Plan]** の順に選択します。

ステップ 2 [Delete FW and LB from Tenant Network - VPC Plan] を選択し、[Request] をクリックします。

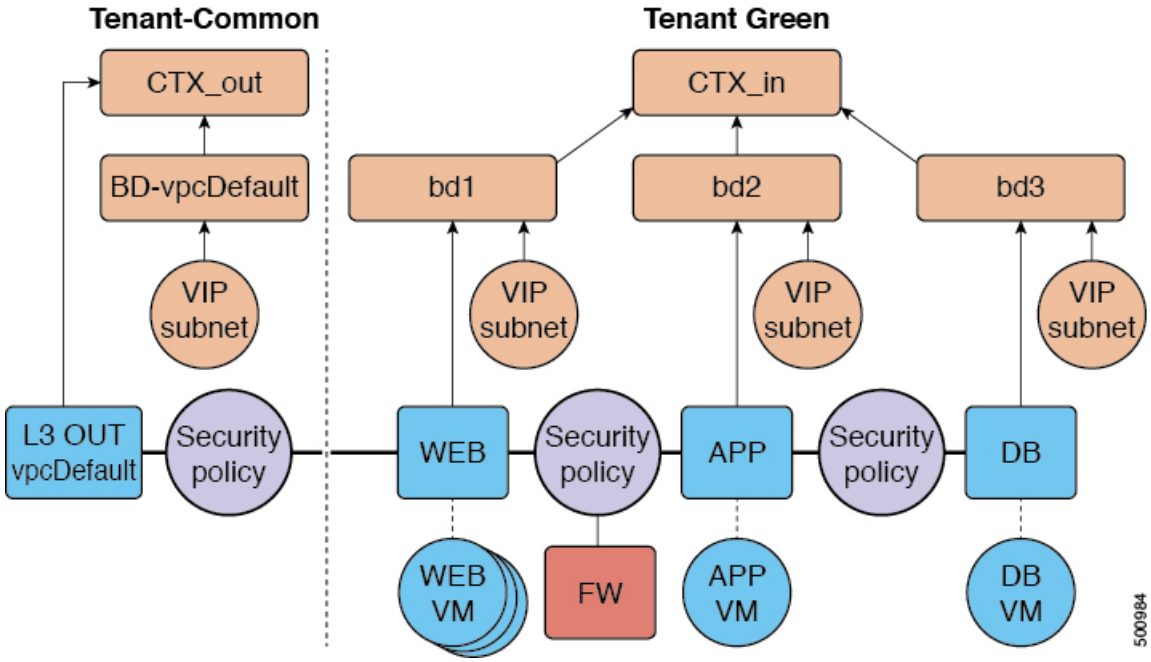
ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

EPG 間のファイアウォールの設定

このセクションでは、テナント ネットワーク (アプリケーション ポリシー インフラストラクチャ コントローラのエンドポイント グループ) に対して EPG 間ファイアウォール サービスを設定する方法について説明します。

図 9 : VPC プラン - EPG 間の FW



VPC プランのテナント ネットワークにファイアウォールを追加する

このセクションでは、ファイアウォールを既存のテナント ネットワークまたはエンドポイント グループ (EPG) に追加する方法について説明します。テナントを追加するときには、[Enable Inter-EPG Firewall] を [yes] に設定し、アプリケーションで使用する層の数を設定する必要があります。ネットワーク (EPG) を設定するときに層の数を設定する必要があります。このシナリオでは、ファイアウォールは、プロバイダー EPG とコンシューマ EPG の間に設定されます。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**Catalog** > **Tenant VPC Plan** にログインします。

ステップ 2 **Add FW to Tenant Network - VPC Plan** を選択し、**Request** をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

VPC プランのテナント ネットワークからファイアウォールを削除する

このセクションでは、ファイアウォールを既存のテナント ネットワークまたはエンドポイント グループ (EPG) から削除する方法について説明します。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[カタログ]** > **[テナント VPC プラン]** の順に選択します。

ステップ 2 **[テナント ネットワークから FW を削除する - VPC プラン]** を選択し、**[要求]** をクリックします。

ステップ 3 フィールドに必要な情報を入力します。

ステップ 4 [Submit] をクリックします。

外部 L3 ネットワーク インターネット アクセスの接続

ここでは、外部レイヤ 3（L3）ネットワーク インターネット アクセスを接続する方法を説明します。

始める前に

- L3 ポリシーには任意の名前を選択できます。
- 外部 L3 ポリシー インスタンスの名前は [L3OutName|InstP] にする必要があります。

手順

ステップ 1 vRealize Automation にテナントとしてログインし、**[Catalog]** > **[Tenant Network Service]** の順に選択します。

ステップ 2 [Attach or Detach L3 external connectivity to Network] を選択します。

ステップ 3 [Request] を選択します。

ステップ 4 [Request Information] タブで、要求の説明を入力します。

ステップ 5 [Next] を選択します。

ステップ 6 [Step] タブで、次の操作を実行します。

a) [Rule Entry List] フィールドに値を入力し、[Save] をクリックします。

次の表は、各ルール エントリの値を示しています。

ルール エントリ リスト	値
dstFormPort	• ブランク • 未指定 • 1 ～ 65535
dstToPort	• ブランク • 未指定 • 1 ～ 65535
protocol	• icmp • icmpv6 • tcp • udp • ブランク
etherType	• IP • 『ARP』

b) [L3out Policy] フィールドで [Add] をクリックして、共通テナントの L3 接続ポリシーを検索し選択します。（デフォルト）

c) [Network/EPG Name] フィールドで [Add] をクリックして、共通テナントのネットワーク/EPG を検索し選択します。（Web ホスト）

d) [EPG/Network plan type] フィールドで [Add] をクリックして、共通テナントのネットワーク/EPG を検索し選択します。（Web ホスト）

e) [Operation] フィールドで [Add] をクリックして、レイヤ 3 出力を追加します。

ステップ 7 要求を確認するには、[Requests] タブを選択します。

a) 送信した要求を選択し、[view details] をクリックします。ステータスが [Succesful] であることを確認します。

APIC でセキュリティおよび L3 ポリシーを確認する APIC

ここでは、APIC でセキュリティおよびレイヤ 3（L3）ポリシーを確認する方法について説明します。

手順

ステップ 1 Cisco APICへテナントとしてログインして、 **テナント** > **一般的な** を選択します。

ステップ 2 ナビゲーション ウィンドウで、**[Tenant Common]** > **[Networking]** > **[Security Policies]** > **[Contracts]** の順に展開します。

a) [Contracts] の下にネストされて、接続先の *end_user_tenant name*-L3ext_ctrct_*network_name* との新しい契約があります。（green-L3ext_ctrct_web-hosts）

b) *end_user_tenant name*-L3ext_ctrct_*network_name* を展開します。（green-L3ext_ctrct_web-hosts）

c) *end_user_tenant name*-L3ext_ctrct_*network_name* を展開します。（green-L3ext_ctrct_web-hosts）

d) [Property] ペインの [Filter] フィールドで、フィルタをクリックします。（green-L3ext_filt_web-hosts）

e) [Properties] ペインで、フィルタが vRealize にマッピングされていることを確認できます。

ステップ 3 ナビゲーション ウィンドウで、**[Tenant Common]** > **[Networking]** > **[External Routed Networks]** > **[default]** > **[Networks]** > **[defaultInstP]** の順に展開します。

a) [Properties] ペインの [Provided Contracts] フィールドに、*end_user_tenant name*-L3ext_ctrct_*network_name* が表示されています。（green-L3ext_filt_web-hosts）

b) [Consumed Contracts] フィールドに、*end_user_tenant name*-L3ext_ctrct_*network/EPG_name* が表示されています。（green-L3ext_filt_web-hosts）

ステップ 4 メニュー バーで、**[TENANTS]** > ***[your_tenant]*** の順に選択します。

ステップ 5 ナビゲーション ウィンドウで、**[Tenant *your_tenant*]** > **[Application Profile]** > **[default]** > **[Application EPGs]** > **[EPG web-hosts]** > **[Contracts]** の順に展開します。

a) [Contracts] ペインで、契約および消費される契約が存在することを確認できます。

ネットワークの接続性の確認

ここでは、ネットワークの接続性を確認する方法について説明します。

手順

仮想マシン（Web ホスト）ログインし、コマンドラインから他の VM を ping します。

アプリケーションの導入シナリオ

次の表に、サポートされる導入シナリオを示します。

導入シナリオ	説明
Web > **L3out**	セキュリティ ポリシー（「デフォルト」VRF で設定された L3out）を使用して接続された Web 層から L3 外部接続ポリシー
Web > ファイアウォール > **L3out**	Web 層とファイアウォールおよびL3out（「外部」VRF で設定された L3out）
Web > ロード バランサ > **L3out**	Web 層と L3out（「外部」VRF で設定された L3out）に接続された ロード バランサ
Web > ロード バランサおよびファイアウォール > **L3out**	Web 層と L3out（「外部」で設定された L3out）に接続されたロードバランサとファイアウォール サービス
アプリケーション > **Web**	セキュリティポリシーを使用して接続された、アプリケーション層から Web 層
Application > **Web**	セキュリティポリシーを使用して接続された、データベース層からアプリケーション層
Application > **Load Balancer** > **Web**	ロード バランサを使用したアプリケーション層から Web 層。Web 層からアプリケーション層へのトラフィックは、ロード バランスされます。
アプリケーション > ファイアウォール > **Web**	ロード バランサを使用したアプリケーション層から Web 層。

マルチテナント環境では、サービス導入の設定にいくつかの制限があります。管理者は、この導入においてアプリケーションが最初の（Web）層で、ファイアウォールサービスを使用するか、ロード バランサのみのサービスを使用するかを決定する必要があります。

次の表に、共有プランでサポートされるサービスの組み合わせを示します。

展開タイプ	FW + LB > L3out	LB のみ> L3out	FW > L3out	EPG 間の LB	EPG 間の FW
ファイアウォールのみまたはファイアウォールとロードバランサ	はい		はい	はい	対応
ロードバランサのみ		はい		○	

マルチテナントの場合は、各テナントに専用のサービスデバイスを使用する必要があります。

プロパティ グループについて

プロパティ グループは、仮想マシンのカスタマイズを提供する vRealize Automation（vRA）コンストラクトです。プロパティ グループを使用すると、vRA は仮想マシンのライフサイクルの指定された段階で vRealize Orchestration（vRO）のワークフローを呼び出すことができます。この仮想マシン拡張機能は、Application Policy Infrastructure Controller（APIC）vRealize によって、APIC vRA ワークフローの呼び出しと APIC ポリシーの設定に使用されます。

APIC vRealize は、多数のアプリケーション導入シナリオをサポートします。複数層アプリケーションでは、APIC セキュリティ ポリシー、ロード バランシング、またはファイアウォール サービスを各層の間に挿入できます。これは、次の手順で達成されます。

1. プロパティ グループを作成するには、**Configure Property Group** カタログ項目 (**Admin Services** カタログ内) を実行します。
2. プロパティ グループをカスタマイズするには、**Security Policy**、**Load Balancer**、および **Firewall** タブを使用します
3. vRealize の **Infrastructure** > **Blueprints** > **Single Machine Blueprint** レベルで、単一マシンのブループリント内のプロパティ グループを有効にします。

サービス ブループリントについて

ここでは、サービス ブループリントについて説明します。

vRealize には 2 セットのブループリントがあります。1 つはマシン ブループリントで、VM のインストール、セットアップ、およびスピンの計算用です。ネットワーキング ワークフローのマシン ブループリントと呼ばれる、単一層アプリケーション ワークロードまたは複数層アプリケーション ワークロードを起動するための単一マシンおよび複数マシンのブループリントが存在します。

管理ワークフロー：

- APIC ハンドルの作成
- VMM ドメインの作成
- テナントの作成
- 共通のサブネットの作成
- レイヤ 4 ～ 7 のデバイスの使用

テナント ワークフロー：

- EPG の作成
- コントラクトの作成

- コントラクトの提供
- コントラクトの使用
- L3Out の使用
- レイヤ 4 ～ 7 のデバイスの使用

vRealize ネットワーク プロファイルとの統合 (IPAM)

vRealize IP アドレス管理 (IPAM) では、ネットワーク プロファイルの概念を使用して、アドレスのプールを 1 つ以上のネットワークに割り当てます。ネットワーク プロファイルを通常の vRealize ネットワークと同じ方法で ACI ベースのネットワークに割り当てることができます。

vRealize IPAM と統合するには、次の手順を実行します。

手順

ステップ 1 ブリッジ ドメインへのサブネットがあることを確認します。

「**テナント共通のブリッジ ドメインのサブセットの追加または削除**」を参照してください。

ステップ 2 ネットワーク プロファイルを作成します。

ネットワークプロファイルの作成については、VMwareのドキュメントを参照してください。

ステップ 3 これは、ブループリントで新しいネットワークを生成するかどうかによって異なります。

各マシンのブループリントに同じネットワークを使用する場合は、次の手順を実行します。

vCenter の予約で EPG (ネットワーク パス) を探し、ネットワーク プロファイルをそれに割り当てます。

a) vCenter で、**[Infrastructure]** > **[Reservations]** に移動します。
b) [Your Reservation] を見つけてその上にカーソルを置き、**[Edit]** をクリックします。
c) **[Network]** > **[Find desired Network Path (EPG)]** に移動し、ドロップダウン リストからネットワーク プロファイルを選択して **[Ok]** をクリックします。

VM ごとにネットワークを生成するには、次の手順を実行します。

ネットワーク プロファイルを値としてプロパティ グループにプロパティを追加します。

a) vCenter で、**[Infrastructure** > **Blueprints]** > **[Property Groups]** に移動します。
b) [Your Blueprint] を見つけてその上にカーソルを置き、**[Edit]** をクリックします。
c) **[+ New Property]** をクリックします。
d) 名前を「*VirtualMachine.NetworkX.NetworkProfileName*」に設定します。

   ここで、*X* は VM NIC 番号です ([0-9] の範囲) 。
e) 値を作成したネットワーク プロファイルの名前に設定します。
f) 緑色のチェック アイコンをクリックし、**[Ok]** をクリックします。

このプールから新しいアプリケーションにアドレスが割り当てられます。

ステップ 4 ゲストのカスタマイズを使用して IP アドレスをサーバに割り当てます。

ゲストのカスタマイズについては、VMware のドキュメントを参照してください。

vRealize Orchestrator の APIC ワークフローのマニュアル

APIC のメソッドとタイプに関するドキュメントを入手するために、vRO API の検索を使用できます。

1. vRO GUI にログインし、**[ツール（Tools）]** > **[API 検索（API Search）]** を選択します。
2. **APIC** を入力します。

   これにより、APIC のすべてのメソッドとタイプの一覧が表示されます。

ApicConfigHelper クラスのメソッド一覧

ここでは `ApicConfigHelper` クラスのメソッド一覧を示します。

- リポジトリに APIC ホストを追加し、APIC にログインします。

```
ApicHandle addHost(String hostName,
       String hostIp0,
       String hostIp1,
       String hostIp2,
       String  userName,
       String pwd,
       int port,
       boolean noSsl,
       String role,
       String tenantName)
```

- APIC 名を指定して APIC ハンドルを取得します。

```
ApicHandle getApicHandle(String hostName)
```

- <role, username> を指定して APIC ハンドルの一覧を取得します。

```
List<ApicHandle> getApicHandleByRole(String role, String userName)
```

- リポジトリから APIC ホストを削除します。

```
boolean removeHost(String inApicName)
```

- APIC でテナントのエンドポイント グループと vmmDomain への関連付けを作成します。

```
ApicResponse addNetwork(ApicHandle handle,
       String tenantName,
       String apName,
       String epgName,
       String bdName,
       String ctxName,
       String subnet,
       String domName,
       boolean vmm,
```

```
        boolean vpc,
        boolean intraEpgDeny,
        boolean allowUseg,
        String  encapMode)
```

- 追加または削除することで、エンドポイント グループのドメインを更新します。

```
ApicResponse updateNetwork(ApicHandle handle,
        String tenantName,
        String apName,
        String epgName,
        String domName,
        boolean vmm,
        boolean add,
        String encapMode)
```

- 仮想プライベート クラウド（VPC）テナントのブリッジ ドメインのサブネットを追加または削除します。

```
ApicResponse updateSubnets(ApicHandle handle,
        String tenantName,
        String bdName,
        fvSubnet subnetList[],
        boolean add)
```

- テナントのブリッジ ドメインを追加または削除します。

```
ApicResponse updateBD(ApicHandle handle,
        String tenantName,
        String bdName,
        String ctxName,
        boolean arpFlooding,
        String l2UnknownUnicast,
        String l3UnknownMulticast,
        boolean add)
```

- テナントのコンテキスト（Ctx）を追加または削除します。

```
ApicResponse updateCtx(ApicHandle handle,
        String tenantName,
        String ctxName,
        boolean add)
```

- 追加または削除に基づいて以下を追加または削除します。

```
ApicResponse addOrDeleteLBToNetwork(ApicHandle handle,
        String tenantName,
        String apName,
        String epgName,
        String bdName,
        String ctxName,
        boolean vpc,
        String planName,
        String lbVendor,
        String ldevName,
        String graphName,
        boolean sharedLb,
        String protocol,
        String port,
        String consumerDn,
        String snipIntAddress,
        String snipIntNetMask,
        String snipExtAddress,
        String snipExtNetMask,
```

```
        String snipNextHopGW,
        boolean addOperation)
```

- URL への接続を開き、URL の場所に postBody 文字列を送信して、結果を返します。

```
ApicResponse addOrDelFWReq(ApicHandle handle,
        String tenantName,
        String apName,
        String epgName,
        String ctrctName,
        String graphName,
        vzEntry entryList[],
        String consumerDn,
        boolean addOp,
        boolean updateOp)
```

- 共有および VPC プランのエンドポイント グループにファイアウォール サービスを追加します。

```
ApicResponse addFWToNetwork(ApicHandle handle,
        String tenantName,
        String apName,
        String epgName,
        boolean vpc,
        String fwVendor,
        String ldevName,
        String graphName,
        vzEntry entryList[],
        String fwL3extExternal,
        String fwL3extInternal,
        boolean skipFWReq,
        String consumerDn)
```

- 共有および VPC プランのエンドポイント グループからファイア ウォールを削除します。

```
ApicResponse deleteFWFromNetwork(ApicHandle handle,
        String tenantName,
        String apName,
        String epgName,
        boolean vpc,
        String graphName,
        String ctrctName,
        String protocol,
        String startPort,
        boolean skipFWReq,
        String consumerDn)
```

- REST API を APIC に対して実装します。

```
String apicRestApi(ApicHandle handle,
        String apiUrl,
        String method,
        String postBody)
```

- テナントのルータ ID を追加または削除します。

```
ApicResponse addOrDelRouterId(ApicHandle handle,
        String rtrId,
        boolean addOp)
```

- テナントのエンドポイント グループと関連付けを削除します。

```
ApicResponse deleteNetwork(ApicHandle handle,
        String tenantName,
```

```
        String apName,
        String epgName)
```

- APIC でテナント、ブリッジ ドメイン、およびコンテキスト（Ctx）を作成します。

```
ApicResponse addTenant(ApicHandle handle,
        String tenantName,
        String bdName,
        String ctxName,
        String aaaDomain)
```

- APIC でテナントを削除します。

```
ApicResponse deleteTenant(ApicHandle handle,
        String tenantName)
```

- VlaNS、vmmDomP、vmmCtrlP、vmmUsrAccp、および必要な関係オブジェクトを APIC に追加します。

```
ApicResponse addVmmDomain(ApicHandle handle,
        String dvsName,
        String vcenterIP,
        String userName,
        String passwd,
        String datacenter,
        String vlanPoolName,
        int vlanStart,
        int vlanEnd,
        String aaaDomain)
```

- VlanNS オブジェクトと vmmDomP オブジェクトを APIC から削除します。

```
ApicResponse deleteVmmDomain(ApicHandle handle,
        String domName,
        String vlanPoolName)
```

- VLAN プールのカプセル化ブロックを追加または削除します。

```
ApicResponse updateVlanPool(ApicHandle handle,
        String vlanPoolName,
        fvnsEncapBlk encapList[])
```

- セキュリティ ポリシー（契約エントリ）を追加します。

```
ApicResponse addSecurityPolicySet(ApicHandle handle,
        String tenant,
        String ap,
        String srcEpg,
        String dstEpg,
        vzEntry entryList[],
        boolean createFlg
        )
```

- セキュリティ ポリシー（契約エントリ）を更新します。

```
ApicResponse updateSecurityFilters(ApicHandle handle,
        String tenant,
        String filterName,
        vzEntry entryList[]
        )
```

- コンシューマ契約インターフェイスを追加または削除します。

```
ApicResponse updateSharedSvcConsumer(ApicHandle handle,
        String tenant,
```

```
        String ap,
        String consumerEpg,
        vzBrCP contract,
        boolean add
        )
```

- セキュリティ ポリシー（契約エントリ）を更新します。

```
ApicResponse updateL3outPolicy(ApicHandle handle,
        String tenant,
        String ap,
        String dstEpg,
        vzEntry entryList[],
        l3extOut l3out,
        boolean vpc,
        boolean add
        )
```

- すべてのセキュリティ ポリシー（契約）を削除します。

```
ApicResponse deleteSecurityPolicy(ApicHandle handle,
        String tenant,
        String ap,
        String srcEpg,
        String dstEpg
        )
```

- TN 共通の VIP アドレス ブロックを作成します。

```
ApicResponse addVipPool(ApicHandle handle,
        String planName,
        String addrStart,
        String addrEnd)
```

- TN 共通の VIP アドレス ブロックを削除します。

```
ApicResponse deleteVipPool(ApicHandle handle,
        String planName,
        String addrStart,
        String addrEnd)
```

- セキュリティ ドメインの関連付けを追加または削除します。

```
ApicResponse updateVmmDomain(ApicHandle handle,
        String domName,
        aaaDomainRef aaaList[])
```

- 契約から共有サービス プロバイダー（エンドポイント グループ）を削除します。

```
ApicResponse deleteSharedServiceProvider(ApicHandle handle,
        String tenant,
        String ap,
        String srcEpg,
        String dstEpg,
        vzBrCP contract)
```

- これは、Cisco AVS VMM ドメインを作成し、関連するオブジェクトを APIC に追加します:

```
ApicResponse addAvsVmmDomain(ApicHandle handle,
        String dvsName,
        String aepName,
        String vcenterIP,
        String userName,
        String passwd,
```

```
        String dvsVersion,
        String datacenter,
        String mcastIP,
        String poolName,
        String rangeStart,
        String rangeEnd,
        String aaaDomain,
        int domType,
        String secondRangeStart,
        String secondRangeEnd,
        String secondPoolName)
```

- これにより、次の Cisco AVS VMM ドメインに関連するプール (VLAN、マルチ キャスト アドレス) を更新します:

```
ApicResponse updateAvsVlanMcastPool(ApicHandle handle,
        String poolName,
        fvnsEncapBlk encapList[],
        int poolType)
```

- これは Cisco AVS VMM ドメインを削除します:

```
ApicResponse deleteAvsVmmDomain(ApicHandle handle,
        String domName,
        String poolName,
        int poolType)
```

- これは混合モードである Cisco AVS VMM ドメインを削除します:

```
ApicResponse deleteAvsVmmDomainMixedmode(ApicHandle handle,
        String domName )
```

- これはCisco AVS VMM ドメインの分散ファイアウォールを作成します:

```
ApicResponse createFWPol(ApicHandle handle,
        String polName,
        String vmmName,
        String polMode,
        String pInterval,
        String logLevel,
        String adminState,
        String destGrpName,
        String inclAction,
        int caseVal)
```

- これはCisco AVS VMM ドメインの分散ファイアウォールを更新します:

```
ApicResponse updateFWPolMapping(ApicHandle handle,
        String polName,
        String vmmName,
        Boolean opValue)
```

- これは分散ファイアウォールを削除します:

```
ApicResponse deleteFWPol(ApicHandle handle,
        String polName)
```

- これはマイクロセグメント EPG の属性を追加または削除します:

```
ApicResponse addOrDelUsegAttr(ApicHandle handle,
        String tenantName,
        String apName,
        String epgName,
        String criteriaName,
        fvVmAttrV addFvVmAttrList[],
```

```
        fvMacAttr addFvMacAttrList[],
        fvIpAttr addFvIpAttrList[],
        fvVmAttr delFvVmAttrList[],
        fvMacAttr delFvMacAttrList[],
        fvIpAttr delFvIpAttrList[])
```

- これはマイクロセグメント EPG を追加します:

```
ApicResponse addUsegEpg(ApicHandle handle,
        String tenantName,
        String apName,
        String epgName,
        String bdName,
        String ctxName,
        String subnet,
        String domName,
        String criteriaName,
        boolean vmm,
        boolean vpc,
        boolean intraEpgDeny,
        fvVmAttrV fvVmAttrList[],
        fvMacAttr fvMacAttrList[],
        fvIpAttr fvIpAttrList[],
        String encapMode)
```

APIC プラグイン メソッドを使用してカスタム ワークフローを記述する

ここでは、Application Policy Infrastructure Controller（APIC）プラグイン メソッドを使用してカスタム ワークフローを記述する方法について説明します。テナントには、既定の設計ではカバーされない論理ネットワーク トポロジ固有の要件が存在することがあります。既存の Cisco APIC ワークフローをカスタム ワークフローに統合することで、制限のないネットワーク設計が可能になります。

すべてのワークフローには入力パラメータ セットが必要であり、新しいオブジェクトを作成するワークフローは出力パラメータ セットをエクスポートします。出力パラメータは、次のワークフローの入力パラメータに結合できます。

次の手順例では、新しいネットワークを構築するカスタム ワークフローを作成し、新たに作成したネットワークをアタッチ レイヤ 3 ワークフローの入力に直接渡します。

手順

ステップ 1 vRealize Orchestrator にログインします。

ステップ 2 [Design] モードに切り替えます。

ステップ 3 [Navigation] ペインで、[Custom Workflow] というフォルダを作成します。

ステップ 4 [Custom Workflow] フォルダを選択します。

ステップ 5 [Work] ペインで [New workflow] ボタンをクリックします。

ステップ 6 [Workflow name] ダイアログボックスに、ワークフローの名前を入力します。

例：

```
Create_Network_Attach_L3
```

ステップ 7 [OK] をクリックします。

ステップ 8 [Schema] タブを選択します。

ステップ 9 [Navigation] ペインで、**[All Workflows]** > **[Administrator]** > **[Cisco APIC workflows]** > **[Tenant Shared Plan]** の順に展開します。

ステップ 10 [Add Tenant Network - Shared Plan] を [Work] ペインの青い矢印にドラッグ アンド ドロップします。

ステップ 11 [Do you want to add the activity's parameters as input/output to the current workflow?] ダイアログボックスで、[Setup...] をクリックします。.

ステップ 12 [Promote Workflow Input/Output Parameters] ダイアログボックスで、[Promote] をクリックします。

すべての値をデフォルトのままにします。

ステップ 13 [Navigation] ペインで、**[All Workflows]** > **[Administrator]** > **[APIC workflows]** > **[Advanced Network Services]** の順に展開します。

ステップ 14 [Attach or Detach L3 external connectivity to Network] を [Work] ペインの [Add Tenant Network] オブジェクトの右側にある青い矢印にドラッグ アンド ドロップします。

ステップ 15 [Do you want to add the activity's parameters as input/output to the current workflow?] ダイアログボックスで、[Setup...] をクリックします。.

ステップ 16 [Promote Workflow Input/Output Parameters] ダイアログボックスで、[Promote] をクリックします。

すべての値をデフォルトのままにします。

ステップ 17 [Inputs] タブを選択します。

画面にワークフローの入力が表示されます。入力がすべて表示され、作成されたエンドポイント グループが出力パラメータであることを確認できます。

ステップ 18 [Schema] タブを選択します。

ステップ 19 [Work] ペインで [Validate] をクリックして、カスタム ワークフローが有効であることを確認します。

ステップ 20 [Close] をクリックします。

ステップ 21 [Run] をクリックしてワークフローをテストします。

ステップ 22 [Start Workflow] ダイアログボックスで [Submit] をクリックして、ワークフローを開始します。

マルチテナントおよびセキュリティドメインを使用したロールベースのアクセス制御

APIC と vRA は両方ともネイティブでマルチテナントをサポートしています。vRA テナントユーザは APIC テナント ユーザと 1 対 1 でマッピングされるため、両方のシステムでテナント名が正確に一致する必要があります。

vRA テナントごとに、APIC 管理者はユーザ アカウントと必要なセキュリティ ドメインおよびロールが Day-0 操作の一部として APIC で作成されていることを確認する必要があります。

次の手順として、vRA 管理者はテナント サービス追加ブループリントを実行し（管理者カタログの一部）、APIC でテナントを作成/更新して、適切なセキュリティ ドメインに関連付けます。たとえば、vRA のテナント - グリーンは、「ユーザ - グリーン」に対して有効化されたセキュリティ ドメイン「ドメイン - グリーン」との関連付けで、APIC のテナント - グリーンにマップされます。

テナントを適切なセキュリティ ドメインに関連付けることで、ロール ベースのアクセス制御が実施され、きめ細かいより厳格なテナントのポリシー適用が可能になります。

テナントの追加

ここでは、テナントを追加する方法について説明します。

このブループリントでは、入力パラメータ「Tenant」によって指定されるテナントは、2 番目の入力によって指定されるセキュリティ ドメインと関連付けた状態で APIC に作成されます。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Admin Services]** の順に選択します。

ステップ 2 [Add Tenant] を選択し、フィールドに情報を入力して [Submit] をクリックします。

テナントの削除

ここでは、APIC からテナントを削除する方法について説明します。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Admin Services]** の順に選択します。

ステップ 2 [Delete Tenant] を選択し、フィールドに情報を入力して [Submit] をクリックします。

APIC ワークフロー用の APIC クレデンシャル

vRA との ACI 統合の一部として、このリリースでは、vRA と APIC クラスタで管理される ACI ファブリックとのペアリングをサポートしています。

ネットワーク サービス ブループリントは管理者ワークフローとテナント ワークフローに分類されるため、vRA 管理者は vRA-Tenant ごとに、APIC-Admin クレデンシャルと APIC-Tenant クレデンシャルの APIC 接続ハンドルを設定する必要があります。

プラグインの一部として、ワークフローのコンテキストおよび APIC でのオブジェクトの作成と管理に必要な権限に基づいて、適切なハンドル（管理者 vs テナント）が暗黙的に自動選択されます。これにより、テナントに強力なアクセス制御と分離が提供されます。

管理者クレデンシャルを用いた APIC の追加

ここでは、管理者クレデンシャルで APIC を追加する方法について説明します。

管理者ポータルのカタログ項目に含まれるすべてのブループリントとワークフローは管理者クレデンシャルを使用して実行されます。

手順

ステップ 1 vRealize Automation に管理者としてログインし、[Catalog] > [VM Services] の順に選択します。

ステップ 2 [Add APIC with Admin Credentials] を選択し、フィールドに情報を入力して、[Submit] をクリックします。

ステップ 3 証明書を使用して APIC にアクセスするには、[Use certificate authentication] を **yes** に設定し、**Certificate Name** と **Private Key** パラメータを入力します。

テナント クレデンシャルを用いた APIC の追加

ここでは、テナントの管理者クレデンシャル（セキュリティ ドメイン）の使用方法について説明します。

手順

ステップ 1 vRealize Automation に管理者としてログインし、**[Catalog]** > **[Admin Services]** の順に選択します。

ステップ 2 [Add APIC with Tenant credentials] を選択し、フィールドに情報を入力して [Submit] をクリックします。

ステップ 3 証明書を使用して APIC にアクセスするには、[Use certificate authentication] を **yes** に設定し、**Certificate Name** と **Private Key** パラメータを入力します。

トラブルシューティング

ここでは、トラブルシューティング テクニックについて説明します。

レポート対象ログの収集

ここでは、レポートするvRealizeアプライアンスからログ ファイルを収集する方法を説明します。

手順

ログ ファイルを収集するには、次のコマンドを入力します。

```
tar xvfz apic-vrealize-1.2.1x.tgz
cd apic-vrealize-1.2.1x
cd scripts/
./get_logs.sh
Usage:  get_logs.sh  [-u] [-p <password>] [-s <vra_setup>]
       -p    password (can be skipped for default passwd)
       -s    vra_setup
       -u    un-compress (ie., don't create .tar.gz file)

Example:
./get_logs.sh -p ***** -s vra-app
…
VMware vRealize Automation Appliance
Compressing Logs
logs/
logs/app-server/
logs/app-server/catalina.out
logs/app-server/server.log
logs/configuration/
logs/configuration/catalina.out
Logs saved in vra_logs_201511251716.tar.gz
```

ACI ヘルパー スクリプトのインストール

ここでは、ヘルパー スクリプトのインストール方法について説明します。ACI ヘルパー スクリプトは以下を実行します。

- vco サーバと vco コンフィギュレータを再起動します。
- APIC プラグインをアンインストールします

手順

ヘルパー スクリプトをインストールするには、次のコマンドを入力します:

```
cd scripts
./install_apic_scripts.sh
Usage:  install_apic_scripts.sh  [-p <password>] [-s <vra_setup>]
       -p    password
       -s    vra_setup

Example:
./install_apic_scripts.sh -p ***** -s vra-app
Copying APIC scripts 'rmapic', 'restart' to vra: vra-app
```

APIC プラグインの削除

このセクションでは、APIC プラグインの削除方法について説明します。

手順

ステップ 1 VMware vRealize Orchestrator に管理者としてログインします。

ステップ 2 APIC のすべてのハンドルに対し、削除 APIC ワークフローを実行します。

ステップ 3 ACI ヘルパー スクリプトをインストールします。これは ACI ヘルパー スクリプトのインストール （112 ページ）にあります。.

ステップ 4 次の SSH コマンドを使用して、VRA アプライアンスにルートとしてログインします:**$ssh root@*vra_ip*.**

ステップ 5 **rmapic** bash スクリプトの属性を実行可能に変更します。

```
$ chmod a+x rmapic
```

ステップ 6 **rmapic** bash スクリプトを実行して、APIC プラグインを削除します:

```
$ ~/rmapic
```

ステップ 7 プラグインがアンインストールされたことを確認するには、Firefox ブラウザを使用して、次の URL で VMware アプライアンスにログインします:
`https://appliance_address:8283/vco-controlcenter`

ステップ 8 **Plug-Ins** セクションで、**Manage Plug-Ins** をクリックします。

ステップ 9 Cisco APIC プラグインが **Plug-In** の下に表示されていないことを確認します。

プラグインの概要

vRA ブループリント入力パラメータ	vRO JavaScript オブジェクト名	APIC マネージドオブジェクト名
テナント	ApicTenant	com.cisco.apic.mo.fvTenant
ブリッジ ドメイン	ApicBridgeDomain	com.cisco.apic.mo.fvBD
VRF	ApicL3Context	com.cisco.apic.mo.fvCtx
テナント ネットワーク（EPG）	ApicEPG	com.cisco.apic.mo.fvAEPg
セキュリティ ポリシー（契約）	ApicSecurityPolicy	com.cisco.apic.mo.vzBrCP
セキュリティ フィルタ	ApicSecurityFilter	com.cisco.apic.mo.vzFilter
セキュリティ ルール	ApicSecurityRule	com.cisco.apic.mo.vzEntry
AAA ドメイン	ApicAAADomain	com.cisco.apic.mo.aaaDomain
VMM ドメイン	ApicVmmDomain	com.cisco.apic.mo.vmmDomP
VMM コントローラ	ApicVmmController	com.cisco.apic.mo.vmmCtrlrP
物理的なドメイン	ApicPhysicalDomain	com.cisco.apic.mo.physDomP
L4-L7 デバイス クラスタ	ApicLogicalLBDevice	com.cisco.apic.mo.vnsLDevVip
L3 外部接続	ApicL3Connectivity	com.cisco.apic.mo.l3extOut

vRealize Orchestrator におけるテナント用 vRA ホストの設定

ここでは、vRealize Orchestratorr (vRO) でテナント用 vRA ホストを設定する方法を説明します。

（注） デフォルトで作成された vRA ホスト ハンドルがすでに 1 つ存在します。これはグローバルなテナント用で、管理を目的として、IaaS ホスト ハンドルを作成するために使用します。

手順

ステップ 1 VMware vRealize Orchestrator に管理者としてログインします。

ステップ 2 VMware vRealize Ochestrator GUI が表示されたら、メニュー バーのドロップダウン リストから [Run] を選択します。

ステップ 3 [Navigation] ウィンドウで、[Workflows] アイコンを選択します。

ステップ 4 **[Adminstrator@]*[vra_name]*** > **[Library]** > **[vRealize Automation]** > **[Configuration]** > **[Add a vRA host]** の順に選択します。

ステップ 5 **[Add a vRA host]** を右クリックして、**[Start Workflow]** を選択します。

ステップ 6 **[Start Workflow: Add a vRA host]** ダイアログボックスで、次の操作を実行します。

a) **[Host Name]** フィールドにホスト名を入力します。
b) **[Host URL]** フィールドにホストの URL を入力します。
c) **[Autotmatically install SSL certificates]** は **[Yes]** を選択します。
d) [Connection timeout] フィールドに "30" と入力します。
e) **[Operation timeout]** フィールドに "60" と入力します。
f) [Session Mode] は [Shared session] を選択します。
g) **[Tenant]** フィールドに、テナント名を入力します。
h) **[Authentication username]** フィールドに、テナント管理者のユーザ名を入力します。
i) **[Authentication pwd]** フィールドに、テナント管理者のパスワードを入力します。
j) [Submit] をクリックします。

vRealize Orchestrator における IaaS ホストの設定

ここでは、vRealize Orchestratorr（vRO）で IaaS ホストを設定する方法を説明します。

手順

ステップ 1 VMware vRealize Orchestrator に管理者としてログインします。

ステップ 2 VMware vRealize Ochestrator GUI が表示されたら、メニュー バーのドロップダウン リストから [Run] を選択します。

ステップ 3 [Navigation] ウィンドウで、[Workflows] アイコンを選択します。

ステップ 4 **[Adminstrator@]*[vra_name]*** > **[ライブラリ]** > **[vRealize 自動化]** > **[設定]** > **[vRA ホストの Iaas ホストの追加]** を選択します。

ステップ 5 **[vRA ホストの IaaS ホストの追加]** を右クリックして、**[ワークフローの開始]** を選択します。

ステップ 6 **[ワークフローの開始：vRA ホストの IaaS ホストの追加]** ダイアログボックスで、次の操作を実行します:

a) **[vRA ホスト]** ドロップダウン リストで、システムによって作成されたデフォルトの vRA ホストを選択します。テナント ハンドルは選択しないでください。
b) [Host Name] フィールドは、自動で設定された名前をそのまま残します。
c) [Host URL] フィールドに vRA ホストの URL を入力します。
d) [Connection timeout] フィールドに "30" と入力します。
e) **[Operation timeout]** フィールドに "60" と入力します。
f) [Session Mode] は [Shared session] を選択します。
g) [Authentication username] フィールドに、IaaS 管理者のユーザ名を入力します。
h) [Authentication pwd] フィールドに、IaaS 管理者のパスワードを入力します。
i) [Workstation for NTLM authentication] フィールドに、IaaS ホスト名を入力します。
j) [Domain for NTLM authentication] フィールドに、IaaS ドメイン名を入力します。
k) [Submit] をクリックします。

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