Cisco ACI リリース 4.0(2) 仮想化ガイド

初版：2018 年 12 月 20 日

最終更新：2019 年 1 月 4 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- 仮想マシンのインストールと管理
- サーバ管理
- スイッチおよびネットワークの管理

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。

表記法	説明
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保存しておいてください。

関連資料

Application Policy Infrastructure Controller（APIC）のマニュアル

次のガイドでは、APIC のドキュメントを提供します。

- 『*Cisco APIC Getting Started Guide*』
- 『*Cisco APIC Basic Configuration Guide*』
- 『*Cisco ACI Fundamentals*』
- 『*Cisco APIC Layer 2 Networking Configuration Guide*』
- 『*Cisco APIC Layer 3 Networking Configuration Guide*』
- 『*Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*』
- 『*Cisco APIC REST API Configuration Guide*』
- 『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』
- 『*Cisco ACI* 仮想化ガイド』
- 『*Cisco Application Centric Infrastructure Best Practices Guide*』

これらすべてのドキュメントは、次の URL で入手できます。 http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

シスコ 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）のマニュアル

ACI の各種マニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

シスコ 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）シミュレータのマニュアル

Cisco ACI Simulator のマニュアルは、次の URL から入手できます：http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html

Cisco Nexus 9000 シリーズ スイッチのマニュアル

Cisco Nexus 9000 シリーズ スイッチのマニュアルは、次の URL で入手できます。
http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Cisco Application Virtual Switch のマニュアル

Cisco Application Virtual Switch（AVS）のマニュアルは、次の URL で入手できます。
http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html

シスコ 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）と OpenStack の統合に関するマニュアル

Cisco ACI と OpenStack の統合に関するマニュアルは、次の URL から入手できます。
http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

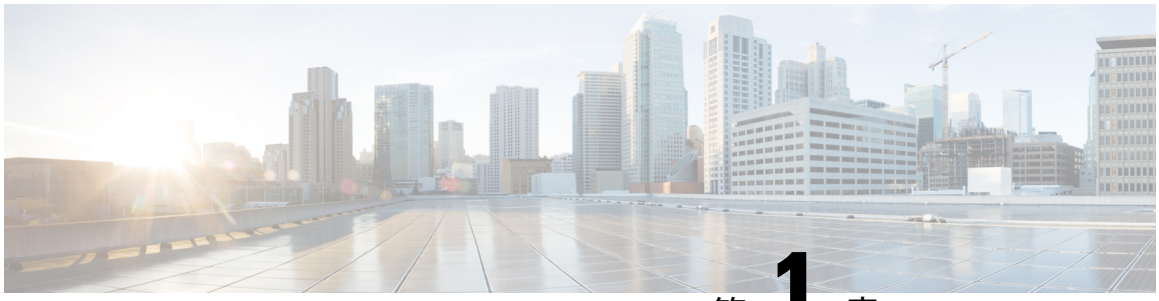
マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、apic-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、Cisco バグ検索ツール（BST）の使用法、テクニカル サポートの依頼方法、および追加情報の収集方法については、『*What's New in Cisco Product Documentation*』（http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）を参照してください。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに直接配信することもできます。RSS フィードは無料のサービスです。



第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

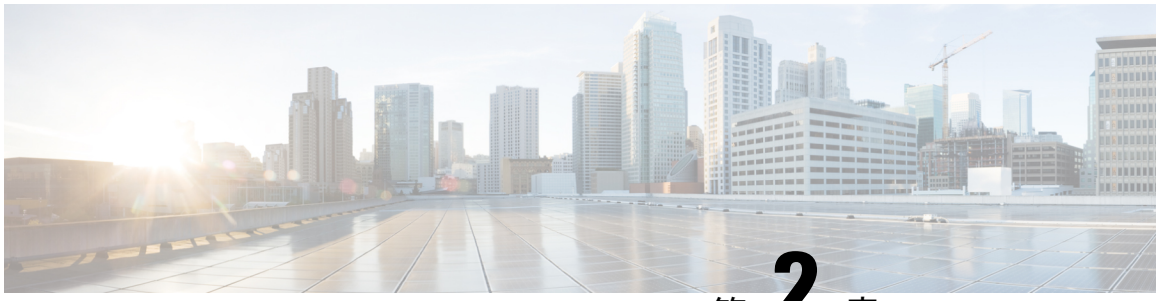
新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco ACI* 仮想化ガイドの新機能と変更された機能

Cisco APIC のリリース バージョン	機能	説明	参照先
4.0(2)	Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) （注） Cisco ACI vPod は、Cisco APIC リリース 4.0(2) 以降で一般に利用可能です。	Cisco ACI vPod は、さまざまなリモート ロケーションに Cisco ACI ファブリックを拡張できるようにする、ソフトウェアのみのソリューションです。 Cisco ACI vPod とそのコンポーネント（Cisco Application Centric Infrastructure Virtual Edge を含む）は、VMware ESXi ハイパーバイザを実行できるサーバが少なくとも 2 台存在する任意の場所に展開できます。	Cisco.com では Cisco ACI vPod の次のマニュアルを入手できます。 • *Cisco ACI vPod* リリース ノート • *Cisco ACI vPod* インストール ガイド • *Cisco ACI vPod* クイック スタート ガイド

新機能および変更された機能に関する情報



第 2 章

Cisco ACI の仮想マシン ネットワーキング

この章の内容は、次のとおりです。

Cisco ACI の VM ネットワーキングによる Virtual Machine Manager のサポート

ACI VM ネットワー キングの利点

Cisco ACI 仮想マシン（VM） ネットワーキングは、複数のベンダーからのハイパーバイザをサポートしています。ハイパーバイザに対し、高パフォーマンスでスケーラブルな仮想データセンター インフラストラクチャへのプログラム可能で自動化されたアクセスを提供します。

プログラム可能性と自動化は、スケーラブルなデータ センター仮想化インフラストラクチャにおける重要な機能です。Cisco ACI オープン REST API により、ポリシー モデル ベースの Cisco ACI ファブリックのオーケストレーションと仮想マシン統合できます。Cisco ACI VM ネットワーキングにより、複数のベンダーのハイパーバイザで管理される仮想ワークロードと物理ワークロードの両方にわたって一貫してポリシーを適用できます。

接続可能エンティティ プロファイルにより、VM モビリティと Cisco ACI ファブリック内の任意の場所のワークロードの配置を簡単に実現できます。Cisco Application Policy Infrastructure Controller (APIC) は、一元化されたトラブルシューティング、アプリケーションのヘルス スコア、および仮想化のモニタリングを提供します。Cisco ACI マルチ ハイパーバイザ VM の自動化は、手動による構成の必要性と人的エラーの発生を抑えるか、さらには排除します。これにより、仮想化データセンターが多数の VM を信頼性が高く、コスト効率の優れた方法でサポートすることが可能になります。

サポートされているベンダー

Cisco ACI では、次の製品とベンダーからの仮想マシン マネージャ (VMM) をサポートしています。

- Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod)

  詳細については、Cisco.com で Cisco ACI vPod のマニュアルを参照してください。

  （注） Cisco ACI vPod は、Cisco APIC リリース 4.0(2) 以降で一般に利用可能です。

- Cisco Application Centric Infrastructure Virtual Edge

  詳細については、Cisco.com の Cisco ACI Virtual Edge のマニュアルを参照してください。

- Cisco Application Virtual Switch（AVS）

  詳細については、Cisco.com の『Cisco ACI 仮想化ガイド』の「Cisco AVS での Cisco ACI」の章と Cisco AVS のマニュアルを参照してください。

- クラウド ファンドリー

  Cisco ACI とクラウド ファンドリーの統合は、Cisco APIC リリース 3.1(2) 以降でサポートされます。

- Kubernetes

  詳細については、Cisco.com の ナレッジ ベースの記事、『Cisco ACI と Kubernetes の統合』を参照してください。

- Microsoft System Center Virtual Machine Manager（SCVMM）

  詳細については、『Cisco ACI 仮想化ガイド』の「Cisco ACI と Microsoft SCVMM」および「Cisco ACI と Microsoft Windows Azure Pack」の章を参照してください。

- OpenShift

  詳細については、Cisco.com の OpenShift のマニュアルを参照してください。

- Openstack

  詳細については、Cisco.com の OpenStack のマニュアルを参照してください。

- Red Hat 仮想化 (RHV)

詳細については、Cisco.com のナレッジ ベースの記事、『Cisco ACI および Red Hat の統合』を参照してください。

- VMware 仮想分散スイッチ（VDS）

  詳細については、『Cisco ACI 仮想化ガイド』の「Cisco "ACI と VMware VDSの統合」の章を参照してください。

検証済みの相互運用可能な製品の最新のリストについては、『Cisco ACI Virtualization Compatibility Matrix』を参照してください）。

Virtual Machine Manager ドメインの主要コンポーネント

ACI ファブリック Virtual Machine Manager（VMM）ドメインにより、管理者は仮想マシン コントローラの接続ポリシーを設定できます。ACI VMM ドメイン ポリシーの基本的なコンポーネントは次のとおりです。

- **Virtual Machine Manager ドメイン プロファイル**：同様のネットワーキング ポリシー要件を持つ VM コントローラをグループ化します。たとえば、VM コントローラは VLAN プールとアプリケーション エンドポイント グループ（EPG）を共有できます。APIC はコントローラと通信し、のちに仮想ワークロードに適用されるポート グループなどのネットワーク設定を公開します。VMM ドメイン プロファイルには、次の基本コンポーネントが含まれます。
  - **クレデンシャル**：有効な VM コントローラ ユーザ クレデンシャルを APIC VMM ドメインと関連付けます。
  - **コントローラ**：ポリシーの適用ドメインの一部である VM コントローラへの接続方法を指定します。たとえば、コントローラは VMM ドメインの一部である VMware vCenter への接続を指定します。

  （注） 1 つのドメインに VM コントローラの複数のインスタンスを含めることができますが、それらは同じベンダーのものである必要があります（VMware または Microsoft など）。

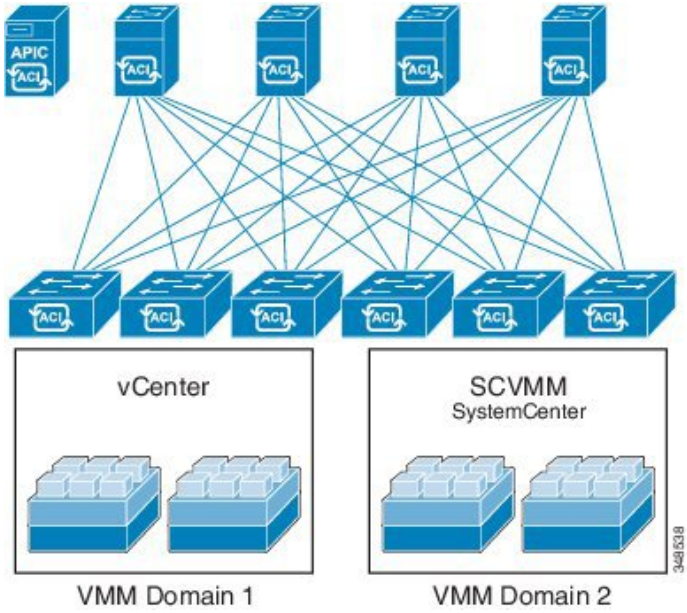
- **EPG の関連付け**：エンドポイント グループにより、エンドポイント間の接続と可視性が VMM ドメイン ポリシーの範囲内に規制されます。VMM ドメイン EPG は次のように動作します。
  - APIC は、これらの EPG をポート グループとして VM コントローラにプッシュします。
  - 1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。

- **接続可能エンティティ プロファイルの関連付け**：VMM ドメインを物理ネットワーク インフラストラクチャと関連付けます。接続可能エンティティ プロファイル（AEP）は、多数のリーフ スイッチ ポートで VM コントローラ ポリシーを展開するための、ネットワーク インターフェイス テンプレートです。AEP は、使用できるスイッチやポートおよびその設定方法を指定します。
- **VLAN プールの関連付け**：VLAN プールは、VMM ドメインが消費する VLAN カプセル化に使用する VLAN ID または範囲を指定します。

Virtual Machine Manager のドメイン

APIC VMM ドメイン プロファイルは、VMM ドメインを定義するポリシーです。VMM ドメイン ポリシーは APIC で作成され、リーフ スイッチにプッシュされます。

図 *1: ACI VMM* ドメイン *VM* コントローラの統合



VMM ドメインは以下を提供します。

- 複数の VM コントローラ プラットフォームに対してスケーラブルな耐障害性サポートを可能にする、ACI ファブリックの共通レイヤ
- ACI ファブリック内の複数のテナントに対する VMM サポート

VMM ドメインには、VMware vCenter や Microsoft SCVMM Manager などの VM コントローラと、VM コントローラと対話するための ACI API に必要なクレデンシャルが含まれます。VMM ドメインはドメイン内の VM モビリティを実現できますが、ドメイン間は実現できません。単一の VMM ドメイン コントローラに VM コントローラの複数のインスタンスを含めることはできますが、同じタイプである必要があります。たとえば、1 つの VMM ドメインに、それぞれが複数の VM を実行する複数のコントローラを管理する多くの VMware vCenter を含めるこ

とができますが、SCVMM Manager も含めることはできません。VMM ドメインはコントローラ要素（pNIC、vNIC、VM 名など）をインベントリに含め、コントローラにポリシーをプッシュして、ポート グループなどの必要な要素を作成します。ACI VMM ドメインは VM モビリティなどのコントローラ イベントを監視し、状況に応じて応答します。

VMM ドメイン VLAN プールの関連付け

VLAN プールは、トラフィック VLAN ID のブロックを表します。VLAN プールは共有リソースで、VMM ドメインおよびレイヤ 4 ～レイヤ 7 のサービスなど、複数のドメインで使用できます。

各プールには、作成時に定義された割り当てタイプ（静的または動的）があります。割り当てタイプによって、含まれる ID が APIC で自動割り当てに使用されるか（動的）、管理者によって明示的に設定されるか（静的）が決まります。デフォルトでは、VLAN プールに含まれるすべてのブロックの割り当てタイプはプールと同じですが、ユーザは動的プールに含まれるカプセル化ブロックの割り当てタイプを静的に変更できます。これを行うと、動的割り当てからそれらが除外されます。

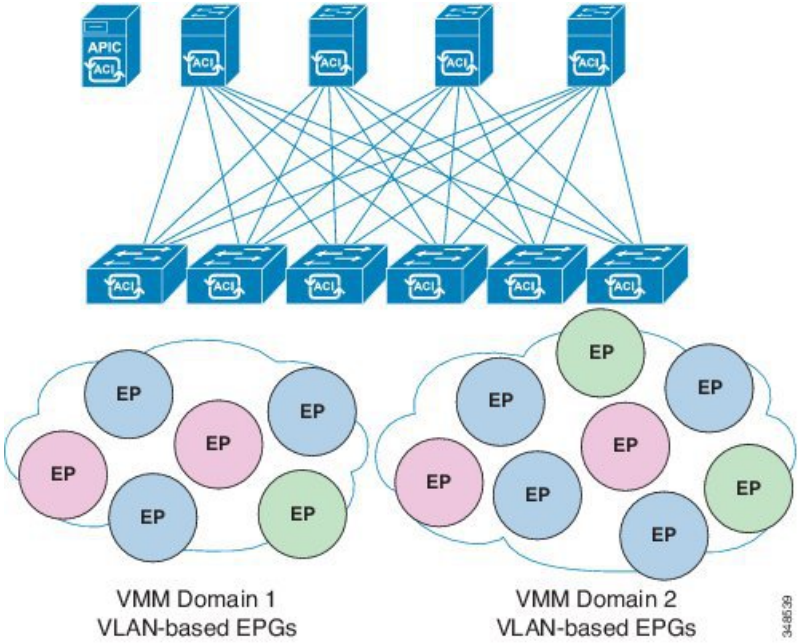
VMM ドメインは、1 つの動的 VLAN プールにのみ関連付けることができます。デフォルトでは、VMM ドメインに関連付けられた EPG への VLAN ID の割り当ては、APIC によって動的に行われます。動的割り当てがデフォルトであり、推奨設定ですが、管理者は代わりに EPG に静的に VLAN ID を割り当てることができます。この場合、使用する ID は VMM ドメインに関連付けられている VLAN プールのカプセル化ブロックから選択し、その割り当てタイプを静的に変更する必要があります。

APIC は、リーフ ポート上の VMM ドメイン VLAN を EPG イベントに基づいてプロビジョニングします（リーフ ポート上の静的バインドまたは VMware vCenter や Microsoft SCVMM などのコントローラからの VM イベントに基づいて）。

VMM ドメイン EPG の関連付け

ACI ファブリックは、Microsoft Azure などのオーケストレーション コンポーネントによって自動的に、またはその設定を作成する APIC 管理者によって、VMM ドメインにテナント アプリケーション プロファイル EPG を関連付けます。1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。

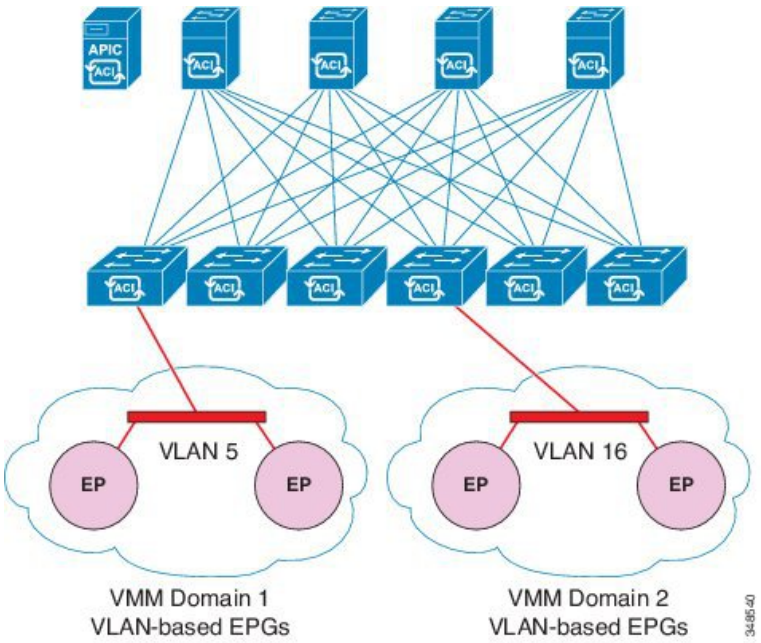
図 *2 : VMM* ドメイン *EPG* の関連付け



上の図では、同じ色のエンド ポイント（EP）は同じエンド ポイント グループに属しています。たとえば、緑色のすべての EP は 2 つの異なる VMM ドメインに含まれていますが同じ EPG に属しています。

仮想ネットワークと VMM ドメイン EPG 機能の情報については、Cisco ACI ドキュメントの最新の『Verified Scalability Guide』を参照してください。

図 *3 : VMM* ドメイン *EPG VLAN* の消費



（注） 同じポートに重複する VLAN プールがない場合は、複数の VMM ドメインを同じリーフ スイッチに接続できます。同様に、リーフ スイッチの同じポートを使用していない場合は、同じ VLAN プールを異なるドメイン間で使用できます。

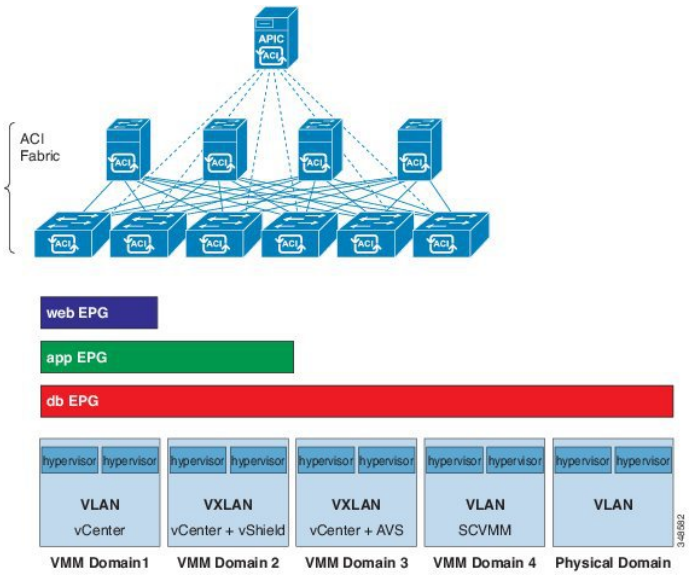
EPG は複数の VMM ドメインを次のように使用できます。

- VMM ドメイン内の EPG は、APIC によって自動的に管理されるか管理者によって固定で選択されたカプセル化識別子を使用して識別されます。一例は、VLAN、仮想ネットワーク ID（VNID）です。
- EPG は複数の物理ドメイン（baremetal サーバの場合）または仮想ドメインにマッピングできます。各ドメインで異なる VLAN または VNID カプセル化を使用できます。

（注） デフォルトでは、APIC は動的に EPG の VLAN の割り当てを管理します。VMware DVS 管理者は、EPG に対して特定の VLAN を設定できます。その場合は、VLAN は VMM ドメインに関連付けられたプール内のスタティック割り当てブロックから選択します。

アプリケーションは、複数の VMM ドメインに導入できます。

図 *4:* ファブリック内の複数の *VMM* ドメインと *EPG* の増大



VMM ドメイン内の VM のライブ マイグレーションがサポートされていても、VMM ドメイン間の VM のライブ マイグレーションはサポートされません。

トランク ポート グループについて

トランク ポート グループを使用して EPG のトラフィックを集約します。現時点では、VMware ドメインのみでサポートされます。トランク ポート グループの名前付けスキームが EPG の T|A|E 形式に従っていません。トランク ポート グループはテナントに対応しないため、名前には任意の ASCII 文字列を使用できます。

同じドメインの EPG の集約は、トランク ポート グループに含まれるカプセル化ブロックとして指定された VLAN の範囲に基づきます。EPG のカプセル化を変更するか、またはトランク ポート グループのカプセル化ブロックを変更した場合は、常に集約が再評価され、EGP を集約するかどうかが決まります。トランク ポート グループは、ベース EPG と uSeg EPG の両方を含む、集約される EPG に割り当てられた VLAN などのネットワーク リソースのリーフでの導入を制御しますuSeg EPG の場合、トランク ポート グループの VLAN の範囲には、プライマリ VLAN とセカンダリ VLAN の両方を含める必要があります。

（注） ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット サイズは 8986 バイトになります）。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

注意 ファブリックのリーフ スイッチとスパイン スイッチの間に 1 ギガビット イーサネット (GE) または 10GE リンクを設置すると、帯域幅が不十分なために、パケットが転送されずにドロップされる可能性があります。これを避けるためには、リーフ スイッチとスパイン スイッチの間で 40GE または 100GE リンクを使用してください。

（注） ポート VLAN ごとの機能 (localPort 範囲に同じ VLAN ID を使用してリーフ スイッチで複数の EPG を設定する) で設定されたインターフェイスでは、マルチ スパニング ツリー (MST) はサポートされません。

（注） この Cisco APIC クラスタ/ファブリックで Cisco ACI マルチサイト を使用している場合、ナビゲーション バーのオブジェクト名のクラウド アイコンを検索します。これは、情報が マルチサイト から派生したことを示します。マルチサイト GUI からのみ変更を加えることをお勧めします。ここで変更を行い前に、マルチサイト ドキュメンテーションを確認してください。

（注） イベント レコードの Cisco APIC REST API クエリについて、APIC システムでは最大 500,000 イベント レコードへの応答に制限しています。応答が 500,000 イベント以上の場合は、エラーが返されます。クエリを絞り込むためにフィルタを使用します。詳細については、クエリー フィルタ式の作成を参照してください。

詳細については、次を参照してください:

- GUI を使用した トランク ポート グループの作成 （58 ページ）
- NX-OS スタイルの CLI を使用したトランク ポート グループの作成 （59 ページ）
- REST API を使用した トランク ポート グループの作成 （62 ページ）

接続可能エンティティ プロファイル

ACI ファブリックにより、リーフ ポートを通してベア メタル サーバ、仮想サーバ、ハイパーバイザ、レイヤ 2 スイッチ（たとえば、Cisco UCS ファブリック インターコネクト）、またはレイヤ 3 ルータ（たとえば、Cisco Nexus 7000 シリーズ スイッチ）などのさまざまな外部エンティティに接続する複数の接続ポイントが提供されます。これらの接続ポイントは、リーフ スイッチ上の物理ポート、FEX ポート、ポート チャネル、またはバーチャル ポート チャネル（vPC）にすることができます。

（注） 2 つのリーフ スイッチ間での VPC ドメインを作成するとき、同じスイッチの生成を次のいずれかのどちらのスイッチも必要があります。

- 1: なしで Cisco Nexus N9K スイッチの生成」EX」または「FX」、スイッチ名前末尾にたとえば、N9K 9312TX
- 2: Cisco Nexus N9K スイッチ間での生成」EX」または「FX」スイッチ モデルの名前の末尾にたとえば、N9K-93108TC-EX

スイッチなど、これらの 2 つが互換性のある VPC ピアではありません。代わりに、同じ世代のスイッチを使用します。

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。インフラストラクチャ ポリシーは、Cisco

Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Link Aggregation Control Protocol（LACP）などのさまざまなプロトコル オプションを設定する物理インターフェイス ポリシーで構成されます。

AEP は、リーフ スイッチで VLAN プールを展開するのに必要です。カプセル化ブロック（および関連 VLAN）は、リーフ スイッチで再利用可能です。AEP は、VLAN プールの範囲を物理インフラストラクチャに暗黙的に提供します。

次の AEP の要件と依存関係は、さまざまな設定シナリオ（ネットワーク接続、VMMドメイン、マルチポッド設定など）でも考慮する必要があります。

- AEP は許容される VLAN の範囲を定義しますが、それらのプロビジョニングは行いません。EPG がポートに展開されていない限り、トラフィックは流れません。AEP で VLAN プールを定義しないと、EPGがプロビジョニングされてもVLANはリーフ ポートでイネーブルになりません。
- リーフ ポートで静的にバインディングしているEPGイベントに基づいて、またはVMware vCenter や Microsoft Azure Service Center Virtual Machine Manager（SCVMM）などの外部コントローラからのVMイベントに基づいて、特定のVLANがリーフ ポート上でプロビジョニングされるかイネーブルになります。
- 添付されているエンティティ プロファイルに関連付けられているすべてのポートに関連付けられているアプリケーション Epg を導入するアプリケーション Epg に直接と関連付けることができますプロファイルのエンティティが添付されています。AEP では、アタッチ可能なエンティティ プロファイルに関連付けられているセレクタの一部であるすべてのインターフェイスで導入されている EPG (infraRsFuncToEpg) との関係が含まれている設定可能な一般的な機能 (infraGeneric) があります。

Virtual Machine Manager（VMM）ドメインは、AEP のインターフェイス ポリシー グループから物理インターフェイス ポリシーを自動的に取得します。

AEP のオーバーライド ポリシーを VMM ドメイン用の別の物理インターフェイス ポリシーを指定するために使用できます。このポリシーは、VM コントローラが中間レイヤ 2 ノードを介してリーフ スイッチに接続され、異なるポリシーがリーフ スイッチおよび VM コントローラの物理ポートで要求される場合に役立ちます。たとえば、リーフスイッチとレイヤ2ノード間で LACP を設定できます。同時に、AEP オーバーライド ポリシーで LACP をディセーブルにすることで、VM コントローラとレイヤ 2 スイッチ間の LACP をディセーブルにできます。

EPG ポリシーの解決および展開の緊急度

EPGがVMMドメインに関連付けられるたびに、管理者は解決と展開の優先順位を選択して、ポリシーをいつリーフ スイッチにプッシュするかを指定できます。

解決の緊急性

- [Pre-provision] — VM コントローラが仮想スイッチ（たとえば、VMware VDS など）に接続される前でもポリシー（たとえば、VLAN、VXLAN バインディング、コントラクト、

フィルタなど）をリーフスイッチにダウンロードすることを指定します。これにより、スイッチ上の設定が事前プロビジョニングされます。

これは、ハイパーバイザ/VM コントローラの管理トラフィックも APIC VMM ドメイン (VMM スイッチ) に関連付けられている仮想スイッチを使用しているような状況で役に立ちます。

VLAN などの VMM ポリシーを ACI リーフ スイッチ上に展開するには、 APIC が、VM コントローラ経由のハイパーバイザと ACI リーフ スイッチの両方から、CDP/LLDP 情報を収集する必要があります。ただし、VM コントローラ がそのハイパーバイザ、さらには APICと通信するのに同じ VMM ポリシー (VMM スイッチ) を使用することになっている場合には、ハイパーバイザの CDP/LLDP 情報を収集できません。VM コントローラ/ハイパーバイザの管理トラフィックに必要なポリシーがまだ展開されていないからです。

事前プロビジョニングを直ちに使用する場合、ポリシーは、CDP/LLDP のネイバーシップには関係なく、ACI リーフ スイッチにダウンロードされます。これは、VMM スイッチに接続されたハイパーバイザ ホストがない場合もです。

- [Immediate]—ESXi ホストが DVS に接続すると、EPG ポリシー（コントラクトおよびフィルタを含む）が、関連付けられているリーフ スイッチ ソフトウェアにダウンロードされるよう指定します。VM コントローラ/リーフ ノード接続を解決するために LLDP または OpFlex 権限が使用されます。

  VMM スイッチにホストを追加すると、ポリシーがリーフにダウンロードされます。ホストからリーフへの CDP または LLDP のネイバーシップが必要です。

- [On Demand] — ESXi ホストがDVSに接続され、VM がポート グループ（EPG）に配置されている場合にのみ、ポリシー（たとえば、VLAN、VXLAN バインディング、コントラクト、フィルタ）がリーフ ノードにプッシュされるよう指定します。

  ホストが VMM スイッチに追加され、仮想マシンをポート グループ（EPG）に配置する必要がある場合、ポリシーがリーフにダウンロードされます。ホストからリーフへの CDP または LLDP のネイバーシップが必要です。

  即時とオンデマンドの両方において、ホストおよびリーフが LLDP または CDP のネイバーシップを失うと、ポリシーは削除されます。

展開の緊急性

ポリシーがリーフ ソフトウェアにダウンロードされると、展開の緊急度によってポリシーをいつハードウェア ポリシーの Content-Addressable Memory (CAM) にプッシュするかを指定できます。

- [Immediate] — ポリシーがリーフ ソフトウェアでダウンロードされるとすぐにポリシーがハードウェアのポリシー CAM でプログラムされるよう指定します。

- [On Demand]—最初のパケットがデータ パス経由で受信された場合にのみポリシーがハードウェアのポリシー CAM でプログラムされるよう指定します。このプロセスは、ハードウェアの領域を最適化するのに役立ちます。

（注） オン デマンドの緊急性指定と MAC 固定の VPC の両方を使用する場合、 最初のエンドポイントがリーフごとのEPGを学習するまでは、EPGコントラクトはリーフの三重Content-Addressable Memory (TCAM) にプッシュされません。このような場合、VPC ピア間での TCAM 使用率が不均一になる可能性があります。(通常、コントラクトは両方の両方のピアにプッシュされます)。

VMM ドメインを削除するためのガイドライン

次の手順に従って、VMM ドメインを自動的に削除するAPICリクエストによって関連するVMコントローラ（VMware vCenter または Microsoft SCVMM）がトリガーされ、プロセスが正常に完了すること、および ACI ファブリックに孤立した EPG が残されないことを確認します。

1. VM 管理者は、APIC によって作成されたすべての VM を、ポート グループ（VMware vCenter の場合）または VM ネットワーク（SCVMM の場合）からデタッチする必要があります。

   Cisco AVS の場合、VM 管理者は Cisco AVS に関連付けられている vmk インターフェイスも削除する必要があります。

2. ACI 管理者は、APIC で VMM ドメインを削除します。APIC は、VMware VDS または Cisco AVS または SCVMM 論理スイッチおよび関連するオブジェクトの削除をトリガーします。

（注） VM管理者が仮想スイッチまたは関連オブジェクト（ポートグループまたはVMネットワークなど）を削除することはできません。上記のステップ 2 の完了時に、APIC に仮想スイッチの削除を許可します。VMM ドメインが APIC で削除される前に VM 管理者が VM コントローラから仮想スイッチを削除した場合、EPG は APIC で孤立する可能性があります。

このシーケンスに従わない場合、VM コントローラは APIC VMM ドメインに関連付けられている仮想スイッチを削除します。このシナリオでは、VM 管理者は VM コントローラから VM および vtep アソシエーションを手動で削除してから、以前に APIC VMM ドメインに関連付けられていた仮想スイッチを削除します。

NetFlow と仮想マシン ネットワーキング

NetFlow と仮想マシン ネットワーキングについて

NetFlowテクノロジは、ネットワーク トラフィック アカウンティング、従量制のネットワーク課金、ネットワーク プランニング、そしてサービス拒絶に対する監視機能、ネットワーク監視、社外マーケティング、およびサービス プロバイダと企業顧客向け両方のデータ マイニングなど、主要な一連のアプリケーションの計測基盤を効果的にします。Cisco は NetFlow エク

スポート データの収集、データ量削減、ポスト プロセッシングを行う一連の NetFlow アプリケーションを提供し、エンド ユーザー アプリケーションが NetFlow データへ簡単にアクセスできるようにします。この機能により、同じレベルを介したトラフィックのモニタリングを実行する、NetFlowがデータ センターを通過するトラフィックのモニタリングを有効にすると、Cisco Application Centric Infrastructure (Cisco ACI) ファブリック。

ハードウェアがレコードからコレクタに直接エクスポートする代わりに、レコードはスーパーバイザ エンジンで処理され、必要な形式で標準の NetFlow コレクタにエクスポートされます。

NetFlow の詳細については、*Cisco APIC* と *NetFlow* ナレッジ ベース記事を参照してください。

仮想マシンのネットワーキングの NetFlow エクスポータ ポリシーについて

仮想マシン manager エクスポータ ポリシー (netflowVmmExporterPol) では、レポートのサーバまたはNetFlow コレクタに送信されたフローの収集されたデータに関する情報について説明します。NetFlow コレクタは、外部、標準の NetFlow プロトコルをサポートし、パケットを受け入れているエンティティが付いている NetFlow ヘッダーが無効です。

エクスポータ ポリシーには、次のプロパティがあります。

- VmmExporterPol.dstAddr]: この必須プロパティは、NetFlow フロー パケットを受信する NetFlow コレクタの IPv4 または IPv6 アドレスを指定します。このホストの形式である必要があります (つまり、「/32」または「/128」)。IPv6 アドレスは、vSphere 分散スイッチ (vDS) バージョン 6.0 でサポートされている以降です。
- VmmExporterPol.dstPort]: この必須プロパティは着信接続を受け入れるコレクタを有効に NetFlow コレクタ アプリケーションでリッスンするポートを指定します。
- VmmExporterPol.srcAddr]: このオプションのプロパティは、エクスポートされた NetFlow フロー パケットで発信元アドレスとして使用される IPv4アドレスを指定します。

VMware vSphere 分散スイッチでの NetFlow サポート

VMware vSphere 分散スイッチ (VDS) では、次の注意事項と NetFlow をサポートしています。

- 外部のコレクタは、ESX 経由で到達可能である必要があります。ESX は、仮想ルーティングおよび一般 (Vrf) をサポートしていません。
- ポート グループでは、有効にしたり、NetFlow を無効にすることができます。
- VDS は、フロー レベルのフィルタ リングをサポートしていません。

VMware vCenter で、次の VDS パラメータを設定します。

- コレクタの IP アドレスとポート。IPv6は、 VDS バージョン 6.0 以降でサポートされています。これらは必須です。
- 発信元の IP アドレス。これは任意です。

- アクティブなフロー タイムアウト、フローのアイドル タイムアウト、およびサンプリング レート。これらは任意です。

Cisco Application Virtual Switch でサポートされている NetFlow

Cisco Application Virtual Switch（AV）は、次の注意事項と NetFlow がサポートされています。

- 外部のコレクタは、ESX 経由で到達可能である必要があります。ESX は、仮想ルーティングおよび一般（VRF）をサポートしていません。
- ポート グループ NetFlow を有効または無効にして、収集されるトラフィックの方向を指定できます。
- Cisco AV は、フロー レベルのフィルタ リングをサポートしていません。

GUI を使用した、VM ネットワーキングのための NetFlow エクスポータ ポリシーの設定

次の手順では、VM のネットワー キングの NetFlow エクスポータ ポリシーを設定します。

手順

ステップ 1 メニュー バーで、**[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、[展開 **ポリシー** > **インターフェイス** > **NetFlow** 。
ステップ 3 右クリックして **VM Networking 社で働いて NetFlow エクスポータ**] を選択します **VM Networking 社で働いて NetFlow エクスポータを作成** します。
ステップ 4 **Create NetFlow Exporter for VM Networking** ダイアログボックスで、必要に応じてフィールドに入力します。
ステップ 5 [Submit] をクリックします。

GUI を使用した VMM ドメイン下での NetFlow エクスポータ ポリシーの利用

次の手順では、GUI を使用して VMM ドメイン下で NetFlow エクスポータ ポリシーを利用します。

手順

ステップ 1 メニュー バーで、 **[Virtual Networking]** > **[Inventory]** を選択します。

ステップ 2 **Navigation** ウィンドウで **VMM Domains** フォルダを展開し **VMware** を右クリックし、**Create vCenter Domain** を選択します。

ステップ 3 **Create vCenter Domain** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します:

a) **NetFlow Exporter Policy** ドロップダウンリストで、目的のエクスポータ ポリシーを選択します。 または、新しいポリシーを作成します。

b) **Active Flow Timeout** フィールドで、秒単位で目的のアクティブなフロータイムアウトを入力します。

Active Flow Timeout パラメータでは、アクティブなフローが開始してから NetFlow が待機する遅延を指定します。その後で、NetFlow は集したデータを送信します。範囲は 60 ～ 3600 です。デフォルト値は 60 です。

c) **Idle Flow Timeout** フィールドで、目的のアイドル フロー タイムアウトを秒単位で入力します。

Idle Flow Timeout パラメータでは、アイドルなフローが開始してから NetFlow が待機する遅延を指定します。その後で、NetFlow は集したデータを送信します。範囲は 10 ～ 300 です。デフォルト値は 15 です。

d) (VDS のみ) **Sampling Rate** フィールドに、目的のサンプリング レートを入力します。

Sampling Rate パラメータでは、毎回収集したパケットの後で、NetFlow がいくつのパケットをドロップするかを指定します。0 の値を指定した場合、NetFlow はパケットをドロップしません。範囲は 0 ～ 1000 です。デフォルト値は 0 です

ステップ 4 [Submit] をクリックします。

GUI を使用してエンドポイント グループ上の NetFlow から VMM ドメインへの関連付けを有効化する

次の手順により、エンドポイント グループ上の NetFlow と VMM ドメインの関連付けを有効にします。

始める前に

次を設定する必要があります。

- アプリケーション プロファイル
- アプリケーション エンドポイント グループ

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 **[作業]** ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 左側の [ナビゲーション] ウィンドウで、***tenant_name*** > **[アプリケーション プロファイル]** > ***application_profile_name*** > **[アプリケーション EPG]** > ***application_EPG_name*** を展開します。

ステップ 4 [Domains (VMs and Bare-Metals)] を右クリックし [Add VMM Domain Association] をクリックします。

ステップ 5 **[VMM ドメイン関連付けの追加]** ダイアログ ボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します:

a) **[NetFlow]** では **[有効]** を選択します。

b) （Cisco AVS のみ）**[NetFlow 方向]** を選択し、モニタおよび収集する必要があるフローの **[入力]**、**[出力]**、**[両方]** 選択します。

ステップ 6 [Submit] をクリックします。

NX OS スタイル CLI を使用した仮想マシン ネットワーキングの NetFlow エクスポータ ポリシーの設定

次の手順の例では、NX OS スタイル CLI を使用して、仮想マシン ネットワーキングの NetFlow エクスポータ ポリシーを設定します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 エクスポータ ポリシーを設定します。

例：

```
apic1(config)# flow vm-exporter vmExporter1 destination address 2.2.2.2 transport udp
1234
apic1(config-flow-vm-exporter)# source address 4.4.4.4
apic1(config-flow-vm-exporter)# exit
apic1(config)# exit
```

VMware VDS の NX-OS スタイル CLI を使用して VMM ドメインで NetFlow エクスポータ ポリシーを利用する

次の手順では、VMM ドメインで NetFlow エクスポータ ポリシーを消費するために、NX OS スタイル CLI を使用します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 NetFlow エクスポータ ポリシーを消費します。

例：

```
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# flow exporter vmExporter1
apic1(config-vmware-dvs-flow-exporter)# active-flow-timeout 62
apic1(config-vmware-dvs-flow-exporter)# idle-flow-timeout 16
apic1(config-vmware-dvs-flow-exporter)# sampling-rate 1
apic1(config-vmware-dvs-flow-exporter)# exit
apic1(config-vmware-dvs)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

Cisco AVS の NX-OS スタイル CLI を使用して、VMM ドメイン下の NetFlow エクスポータ ポリシーを利用する

次の手順では、VMM ドメインで NetFlow エクスポータ ポリシーを消費するために、NX OS スタイル CLI を使用します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 NetFlow エクスポータ ポリシーを消費します。

例：

```
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-avs
apic1(config-vmware-dvs)# flow exporter vmExporter1
apic1(config-vmware-dvs-flow-exporter)# active-flow-timeout 62
apic1(config-vmware-dvs-flow-exporter)# idle-flow-timeout 16
apic1(config-vmware-dvs-flow-exporter)# exit
apic1(config-vmware-dvs)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

VMware 用 NX OS スタイル CLI を使用したエンドポイント グループ上の NetFlow の有効化または無効化

次の手順では、NX OS スタイル CLI を使用してエンドポイント グループ上で NetFlow を有効または無効にします。

手順

ステップ 1 NetFlow の有効化：

例：

```
apic1# config
apic1(config)# tenant tn1
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# vmware-domain member mininet
apic1(config-tenant-app-epg-domain)# flow monitor enable
apic1(config-tenant-app-epg-domain)# exit
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# exit
```

ステップ 2 （任意） NetFlow を使用しない場合は、この機能を無効にします。

例：

```
apic1(config-tenant-app-epg-domain)# no flow monitor enable
```

Cisco AVS の NX-OS スタイルの CLI を使用して、エンドポイント グループ上の NetFlow を有効または無効にする

NX-OS スタイルの CLI を使用して、エンドポイント グループでの NetFlow を有効または無効にするには、次の手順を実行します。

手順

ステップ 1 NetFlow の有効化：

例：

```
apic1# config
apic1(config)# tenant tn1
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# vmware-domain member mininet
apic1(config-tenant-app-epg-domain)# flow monitor enable
apic1(config-tenant-app-epg-domain)#flow direction {ingress | egress | both}
```

```
apic1(config-tenant-app-epg-domain)# exit
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# exit
```

ステップ 2 （任意） NetFlow を使用しない場合は、この機能を無効にします。

例：

```
apic1(config-tenant-app-epg-domain)# no flow monitor enable
```

REST API を使用した、VM ネットワーキングのための NetFlow エクスポータ ポリシーの設定

XML の次の例では、REST API を使用して VM ネットワー キングの NetFlow エクスポータ ポリシーを設定する方法を示します。

```
<polUni>
    <infraInfra>
        <netflowVmmExporterPol name="vmExporter1" dstAddr="2.2.2.2" dstPort="1234"
srcAddr="4.4.4.4"/>
    </infraInfra>
</polUni>
```

VMware VDS に REST API を使用して VMM ドメインで NetFlow エクスポータ ポリシーを使用する

次に示すのは、REST API を使用して VMM ドメインで NetFlow エクスポータ ポリシーを利用する方法を示す XML の例です:

```
<polUni>
    <vmmProvP vendor="VMware">
        <vmmDomP name="mininet">
            <vmmVSwitchPolicyCont>
                <vmmRsVswitchExporterPol tDn="uni/infra/vmmexporterpol-vmExporter1"
activeFlowTimeOut="62" idleFlowTimeOut="16" samplingRate="1"/>
            </vmmVSwitchPolicyCont>
        </vmmDomP>
    </vmmProvP>
</polUni>
```

Cisco AVS 用の REST API を使用して VMM ドメイン下で NetFlow エクスポータ ポリシーを使用する

手順

VMM ドメインで NetFlow エクスポータ ポリシーを消費するには、次の例のように POST メッセージを送信します。

例：

```
<polUni>
    <vmmProvP vendor="VMware">
        <vmmDomP name="mininet">
            <vmmVSwitchPolicyCont>
                <vmmRsVswitchExporterPol tDn="uni/infra/vmmexporterpol-vmExporter1"
activeFlowTimeOut="62" idleFlowTimeOut="16"/>
            </vmmVSwitchPolicyCont>
        </vmmDomP>
    </vmmProvP>
</polUni>
```

VMware VDS の VMM ドメイン アソシエーションのエンドポイント グループ上で NetFlow を有効にする

次の XML の例では、REST API を使用して、VMM ドメイン アソシエーションのためのエンドポイント グループ上で NetFlow を有効化する方法を示しています:

```
<polUni>
    <fvTenant name="t1">
        <fvAp name="a1">
            <fvAEPg name="EPG1">
                <fvRsDomAtt tDn="uni/vmmp-VMware/dom-mininet" netflowPref="enabled" />
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

Cisco AVS の VMM ドメイン アソシエーションのエンドポイント グループで NetFlow を有効にする

手順

次の例のような POST メッセージの送信によって、VMM ドメイン アソシエーションのために、エンドポイント グループの NetFlow を有効にします。

例：

（注） この例では、NetFlowの方向を「入力」にしています。また、「出力」または「両方」を選択できます。

```
<polUni>
    <fvTenant name="t1">
        <fvAp name="a1">
            <fvAEPg name="EPG1">
                <fvRsDomAtt tDn="uni/vmmp-VMware/dom-mininet" netflowPref="enabled"
netflowDir="ingress"/>
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

VMM 接続のトラブルシューティング

次の手順では、VMM 接続の問題を解決します。

手順

ステップ 1 Application Policy Infrastructure Controller（APIC）でインベントリの再同期をトリガします。

APIC で、インベントリの再同期をトリガする方法の詳細については、次のナレッジ ベース記事を参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_VMM_OnDemand_Inventory_in_APIC.html

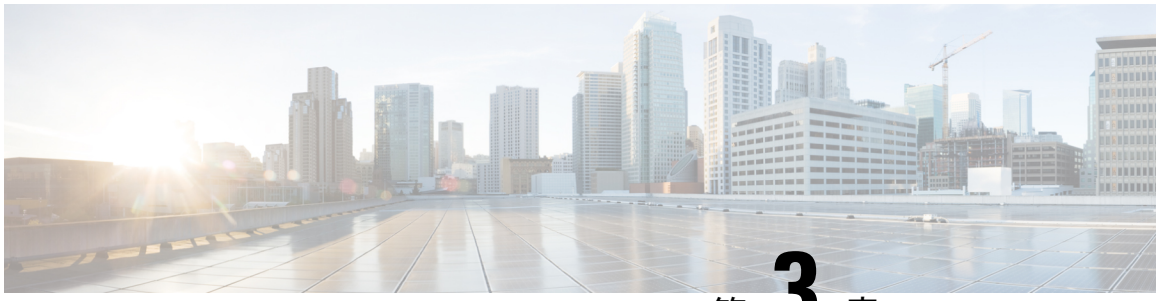
ステップ 2 手順 1 で、影響を受ける EPG の問題が解決しない場合は、VMM ドメインの事前プロビジョニングを使用して解決の緊急性を設定します。

「事前プロビジョニング」は、ネイバー隣接関係または OpFlex 許可、その後の VMM ドメイン VLAN プログラミングのダイナミック特性の必要性がありません。解決の緊急度に関する詳細は、次の EPG ポリシーの解決および展開の緊急度を参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals/b_ACI-Fundamentals_chapter_01011.html#concept_EF87ADDAD4EF47BDA741EC6EFDAECBBD

ステップ 3 手順 1 と 2 では問題が解決せず、すべての VM に問題が見られる場合は、VM コントローラ ポリシーを削除し、ポリシーを再度追加します。

（注） そのコントローラ ポリシーを削除すると、コントローラ上のすべての VM のトラフィックに影響があります。



第 3 章

Cisco ACI の VMware VDS との統合

この章の内容は、次のとおりです。

仮想マシン ネットワーキング ポリシーの設定

Cisco APIC は、Cisco ACI の利点を仮想インフラストラクチャに拡張するために、サードパーティの VM マネージャ (VMM) (たとえば VMware vCenter) と統合するようになっています。Cisco APIC は、VMM システム内の CIsco ACI ポリシーを有効にして、管理者が使用できるようにします。

Cisco ACI と VMware の VMM 統合では以下のモードがサポートされます。

- VMware VDS：Cisco ACI と統合するときに、VMware vSphere Distributed Switch（VDS）によって、ACI ファブリックの VM ネットワーキングが設定できるようになります。
- Cisco ACI Virtual Edge: Cisco ACI Virtual Edge をインストールして設定する方法の詳細については、 *Cisco ACI Virtual Edge*『インストレーション ガイド』および *Cisco ACI Virtual Edge*『構成ガイド』を参照してください。Cisco.com からアクセスできます。
- Cisco Application Virtual Switch (AVS): Cisco AVS を Cisco ACI とともにインストールして構成する方法については、Cisco AVS のマニュアルを参照してください。Cisco.com からアクセスできます。

APIC でサポートされる VMware VDS バージョン

次の表は、Cisco APIC で VMware VDS と VMware vCenter 用にサポートされている VMware vSphere のバージョンを示しています。

バージョン	VMware VDS	VMware vCenter
リリース 5.5	サポート対象	サポート対象
リリース 6.0	サポート対象	サポート対象
リリース 6.5	サポート対象	サポート対象
リリース 6.6	サポート対象	サポート対象外
リリース 6.7	サポート対象外	サポート対象

（注） VMware vSphere バージョン 6.7 には、vCenter 6.7、ESXi 6.7、および DVS 6.6 が含まれています。

（注） VMware vSphere Distributed Switch（VDS）を使用した VMM ドメインに VMware ESXi ホストを追加するときは、ESXi ホストのバージョンが、vCenter にすでに導入されている Distributed Virtual Switch（DVS）バージョンと互換性があることを確認してください。ESXi ホストに関する VMware VDS 互換性要件の詳細については、VMware のマニュアルを参照してください。

ESXi ホスト バージョンに既存の DVS との互換性がない場合、vCenter はその ESXi ホストを DVS に追加することはできず、非互換性エラーが発生します。Cisco APIC から既存の DVS バージョン設定を変更することはできません。vCenter で DVS バージョンを低くするには、VMM ドメイン設定を削除してから、低くした設定で再適用する必要があります。

重要 VIC カードで UCS B シリーズまたは C シリーズ サーバを実行している ESXi 6.5 ホストがある場合には、一部の VMNIC が、リンク フラップや TOR リロードなどのポート状態イベントの際にダウンすることがあります。この問題を防ぐため、デフォルトの eNIC ドライバを使用せず、VMware Web サイト、https://my.vmware.com/web/vmware/details?downloadGroup=DT-ESXI65-CISCO-NENIC-1020&productId=614 からのものをインストールしてください。

5.X から 6.x への VMware DVS のアップグレードと VMM 統合に関するガイドライン

ここでは、VMware 分散仮想スイッチ（DVS）の 5.x から 6.x へのアップグレードおよび VMM 統合のガイドラインを説明します。

- DVS のバージョニングは VMware DVS にのみ適用され、Cisco Application Virtual Switch（AVS）には適用されません。DVS のアップグレードは、ACI からではなく VMware vCenter または関連するオーケストレーション ツールから開始されます。vCenter 内の AVS スイッチの場合、 **Upgrade Version** オプションはグレー表示になります。
- DVS を 5.x から 6.x にアップグレードする場合、vCenter Server をバージョン 6.0 に、および分散スイッチに接続されているすべてのホストを ESXi 6.0 にアップグレードする必要があります。vCenter およびハイパーバイザ ホストのアップグレードの詳細については、VMware のアップグレード マニュアルを参照してください。DVS をアップグレードするには、Web クライアントに移動します（**[Home]** > **[Networking]** > **[DatacenterX]** > **[DVS-X]** > **[Actions Menu]** > **[Upgrade Distributed Switch]**）。
- vCenter に表示される DVS バージョンが APIC で設定された VMM ドメインの DVS バージョンと一致しない場合でも、DVS の機能、能力、パフォーマンス、スケールへの機能上の影響はありません。APIC および VMM ドメインの DVS バージョンは、初期導入にのみ使用されます。

VMware VDS 統合のためのガイドライン

VMware vSphere 分散スイッチ (VDS) を Cisco Application Centric Infrastructure (ACI) に統合するときには、このセクションのガイドラインに従う必要があります。

- VMM 統合用に設定された VMware VDS では次の設定を変更しないでください:
  - VMware vCenter のホスト名 (DNS を使用している場合)。
  - VMware vCenter IP アドレス (IP を使用している場合)。
  - Cisco APIC が使用している VMware vCenter のクレデンシャル。
  - データセンター名
  - フォルダ、VDS、またはポート グループの名前。
  - VMware VDS が含まれているフォルダ構造。

    たとえば、フォルダを別のフォルダに入れるようなことはしないでください。
  - LACP/ポート チャネル、LLDP、CDP などの設定を含む、アップリンク ポート チャネル設定
  - ポートグループの VLAN
  - Cisco APIC がプッシュするポート グループのアクティブなアップリンク。

- Cisco APIC がプッシュするポートグループのセキュリティ パラメータ (無差別モード、MAC アドレスの変更、偽造送信)。

- 実行している Cisco ACI のバージョンでサポートされている VMware vCenter/vSphere のバージョンを使用します。
- いずれかのポートグループを追加または削除する場合は、Cisco APIC または VMware vCenter の Cisco ACI vCenter プラグインを使用します。
- Cisco APIC は、VMware vCenter で行われた変更の一部を上書きする可能性があることに注意してください。

  たとえば、Cisco APIC がポートグループを更新すると、ポート バインディング、無差別モード、およびロード バランシングが上書きされることがあります。

ACI と VMware の構造のマッピング

表 *2: ACI* と *VMware* の構造のマッピング

Cisco APIC 用語	VMware 用語
VM コントローラ	vCenter (データセンター)
Virtual Machine Manager（VMM） ドメイン	vSphere Distributed Switch（VDS）
エンドポイント グループ（EPG）	ポート グループ

APIC によって管理される VMware VDS パラメータ

APIC によって管理される VDS パラメータ

VMware VDS	デフォルト値	APIC ポリシーを使用して設定可能か
名前	VMM ドメイン名	はい（ドメインから派生）
説明	"APIC Virtual Switch"	いいえ
フォルダ名	VMM ドメイン名	はい（ドメインから派生）
バージョン	vCenter でサポートされる最新	はい
Discovery プロトコル	LLDP	はい
アップリンク ポートおよびアップリンク名	8	いいえ

VMware VDS	デフォルト値	APIC ポリシーを使用して設定可能か
アップリンク名プレフィックス	uplink	いいえ
最大 MTU	9000	はい
LACP ポリシー	disabled	はい
ポートのミラーリング	0 セッション。	はい
アラーム	フォルダ レベルに 2 アラーム追加	いいえ

APIC によって管理される VDS ポート グループ パラメータ

VMware VDS ポート グループ	デフォルト値	APIC ポリシーを使用して設定可能か
名前	テナント名|アプリケーション プロファイル名|EPG 名	はい（EPG から導出）
ポート バインディング	スタティック バインディング	いいえ
VLAN	VLAN プールから選択	はい
ロードバランシング アルゴリズム	APIC のポート チャネル ポリシーに基づいて派生	はい
無差別モード	ディセーブル	はい
偽装された転送	Disabled	はい
MAC 変更	Disabled	はい
すべてのポートをブロック	False	いいえ

VMM ドメイン プロファイルの作成

VMM ドメイン プロファイルは、仮想マシン コントローラを Cisco ACI ファブリックに接続させる接続ポリシーを指定します。同様のネットワーキング ポリシー要件を持つ VM コントローラをグループ化します。たとえば、VM コントローラは VLAN プールとアプリケーション エンドポイント グループ（EPG）を共有できます。Cisco APIC はコントローラと通信して、仮想ワークロードに適用するポート グループなどのネットワーク設定をパブリッシュします。詳細については、 Cisco.com の『Cisco Application Centric Infrastructure Fundamentals』を参照してください。 on Cisco.com.

Cisco APIC リリース 3.1(1) 以降では、読み取り専用の VMM ドメインを作成することもできます。読み取り専用 VMM ドメインを使用すればと、Cisco APIC が管理していない VMware vCenter での VDS のインベントリ情報を表示できます。読み取り専用 VMM ドメインを設定する手順は、他の VMM ドメインを作成する手順とは若干異なります。ただし、同じワークフローと前提条件が適用されます。

Cisco APIC リリース 3.2(2) 以降では、すでに作成済みの読み取り専用 VMM のドメインを、完全管理の VMM ドメインに昇格することができます。読み取り専用 VMM ドメインに昇格させる手順については、「読み取り専用 VMM ドメインを読み取り/書き込みに昇格させる （45 ページ）」の項を参照してください。

VMware vCenter で設定した VMware VDS を Cisco Application Centric Infrastructure VMM ドメインにインポートすることができます。

VDS は、VDS と同じ名前のネットワーク フォルダに存在する場合にインポートできます。インポートするには、VDS と同じ名前の VDS ドメインを Cisco Application Policy Infrastructure Controller（APIC）で作成します。

（注）
- VDS 上の既存のポート グループは変更されません。ただし、Cisco APIC で障害が発生し、ポート グループが EPG にバインドされていないことが示されます。
- VDS 検出プロトコル ポリシーと MTU の設定は、Cisco APIC VDS ポリシーに従って更新されます。

このガイドの次の項を参照してください。

- GUI を使用した vCenter ドメイン プロファイルの作成 （32 ページ）
- REST API を使用した vCenter ドメイン プロファイルの作成 （36 ページ）
- NX-OS スタイルの CLI を使用した vCenter ドメイン プロファイルの作成 （34 ページ）

（注） この項での VMM ドメインの例は、VMware vCenter ドメインです。

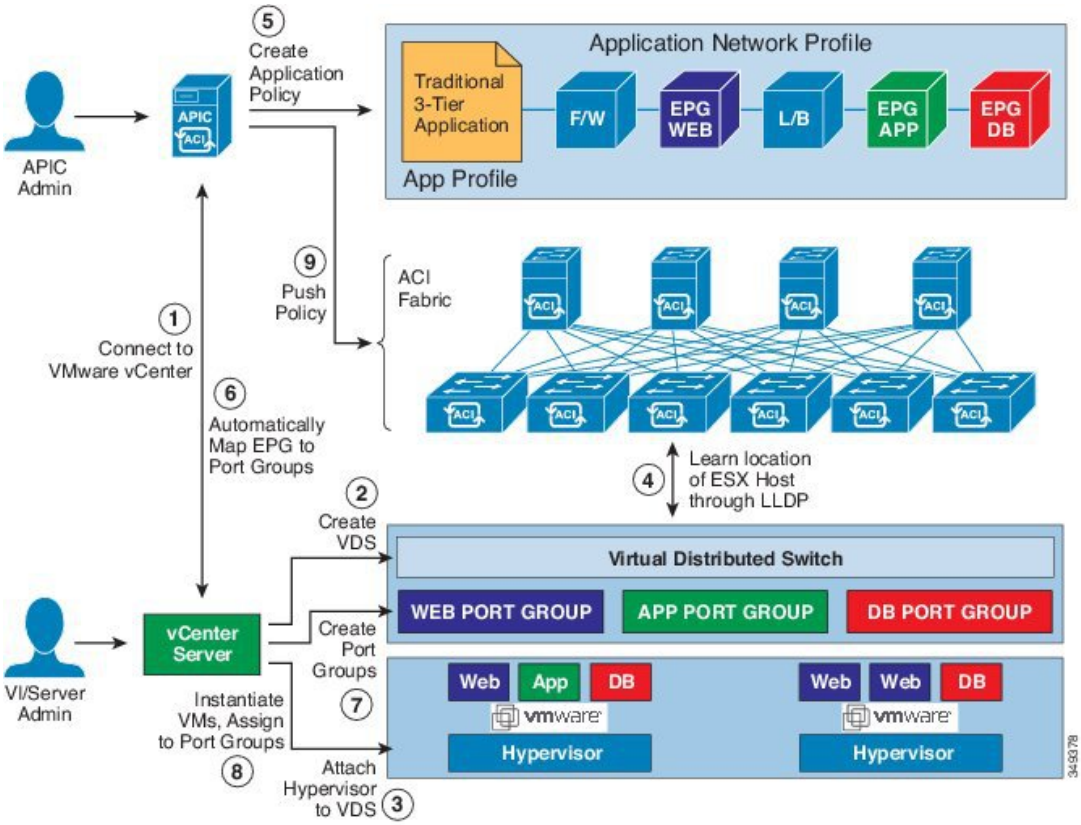
VMM ドメイン プロファイルを作成するための前提条件

VMM ドメイン プロファイルを設定するには、次の前提条件を満たす必要があります。

- すべてのファブリック ノードが検出され、設定されている。
- インバンド（inb）またはアウトオブバンド（oob）管理が APIC 上で設定されている。
- Virtual Machine Manager（VMM）がインストールされ、設定されて、inb/oob 管理ネットワーク（たとえば、vCenter）経由で到達可能である。

vCenter ドメイン運用ワークフロー

図 *5 : vCenter* ドメイン運用ワークフロー順の説明



APIC管理者は、APIC の vCenter ドメイン ポリシーを設定します。APIC 管理者は、次の vCenter 接続情報を提供します。

- vCenter IP アドレス、vCenter クレデンシャル、VMM ドメイン ポリシー、VMM ドメイン SPAN
- ポリシー（VLAN プール、VMware VDS などのドメイン タイプ、Cisco Nexus 1000V スイッチ）
- 物理リーフ インターフェイスへの接続性（接続エンティティ プロファイルを使用）

1. APIC が自動的に vCenter に接続します。
2. APICVDS の作成: すでに作成されている場合は、既存の VDS を使用または: VMM ドメインの名前に一致します。

（注） 既存の VDS を使用する場合、同じ名前でフォルダ内に VDS 必要があります。

（注） VCenter から既存の VDS を表示する場合は、これを行う指定することにより、 **読み取り専用モード** で、 **アクセス モード** エリア Cisco APIC を使用して vCenter で VDS と同じ名前の VMM ドメインを作成する際にします。この VMM で **読み取り専用モード** APIC で管理されていません。VCenter のユーザ クレデンシャルと vCenter IP アドレスを除くこの VMM ドメインの任意のプロパティを変更することはできません。

3. vCenter の管理者やコンピューティングの管理ツールは、APIC VDS に ESX ホストまたはハイパーバイザを追加し、APIC VDS 上にアップリンクとして ESX ホスト ハイパーバイザ ポートを割り当てます。これらのアップリンクは ACI リーフ スイッチを接続する必要があります。
4. APIC がハイパーバイザの LLDP または CDP 情報を使用して、リーフ接続へのハイパーバイザ ホストの場所を学習します。
5. APIC 管理者がアプリケーション EPG ポリシーを作成して関連付けます。
6. APIC 管理者が VMM ドメインに EPG ポリシーを関連付けます。
7. APIC は、VDS 下の VMware vCenter でポート グループを自動的に作成します。このプロセスは VMware vCenter でネットワーク ポリシーをプロビジョニングします。

（注）
- ポート グループ名は、テナント名、アプリケーション プロファイル名および EPG 名を連結したものです。
- ポート グループは、VDS 下で作成され、APIC によって以前に作成されたものです。

8. vCenter の管理者やコンピューティングの管理ツールは、VM をインスタンス化しポート グループに割り当てます。
9. APIC は、vCenter イベントに基づいて VM の配置について学習します。APIC は、アプリケーション EPG および関連するポリシー（たとえば、コントラクトやフィルタ）を ACI ファブリックに自動的にプッシュします。

GUI を使用した vCenter ドメイン プロファイルの作成

vCenter ドメインの作成時に行う作業の概要は次のとおりです（詳細は下のステップで説明します）。

- スイッチ プロファイルを作成または選択します。
- インターフェイス プロファイルを作成または選択します。
- インターフェイス ポリシー グループを作成または選択します。
- VLAN プールを作成または選択します。

- vCenter ドメインを作成します。
- vCenter クレデンシャルを作成します。

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順にクリックします。

ステップ 2 ナビゲーション ウィンドウで、[Quick Start] をクリックし、中央ペインで [Configure an interface, PC, and VPC] をクリックします。

ステップ 3 [Configure an interface, PC, and VPC] ダイアログ ボックスで、次のアクションを実行します。

a) [Configured Switch Interfaces] を展開します。
b) [+] アイコンをクリックします。
c) [Quick] オプション ボタンが選択されていることを確認します。
d) [Switches] ドロップダウン リストから、適切なリーフ ID を選択します。

[Switch Profile Name] フィールドに、スイッチ プロファイル名が自動的に入力されます。

e) スイッチ インターフェイスを設定するために [+] アイコンをクリックします。
f) [Interface Type] エリアで、適切なラジオ ボタンをオンにします。
g) [Interfaces] フィールドに、目的のインターフェイス範囲を入力します。
h) [Interface Selector Name] フィールドに、セレクタ名が自動的に入力されます。
i) [Interface Policy Group] 領域で、[Create One] オプション ボタンを選択します。
j) [Link Level Policy] ドロップダウン リストから、目的のリンク レベル ポリシーを選択します。
k) [CDP Policy] ドロップダウン リストから、目的の CDP ポリシーを選択します。

（注） 同様に、利用可能なポリシーエリアから目的のインターフェイス ポリシーを選択します。

l) [Attached Device Type] エリアで、[ESX Hosts] を選択します。
m) [Domain] エリアで、[Create One] ラジオ ボタンが選択されていることを確認します。
n) [Domain Name] フィールドに、ドメイン名を入力します
o) [VLAN] エリアで、[Create One] ラジオ ボタンが選択されていることを確認します。
p) [VLAN Range] フィールドに、必要に応じて VLAN の範囲を入力します。

（注） 少なくとも 200 の VLAN 番号の範囲を推奨します。手動で割り当てたインフラ VLAN を含む範囲を定義しないでください。そのような定義をした場合、Cisco Application Policy Infrastructure Controller（APIC）のバージョンによっては障害が発生することがあります。インフラ VLAN を OpFlex 統合の一部として拡張する必要がある場合は、特定の使用例やオプションを設定します。

q) [vCenter Login Name] フィールドに、ログイン名を入力します。
r) （任意） [Security Domains] ドロップダウン リストから、適切なセキュリティ ドメインを選択します。
s) [Password] フィールドに、パスワードを入力します。

t) [Confirm Password] フィールドにパスワードを再入力します。

u) **vCenter** を展開します。

ステップ 4 [Create vCenter Controller] ダイアログボックスに適切な情報を入力し、[OK] をクリックします。

ステップ 5 [Configure Interface, PC, And VPC] ダイアログボックスで、次の操作を実行します。

[Port Channel Mode] および [vSwitch Policy] エリアでポリシーを指定しなかった場合、この手順の前の部分で設定したのと同じポリシーが vSwitch でも有効になります。

a) [Port Channel Mode] ドロップダウンリストからモードを選択します。

b) [vSwitch Policy] エリアで、必要なラジオ ボタンをクリックして CDP または LLDP をクリックします。

c) [NetFlow Exporter Policy] ドロップダウンリストで、ポリシーを選択するか、作成します。

NetFlow エクスポータ ポリシーは、外部コレクタの到達可能性を設定します。

d) [Active Flow Time0ut]、 [Idle Flow Timeout]、および [Sampling Rate] ドロップダウンリストから値を選択します。

e) [SAVE] を 2 回クリックしてから [SUBMIT] をクリックします。

ステップ 6 次の手順に従って、新しいドメインとプロファイルを確認します。

a) メニュー バーで、 **[Virtual Networking]** > **[Inventory]** を選択します。

b) [Navigation] ウィンドウで、 **[VMM Domains]** > **[VMware]** > ***[Domain_name]*** > **[vCenter_name]** を展開します。

作業ペインの [Properties] に VMM ドメイン名を表示して、コントローラがオンラインであることを確認します。[Work] ペインに、vCenter のプロパティが動作ステータスとともに表示されます。表示される情報によって、APIC コントローラから vCenter Server への接続が確立され、インベントリが使用できることを確認します。

NX-OS スタイルの CLI を使用した vCenter ドメイン プロファイルの作成

始める前に

ここでは、NX-OS スタイルの CLI を使用して vCenter ドメイン プロファイルを作成する方法を説明します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

ステップ 3 この VLAN ドメインにインターフェイスを追加します。これらは VMware ハイパーバイザのアップリンク ポートに接続されるインターフェイスです。

例：

```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 4 VMware ドメインを作成して VLAN ドメイン メンバーシップを追加します。

例：

```
apic1(config)# vmware-domain vmmdom1
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

特定のデリミタを使用してドメインを作成します。

例：

```
apic1(config)# vmware-domain vmmdom1 delimiter @
```

ステップ 5 DVS にドメイン タイプを設定します。

例：

```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

ステップ 6 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延時間は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 です。

例：

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

ステップ 7 ドメインのコントローラを設定します。

例：

```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator
Password:
Retype password:
apic1(config-vmware-vc)# exit
apic1(config-vmware)# exit
```

```
apic1(config)# exit
```

（注） パスワードを設定する際には、Bashシェルが間違えて解釈することを避けるために、「$」または「!」などの特殊文字の前にバックスラッシュを付ける必要があります（「\$」）。エスケープのバックスラッシュは、パスワードを設定するときにだけ必要です。実際のパスワードにはバックスラッシュは表示されません。

ステップ 8 設定を確認します。

例：

```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
    configure-dvs
      exit
    exit
```

REST API を使用した vCenter ドメイン プロファイルの作成

手順

ステップ 1 VMM ドメイン名、コントローラおよびユーザ クレデンシャルを設定します。

例：

```
 POST URL: https://<api-ip>/api/node/mo/.xml

<polUni>
<vmmProvP vendor="VMware">
<!-- VMM Domain -->
<vmmDomP name="productionDC">
<!-- Association to VLAN Namespace -->
<infraRsVlanNs tDn="uni/infra/vlanns-VlanRange-dynamic"/>
<!-- Credentials for vCenter -->
<vmmUsrAccP name="admin" usr="administrator" pwd="admin" />
<!-- vCenter IP address -->
<vmmCtrlrP name="vcenter1" hostOrIp="<vcenter ip address>" rootContName="<Datacenter
Name in vCenter>">
<vmmRsAcc tDn="uni/vmmp-VMware/dom-productionDC/usracc-admin"/>
</vmmCtrlrP>
</vmmDomP>
</vmmProvP>
```

例：

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" delimiter="@" >
   </vmmDomP>
</vmmProvP>
```

```
</polUni>
```

ステップ 2 VLAN ネームスペースの導入用の接続可能エンティティ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<infraInfra>
<infraAttEntityP name="profile1">
<infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
</infraAttEntityP>
</infraInfra>
```

ステップ 3 インターフェイス ポリシー グループおよびセレクタを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraAccPortP name="swprofile1ifselector">
        <infraHPortS name="selector1" type="range">
            <infraPortBlk name="blk"
             fromCard="1" toCard="1" fromPort="1" toPort="3">
            </infraPortBlk>
     <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-group1" />
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
        <infraAccPortGrp name="group1">
            <infraRsAttEntP tDn="uni/infra/attentp-profile1" />
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

ステップ 4 スイッチ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraNodeP name="swprofile1">
        <infraLeafS name="selectorswprofile11718" type="range">
            <infraNodeBlk name="single0" from_="101" to_="101"/>
            <infraNodeBlk name="single1" from_="102" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-swprofile1ifselector"/>
    </infraNodeP>
</infraInfra>
```

ステップ 5 VLAN プールを設定します。

例：

```
 POST URL: https://<apic-ip>/api/node/mo/.xml

<polUni>
<infraInfra>
<fvnsVlanInstP name="VlanRange" allocMode="dynamic">
```

```
   <fvnsEncapBlk name="encap" from="vlan-100" to="vlan-400"/>
</fvnsVlanInstP>
</infraInfra>
</polUni>
```

ステップ 6 設定されたすべてのコントローラとそれらの動作状態を検索します。

例：

```
GET:
https://<apic-ip>/api/node/class/compCtrlr.xml?
<imdata>
<compCtrlr apiVer="5.1" ctrlrPKey="uni/vmmp-VMware/dom-productionDC/ctrlr-vcenter1"
deployIssues="" descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1" domName="
productionDC"
hostOrIp="esx1" mode="default" model="VMware vCenter Server 5.1.0 build-756313"
name="vcenter1" operSt="online" port="0" pwd="" remoteOperIssues="" scope="vm"
usr="administrator" vendor="VMware, Inc." ... />
</imdata>
```

ステップ 7 「ProductionDC」という VMM ドメイン下の「vcenter1」という名前の vCenter をハイパーバイザと VM で検索します。

例：

```
GET:
https://<apic-ip>/api/node/mo/comp/prov-VMware/ctrlr-productionDC-vcenter1.xml?query-target=children

<imdata>
<compHv descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/hv-host-4832" name="esx1"
state="poweredOn" type="hv" ... />
<compVm descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/vm-vm-5531" name="AppVM1"
state="poweredOff" type="virt" .../>
<hvsLNode dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/sw-dvs-5646" lacpEnable="yes"
lacpMode="passive" ldpConfigOperation="both" ldpConfigProtocol="lldp" maxMtu="1500"
mode="default" name="apicVswitch" .../>
</imdata>
```

ステップ 8 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 秒です。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >
<vmmDomP name="mininetavs" mode="n1kv" enfPref="sw" epRetTime=”60”>
<infraRsVlanNs tDn="uni/infra/vlanns-inst-dynamic"/>
<vmmUsrAccP
name="defaultAccP"
usr="administrator"
pwd="admin"
/>
</vmmDomP>
</vmmProvP>
```

読み取り専用 VMM ドメインの作成

Cisco APIC リリース 3.1 (1) 以降では、読み取り専用 VMM ドメインを作成することができます。これにより、Cisco APIC は管理されませんする VMware vCenter での VDS のインベントリの情報を表示します。

読み取り専用 VMM ドメインを作成したら、通常の VMM ドメインと同じように、ハイパーバイザ、VM、NIC のステータス、およびその他のインベントリ情報を表示できます。EPG を VMM ドメインに関連付けて、そのためのポリシーを構成できます。ただし、読み取り専用 VMM ドメインから VDS にポリシーがプッシュされることはありません。また、読み取り専用 VMM ドメインでは障害は発生しません。

Cisco APIC GUI、NX-OS スタイルの CLI、または REST API を使用して、読み取り専用 VMM ドメインを作成することができます。手順については、このガイドの次のセクションを参照してください。

- Cisco APIC GUI を使用した読み取り専用 VMM ドメインの作成 （39 ページ）
- REST API を使用した読み取り専用 VMM ドメインの作成 （42 ページ）
- NX-OS スタイルの CLI を使用した 読み取り専用 VMM ドメインの作成 （40 ページ）

Cisco APIC GUI を使用した読み取り専用 VMM ドメインの作成

読み取り専用 VMM ドメインを作成するため、[Virtual Networking] タブの [Create vCenter Domain] ダイアログ ボックスでドメインを作成します。ドメインを作成するためにセクション「GUI を使用した vCenter ドメイン プロファイルの作成 （32 ページ）」の手順に従わないでください。その手順では、VMM ドメインのアクセス モードを設定できません。

始める前に

- セクション「VMM ドメイン プロファイルを作成するための前提条件 （30 ページ）」の前提条件を満たします。
- VMware vCenter の [Networking] タブの下で、フォルダに VDS が含まれていることを確認します。

  また、フォルダと VDS の名前が、作成する読み取り専用 VMM ドメインと正確に一致していることを確認します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Virtual Networking]** > **[Inventory]** を選択し、[VMM Domains] フォルダを展開します。

ステップ 3 [VMM Domains] フォルダを右クリックし、[Create vCenter Domain] を選択します。

ステップ 4 [Create vCenter Domain] ダイアログ ボックスで、次の手順を完了します。

a) [Virtual Switch Name] フィールドで、 ドメインの名前を入力します。

（注） 読み取り専用のドメインの名前は、VDS と VMware vCenter が含まれているフォルダの名前と同じにする必要があります。

b) [Virtual Switch] エリアで、[VMware vSphere Distributed Switch] を選択します。
c) [Access Mode] エリアで、[Read Only Mode] を選択します。
d) [vCenter Credentials] エリアで、[+]（プラス）アイコンをクリックし、ドメインの VMware vCenter クレデンシャルを作成します。
e) [VCenter] エリアで、[+]（プラス）アイコンをクリックし、ドメインの vCenter コントローラを追加します。
f) [Submit] をクリックします。

次のタスク

EPG を読み取り専用 VMM ドメインにアタッチして、そのポリシーを設定することができます。ただし、これらのポリシーは、VMware vCenter の VDS へはプッシュされません。

NX-OS スタイルの CLI を使用した 読み取り専用 VMM ドメインの作成

NX-OS スタイルの CLI を使用すれば、読み取り専用VMM ドメインを作成できます。

始める前に

- セクション「VMM ドメイン プロファイルを作成するための前提条件 （30 ページ）」の前提条件を満たします。
- VMware vCenter の [Networking] タブの下で、フォルダに VDS が含まれていることを確認します。

  また、フォルダと VDS の名前が、作成する読み取り専用 VMM ドメインと正確に一致していることを確認します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

ステップ 3 この VLAN ドメインにインターフェイスを追加します。これらは VMware ハイパーバイザのアップリンク ポートに接続されるインターフェイスです。

例：

```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 4 VMware ドメインを作成して VLAN ドメイン メンバーシップを追加します。

例：

```
apic1(config)# vmware-domain vmmdom1 access-mode readonly
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

特定のデリミタを使用してドメインを作成します。

例：

```
apic1(config)# vmware-domain vmmdom1 delimiter @
```

ステップ 5 DVS にドメイン タイプを設定します。

例：

```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

ステップ 6 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延時間は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 です。

例：

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

ステップ 7 ドメインのコントローラを設定します。

例：

```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator
Password:
Retype password:
apic1(config-vmware-vc)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

（注） パスワードを設定する際には、Bash シェルが間違えて解釈することを避けるために、「$」または「!」などの特殊文字の前にバックスラッシュを付ける必要があります（「\$」）。エスケープのバックスラッシュは、パスワードを設定するときにだけ必要です。実際のパスワードにはバックスラッシュは表示されません。

ステップ 8 設定を確認します。

例：

```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
    configure-dvs
      exit
    exit
```

次のタスク

EPG を読み取り専用 VMM ドメインにアタッチして、そのポリシーを設定することができます。ただし、これらのポリシーは、VMware vCenter の VDS へはプッシュされません。

REST API を使用した読み取り専用 VMM ドメインの作成

読み取り専用 VMM ドメインは、REST API を使用して作成することができます。

始める前に

- セクション「VMM ドメイン プロファイルを作成するための前提条件 （30 ページ）」の前提条件を満たします。
- VMware vCenter の [Networking] タブの下で、フォルダに VDS が含まれていることを確認します。

  また、フォルダと VDS の名前が、作成する読み取り専用 VMM ドメインと正確に一致していることを確認します。

手順

ステップ 1 VMM ドメイン名、コントローラおよびユーザ クレデンシャルを設定します。

例：

```
POST URL: https://<api-ip>/api/node/mo/.xml
<polUni>
<vmmProvP vendor="VMware">
<!-- VMM Domain -->
<vmmDomP name="productionDC" accessMode="read-only">
<!-- Association to VLAN Namespace -->
<infraRsVlanNs tDn="uni/infra/vlanns-VlanRange-dynamic"/>
<!-- Credentials for vCenter -->
<vmmUsrAccP name="admin" usr="administrator" pwd="admin" />
<!-- vCenter IP address -->
<vmmCtrlrP name="vcenter1" hostOrIp="<vcenter ip address>" rootContName="<Datacenter
Name in vCenter>">
```

```
<vmmRsAcc tDn="uni/vmmp-VMware/dom-productionDC/usracc-admin"/>
</vmmCtrlrP>
</vmmDomP>
</vmmProvP>
```

例：

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" delimiter="@" >
   </vmmDomP>
</vmmProvP>
</polUni>
```

ステップ 2 VLAN ネームスペースの導入用の接続可能エンティティ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<infraInfra>
<infraAttEntityP name="profile1">
<infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
</infraAttEntityP>
</infraInfra>
```

ステップ 3 インターフェイス ポリシー グループおよびセレクタを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraAccPortP name="swprofile1ifselector">
        <infraHPortS name="selector1" type="range">
            <infraPortBlk name="blk"
             fromCard="1" toCard="1" fromPort="1" toPort="3">
            </infraPortBlk>
     <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-group1" />
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
        <infraAccPortGrp name="group1">
            <infraRsAttEntP tDn="uni/infra/attentp-profile1" />
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

ステップ 4 スイッチ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraNodeP name="swprofile1">
        <infraLeafS name="selectorswprofile11718" type="range">
            <infraNodeBlk name="single0" from_="101" to_="101"/>
            <infraNodeBlk name="single1" from_="102" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-swprofile1ifselector"/>
    </infraNodeP>
```

```
</infraInfra>
```

ステップ 5 VLAN プールを設定します。

例：

```
 POST URL: https://<apic-ip>/api/node/mo/.xml

<polUni>
<infraInfra>
<fvnsVlanInstP name="VlanRange" allocMode="dynamic">
   <fvnsEncapBlk name="encap" from="vlan-100" to="vlan-400"/>
</fvnsVlanInstP>
</infraInfra>
</polUni>
```

ステップ 6 設定されたすべてのコントローラとそれらの動作状態を検索します。

例：

```
GET:
https://<apic-ip>/api/node/class/compCtrlr.xml?
<imdata>
<compCtrlr apiVer="5.1" ctrlrPKey="uni/vmmp-VMware/dom-productionDC/ctrlr-vcenter1"
deployIssues="" descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1" domName="
productionDC"
hostOrIp="esx1" mode="default" model="VMware vCenter Server 5.1.0 build-756313"
name="vcenter1" operSt="online" port="0" pwd="" remoteOperIssues="" scope="vm"
usr="administrator" vendor="VMware, Inc." ... />
</imdata>
```

ステップ 7 「ProductionDC」という VMM ドメイン下の「vcenter1」という名前の vCenter をハイパーバイザと VM で検索します。

例：

```
GET:
https://<apic-ip>/api/node/mo/comp/prov-VMware/ctrlr-productionDC-vcenter1.xml?query-target=children

<imdata>
<compHv descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/hv-host-4832" name="esx1"
state="poweredOn" type="hv" ... />
<compVm descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/vm-vm-5531" name="AppVM1"
state="poweredOff" type="virt" .../>
<hvsLNode dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/sw-dvs-5646" lacpEnable="yes"
lacpMode="passive" ldpConfigOperation="both" ldpConfigProtocol="lldp" maxMtu="1500"
mode="default" name="apicVswitch" .../>
</imdata>
```

ステップ 8 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 秒です。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >
<vmmDomP name="mininetavs" mode="n1kv" enfPref="sw" epRetTime=”60”>
<infraRsVlanNs tDn="uni/infra/vlanns-inst-dynamic"/>
<vmmUsrAccP
name="defaultAccP"
```

```
usr="administrator"
pwd="admin"
/>
</vmmDomP>
</vmmProvP>
```

次のタスク

読み取り専用 VMM ドメインを EPG にアタッチし、そのポリシーを設定できます。ただし、これらのポリシーは、VMware vCenter で VD へプッシュされません。

読み取り専用 VMM ドメインを読み取り/書き込みに昇格させる

Cisco APIC リリース 4.0(1) 以降では、既存の読み取り専用 VMM ドメインを、完全管理の読み取り/書き込み VMM ドメインに昇格させることができます。これにより、VMware vCenter での VDS のインベントリの情報を表示できるだけでなく、Cisco APIC を利用して管理することができます。

読み取り専用の VMM ドメインの作成方法は 読み取り専用 VMM ドメインの作成 （39 ページ） で説明されています。

既存の読み取り専用 VMM ドメインを昇格させる前に、「読み取り専用 VMM ドメインの昇格に関する注意事項」で説明されているガイドラインと制限事項を慎重に検討してください。

VMM ドメインを読み取り専用から読み取り/書き込みに昇格させることで、APIC が VMM ドメインを監視および管理できるだけでなく、EPG をポート グループとして関連付けできるようになります。読み取り専用 VMM ドメインの昇格には、Cisco APIC GUI、NX-OS スタイル CLI、または REST API を使用できます。詳細については、次の各項を参照してください。

- Cisco APIC GUI を使用して読み取り専用 VMM ドメインを昇格させる （46 ページ）
- NX-OS スタイルの CLI を使用した、読み取り専用 VMM ドメインのプロモート （48 ページ）
- REST API を使用して読み取り専用 VMM ドメインに昇格させる （49 ページ）

読み取り専用 VMM ドメインの昇格に関する注意事項

読み取り専用 VMM ドメインを読み取り/書き込みに昇格させる際は、次の点に注意してください。

- 読み取り専用のドメインを昇格させるには、vCenter サーバ上のドメインの VDS のための、特定のネットワーク フォルダ構造が必要です。既存の VDS がフォルダに収められておらず、データセンターの直下に置かれている場合には、VDS と同じ名前のフォルダを作成し、VDS をそのフォルダに入れてから、ドメインを読み取り/書き込みに昇格させてください。これは、APIC が適切に管理できるようにするためです。VDS がデータセンターの直下に設定されているドメインを昇格させると、APIC は、新しいフォルダの内部に新しい VDS を作成します。

- 完全管理に昇格させようとする読み取り専用VMMドメイン用のポートグループをvCenterに作成する際は、<テナント名>|<アプリケーション名>|<*EPG* 名>という形式の名前を付けることをお勧めします。

  VMMドメインを完全管理に昇格させて、ドメインにEPGを関連付けるときに、この標準形式の名前が付いているポート-グループはすべて、自動的にEPGに追加されます。

  ポート グループ名の別の形式を選択した場合は、ドメインの昇格後に、既存のポート グループから、APICによってEPG用に作成された新しいポート グループに、すべてのVMを手動で再割り当てする必要があります。

  - EPGを作成してVMMドメインに関連付けます。

    VMMドメインで、ポート グループのEPGポリシーを見つけられないと障害が発生します。

  - 既存のポート グループから仮想マシン（VM）を削除し、EPGに接続します。

    （注） このプロセスの実行時にトラフィックが消失する場合があります。

  - VMがポート グループから分離されたら、古いポート グループをvCenterから削除します。

    すべてのVMをポート グループから分離する必要があります。そうしないとポート グループを削除できません。

- ドメインを読み取り専用から読み取り/書き込みに移行する際は、移行プロセス時に使用可能なVLANが使い果たされる可能性を避けるために、一意で、かつ物理ドメイン範囲から独立しているVLAN範囲を使用することをお勧めします。
- 複数のVMMおよびVMware vCenterで同じEPGを使用する必要がある場合は、ドメインと同じ名前のLink Aggregation Group（LAG）ポリシーを設定します。EPGは1つのLAGポリシーにのみ接続できます。異なるLAGポリシーを使用する場合は、それぞれのLAGポリシーを異なるEPGに関連付ける必要があります。

  詳細については、このガイドのEnhanced LACP ポリシーのサポート （50 ページ） に関する項を参照してください。

Cisco APIC GUI を使用して読み取り専用 VMM ドメインを昇格させる

Cisco APIC GUIを使用して、読み取り専用VMMドメインを昇格させることができます。

始める前に

管理対象のドメインに読み取り専用VMMドメインを昇格するための手順では、次の前提条件を満たすことを前提にしています。

- セクション VMM ドメイン プロファイルを作成するための前提条件 （30 ページ）の前提条件を満たす
- 読み取り専用 VMM ドメインの作成 （39 ページ）に記載されているとおりに、読み取り専用を構成する
- VMware vCenter の [Networking] タブで、昇格しようとしている読み取り専用 VMM ドメインと全く同じ名前のネットワーク フォルダに VDS が含まれていることを確認します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 アクセスエンティティ プロファイル（AEP）を読み取り専用 VMM ドメインに関連付けます。

a) **[Fabric]** > **[Access Policies]** > **[Policies]** > **[Global]** > **[Attachable Access Entity Profiles]** に移動します。

b) AEP を選択し、完全管理に昇格させる読み取り専用 VMM ドメインに関連付けます。

ステップ 3 VMM ドメインを昇格させます。

a) **[Virtual Networking]** > **[Inventory]** に移動します。

b) **[VMM Domains]** > **[Vmware]** フォルダーを展開します。

c) 昇格する読み取り専用 VMM ドメインを選択します。

d) [Access Mode] の設定を [Read Write Mode] に変更します。

e) ドロップダウンメニューから [VLAN Pool] を選択し、VLAN プールをドメインに関連付けます。

f) [Submit] をクリックして変更を保存します。

ステップ 4 新しい Link Aggregation Group（LAG）ポリシーを作成します。

vCenter バージョン 5.5 以降を使用している場合は、「Cisco APIC GUI を使用した DVS アップリンク ポート用 LAG の作成 （51 ページ）」の説明に従って、ドメインで Enhanced LACP 機能を使用するために LAG ポリシーを作成する必要があります。

それ以外の場合は、このステップを省略できます。

ステップ 5 LAG ポリシーを適切な EPG に関連付けます。

vCenter バージョン 5.5 以降を使用している場合は、「Enhanced LACP ポリシーを持つ VMware vCenter ドメインへのアプリケーション EPG の関連付け（Cisco APIC GUI を使用する方法） （53 ページ）」の説明に従って、Enhanced LACP 機能を使用するために LAG ポリシーを EPG に関連付ける必要があります。

それ以外の場合は、このステップを省略できます。

次のタスク

これで、VMM ドメインに接続したすべての EPG と、設定したすべてのポリシーが、VMware vCenter で VDS にプッシュされます。

NX-OS スタイルの CLI を使用した、読み取り専用 VMM ドメインのプロモート

NX-OS スタイル CLI を使用して、読み取り専用 VMM ドメインをプロモートできます。

始める前に

読み取り専用 VMM ドメインを管理対象のドメインにプロモートするための手順では、次の点を前提条件としています。

- セクション VMM ドメイン プロファイルを作成するための前提条件 （30 ページ）の前提条件を満たす
- 読み取り専用 VMM ドメインの作成 （39 ページ）に記載されているとおりに、読み取り専用を構成する
- VMware vCenter の [Networking] タブで、昇格しようとしている読み取り専用 VMM ドメインと全く同じ名前のネットワーク フォルダに VDS が含まれていることを確認します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに移行します。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 VMM ドメインのアクセス モードを管理型に変更します。

次の例では、交換 *vmmDom1* を以前に読み取り専用として設定した VMM ドメインに置き換えます。

例：

```
apic1(config)# vmware-domain vmmDom1 access-mode readwrite
apic1(config-vmware)# exit
apic1(config)# exit
```

ステップ 3 新しい Link Aggregation Group（LAG）ポリシーを作成します。

vCenter バージョン 5.5 以降を使用している場合は、「NX-OS スタイル CLI を使用した DVS アップリンク ポート用 LAG の作成 （52 ページ）」の説明に従って、ドメインで Enhanced LACP 機能を使用するために LAG ポリシーを作成する必要があります。

それ以外の場合は、このステップを省略できます。

ステップ 4 LAG ポリシーを適切な EPG に関連付けます。

vCenter バージョン 5.5 以降を使用している場合は、「Enhanced LACP ポリシーを持つ VMware vCenter ドメインへのアプリケーション EPG の関連付け（NX-OS スタイル CLI を使用する方法）（54 ページ）」の説明に従って、Enhanced LACP 機能を使用するために LAG ポリシーを EPG に関連付ける必要があります。

それ以外の場合は、このステップを省略できます。

次のタスク

これで、VMM ドメインに接続したすべての EPG と、設定したすべてのポリシーが、VMware vCenter で VDS にプッシュされます。

REST API を使用して読み取り専用 VMM ドメインに昇格させる

REST API を使用して、読み取り専用 VMM ドメインに昇格させることができます。

始める前に

管理対象のドメインに読み取り専用 VMM ドメインを昇格するための手順では、次の前提条件を満たすことを前提にしています。

- セクション VMM ドメイン プロファイルを作成するための前提条件 （30 ページ）の前提条件を満たす
- 読み取り専用 VMM ドメインの作成 （39 ページ）に記載されているとおりに、読み取り専用を構成する
- VMware vCenter の [Networking] タブで、昇格しようとしている読み取り専用 VMM ドメインと全く同じ名前のネットワーク フォルダに VDS が含まれていることを確認します。

手順

ステップ 1 VMM ドメイン名、コントローラおよびユーザ クレデンシャルを設定します。

次の例では、交換 *vmmDom1* を以前に読み取り専用として設定した VMM ドメインに置き換えます。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/.xml

<vmmDomP dn="uni/vmmp-VMware/dom-vmmDom1" accessMode="read-write"
prefEncapMode="unspecified" enfPref="hw">
</vmmDomP>
```

ステップ 2 新しい Link Aggregation Group（LAG）ポリシーを作成します。

vCenter バージョン 5.5 以降を使用している場合は、「REST API を使用した DVS アップリンク ポート用 LAG の作成 （53 ページ）」の説明に従って、ドメインで Enhanced LACP 機能を使用するために LAG ポリシーを作成する必要があります。

それ以外の場合は、このステップを省略できます。

ステップ 3 LAG ポリシーを適切な EPG に関連付けます。

vCenter バージョン 5.5 以降を使用している場合は、「Enhanced LACP ポリシーを持つ VMware vCenter ドメインへのアプリケーション EPG の関連付け（REST API を使用する方法）（55 ページ）」の説明に従って、Enhanced LACP 機能を使用するために LAG ポリシーを EPG に関連付ける必要があります。

それ以外の場合は、このステップを省略できます。

次のタスク

これで、VMM ドメインに接続したすべての EPG と、設定したすべてのポリシーが、VMware vCenter で VDS にプッシュされます。

Enhanced LACP ポリシーのサポート

Cisco Application Policy Infrastructure Controller（APIC）リリース 4.0(1) 以降では、さまざまな分散型仮想スイッチ（DVS）アップリンク ポート グループごとに異なる Link Aggregation Control Protocol（LACP）ポリシーを適用して、アップリンクのロードバランシングを向上させることができます。

Cisco APIC では VMware の Enhanced LACP がサポートされるようになりました。この機能は DVS 5.5 以降で使用できます。以前は、同じ LACP ポリシーをすべての DVS アップリンク ポート グループに適用していました。Cisco APIC リリース 4.0(1) では、Cisco APIC を使用して VMware の Link Aggregation Group（LAG）を管理することができませんでした。

VMware vCenter 仮想マシン マネージャ（VMM）ドメインを Cisco Application Centric Infrastructure Virtual Edge または VMware VDS 用に作成する場合、最大 20 個のさまざまなロードバランシング アルゴリズムから選択することができます。アップリンク ポートグループごとに異なるポリシーを適用します。

8 つの DVS アップリンク ポートグループがあり、少なくとも 2 つのアップリンクを同じポリシーで設定する必要があります。したがって、DVS ごとに最大 4 つの異なる LACP ポリシーを設定できます。Enhanced LACP では、アクティブおよびパッシブの LACP モードのみがサポートされます。

（注） Cisco ACI Virtual Edge VXLAN モードでは、UDP ポートを持つロードバランシング アルゴリズムの使用が必須になります。アルゴリズム「**Source and Destination TCP/UDP Port**」の使用をお勧めします。VLXAN モードでは、トラフィックは常に VTEP 間で FTEP IP に送信されます。そのため、通信は常に 1 ペアの IP アドレス間で行われます。したがって、VXLAN トラフィックでは、UDP ポート番号を使用することがトラフィックを区別する唯一の方法になります。

以降のセクションでは、Cisco APIC GUI、NX-OS スタイル CLI、または REST API を使用して複数の LACP ポリシーを DVS アップリンク用に設定する手順について説明します。

Enhanced LACP の制限事項

Enhanced Link Aggregation Control Protocol（LACP）ポリシーを使用する際は、次の制限事項に留意してください。

- Enhanced LACP へのアップグレード後に以前のバージョンの LACP に戻すことはできません。
- Enhanced LACP の設定を削除せずに、4.0(1) よりも前のバージョンの Cisco Application Policy Infrastructure Controller（APIC）にダウングレードすることはできません。このガイドの手順「ダウングレード前の Enhanced LACP 設定の削除 （56 ページ）」を参照してください。
- Cisco Application Centric Infrastructure Virtual Edge の VXLAN モードのトラフィックでは、常に送信元 IP アドレスが TEP IP アドレスとして使用されます。適切なロード バランシングを確保するため、アルゴリズム「**Source and Destination TCP/UDP Port**」をお勧めします。

Cisco APIC GUI を使用した DVS アップリンク ポート用 LAG の作成

分散型仮想スイッチ（DVS）のアップリンク ポート グループを Link Aggregation Group（LAG）に配置し、特定のロードバランシング アルゴリズムに関連付けることによって、ポート グループのロード バランシングを向上させます。Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してこのタスクを実行することができます。

始める前に

- VMware VDS または Cisco Application Centric Infrastructure Virtual Edge 用に VMware vCenter 仮想マシン マネージャ（VMM）ドメインを作成する必要があります。
- vSwitch ポリシー コンテナが存在しない場合は、1 つ作成します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Virtual Networking]** > **[Inventory]** > **[VMM Domains]** > **[VMware]** > ***[domain]*** に移動します。

ステップ 3 作業ペインで、**[Policy]** > **[VSwitch Policy]** を選択します。

ステップ 4 [Properties] 領域でまだポリシーを選択していない場合は、選択します。

ステップ 5 [Enhanced LAG Policy] 領域で、[+]（プラス記号）アイコンをクリックし、次の手順を実行します。

a) [Name] フィールドに、LAG の名前を入力します。
b) [Mode] ドロップダウン リストで、[LACP Active] または [LACP Passive] を選択します。

c) [Load Balancing Mode] ドロップダウン リストで、ロード バランシング方式を選択します。
d) [Number of Links] セレクターで、LAG に含める DVS アップリンク ポート グループの数を選択します。

   2 ～ 8 個のアップリンク ポート グループを LAG に配置できます。

e) [Update] をクリックし、[Submit] をクリックします。

ステップ 6 ステップ 5 を繰り返して、DVS 用の他の LAG を作成します。

次のタスク

VMware VDS を使用している場合は、エンドポイント グループ（EPG）を、Enhanced LACP ポリシーを持つドメインに関連付けます。Cisco Application Centric Infrastructure Virtual Edge を使用している場合は、内部的に作成した内部および外部ポート グループを Enhanced LACP ポリシーに関連付けてから、ポリシーを持つドメインに EPG を関連付けます。

NX-OS スタイル CLI を使用した DVS アップリンク ポート用 LAG の作成

分散型仮想スイッチ（DVS）のアップリンク ポート グループをリンク集約グループ（LAG）に配置し、特定のロードバランシング アルゴリズムに関連付けることによって、ポート グループのロード バランシングを向上させます。NX-OS スタイル CLI を使用してこのタスクを実行することができます。

始める前に

VMware VDS または Cisco Application Centric Infrastructure Virtual Edge 用に VMware vCenter 仮想マシン マネージャ（VMM）ドメインを作成する必要があります。

手順

Enhanced LACP ポリシーを作成または削除します。

例：

```
apic1(config-vmware)# enhancedlacp  LAG name
apic1(config-vmware-enhancedlacp)# lbmode loadbalancing mode
apic1(config-vmware-enhancedlacp)# mode mode
apic1(config-vmware-enhancedlacp)# numlinks max number of uplinks
apic1(config-vmware)# no enhancedlacp LAG name to delete
```

次のタスク

VMware VDS を使用している場合は、Enhanced LACP ポリシーを設定しているドメインにエンドポイント グループ（EPG）を関連付けます。Cisco Application Centric Infrastructure Virtual Edge を使用している場合は、内部的に作成した内部および外部ポート グループを Enhanced LACP ポリシーに関連付けてから、EPG をポリシーとともにドメインに関連付けます。

REST API を使用した DVS アップリンク ポート用 LAG の作成

分散型仮想スイッチ（DVS）のアップリンク ポート グループをリンク集約グループ（LAG）に配置し、特定のロードバランシング アルゴリズムに関連付けることによって、ポート グループのロード バランシングを向上させます。REST API を使用してこのタスクを実行することができます。

始める前に

VMware VDS または Cisco Application Centric Infrastructure Virtual Edge 用に VMware vCenter 仮想マシン マネージャ（VMM）ドメインを作成する必要があります。

手順

ステップ 1 LAG を作成し、ロードバランシング アルゴリズムに関連付けます。

例：

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininetlacpavs">
        <vmmVSwitchPolicyCont>
            <lacpEnhancedLagPol name="lag2" mode="passive" lbmode="vlan" numLinks="4">
            </lacpEnhancedLagPol>
        </vmmVSwitchPolicyCont>
   </vmmDomP>
</vmmProvP>
</polUni>
```

ステップ 2 手順を繰り返して、DVS 用の他の LAG を作成します。

次のタスク

VMware VDS を使用している場合は、Enhanced LACP ポリシーを設定しているドメインにエンドポイント グループ（EPG）を関連付けます。Cisco Application Centric Infrastructure Virtual Edge を使用している場合は、内部的に作成した内部および外部ポート グループを Enhanced LACP ポリシーに関連付けてから、EPG をポリシーとともにドメインに関連付けます。

Enhanced LACP ポリシーを持つ VMware vCenter ドメインへのアプリケーション EPG の関連付け（Cisco APIC GUI を使用する方法）

LAG とロードバランシング アルゴリズムを持つ VMware vCenter ドメインに、アプリケーション エンドポイント グループ（EPG）を関連付けます。Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してこのタスクを実行することができます。

始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

（注） この手順では、まだアプリケーション EPG を VMware vCenter ドメインに関連付けていないと仮定します。すでに関連付けを済ませている場合は、ドメインの関連付けを編集します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > ***[tenant]*** > **[Application Profiles]** > ***[application_profile]*** > **[Application EPGs]** > ***[EPG]*** > **[Domains(VMs and Bare-Metals)]** に移動します。

ステップ 3 [Domains (VMs and Bare-Metals)] を右クリックし [Add VMM Domain Association] をクリックします。

ステップ 4 [Add VMM Domain Association] ダイアログ ボックスで、次の手順を完了します。

a) [VMM Domain Profile] ドロップダウン リストで、EPG を関連付けるドメインを選択します。

b) [Enhanced Lag Policy] で、EPG に適用するドメイン用に設定したポリシーを選択します。

c) ドメインの関連付けについて残りの適切な値を追加し、[Submit] をクリックします。

ステップ 5 必要に応じて、テナント内の他のアプリケーション EPG についてステップ 2 ～ 4 を繰り返します。

Enhanced LACP ポリシーを持つ VMware vCenter ドメインへのアプリケーション EPG の関連付け（NX-OS スタイル CLI を使用する方法）

LAG とロードバランシング アルゴリズムを持つ VMware vCenter ドメインに、アプリケーション エンドポイント グループ（EPG）を関連付けます。NX-OS スタイル CLI を使用してこのタスクを実行することができます。アプリケーション EPG とドメインとの関連付けを解除することもできます。

始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

手順

ステップ 1 アプリケーション EPG をドメインに関連付けるか、または関連付けを解除します。

例：

```
apic1(config-tenant-app-epg-domain)#  lag-policy name of the LAG policy to associate
apic1(config-tenant-app-epg-domain)# no  lag-policy name of the LAG policy to deassociate
```

ステップ 2 必要に応じて、テナント内の他のアプリケーション EPG についてステップ 1 を繰り返します。

Enhanced LACP ポリシーを持つ VMware vCenter ドメインへのアプリケーション EPG の関連付け（REST API を使用する方法）

LAG とロードバランシング アルゴリズムを持つ VMware vCenter ドメインに、アプリケーション エンドポイント グループ（EPG）を関連付けます。REST API を使用してこのタスクを実行することができます。アプリケーション EPG とドメインとの関連付けを解除することもできます。

始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

手順

ステップ 1 EPG を VMware vCenter ドメインに関連付け、LAG をロードバランシング アルゴリズムに関連付けます。

例：

```
<polUni>
  <fvTenant
    dn="uni/tn-coke"
    name="coke">
    <fvCtx name="cokectx"/>
    <fvAp
      dn="uni/tn-coke/ap-sap"
      name="sap">
      <fvAEPg
        dn="uni/tn-coke/ap-sap/epg-web3"
        name="web3" >
          <fvRsBd tnFvBDName="cokeBD2" />
          <fvRsDomAtt resImedcy="immediate" switchingMode="native"
            tDn="uni/vmmp-VMware/dom-mininetlacpavs">
            <fvAEPgLagPolAtt >
              <fvRsVmmVSwitchEnhancedLagPol
tDn="uni/vmmp-VMware/dom-mininetlacpavs/vswitchpolcont/enlacplagp-lag2"/>
            </fvAEPgLagPolAtt>
          </fvRsDomAtt>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

ステップ 2 必要に応じて、テナント内の他のアプリケーション EPG についてステップ 1 を繰り返します。

ダウングレード前の Enhanced LACP 設定の削除

Cisco Application Policy Infrastructure Controller（APIC）を 4.0(1) よりも前のリリースにダウングレードする場合、事前に Enhanced LACP の設定を削除する必要があります。設定を削除するには、ここで説明している手順を実行します。

手順

ステップ 1 すべての ESXi ホスト上のアップリンクを、リンク集約グループ（LAG）から通常のアップリンクに再割り当てします。

ステップ 2 分散型仮想スイッチ（DVS）に関連付けられているすべての EPG から、LAG との関連付けを削除します。

この手順の実行中はトラフィックの消失が予想されます。

ステップ 3 ポートチャネル設定を、スタティックチャネルまたはMAC固定に変更します。これで、ポートチャネルが起動するとトラフィックが回復します。

ステップ 4 仮想マシン マネージャ（VMM）から LAG 関連の設定をすべて削除します。

ステップ 5 VMware vCenter から、LAG 関連のすべてのポリシーが削除されたことを確認します。

次のタスク

4.0(1) よりも前のリリースの Cisco APIC にダウングレードします。

エンドポイント保持の設定

vCenter ドメインを作成した後は、エンドポイントの保持を設定できます。この機能では、エンドポイントの削除の遅延を有効にして、トラフィックがドロップされる可能性を小さくすることができます。

エンドポイントの保持は、APIC GUI、NX-OS スタイル CLI または REST API を使用して設定できます。詳細については、該当するガイドの次のセクションを参照してください:

- GUI を使用したエンドポイント保持の設定 （56 ページ）
- NX-OS スタイルの CLI を使用したエンドポイント保持の設定 （57 ページ）
- REST API を使用したエンドポイント保持の設定 （57 ページ）

GUI を使用したエンドポイント保持の設定

始める前に

vCenter ドメインを作成している必要があります。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **VM Networking** > **Inventory** を選択します。

ステップ 3 左側のナビゲーション ウィンドウで、**VMware** フォルダを展開し、以前に作成した vCenter ドメインをクリックします。

ステップ 4 中央の **Domain** 作業ウィンドウで、**Policy** および **General** タブが選択されていることを確認します。

ステップ 5 **End Point Retention Time (seconds)** カウンタで、エンドポイントを解除するまで保持する時間の秒数を選択します。

0 ～ 600 秒を選択できます。デフォルトは 0 です。

ステップ 6 [Submit] をクリックします。

NX-OS スタイルの CLI を使用したエンドポイント保持の設定

始める前に

vCenter ドメインを作成している必要があります。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります:

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 分離されたエンドポイントの保持時間を設定します:

遅延時間は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 です。

例：

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

REST API を使用したエンドポイント保持の設定

始める前に

vCenter ドメインを設定済みである必要があります。

手順

デタッチされたエンドポイントの保持時間を設定するには、次の手順に従います:

遅延は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 秒です。

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >

<vmmDomP name="mininetavs" epRetTime=”60”>
</vmmDomP>
</vmmProvP>
```

VDS アップリンク ポート グループの作成

各 VMM ドメインは vSphere Distributed Switch（VDS）として vCenter に表示されます。仮想化管理者は、APIC によって作成された VDS にホストを関連付け、特定の VDS に使用する vmnic を選択します。VDS アップリンクの設定は、APIC コントローラから VMM ドメインに関連付けられている接続エンティティ プロファイル（AEP）の vSwitch 設定を変更することによって行います。AEP は、[Fabric Access Policies] 設定領域の APIC の GUI に含まれています。

（注） ACI と vSphere VMM の統合を使用するときは、リンク集約グループ（LAG）は、APIC によって作成された分散スイッチでインターフェイス チームを作成するための方法としてはサポートされません。APIC は、インターフェイス ポリシー グループや AEP vSwitch ポリシーの設定に基づいて、必要なインターフェイス チーミングの設定をプッシュします。vCenter のインターフェイス チームはサポートされません。つまり、手動で作成する必要があります。

トランク ポート グループの作成

GUI を使用した トランク ポート グループの作成

ここでは、GUI を使用してトランク ポート グループを作成する方法を説明します。

始める前に

- トランク ポート グループはテナントから独立している必要があります。

手順

ステップ 1 APIC GUI にログインします。

ステップ 2 メニュー バーで、[Virtual Networking] を選択します。

ステップ 3 ナビゲーション ウィンドウで、**VMM Domains** > **VMware** > **Domain_name** > **Trunk Port Groups** を選択し、**Create Trunk Port Group** を右クリックします。

ステップ 4 [Create Trunk Port Group] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに EPG 名を入力します。

b) **Promiscuous Mode** ボタンについては、**Disabled** または **Enabled** のいずれかをクリックします。デフォルトは **Disabled** です。

c) **Trunk Portgroup Immediacy** ボタンについては、**Immediate** または **On Demand** のいずれかをクリックします。デフォルトは **On Demand** です。

d) **MAC changes** ボタンについては、**Disabled** または **Enabled** のいずれかをクリックします。デフォルトは [Enabled] です。

e) **Forged transmits** ボタンについては、**Disabled** または **Enabled** のいずれかをクリックします。デフォルトは [Enabled] です。

f) **VLAN Ranges** フィールドで、+ アイコンを選択して、 VLAN の範囲 (vlan-100 vlan-200) を入力します。

（注） VLAN の範囲を指定しない場合、VLAN のリストはドメインの VLAN の名前空間から取られます。

g) [Update] をクリックします。

ステップ 5 [Submit] をクリックします。

NX-OS スタイルの CLI を使用したトランク ポート グループの作成

ここでは、NX-OS スタイルの CLI を使用してトランク ポート グループを作成する方法を説明します。

始める前に

- トランク ポート グループはテナントから独立している必要があります。

手順

ステップ 1 Vmware-domain コンテキストに移動し、次のコマンドを入力します。

例：

```
apic1(config-vmware)# vmware-domain ifav2-vcenter1
```

ステップ 2 トランク ポート グループを作成するには、次のコマンドを入力します。

例：

```
apic1(config-vmware)# trunk-portgroup trunkpg1
```

ステップ 3 VLAN の範囲を入力します。

例：

```
apic1(config-vmware-trunk)# vlan-range 2800-2820, 2830-2850
```

（注） VLAN の範囲を指定しない場合、VLAN リストはドメインの VLAN ネームスペースから取得されます。

ステップ 4 mac の変更はデフォルトで受け入れられます。mac の変更を受け入れないことを選択した場合は、次のコマンドを入力します。

例：

```
apic1(config-vmware-trunk)# no mac-changes accept
```

ステップ 5 forged transmit はデフォルトで受け入れられます。forged transmit を受け入れないことを選択した場合は、次のコマンドを入力します。

例：

```
apic1(config-vmware-trunk)# no forged-transmit accept
```

ステップ 6 無差別モードは、デフォルトでは無効になっています。トランク ポート グループでプロミスキャス モードをイネーブルにする場合は、次のように入力します。

例：

```
apic1(config-vmware-trunk)# allow-promiscuous enable
```

ステップ 7 トランク ポート グループの即時性は、デフォルトでオンデマンドに設定されます。即時即時性をイネーブルにするには、次のコマンドを入力します。

例：

```
apic1(config-vmware-trunk)# immediacy-immediate enable
```

ステップ 8 VMware ドメインを表示します。

例：

```
apic1(config-vmware)# show vmware domain name mininet
Domain Name                          : mininet
Virtual Switch Mode                  : VMware Distributed Switch
Switching Encap Mode                 : vlan
Vlan Domain                          : mininet (2800-2850, 2860-2900)
Physical Interfaces                  :
Number of EPGs                       : 2
Faults by Severity                   : 0, 2, 4, 0
LLDP override                        : no
CDP override                         : no
Channel Mode override                : no

vCenters:
Faults: Grouped by severity (Critical, Major, Minor, Warning)
 vCenter               Type      Datacenter            Status    ESXs   VMs    Faults

 --------------------  --------  --------------------  --------  -----  -----
---------------
 172.22.136.195        vCenter   mininet               online    2      57     0,0,4,0


Trunk Portgroups:
 Name                                          VLANs
```

```
 ---------------------------------------------
---------------------------------------------
 epgtr1                                       280-285

 epgtr2                                       280-285

 epgtr3                                       2800-2850


apic1(config-vmware)# show vmware domain name mininet trunk-portgroup

 Name                           Aggregated EPG
 -----------------------------  ---------------------------------------------
 epgtr1                         test|wwwtestcom3|test830
 epgtr2
 epgtr3                         test|wwwtestcom3|test830
                                test|wwwtestcom3|test833


apic1(config-vmware)# )# show vmware domain name ifav2-vcenter1 trunk-portgroup name
trunkpg1
Name                           Aggregated EPG                  Encap
 -----------------------------  ------------------------------  ------------
 trunkpg1                       LoadBalance|ap1|epg1            vlan-318
                                LoadBalance|ap1|epg2            vlan-317
                                LoadBalance|ap1|failover-epg    vlan-362
                                SH:l3I:common:ASAv-HA:test-     vlan-711
                                rhi|rhiExt|rhiExtInstP
                                SH:l3I:common:ASAv-HA:test-     vlan-712
                                rhi|rhiInt|rhiIntInstP
                                test-dyn-ep|ASA_FWctxctx1bd-    vlan-366
                                inside|int
                                test-dyn-ep|ASA_FWctxctx1bd-    vlan-888
                                inside1|int
                                test-dyn-ep|ASA_FWctxctx1bd-    vlan-365
                                outside|ext
                                test-dyn-ep|ASA_FWctxctx1bd-    vlan-887
                                outside1|ext
                                test-inb|FW-Inbctxtrans-        vlan-886
                                vrfinside-bd|int
                                test-inb|FW-Inbctxtrans-        vlan-882
                                vrfoutside-bd|ext
                                test-inb|inb-ap|inb-epg         vlan-883
                                test-pbr|pbr-ap|pbr-cons-epg    vlan-451
                                test-pbr|pbr-ap|pbr-prov-epg    vlan-452
                                test1|ap1|epg1                  vlan-453
                                test1|ap1|epg2                  vlan-485
                                test1|ap1|epg3                  vlan-454
                                test2-scale|ASA-                vlan-496
                                Trunkctxctx1bd-inside1|int
                                test2-scale|ASA-                vlan-811
                                Trunkctxctx1bd-inside10|int


apic1(config-vmware)# show running-config vmware-domain mininet
# Command: show running-config vmware-domain mininet
# Time: Wed May 25 21:09:13 2016
  vmware-domain mininet
    vlan-domain member mininet type vmware
    vcenter 172.22.136.195 datacenter mininet
      exit
    configure-dvs
      exit
    trunk-portgroup epgtr1 vlan 280-285
```

```
trunk-portgroup epgtr2 vlan 280-285
trunk-portgroup epgtr3 vlan 2800-2850
exit
```

REST API を使用した トランク ポート グループの作成

ここでは、REST API を使用してトランク ポート グループを作成する方法を説明します。

始める前に

- トランク ポート グループはテナントから独立している必要があります。

手順

トランク ポート グループを作成します。

例：

```
<vmmProvP vendor="VMware">
 <vmmDomP name=”DVS1">
  <vmmUsrAggr name="EPGAggr_1">
   <fvnsEncapBlk name="blk0" from="vlan-100” to="vlan-200"/>
  </vmmUsrAggr>
 </vmmDomP>
</vmmProvP>
```

ブレード サーバの使用

Cisco UCS B シリーズ サーバに関するガイドライン

ブレード サーバ システムを VMM 統合の目的で Cisco ACI に統合するとき（たとえば Cisco UCS ブレード サーバまたは他のシスコ以外のブレード サーバを統合するとき）は、次のガイドラインを検討する必要があります。

（注） この例では、Cisco UCS ブレード サーバを統合するためにポート チャネル アクセス ポリシーを設定する方法を示します。同様の手順は、Cisco UCS ブレード サーバ アップリンクをファブリックに接続する方法に応じて、バーチャル ポート チャネルまたは個別のリンク アクセス ポリシーの設定に使用できます。UCS ブレード サーバ アップリンクの APIC で明示的にポート チャネルを設定しない場合、デフォルトの動作は MAC Pinning になります。

- VM エンドポイントの学習は、CDP または LLDP プロトコルに依存します。CDP がサポートされる場合は、ブレード スイッチ経由のリーフ スイッチ ポートからブレード アダプタまで、すべてを有効にする必要があります。
- 管理アドレスのタイプ、長さ、および値（TLV）がブレード スイッチ（CDP プロトコルまたは LLDP プロトコル）上で有効になっていて、サーバとファブリック スイッチに対してアドバタイズされることを確認します。管理 TLV アドレスの設定がブレード スイッチの CDP プロトコルと LLDP プロトコルで一貫している必要があります。
- APIC はファブリック インターコネクトとブレード サーバを管理しません。そのため、CDP やポート チャネル ポリシーなどの UCS 固有のポリシーは、UCS Manager で設定する必要があります。
- APIC の接続可能アクセス エンティティ プロファイルで使用される VLAN プールで定義される VLAN も、UCS で手動で作成し、ファブリックに接続する適切なアップリンクで許可する必要があります。これには、該当する場合は、インフラストラクチャ VLAN を含める必要もあります。詳細については、『*Cisco UCS Manager GUI Configuration Guide*』を参照してください。
- Cisco UCS B シリーズ サーバを使用し、APIC ポリシーを使用している場合は、Link Layer Discovery Protocol（LLDP）はサポートされません。
- Cisco Discovery Protocol （CDP） は、Cisco UCS Manager ではデフォルトで無効にされています。Cisco UCS Manager では、ネットワーク コントロール ポリシーを作成して、CDP を有効にする必要があります。
- UCS サーバ サービス プロファイルでアダプタのファブリック フェールオーバーを有効にしないでください。シスコは、トラフィックのロードバランシングが適切に行われるように、ハイパーバイザが仮想スイッチ レイヤでフェールオーバーを処理できるようにすることを推奨します。

（注） 症状：ブレード スイッチやファブリック インターコネクトのようなアンマネージド ノードの管理 IP の変更は VMware vCenter で更新されますが、VMware vCenter はイベントを APIC に送信しません。

状況：これにより、VMware vCenter と APIC との同期外れが発生します。

回避策：アンマネージド ノードの背後の ESX サーバを管理する VMware vCenter コントローラのインベントリ プルをトリガーする必要があります。

GUI を使用した、ブレード サーバのアクセス ポリシーのセットアップ

始める前に

Cisco APIC と動作するには、Cisco UCS ファブリック インターコネクトは少なくともバージョン 2.2(1c) である必要があります。BIOS、CIMC およびアダプタなどのすべてのコンポーネン

トは、バージョン 2.2(1c) 以降である必要があります。その他の詳細については、『*Cisco UCS Manager CLI Configuration Guide*』を参照してください。

手順

ステップ 1 メニュー バーで、**[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、**Quick Start** クリックします。

ステップ 3 中央ペインで、**Configure an interface, PC, and VPC** をクリックします。

ステップ 4 [Configure Interface, PC, and VPC] ダイアログボックスで、スイッチを選択するために、[+] アイコンをクリックします。

ステップ 5 [Switches] フィールドで、ドロップダウリストから必要なスイッチ ID を選択します。

ステップ 6 スイッチ インターフェイスを設定するために [+] アイコンをクリックします。

ステップ 7 [Interface Type] フィールドで、[VPC] オプション ボタンをクリックします。

ステップ 8 [Interfaces] フィールドに、ブレード サーバに接続された適切なインターフェイスまたはインターフェイス範囲を入力します。

ステップ 9 [Interface Selector Name] フィールドに名前を入力します。

ステップ 10 [CDP Policy] ドロップダウン リストから、デフォルトを選択します。

デフォルトの CDP ポリシーは無効に設定されています。（リーフ スイッチとブレード サーバ間では、CDP を無効にする必要があります。）

ステップ 11 [LLDP Policy] ドロップダウン リストから、デフォルトを選択します。

デフォルトの LLDP ポリシーは、受信および送信状態に対して有効に設定されています。（リーフ スイッチとブレード サーバ間では、LLDP を有効にする必要があります。）

ステップ 12 [LACP Policy] ドロップダウン リストから、[Create LACP Policy] を選択します。

リーフ スイッチとブレード サーバ間では、LACP ポリシーをアクティブにする必要があります。

ステップ 13 [Create LACP Policy] ダイアログボックスで、次のアクションを実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Mode] フィールドで [Active] オプション ボタンをオンにします。
c) 残りのデフォルト値はそのままにして、[Submit] をクリックします。

ステップ 14 [Attached Device Type] フィールドのドロップダウン リストで、[ESX Hosts] を選択します。

ステップ 15 [Domain Name] フィールドに、適宜名前を入力します。

ステップ 16 [VLAN Range] フィールドに、範囲を入力します。

ステップ 17 [vCenter Login Name] フィールドに、ログイン名を入力します。

ステップ 18 [Password] フィールドおよび [Confirm Password] フィールドに、パスワードを入力します。

ステップ 19 **vCenter** フィールドを展開し、**Create vCenter Controller** ダイアログボックスで必要な情報を入力して **OK** をクリックします。

ステップ 20 [vSwitch Policy] フィールドで、次の操作を実行します。

ブレード サーバと ESX ハイパーバイザ間では、CDP を有効にし、LLDP を無効にし、LACP を無効にして、MAC ピニングを設定する必要があります。

a) [MAC Pinning] チェックボックスをオンにします。
b) [CDP] チェックボックスをオンにします。
c) LLDP は無効のままにする必要があるため、[LLDP] チェックボックスはオフのままにします。

ステップ 21 [Save] をクリックして、もう一度 [Save] をクリックします。[Submit] をクリックします。アクセス ポリシーが設定されます。

REST API を使用した、ブレード サーバのアクセス ポリシーのセットアップ

手順

ブレード サーバのアクセス ポリシーをセットアップします。

例：

```
POST: https://<ip or hostname APIC>/api/node/mo/uni.xml

<polUni>
                <infraInfra>
                <!-- Define LLDP CDP and LACP policies -->
                <lldpIfPol name="enable_lldp" adminRxSt="enabled" adminTxSt="enabled"/>
              <lldpIfPol name="disable_lldp" adminRxSt="disabled" adminTxSt="disabled"/>

                <cdpIfPol name="enable_cdp" adminSt="enabled"/>
                <cdpIfPol name="disable_cdp" adminSt="disabled"/>
<lacpLagPol name='enable_lacp' ctrl='15' descr='LACP' maxLinks='16' minLinks='1'
mode='active'/>
                <lacpLagPol name='disable_lacp' mode='mac-pin'/>


        <!-- List of nodes. Contains leaf selectors. Each leaf selector contains list
of node blocks -->
        <infraNodeP name="leaf1">
                <infraLeafS name="leaf1" type="range">
                <infraNodeBlk name="leaf1" from_="1017" to_="1017"/>
            </infraLeafS>
            <infraRsAccPortP tDn="uni/infra/accportprof-portselector"/>
        </infraNodeP>


        <!-- PortP contains port selectors. Each port selector contains list of ports.
It also has association to port group policies -->
        <infraAccPortP name="portselector">
                <infraHPortS name="pselc" type="range">
               <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="39" toPort="40">

                </infraPortBlk>
                <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-leaf1_PC"/>
            </infraHPortS>
```

```
        </infraAccPortP>

        <!-- FuncP contains access bundle group policies -->
        <infraFuncP>
                <!-- Access bundle group has relation to PC, LDP policies and to attach
 entity profile -->
            <infraAccBndlGrp name="leaf1_PC" lagT='link'>
                <infraRsLldpIfPol tnLldpIfPolName="enable_lldp"/>
                <infraRsLacpPol tnLacpLagPolName='enable_lacp'/>
                <infraRsAttEntP tDn="uni/infra/attentp-vmm-FI2"/>
            </infraAccBndlGrp>
        </infraFuncP>

        <!-- AttEntityP has relation to VMM domain -->
        <infraAttEntityP name="vmm-FI2">
                <infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
            <!-- Functions -->
            <infraProvAcc name="provfunc"/>
            <!-- Policy overrides for VMM -->
            <infraAttPolicyGroup name="attpolicy">
                <!-- RELATION TO POLICIES GO HERE -->
                <infraRsOverrideCdpIfPol tnCdpIfPolName="enable_cdp"/>
                <infraRsOverrideLldpIfPol tnLldpIfPolName="disable_lldp"/>
                <infraRsOverrideLacpPol tnLacpLagPolName="disable_lacp"/>
            </infraAttPolicyGroup/>
        </infraAttEntityP>

        </infraInfra>
</polUni>

OUTPUT:
<?xml version="1.0" encoding="UTF-8"?>
<imdata></imdata>
```

Cisco ACI と VMware VMM システム統合のトラブルシューティング

トラブルシューティングの詳細については、次のリンクを参照してください。

- Cisco APIC Troubleshooting Guide
- ACI Troubleshooting Book

追加参考セクション

最小 VMware vCenter 権限を持つカスタム ユーザ アカウント

VMware vCenter の権限を設定することで、DVS/Cisco Application Virtual Switch（AVS）を作成するための VMware API コマンドを Cisco Application Policy Infrastructure Controller（APIC）から VMware vCenter に送信できるようになります。また、権限を設定することで、Cisco APIC

で VMK インターフェイス（AVS）を作成し、ポート グループを公開し、必要なすべてのアラートをリレーできるようになます。

Cisco APIC から vCenter を設定するには、VMware vCenter で次の最小権限セットが許可されるクレデンシャルである必要があります。

- **アラーム**

  Cisco APIC は 2 つのアラームをフォルダに作成します。1 つは DVS 用で、もう 1 つはポートグループ用です。Cisco APIC でEPG またはドメイン ポリシーが削除されると、アラームが発生します。ただし、関連付けられている仮想マシン（VM）があるため、DVS またはポートグループのアラームを削除することはできません。

- **分散スイッチ**
- **dvPort グループ**
- **フォルダ**
- **ネットワーク**

  Cisco APIC は、ポートグループの追加または削除、ホスト/DVS MTU の設定、LLDP/CDP の設定、LACP の設定などの形で、ネットワーク設定を管理します。

- **Host**

  前述の権限に加えて シスコの AVS を使用する場合は、Cisco APIC が DVS を作成するデータセンターでホスト権限が必要になります。

  - **Host.Configuration.Advanced settings**
  - **Host.Local operations.Reconfigure virtual machine**
  - **Host.Configuration.Network configuration**

    これは、仮想レイヤ 4 ～ レイヤ 7 サービスの VM の シスコの AVS と自動配置機能に必要な権限です。シスコの AVS では、APIC が VMK インターフェイスを作成し、OpFlex に使用される 「vtep」 ポートグループに配置します。

- **仮想マシン**

  前述の権限に加えてサービス グラフを使用する場合、サービス グラフに使用される仮想アプライアンスに仮想マシン権限が必要です。

  - **仮想マシン.構成.デバイス設定の変更**
  - **仮想マシン.構成.設定**

サービス VM のオーケストレーション機能を使用してサービス VM を展開する場合は、前述の権限に加えて次の権限を有効にします。

これらの機能の詳細については、*『Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド』*の「Service VM Orchestration」の章を参照してください。

- **データストア**

- 領域の割り当て
- データストアの参照
- 低レベルのファイル操作
- ファイルの削除

- **Host**
  - **Local operations.Delete virtual machine**
  - **Local operations.Reconfigure virtual machine**
- **Resource**
  - **Assign virtual machine to resource pool**
- 仮想マシン
  - **Inventory.Create new**
  - **Inventory.Create from existing**
  - **Inventory.Remove**
  - **Configuration.Add new disk**
  - **Provisioning.Deploy template**
  - **Provisioning.Clone template**
  - **Provisioning.Clone virtual machine**
  - **Provisioning.Customize**
  - **Interaction（all）**

検疫ポート グループ

検疫ポート グループ機能は、ポート グループの割り当てを特定の状況下でクリアする手段を提供します。VMware vCenter で、VMware vSphere Distributed Switch（VDS）を作成すると、検疫ポート グループが VDS にデフォルトで作成されます。検疫ポート グループのデフォルト ポリシーは、すべてのポートをブロックします。

ロード バランサやファイアウォールなどの Layer 4 to Layer 7 仮想サービス アプライアンス統合の一環として Application Policy Infrastructure Controller（APIC） は、サービスのスティッチングのために vCenter でサービス ポート グループを作成し、サービス グラフ レンダリング機能の一部としてこれらのサービス ポート グループ内でサービス仮想マシン（VM）などの仮想アプライアンスの配置を調整します。サービス グラフを削除すると、サービス VM は検疫ポート グループに自動的に移動されます。削除時の検疫ポート グループへの自動転送は、APIC によって調整されたサービス VM についてのみ実行されます。

必要に応じて、検疫ポート グループのポートについて詳細なアクションを実行できます。たとえば、検疫ポート グループから VM ネットワークなどの別のポート グループにすべてのポートを移行できます。

検疫ポート グループの機能は通常のテナント エンドポイント グループ（EPG）および関連付けられたポート グループとテナント VM には適用されません。したがって、テナント EPG を削除すると、関連付けられたポート グループに存在するすべてのテナント VM はそのまま残り、検疫ポート グループに移動されません。テナント ポート グループへのテナント VM の配置は APIC レルムの外部になります。

オンデマンド VMM インベントリの更新

トリガード インベントリによって、仮想マシン マネージャ（VMM）コントローラから Cisco Application Policy Infrastructure Controller（APIC）のインベントリをプルして更新するための手動トリガー オプションが提供されます。これは通常のシナリオでは必要ありません。Cisco APIC でのインベントリの更新操作は、大規模な環境の VMM コントローラでは煩雑になるため、十分な検討のもとに使用する必要があります。

プロセスの再起動、リーダーシップの変更、バックグラウンドでの定期的な 24 時間インベントリ監査が生じた場合、Cisco APIC はインベントリのプルを行って、VMM インベントリと VMM コントローラ インベントリ間の適合性を維持します。負荷が大きくなると、VMware vCenter では適切なインベントリ イベントの通知を提供できなくなります。こうした場合に、トリガード インベントリは、Cisco APIC VMM インベントリと VMware vCenter インベントリ間の適合性の維持に役立ちます。

Cisco APIC は、VMM の設定と VMware vCenter VDS の設定間で同期状態を維持しません。そのため、VMware vCenter から直接 VDS 設定を変更した場合、Cisco APIC は（PVLAN 設定を除く）ユーザ設定の上書きを試みません。

ESXi ホストの物理的な移行

ESXi ホストを物理的に移行するには、この手順のタスクを実行します。

手順

ステップ 1 ホストをメンテナンス モードにするか、別の方法で仮想マシン（VM）のワークロードを退避させます。

ステップ 2 VMware VDS、Cisco Application Centric Infrastructure Virtual Edge、または Cisco Application Virtual Switch から ESXi ホストを削除します。

ステップ 3 新しいリーフ スイッチまたはリーフ スイッチのペアに ESXi ホストを物理的に配線し直します。

ステップ 4 VMware VDS、Cisco Application Centric Infrastructure Virtual Edge、または Cisco Application Virtual Switch に ESXi ホストを再び追加します。

ACI インバンド VLAN に vCenter ハイパーバイザ VMK0 を移行するためのガイドライン

ACI のインバンドポートにバインドされた接続からデフォルトの vCenter ハイパーバイザ VMK0 を移行するためには、以下のガイドラインに従います。ACI ファブリック インフラストラクチャ管理者が必要なポリシーを使用して APIC を設定した後、vCenter 管理者が適切な ACI ポート グループに VMK0 を移行します。

APIC での必要な管理 EPG ポリシーの作成

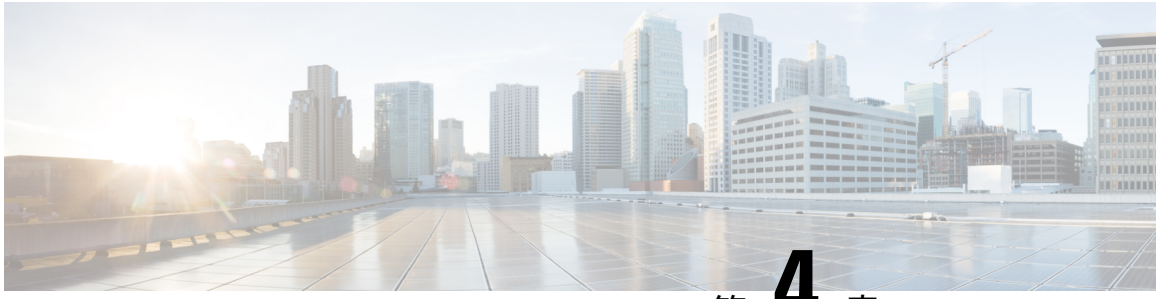
ACI ファブリック インフラストラクチャ管理者として、管理テナントおよび VMM ドメイン ポリシーの作成時に、次のガイドラインを使用します。

- ESX 管理に使用する VLAN を選択します。
- ESX 管理用に選択した VLAN をターゲット VMM ドメインに関連付けられている VLAN プールの範囲（または Encap ブロック）に追加します。この VLAN を追加する範囲は、割り当てモードをスタティック割り当てにする必要があります。
- ACI 管理テナント（mgmt）で管理 EPG を作成します。
- 管理 EPG に関連付けられているブリッジ ドメインがプライベート ネットワーク（inb）にも関連付けられていることを確認します。
- 次のようにターゲット VMM ドメインに管理 EPG を関連付けます。
  - 事前プロビジョニングとして解決の緊急度を使用します。
  - VM ドメイン プロファイル関連付けの [Port Encap] フィールドで管理 VLAN を指定します。

その結果、APIC によって vCenter の下にユーザが指定する VLAN を使用してポート グループが作成されます。APIC は、自動的に VMM ドメインと接続エンティティ プロファイル（AEP）に関連付けられたリーフ スイッチにポリシーをプッシュします。

インバンド ACI VLAN への VMK0 の移行

デフォルトでは、vCenter はハイパーバイザ管理インターフェイスでデフォルト VMK0 を設定します。上述のように作成した ACI ポリシーによって、vCenter 管理者はこのデフォルトの VMK0 を APIC によって作成されたポート グループに移行できるようになります。そうすることで、ハイパーバイザ管理ポートが解放されます。



第 4 章

Cisco ACI でのマイクロセグメンテーション

この章の内容は、次のとおりです。

Cisco ACI でのマイクロセグメンテーション

シスコ 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）を使用したマイクロセグメンテーションを使用すると、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。これらの EPG はさまざまなネットワーク ベースまたは仮想マシン (VM) ベースの属性に基づいています。この章には、Cisco ACI とマイクロセグメンテーションのコンセプトについての情報と、マイクロセグメント (uSeg) EPG の設定の手順が含まれています。

Cisco ACI のマイクロセグメンテーションは、以下のものにアタッチされた仮想エンドポイントをサポートしています:

- Cisco ACI Virtual Edge

（注） Cisco ACI によるマイクロセグメンテーションは、Cisco ACI Virtual Edge が Cisco ACI Virtual Pod（vPod）の一部ではない場合に、Cisco ACI Virtual Edge に対してサポートされます。

- Cisco Application Virtual Switch（AVS）
- Microsoft Hyper-V 仮想スイッチ
- VMware vSphere 分散スイッチ (VDS)

ネットワーク ベースの属性を持つマイクロセグメンテーションは、ベアメタル環境もサポートしています。『*Cisco APIC の基本的なコンフィギュレーション ガイド リリース 3.x*』の、「ネッ

トワークベースの属性を持つマイクロセグメンテーションのベア メタルでの使用」の項を参照してください。

Cisco ACI のマイクロセグメンテーションは、IP ベースの属性を持つ EPG を使用して、物理エンドポイントもサポートします。

（注） Cisco ACI のマイクロセグメンテーションは物理および仮想エンドポイントに合わせて設定することができ、同じ EPG を物理および仮想エンドポイントの両方と共有することができます。

（注） Cisco ACI Virtual Edge、 Cisco AVS、または Microsoft Hyper-V 仮想スイッチを使用する場合には、次の制限に注意してください: MAC ベースの EPG と、仮想エンドポイントの IP 以外の属性を使用する場合には、VDS VMM ドメインの物理エンドポイントまたは仮想エンドポイントに対し、オーバーラップのある IP 属性フィルタを設定しないでください。これに従わないと、Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチでは、マイクロセグメンテーション EPG の分類が上書きされます。

Cisco Application Policy Infrastructure Controller（APIC）は、Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、および Microsoft Hyper-V 仮想スイッチが使用するマイクロセグメンテーションポリシーを管理します。ファブリックはポリシーを適用します。このセクションでは、EPG、テナント、契約、および Cisco ACI ポリシーに関連するその他の主要な概念に精通していることを想定しています。詳細については、『*Cisco Application Centric Infrastructure Fundamentals*』を参照してください。

Cisco APIC リリース 3.2(1) 以降では、マイクロセグメント EPG 同士の間、およびマイクロセグメント EPG と通常の EPG の間の契約で、レイヤ 4 ～ レイヤ 7 のサービス グラフがサポートされます。詳細な情報と設定の手順については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』 を参照してください。Cisco.com から入手できます。

Cisco ACI でのマイクロセグメンテーションの利点

テナント内の仮想マシン（VM）をグループ化してフィルタリングおよび転送ポリシーを適用するには、エンドポイント グループ（EPG）を使用します。Cisco ACI でのマイクロセグメンテーションは、既存のアプリケーション EPG 内のエンドポイントを新しいマイクロセグメント (uSeg) EPG にグループ化し、ネットワークまたは VM ベースの属性をこれらの uSeg EPG に合わせて構成する能力を付与します。これにより、これらの属性をフィルタリングして、より動的なポリシーを適用することができます。Cisco ACI でのマイクロセグメンテーションにより、テナント内の任意のエンドポイントにポリシーを割り当てることもできます。

例：単一 EPG または同じテナント内の複数の EPG における Cisco ACI でのマイクロセグメンテーション

EPG に Web サーバを割り当て、類似したポリシーを適用できるようにすることができます。デフォルトでは、EPG 内のすべてのエンドポイントが自由に相互に通信できます。ただし、こ

の Web EPG に実稼働 Web サーバと開発用 Web サーバが混在する場合は、これらの異なるタイプの Web サーバ間の通信を許可したくない場合があります。Cisco ACI でのマイクロセグメンテーションを使用すると、新しい EPG を作成し、「Prod-xxxx」や「Dev-xxx」などの VM 名属性に基づいてエンドポイントを自動的に割り当てることができます。

例：エンドポイント検疫のためのマイクロセグメンテーション

Web サーバおよびデータベース サーバに個別の EPG があり、それぞれに Windows VM と Linux VM の両方が含まれているとします。Windows のみに影響するウィルスがネットワークに脅威を与えている場合は、たとえば「Windows-Quarantine」という新しい EPG を作成し、VM ベースのオペレーティング システム属性を適用してすべての Windows ベースのエンドポイントをフィルタリングで除去することにより、すべての EPG にわたって Windows VM を分離することができます。この検疫 EPG には、さらに制限された通信ポリシーを適用できます（許可されるプロトコルの制限や、コントラクトを持たないことによるその他の EPG との通信の防御など）。マイクロセグメント EPG は、コントラクトを持っていてもコントラクトを持っていなくてもかまいません。

Cisco ACI を使用するマイクロセグメンテーションの仕組み

Cisco ACI を使用するマイクロセグメンテーションには、Cisco APIC、vCenter または Microsoft System Center Virtual Machine Manager（SCVMM）、およびリーフ スイッチが含まれます。このセクションでは、Cisco ACI Virtual Edge, Cisco AVS、VMware VDS、Microsoft Hyper-V 仮想スイッチを使用するマイクロセグメンテーションのワークフローを説明します。

Cisco APIC

1. ユーザーは、Cisco APIC の Cisco ACI Virtual Edge、Cisco APIC、VMware VDS、Microsoft Hyper-V 仮想スイッチの VMM ドメインを設定します。
2. Cisco APIC は vCenter または SCVMM に接続し、以下を実行します。
    1. Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、または Microsoft Hyper-V 仮想スイッチのインスタンスを作成します。
    2. VM と、関連付けられた VMware vCenter または Microsoft SCVMM からのハイパーバイザのインベントリ情報をプルします。
3. ユーザーはアプリケーション EPG を作成し、vCenter/SCVMM ドメインに関連付けます。各 vCenter/SCVMM ドメインでは、新しいカプセル化がこのアプリケーション EPG に割り当てられます。アプリケーション EPG に属性はありません。

    vCenter/SCVMM 管理者は、マイクロセグメンテーション（uSeg）EPG ではなく、このアプリケーション EPG に仮想エンドポイントを割り当てます。ポート グループとして vCenter/SCVMM に表示されるのはこのアプリケーション EPG です。
4. ユーザは uSeg EPG を作成して VMM ドメインに関連付けます。

    uSeg EPG はポート グループとして vCenter/SCVMM に表示されません。これには特別な機能があります。uSeg EPG には、フィルタ条件と一致する VM ベースの属性があります。

uSeg EPG VM 属性と VM の間に一致がある場合、Cisco APIC はその VM を uSeg EPG に動的に割り当てます。

エンドポイントはアプリケーション EPG から uSeg EPG に転送されます。uSeg EPG が削除されると、エンドポイントは再びアプリケーション EPG に割り当てられます。

Seg EPG を有効にするには、uSeg EPG を VMM ドメインに割り当てる必要があります。uSeg EPG を VMM ドメインに関連付けると、条件はその VMM ドメインにのみ適用されます。VMware VDS がある場合、アプリケーション EPG として同じブリッジ ドメインに uSeg EPG を割り当てる必要があります。

VMware VDS の場合、条件はその VMM ドメインとブリッジ ドメインに適用されます。

リーフ スイッチおよび Cisco ACI Virtual Edge、Cisco AVS、Microsoft Hyper-V 仮想スイッチ

1. 物理リーフ スイッチは Cisco APIC から属性ポリシーを取得します。
2. VM が Cisco ACI Virtual Edge、Cisco AVS、Microsoft Hyper-V 仮想スイッチに接続するとき、OpFlex プロトコルを使用して Cisco ACI Virtual Edge,、Cisco AVS、Microsoft Hyper-V 仮想スイッチは物理リーフ スイッチに VM 接続メッセージを送信します。
3. 物理リーフ スイッチは、テナントに設定された属性ポリシーと VM を照合します。
4. VM が設定された VM 属性と一致する場合、物理リーフ スイッチは、uSeg EPG を対応するカプセル化とともに 、Cisco ACI Virtual Edge、Cisco AVS または Microsoft Hyper-V 仮想スイッチにプッシュします。

   この操作では、vCenter/SCVMM での VM に対する元のポート グループ割り当ては変更されません。

Cisco ACI Virtual Edge、Cisco AVS、Microsoft Hyper-V 仮想スイッチへのパケット転送

1. VM がデータ パケットを送信すると、Cisco ACI Virtual Edge、Cisco AVS または Microsoft Hyper-V 仮想スイッチは、アプリケーション EPG ではなく、uSeg EPG に対応するカプセル化を使用して、それらのパケットにタグ付けします。
2. 物理リーフのハードウェアは、属性ベースのカプセル化された VM パケットを確認して、設定されたポリシーと照合します。

   VM は uSeg EPG に動的に割り当てられ、パケットは、その特定の uSeg EPG に定義されたポリシーに基づいて転送されます。

Cisco ACI でのマイクロセグメンテーションの属性

uSeg EPG に属性を適用すると、属性なしで EPG にポリシーを適用する場合よりも高い精度の転送ポリシーおよびセキュリティ ポリシーを EPG に適用できます。属性はテナント内で固有です。

uSeg EPG に適用可能な属性には、ネットワーク ベースの属性と VM ベースの属性の 2 つのタイプがあります。

ネットワークベースの属性

ネットワーク ベースの属性は、IP（IP アドレス フィルタ）と MAC（MAC アドレス フィルタ）です。uSeg EPG に、1 個以上の MAC アドレスまたは IP アドレスを適用できます。

IP アドレスには単にアドレスまたはサブネットを指定し、MAC アドレスには単にアドレスを指定します。

（注） ネットワークベースの属性を使用し、同じサブネット内のIPアドレスを分類する場合は、MAC ベースのネットワークの属性を使用する必要があります。IP ベースのマイクロセグメンテーション EPG は、同じサブネット内の IP アドレスの分類をサポートしていません。IP ベースのマイクロセグメンテーション EPG は、トラフィックでレイヤ 3 ルーティングが必要な場合にのみサポートされます。トラフィックがブリッジされた場合、マイクロセグメンテーションポリシーは適用できません。

VM ベースの属性

VMware VDS、Cisco AVS、または Cisco ACI Virtual Edge uSeg EPG に複数の VM ベースの属性を適用できます。VM ベースの属性は、VMM ドメイン、オペレーティング システム、ハイパーバイザ ID、データセンタ、VM ID、VM 名、VNic Dn（vNIC ドメイン名）、カスタム属性、タグです。

（注） 属性データセンタは、Microsoft Hyper-V 仮想スイッチのクラウドに対応します。

（注） 属性 VM フォルダは、GUI にも表示されます。この機能はベータ テスト版のみであり、実稼働環境で展開しないでください。

VM ベースの属性を作成する場合、属性に名前を付けるほかに、以下を実行する必要があります。

1. [VM Name] や [Hypervisor Identifier] などの属性タイプを指定します。
2. [Equals] や [Starts With] などの演算子を指定します。
3. 特定の vNIC またはオペレーティング システムの名前などの値を指定します。

カスタム属性およびタグ属性

このカスタム属性およびタグ属性により、他の属性で使用されていない条件に基づいて属性を定義できます。たとえば、vCenter で「セキュリティ ゾーン」というカスタム属性を定義し、「DMZ」や「境界」など値を使用してこの属性を 1 つ以上の VM に関連付けることができます。APIC 管理者は、その VM カスタム属性に基づいて、uSeg EPG を作成できます。

カスタム属性およびタグ属性が、VM の属性として APIC GUI で表示されます。

- カスタム属性
  - VMware vCenter で設定された VM 属性として Cisco ACI Virtual Edge, Cisco AVS、VMware VDS で利用可能です
  - Microsoft SCVMM で設定されているカスタム プロパティとして Microsoft Hyper-V 仮想スイッチで利用可能です
- 属性のタグ：Cisco ACI Virtual Edge 、Cisco AV、VMware VDS のみで利用可能です

Cisco ACI Virtual Edge。Cisco AVS、VMware VDS のカスタム属性またはタグ属性を使用する場合、VMware vSphere Web クライアントにも追加される必要があります。Microsoft Hyper-V の仮想スイッチのカスタム属性を使用する場合は、Microsoft SCVMM のカスタム プロパティとして追加する必要があります。USeg EPG を設定する前に行うことをお勧めします。これにより、Cisco APIC で"マイクロセグメンテーション ポリシーを設定する際、ドロップダウンリストでカスタム属性またはタグ属性を選択することができます。

Cisco APIC で uSeg EPG を設定した後、vSphere Web クライアントまたは SCVMM でカスタム属性またはタグ属性を追加できます。ただし実行する場合、テキストボックスにカスタム属性またはタグ属性の名前を入力可能でも、Cisco APIC のドロップダウンリストでカスタム属性またはタグ属性が表示されません。

vSphere Web クライアントでカスタム属性またはタグ属性を追加する手順については、VMware vSphere ESXi および vCenter Server のマニュアルを参照してください。SCVMM でカスタム属性を追加するための手順については、Microsoft のマニュアルを参照してください。

ただし、カスタム属性と同様に、一部でタグ属性とは異なります。

- タグ属性はホストまたはデータセンタなどの vCenter 内のオブジェクトに適用できます。カスタム属性は VM および ESXi にのみ適用できます。ただし、VM のタグ属性のみがマイクロセグメンテーションに関連します。
- カスタム属性と同様に、タグ属性には名前と値がありません。タグはオブジェクトに適用されるか否かのみラベリングしています。
- カスタム属性を設定するため、演算子や値と同じく、コントローラおよびVMに関する詳細を説明します。タグ属性を設定するには、属性タイプ、カテゴリ、演算子、タグ名を提供します。

（注） VCenter が vSphere 6 以降を実行している場合にのみ、uSeg EPG のタグ属性を定義できます。

テナント内の属性の一意性

属性はテナント内で一意である必要があります。一意性は属性の値によって異なります。

たとえば、ネットワーク ベースの属性については、テナント内の属性 IP アドレスのフィルタを使用できます。その場合、使用されるたびに属性が異なる値の IP アドレスを持つことがで

きます。したがって、アドレス 192.168.33.77 の IP アドレス フィルタ属性は複数回使用できません。ただし、IP アドレスが異なるのであれば（たとえば 192.168.33.78）、IP アドレス フィルタ属性を 2 回使用できます。

uSeg EPG での VM のフィルタリングの方法

複数の属性を持つ uSeg EPG を設定することができます。ただし、VM が所属できるのは 1 つの uSeg EPG だけです。VM がテナントの複数の uSeg EPG に一致する属性を持っている場合には、Cisco APIC はフィルタリング規則に基づいて VM を uSeg EPG に配置します。

属性を定義する方法に応じて、次のような、さまざまなフィルタリング規則を使用できます:

- **任意の属性に一致する**—任意の属性との照合を行えます。Cisco APIC は、VM がどの uSeg に参加する を決定するために、属性間のデフォルトの優先順位に従います。

  詳細については、このガイドの任意の属性に一致した場合の VM フィルタ リング （77 ページ）を参照してください。

- **すべての属性に一致する** —uSeg EPG 用に定義された VM ベースのすべての属性との照合を行えます。複数のネットワーク ベースの属性をすべて照合することはできません。

  詳細については、このガイドのすべての属性に一致するときに VM をフィルタリング （80 ページ）を参照してください。

- **単純な、またはブロック文を使用する** — 複数の属性をフィルタ リングする複数の文を作成することができます。またはブロック構造の、またはネストした文を作成して、正確なフィルタリングを行うルールを作成できます。

  詳細については、このガイドのシンプル ステートメントまたはブロック ステートメントを使用する場合の VM フィルタ （80 ページ）を参照してください。

- **既存のルールをオーバーライドする** — : uSeg EPG を作成する際には、優先順位を設定して、他のルールをオーバーライドできます。任意の属性に一致するか、すべての属性に一致したときの優先順位を設定できます。テナントの EPG 全体での同順位を避けるために、一致の優先順位を設定する必要があります。すべての属性に一致させることにして、一致の優先順位を設定しないこともできます。ただし、そのような場合、同じ属性を持つ uSeg EPG があると、VM が任意の uSeg EPG に一致することになります。

  詳細については、このガイドのEPG 一致の優先順位を使用するときの VM フィルタ リング （81 ページ）を参照してください。

任意の属性に一致した場合の VM フィルタ リング

uSeg EPG のために定義された属性への一致が、デフォルト設定です。

複数の属性があり、任意のものに一致する場合、Cisco APIC は、任意の属性に一致した VM のフィルタリングを行います。VM がテナント内の他の EPG に一致した場合には、属性の優先順位に基づいて uSeg EPG に入れます。

属性の優先順位のルールが適用される方法

次の表に、uSeg EPG に指定できる属性のリストを示します。

属性	タイプ	優先順位	例
MAC	ネットワーク	1- Cisco ACI Virtual Edge/Cisco AVS/Microsoft Hyper-V Virtual Switch 2 - VMware VDS	5c:01:23:ab:cd:ef
IP	ネットワーク	1 - VMware VDS 2- Cisco ACI Virtual Edge/Cisco AVS/Microsoft Hyper-V Virtual Switch	192.168.33.77 10.1.0.0/16
VNic Dn（vNIC ドメイン名）	VM	3	a1:23:45:67:89:0b
VM ID	VM	4	VM-598
VM Name	VM	5	HR_VDI_VM1
ハイパーバイザ ID	VM	6	ホスト - 25
VMM ドメイン	VM	7	AVS-SJC-DC1
データセンター	VM	8	SJC-DC1
カスタム属性	VM	9	SG_DMZ
オペレーティングシステム	VM	10	Windows 2008。
タグ (Cisco ACI Virtual Edge、Cisco AVS、および VMware VDS のみ)	VM	11	Linux

属性	タイプ	優先順位	例
VM のフォルダ (Cisco ACI Virtual Edge、Cisco AVS、および VMware VDS のみ) （注） VM フォルダ属性がベータ試験のためだけの機能です。実稼働環境には展開しないでください。この機能の詳細については Cisco にお問い合わせください。	VM	12	VM_Folder_1

（注） MAC ベースの属性と IP ベースの属性の優先順位は VMware VDS と Cisco ACI Virtual Edge、および Microsoft Hyper-V の仮想スイッチでは異なっています。

優先順位のルールの適用方法についての例

同じ VMと一致する属性を含む 4 つの uSeg EPG があり、それぞれの uSeg EPG は異なるネットワークまたはVM属性を持つものとします。オペレーティング システム、ハイパーバイザ ID、IP、MAC アドレス フィルタです。

Cisco AVS と Microsoft Hyper-V 仮想スイッチのための規則は、MAC、IP、ハイパーバイザ ID、およびオペレーティング システムの順に適用されます。ルールは MAC に適用され、後続のルールはスキップされます。ただし、MAC 属性を持つ uSeg EPG が削除された場合、ルールは IP アドレス フィルタに適用され、後続のルールはスキップされます（他の属性も同様です）。

VMware VDS のルールは、IP アドレス フィルタ、MAC アドレス フィルタ、ハイパーバイザ ID、オペレーティング システムの順序で適用されます。ルールは IP に適用され、後続のルールはスキップされます。ただし、IP 属性を持つ uSeg EPG が削除された場合、ルールは MAC に適用され、後続のルールはスキップされます（他の属性も同様です）。

別のケースとして、同じ VM を含む uSeg EPG があり、それぞれの uSeg EPG には VMM ドメイン、データセンター、カスタム属性および VNic Dn という異なる VM 属性があるとします。

ルールは VNic Dn に適用され、後続のルールはスキップされます。ただし、VNic Dn 属性を持つ uSeg EPG が削除された場合、ルールは VMM ドメインに適用され、後続のルールはスキップされます（他の属性も同様です）。

すべての属性に一致するときに VM をフィルタリング

uSeg EPG では、定義されているすべての VM ベースの属性に一致することを条件としたフィルタ処理を行えます。これは、APIC GUI のドロップダウンリストから **Match All** を選択するか、NX-OS CLI または REST API で一致条件を指定することによって行えます。

すべての属性を一致させる場合、uSeg EPG のために定義されているすべての属性に一致しない限り、Cisco APIC は VM を uSeg EPG に配置しません。

たとえば、ハイパーバイザが存在するハイパーバイザ識別子は host-25 であり、VM 名には「vm」が含まれており、そしてオペレーティング システムは Linux であるという属性を持つ uSeg EPG があるとします。Cisco APIC は、ハイパーバイザが host-25 であり、VM 名に「vm」が含まれており、そしてオペレーティング システム Linux である VM だけを uSeg EPG に配置します。最初の 2 つの属性が一致していても、オペレーティング システムが Microsoft である VM は uSeg EPG に配置しません。

（注） すべての属性の一致では、VMベースの属性のみをサポートします。ネットワーク ベースの属性では、[Match All] を選択することはできません。

すべての VM ベースの属性を一致させる場合には、uSeg EPG を作成する際に、EPG の一致の優先順位を設定しておくとよいでしょう。これにより、どの uSeg EPG が他の uSeg Epg をオーバーライドする必要があるかを決定できます。ただし、EPG の一致の優先順位では、任意の属性またはすべての属性のどちらにするかを設定できます。詳細については、このガイドのEPG 一致の優先順位を使用するときの VM フィルタ リング （81 ページ）を参照してください。

（注） Microsoft Hyper-V の仮想スイッチを使用していて、より新しいリリースから APIC リリース 2.3(1) へダウン グレードする必要がある場合には、まず [Match All] フィルタで設定された uSegs を削除する必要があります。APIC リリース 3.0(1) 以降では、Microsoft での [Match All] フィルタがサポートされています。

シンプル ステートメントまたはブロック ステートメントを使用する場合の VM フィルタ

uSeg EPG の属性を定義するときは、シンプル ステートメントまたはブロック ステートメントで複数の属性を定義できます。単純文とブロック ステートメントを組み合わせて、複雑な属性フィルタを作成することができます。

シンプルなステートメントには単一の属性が含まれています。uSeg EPG ごとに、必要な数だけシンプルなステートメントを作成できます。すべての属性またはすべての属性に一致させることができます。

ブロック ステートメントには、階層内の異なるレベルに複数の属性が含まれています。ブロック ステートメント内には 2 つのサブレベルしか存在できません。ブロック ステートメントの各レベルの任意の属性またはすべての属性を一致させることができます。

（注） ネットワーク ベースの属性をブロック ステートメントのサブレベルに入れることはできません。ただし、ネットワーク ベースの属性がブロック ステートメントの最上位にある場合は、ネットワーク ベースの属性のサブレベルを作成できます。

ブロック ステートメントがある場合、Cisco APIC は最初に最上位で定義された属性をフィルタリングします。次に、次に高いレベルをフィルタリングし、その次に高いレベルをフィルタリングします。

APIC GUI、NX-OS CLI、および REST API でシンプル ステートメントとブロック ステートメントを作成できます。

ブロック ステートメントの使用例

いくつかの VMをuSeg EPG に入れて、Linux をアップデートすることができます。VM は単一のデータセンター内にありますが、更新を 2 つの VMM ドメイン内の VM に限定する必要があります。ブロック ステートメントを使用して、それらの VM のフィルタリングを設定できます。

Linux を実行し、単一のデータセンターにある VM をフィルタリングするので、2 つのシンプル ステートメントを作成します。1 つは Linux の値を持つオペレーティング システム属性用で、もう 1 つは [datacenter3] の値を持つ属性データセンター用です。これらのステートメントでは、Linux を実行し、[datacenter3] に属しているテナント内のすべての VM をキャプチャしたいので、[Match All] を選択します。

ただし、Linux を実行し、[datacenter3] に属している VM では、VMM ドメイン mininet2 または mininet4 にのみ属する VM を取得する必要があります。2 つのシンプル ステートメントのサブレベルとしてブロック ステートメントを作成します。ブロック ステートメントには、2つの属性、1 つは属性 VMM ドメインの値 (mininet 2 の値)、1 つは属性 VMM ドメインの値 (mininet 4 の値) が含まれます。いずれかの VMM ドメインにある VM をキャプチャする必要があるため、ブロック ステートメントに [match any] を選択します。

属性を定義すると、Cisco APIC は最初に Linux を実行し、 [datacenter3] にある VM をフィルタリングします。次に、それらの VM の中から、mininet2 または mininet4 のいずれかに属する VM を検索します。

EPG 一致の優先順位を使用するときの VM フィルタ リング

EPG一致の優先順位を使用すると、VMベースの属性をフィルタリングするときに、uSeg EPG のデフォルト優先順位ルールをオーバーライドすることができます。これは、GUI、NX-OS CLI または REST API で uSeg EPG を作成する時に設定します。

EPG一致の優先順位は、任意の属性またはすべての属性のマッチングを行うときにはオプションです。ただし、すべての属性のマッチングを行い、複数の属性でフィルタリングを行う場

合、優先順位を設定すると、Cisco APIC は uSeg EPG 間の結合を切ることができるようになります。

（注） ネットワーク ベースの属性をフィルタリングする場合は、EPG 一致の優先順位を使用することはできません。これを行うと、エラー メッセージが表示されます。

EPG 一致の優先順位を設定するときには、uSeg EPG に整数値を与えます。数値が大きいほど優先順位が高くなります。優先順位は、ほぼ 43 億 (2^{32}) のレベルに設定できます。デフォルトでは 0 で、優先順位が設定されていないことを示します。

たとえば、それぞれ 1 つだけの属性を持つ 2 つの uSeg EPG があるとします。一方は属性として VM 名を持ち、もう一方はオペレーティング システムを持ちます。ある VM が両方の uSeg EPG と一致する可能性があるとします。デフォルトでは、Cisco APIC はその VM を VM 名属性を持つ uSeg EPG に割り当てます。この属性は、オペレーティング システム属性よりも高い優先順位を持つからです。

ただし、オペレーティング システム属性を持つ uSeg EPG に優先順位 10 を与え、VM 名属性を持つ uSeg EPG に優先順位 7 を与えると、 Cisco APIC は両方の uSeg EPG にマッチした VM をオペレーティング システム属性を持つ uSeg EPG に与えます。

オペレータの優先順位

テナント内で uSeg EPG の属性に基づいてフィルタリング ルールを適用するほかに、Cisco APIC では演算子タイプに基づいて VM ベースの属性内でフィルタリング ルールを適用します。

VM ベースの属性でマイクロセグメントを設定する際、Contains、Ends With、Equals、Starts With の 4 つの演算子のうち 1 つを選択します。各演算子は、特定の属性の文字列または値の一致を指定します。

たとえば、VM 名属性でマイクロセグメントを作成し、「HR_VM」で始まる名前の VM、または名前のどこかに「HR」を含む VM をフィルタリングできます。または、特定の VM に対してマイクロセグメントを設定し、名前「HR_VM_01」をフィルタリングできます。

演算子の優先順位のルールの適用方法

テナント内の特定の VM 属性の演算子により、マイクロセグメントに VM ベース属性を適用する順序が決まります。また、同じ属性および重複する値を共有するマイクロセグメント グループ内での、演算子の優先順位も決定されます。次の表に、Cisco AVS と Microsoft Hyper-V Virtual Switch のデフォルトの演算子の優先順位 Cisco ACI Virtual Edge を示します。

演算子タイプ	優先順位
Equals	1
記載内容	2
Starts With	3

演算子タイプ	優先順位
Ends With	4

優先順位のルールの適用方法についての例

データセンター クラスタで同じテナントの下に VM_01_HR_DEV、VM_01_HR_TEST および VM_01_HR_PROD という 3 つの人事 VM マシンがあります。VM 名属性に基づいて、2 つのマイクロセグメント化された EPG を作成しました。

Criterion	CONTAIN-HR マイクロセグメント	HR-VM-01-PROD マイクロセグメント
属性タイプ。	VM Name	VM Name
演算子タイプ	記載内容	Equals
値	VM_01_HR	VM_01_HR_PROD

演算子タイプ Equals は演算子タイプ Contains よりも優先順位が高いため、値 VM_01_HR の前に値 VM_01_HR_PROD が一致します。したがって、VM 名は両方のマイクロセグメントに当てはまりますが、完全な条件一致であるため、および演算子 Equals は演算子 Contains よりも優先順位が高いため、VM_01_HR_PROD という名前の VM はマイクロセグメント HR-VM-01-PROD に配置されます。他の 2 つの VM は、マイクロセグメント CONTAIN-HR に配置されます。

Cisco ACI でマイクロセグメンテーションを使用するシナリオ

ここでは、ネットワークでマイクロセグメンテーションが役立つ状況の例を示します。

単一アプリケーション EPG 内の VM における Cisco ACI でのマイクロセグメンテーションの使用

Cisco ACI でのマイクロセグメンテーションを使用すると、新しい uSeg EPG を作成して単一アプリケーション EPG の VM を含めることができます。デフォルトでは、アプリケーション EPG 内の各 VM は相互に通信できます。ただし、VMS が強制モードになっていて、uSeg EPG 間にコントラクトがない場合は VM グループ間での通信を防止することができます。

EPG 内の VM 間の通信を制御する EPG 間分離ノブの詳細については、VMware VDS または Microsoft Hyper-V 仮想スイッチの EPG 分離 （97 ページ） を参照してください。

例：同じアプリケーション EPG 内の VM をマイクロセグメント化された EPG に配置

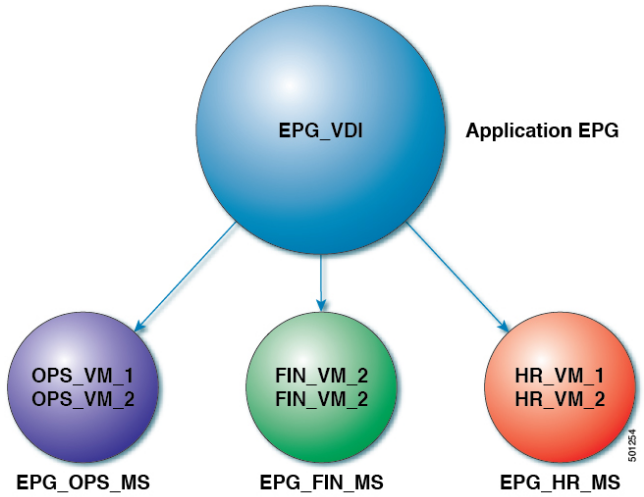
企業が、人事、経理、および業務の各部門に仮想デスクトップインフラストラクチャ（VDI）を導入します。VDI 仮想デスクトップ VM は、EPG_VDI と呼ばれる単一アプリケーション EPG の一部であり、アプリケーション EPG の他の部分とアクセス要件は同じです。

EPG-VDI がインターネット リソースと内部リソースにアクセスできるようにサービス コントラクトが作成されます。ただし、それと同時に、各グループ（人事、経理、および業務）は同じアプリケーション EPG（EPG_VDI）に属していますが、企業は各 VM グループが他のグループにアクセスできないようにする必要があります。

この要件を満たすには、アプリケーション EPG_VDI 内の VM の名前を確認するフィルタを Cisco APIC で作成します。値「HR_VM」を使用してフィルタを作成すると、Cisco APIC はすべての人事 VM 用の uSeg EPG（マイクロセグメント）を作成します。一致する VM を 1 つの EPG にグループ化したいのですが、Cisco APIC はテナント内のすべての EPG 内で一致する値を検索します。したがって、VM を作成する際には、テナント内で一意な名前を選択することを推奨します。

同様に、キーワードとして経理仮想デスクトップ用の「FIN_VMs」および業務仮想デスクトップ用の「OPS_VMs」を使用してフィルタを作成できます。これらの uSeg EPG は、Cisco APIC ポリシー モデル内の新しい EPG として表されます。その後、各 VM グループは同じアプリケーション EPG に属しているのですが、コントラクトとフィルタを適用して VM グループ間のアクセスを制御できます。

図 *6 :* 単一アプリケーション *EPG* の *VM* における *Cisco ACI* でのマイクロセグメンテーション



上の図では、人事、経理、および業務の各グループのすべての仮想デスクトップ VM は、アプリケーション EPG（EPG_VDI）から新しい uSeg EPG（EPG_OPS_MS、EP_FIN_MS、および EPG_HR_MS）に移動しています。各 uSeg EPG は、VM の名前の主要な部分に一致する値を使用した属性タイプ VM 名を持っています。EPG_OPS_MS は値 OPS_VM を持っているため、名前に OPS_VM が含まれるテナント内のすべての VM が EPG_OPS_MS に含まれるようになります。その他の uSeg EPG も対応する値を持っており、一致する名前を持つテナント内の VM が uSeg EPG に移動されます。

別のアプリケーション EPG 内の VM における Cisco ACI でのマイクロセグメンテーションの使用

Cisco ACI でマイクロセグメンテーションを設定して、異なるマイクロセグメンテーション EPG に属する VM を新しい uSeg EPG に配置できます。これを実行することで、異なるアプリケーション EPG に属するものの、特定の特性を共有する VM にポリシーを適用できます。

例：異なるアプリケーション EPG に属する VM を新しい uSeg EPG に配置する

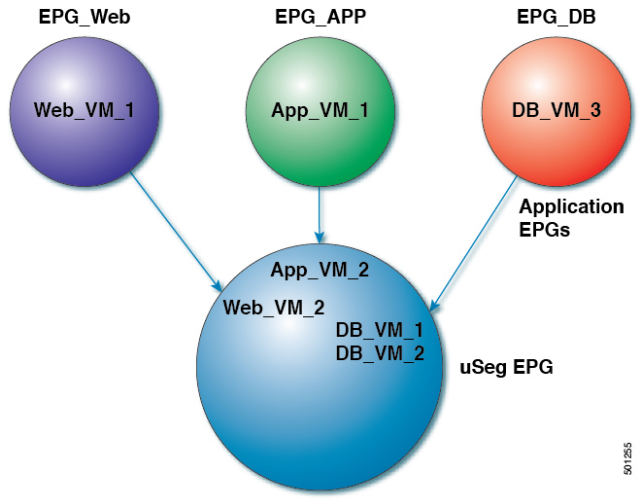
企業で、3 層 Web アプリケーションを導入するとします。アプリケーションは、異なるオペレーティング システムおよび同じオペレーティング システムの異なるバージョンを実行する VM 上に構築されます。たとえば、VM は Linux、Windows 2008 および Windows 2008 R2 を実行する可能性があります。アプリケーションは分散型であり、企業は VM を 3 つの異なる EPG（EPG_Web、EPG_App、EPG_DB）に分割しました。

Windows 2008 オペレーティング システムの脆弱性のため、企業のセキュリティ チームは VM が危険にさらされた場合に備えて、Windows 2008 を実行する VM を隔離することを決定しました。セキュリティ チームはさらに、すべての Windows 2008 VM を Windows 2012 にアップグレードすることにしました。また、すべての EPG ですべての本番 VM をマイクロセグメント化し、これらの VM への外部接続を制限したいと考えています。

この要件を満たすために、Cisco APIC で uSeg EPG を設定できます。属性はオペレーティング システムで、属性の値は Windows 2008 です。

これで、Windows 2008 を実行する VM を隔離し、Windows 2012 にアップグレードできます。アップグレードが完了すると、VM は、Windows 2008 を実行する VM に作成した uSeg EPG の一部ではなくなります。この変更は、Cisco APIC に動的に反映され、それらの仮想マシンは元の EPG に戻ります。

図 *7:* 異なるアプリケーション *EPG* の *Cisco ACI* でのマイクロセグメンテーション



EPG Windows with attribute type **Operating System** and value **Windows**

上の図では、新しい uSeg EPG EPG_Windows は、属性タイプ「オペレーティング システム」と値「Windows」を持ちます。VM App_VM_2、DB_VM_1、DB_VM_2 および Web_VM_2 はオペレーティング システムとして Windows を実行するため、新しい uSeg EPG EPG_Windows に移動されました。ただし、VM App_VM_1、DB_VM_3 および Web_VM_1 は Linux を実行するため、それらのアプリケーション EPG に残ります。

ネットワーク ベースの属性を使用したマイクロセグメンテーションの使用

Cisco APIC を使用して Cisco ACI でのマイクロセグメンテーションを設定し、ネットワークベースの属性、MAC アドレス、または 1 つ以上の IP アドレスを使用した新しい uSeg EPG を作成できます。ネットワーク ベースの属性を使用して Cisco ACI でのマイクロセグメンテーションを設定し、単一のアプリケーション EPG 内の VM またはさまざまな EPG 内の VM を分離できます。

IP ベースの属性の使用

IP ベースのフィルタを使用して、単一 IP アドレス、サブネット、または多様な非連続 IP アドレスを分離できます。単一マイクロセグメントでの複数の IP アドレスの分離は、名前で VM を指定するより便利な場合があります。ファイアウォールの使用と同様に、セキュリティゾーンを作成するための迅速かつ簡単な方法として、IP アドレスに基づいて VM を分離できます。

MAC ベースの属性の使用

MAC ベースのフィルタを使用して、単一 MAC アドレスまたは複数の MAC アドレスを分離できます。ネットワークに不正なトラフィックを送信するサーバがある場合に、これを行うことができます。MAC ベースのフィルタを使用してマイクロセグメントを作成することにより、そのサーバを分離できます。

Cisco ACI でのマイクロセグメンテーションの設定

ここでは、Cisco APIC GUI および NX-OS スタイルの CLI を使用して、Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、または Microsoft Hyper-V 仮想スイッチによるマイクロセグメンテーションを設定する手順を説明します。この手順は、ネットワークの特定のニーズに合わせて調整できます。

（注） VMware vCenter のドメイン プロファイルで VXLAN ロード バランシングが有効の場合、Cisco ACI によるマイクロセグメンテーションはドメインでサポートされません。

Cisco ACI でのマイクロセグメンテーションを設定するための前提条件

Cisco ACI for Cisco ACI Virtual Edge、Cisco AVS、VMware VDS または Microsoft Hyper-V 仮想スイッチでマイクロセグメンテーションを設定する前に、以下の前提条件を満たす必要があります。

- マイクロセグメンテーションのハードウェア要件を満たしていることを確認します:

表 *3:* マイクロセグメンテーションのハードウェア サポート

	Cisco Nexus 9332PQ、9372PX、9372TX、9396PX、9396TX、93120TX、および 93128TX スイッチ	**Cisco Nexus 9372PX-E および 9372TX-E スイッチ**	**Cisco Nexus 93108TC-EX、93180YC-EX、および 93180LC-EX スイッチ**	**Cisco Nexus 93180YC-FX、93108TC-FX、および 9348GC-FXP スイッチ**
Cisco ACI Virtual Edge uSeg (VM、IP、MAC)	○	○	○	○
Microsoft uSeg (VM、IP、MAC)	○	○	○	○
VDS uSeg (VM、IP、MAC)	なし	なし	○	○
ベアメタル (IP-EPG)	なし	○	○	○
ベアメタル (MAC-EPG)	該当なし	○	○	○

（注） Cisco AVS マイクロセグメンテーションがすべてのハードウェアで動作すること。

- uSeg EPG を作成するときに使用するフィルタで使用できる名前を持つ VM がすでに存在している必要があります。

  使用できる名前を持つVMが存在しない場合、手順を進めてuSegEPGを作成し、その後、フィルタで使用できるVM名に変更できます。Cisco APICは、自動的にそれらのVMを新しいuSeg EPGに含めます。

- すでにアプリケーション EPG が存在している必要があります。
- 対応するブリッジ ドメインには、IP サブネットが定義されている必要があります。そうしないと、VM は通信できません。
- 独自の属性、名前、および値が選択済みである必要があります。

  前にシナリオで使用されている属性、名前、および値は、例として提供されているものです。

- コントラクトにEPGを関連付ける場合は、1つ以上の属性を使用してマイクロセグメントを作成する前にコントラクトを作成する必要があります。
- Cisco ACI Virtual Edge、Cisco AVS または VMware VDS があるときに VM カスタム属性を使用する場合は、その属性を VMware vSphere Web クライアントに追加する必要があります。Microsoft Hyper-V 仮想スイッチがあり、VM カスタム属性を使用する必要がある場合には、それを Microsoft SCVMM に追加する必要もあります。

  カスタム属性は、Cisco APIC でマイクロセグメンテーションを設定する前に、VMware vSphere Web クライアントまたは Microsoft SCVMM に追加することを推奨します。これにより、Cisco APIC GUI でマイクロセグメントを設定する際、ドロップダウンリストからカスタム属性を選択できるようになります。

  vSphere Web クライアントでカスタム属性を追加する手順については、VMware vSphere ESXi および vCenter Server のマニュアルを参照してください。SCVMM でカスタム属性を追加するための手順については、Microsoft のマニュアルを参照してください。
- Microsoft Hyper-V 仮想スイッチ ベースのマイクロセグメンテーションでは、次のいずれかが必要です:
  - SCVMM 2012 R2 ビルド 3.2.8145.0 またはそれ以降
  - SCVMM 2016 ビルド 4.0.1662.0 またはそれ以降

  これらのビルドには、「仮想マシン上の vNIC でのダイナミック VLAN の有効化」という機能が含まれています。この機能は Cisco SCVMM エージェントによって自動的に有効になり、ACI でのマイクロセグメンテーションを利用する仮想マシンのライブ マイグレーションを可能にします。詳細については、Microsoft のマニュアルを参照してください:https://support.microsoft.com
- VMware VDS またはベアメタル サーバがある場合は場合に、VRF ポリシーの適用方向が [ingress] になっていることを確認します。そうしないとエラーが発生します。
- VMware VDS がある場合には、ブレードスイッチで PVLAN がセットアップされていることを確認します。また、VLAN の使用率が一貫したものになるように、静的 VLAN が展開されていることを確認します。

Cisco ACI でのマイクロセグメンテーションを設定するためのワークフロー

ここでは、Cisco ACI でのマイクロセグメンテーションを設定するために実行する必要があるタスクの概要を示します。

1	uSeg EPG の作成：新しい uSeg EPG に名前とブリッジ ドメインを指定し、EPG にネットワーク ベースの属性か VM ベースの属性を選択します。 （注） VMware VDS の場合、アプリケーション EPG が使用する新しい uSeg EPG のものと同じブリッジ ドメインを選択する必要があります。そうしないと、VDS uSeg が VM 属性に一致しない、または VM が uSeg EPG に配置されることになります。

2	新しい uSeg EPG を VMM ドメイン プロファイルに関連付けます。アプリケーション EPG で使用されている同じ VMM ドメイン プロファイルと関連付ける必要があります。
3	uSeg EPG の属性を設定します。
4	エンドポイントが アプライアンス EPG から uSeg EPG に移動したことを確認します。

Cisco ACI でのマイクロセグメンテーションの設定 （86 ページ）という項に記載されている手順に従ってください。

GUI を使用して、Cisco ACI とともにマイクロセグメンテーションを設定する

Cisco ACI での Cisco APIC のマイクロセグメンテーションの設定は、異なる複数のアプリケーション EPG または同一の EPG に属する VM を新しい uSeg EPG に配置するために使用できます。タスクは基本的に、Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、および Microsoft Hyper-V 仮想スイッチで同じですが、手順の若干の違いを次に示します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Tenants** を選択し、マイクロセグメントを作成するテナントを選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、テナント フォルダ、**Application Profiles** フォルダ、および ***profile*** フォルダを展開します。

ステップ 4 次のいずれかの操作を実行します。

- Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチを使用している場合には、次の手順をスキップし、ステップ 5 に進みます。
- VMware VDS を使用している場合は、次の手順を実行します。

a) **Application EPGs** フォルダと、アプリケーション EPG のフォルダを展開します。

b) フォルダ **Domains (VMs and Bare-Metals)** を右クリックします。

c) **Add VMM Domain Association** ダイアログボックスで、VMM ドメインを選択してから、**Allow Micro-Segmentation** チェック ボックスをオンにします。

VMware VDS を使用している場合は、必要なすべてのパラメータも設定する必要があります。

d) [Submit] をクリックします。

ステップ 5 テナントのナビゲーション ウィンドウで、**uSeg EPGs** フォルダを右クリックし、**Create Useg EPG** を選択します。

ステップ 6 **Create USeg EPG Step 1 > Identity** ダイアログボックスで、次の手順に従って、VM のグループのための uSeg EPG の作成を開始します:

a) **Name** フィールドに名前を入力します。

新しい uSeg ベースの EPG では、マイクロセグメントであることを示す名前を選択することを推奨します。

b) [intra-EPG isolation] フィールドで **enforced** または **unenforced** を選択します。

enforced を選択した場合は、Cisco ACI によってこの uSeg EPG 内のエンドポイント デバイス間のすべての通信が防止されます。

c) **Bridge Domain** エリアで、ドロップダウン リストからブリッジ ドメインを選択します。

（注） VMware VDS の場合、アプリケーション EPG が使用しているのと同じブリッジ ドメインを選択する必要があります。そうしないと、VM 属性が一致しないため、VDS uSeg は VM を uSeg EPG に入れません。

d) (オプション) **Epg Match Precedence** フィールドで、他の VM ベース属性 uSeg EPG との間での優先順位を設定する整数を選択して、デフォルトのルールをオーバーライドします。

整数の値が大きいほど、優先順位は高くなります。

e) [Next] をクリックします。

ステップ 7 **Create USeg EPG Step 2 > Domains** で、uSeg EPG を VMM ドメインに関連付けるため、次の手順を実行します。

a) ダイアログボックスの右側にある、+ (プラス) のアイコンをクリックします。

b) **Domain Profile** ドロップダウン リストから、プロファイルを選択します。

Cisco ACI Virtual Edge,、Cisco AVS、または VMware VDS がある場合には、VMware ドメインを選択します。Microsoft Hyper-V 仮想スイッチがある場合には、Microsoft ドメインを選択します。

（注） アプリケーション EPG が使用しているのと同じドメインを選択する必要があります。

c) **Deploy Immediacy** ドロップダウンリストでデフォルトの **On Demand** を選択するのは、Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチがある場合です。VMware VDS がある場合には、**Immediate** を選択します。

d) **Resolution Immediacy** ドロップダウンリストでは、デフォルトの **Immediate** のままにします。

e) **Encap Mode** ドロップダウンリストでは、デフォルトの **Auto** にままにします。

f) **Port Encap (or Secondary VLAN for Micro-Seg)** フィールドでは、VMware VDS を使用している場合にはデフォルトの値のままにします。Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチを使用している場合には、デフォルト値のままにします。

g) Cisco ACI Virtual Edge がある場合には、**Switching Mode** ドロップダウンリストで、モードを選択します。

AVE は、Cisco ACI Virtual Edge を通して uSeg EPG を切り替える場合に選択します。VMware VDS を通して uSeg EPG を切り替える場合には **native** を選択します。

h) **Update** をクリックし、**Finish** をクリックします。

ステップ 8 テナントのナビゲーション ページで、作成した uSeg EPG のフォルダを開きます。

ステップ 9 **uSeg Attributes** フォルダをクリックします。
[uSeg Attributes] 作業ウィンドウが表示されます。ここでは、uSeg EPG に入れる VM をフィルタリングするための属性を設定できます。

ステップ 10 (オプション) VM ベースの属性用いてフィルタリングを行う場合には、**uSeg Attributes** 作業ウィンドウで、**Match Any** または **Match All** を選択します。

一致機能を使えば、uSeg EPG の VM をフィルタリングするために、複数の属性を使用できます。デフォルトは **Match Any** です。すべての特徴を一致させる機能がサポートされているのは、VM ベースの属性だけです。『*Cisco ACI Virtualization Guide*』のマイクロセグメントの章に記されている、「いずれかの属性に一致したときに VM のフィルタリング」と「すべての属性に一致したときに VM のフィルタリング」について説明したセクションを参照してください。

ステップ 11 + または **+(** アイコンをクリックして、フィルタリングのステートメントを追加します。

+ アイコンを使えば、1 つの属性に対するフィルタを作成する、シンプルなステートメントを作成できます。複数の属性に対するフィルタリングを行うには、このシンプルなステートメントを順次追加します。**+(** アイコンを使えば、ブロックの、または入れ子になったステートメントを作成できます。これにより、階層構造になった属性を設定して、最上位の属性で最初にフィルタリングし、その後で下位の属性でフィルタリングすることができます。詳細については、このガイドのシンプル ステートメントまたはブロック ステートメントを使用する場合の VM フィルタ （80 ページ）のセクションを参照してください。

ステップ 12 フィルタを設定するには、次のいずれかの一連の手順を実行します。

項目	結果
IP ベースの属性	1. **Select a type...** ドロップダウンリストから、**IP** を選択します。 2. **Use EPG Subnet?** ドロップダウンリストで、**Yes** または **No** を選択します。 **Yes** を選択すると、前に定義したサブネットを IP 属性のフィルタとして使用することができます。 **No** を選択した場合には、**Use EPG Subnet?** ドロップダウンリストの右側にあるフィールドに、VM の IP アドレス、または適切なサブネットマスクを持つサブネットを入力します。 3. （オプション）ステップ a から c を繰り返して、2 番目の IP アドレス フィルタを作成します。 マイクロセグメントに不連続な IP アドレスを含めるために、2 番目の IP アドレス フィルタを作成するのが望ましい場合もあるでしょう。 4. [Submit] をクリックします。
MAC ベースの属性	1. **Select a type...** ドロップダウンリストから、**MAC** を選択します。 2. 右側のフィールドに VM の MAC アドレスを入力します。

項目	結果
	3. [Submit] をクリックします。
VM ベースのカスタム属性	1. **Select a type...** ドロップダウンリストから、**VM - Custom Attribute** を選択します。 2. **Select a type...** ドロップダウンリストの右側にあるフィールドの検索アイコンをクリックします。 3. **Select Custom Attribute** ダイアログボックスで、**Controller** ドロップダウン リストからコントローラを選択します。 4. **VM** ドロップダウンリストから VM を選択します。 5. **Attribute Name** ドロップダウンリストで名前を選択し、**Select** をクリックします。 6. 演算子ドロップダウンリストから、演算子を選択し、ロップダウンリストの右側の フィールドに値を入力します。 7. [Submit] をクリックします。
VM ベースのタグ属性 (Cisco ACI Virtual Edge, Cisco AVS および VMware VDS のみ)	1. **Select a type...** ドロップダウンリストから、**VM - Tag** を選択します。 2. **Category** フィールドの隣にある虫眼鏡アイコンをクリックし、**Select VM Category** ダイアログボックスで、**Category Name** ドロップダウンリストを選択し、**Select** をクリックします。 入力したカテゴリは、VMware vCenter で以前にタグに割り当てたものと同じである必要があります。 3. 演算子のドロップダウンリストから適切な演算子を選択します、 4. 右側のフィールドの隣にある虫眼鏡アイコンをクリックし、**Select VM Tag** ダイアログボックスで、**Tag Name** ドロップダウンリストからタグを選択して、**Select** をクリックします。 5. [Submit] をクリックします。
その他の VM ベースの属性	1. **Select a type...** ドロップダウンリストから、VM の属性を選択します。 2. 演算子のドロップダウンリストから適切な演算子を選択します、 3. 次のいずれかの手順を実行します。 • **Datacenter** VM ベース属性を選択した場合、演算子のドロップダウンリストの右側のフィールドに、データセンターの名前を入力します。 • それ以外の VM ベース属性を選択した場合、演算子のドロップダウンリストの右側にあるフィールドの検索アイコンをクリックし

項目	結果
	て、**Select VM Identifier** ダイアログボックスから属性に適切な値を入力し、**Select** をクリックします。 **4.** [Submit] をクリックします。

ステップ 13 + または +(アイコンをクリックして、uSeg EPG に付加的な属性を追加します。

ステップ 14 ステップ 2 および 13 の操作を繰り返して、追加の uSeg EPG を作成します。

次のタスク

uSeg EPG が正しく作成されたことを確認します。

VM ベースの属性を設定する場合は、次の手順を実行します。

1. Cisco APIC の [Navigation] ペインで、新しいマイクロセグメントをクリックします。
2. 作業ウィンドウで、**Operational** タブをクリックし、**Client End-Points** タブがアクティブであることを確認します。
3. 作業ウィンドウで、アプリケーション EPG から移行する VM が新しい uSeg ベースの EPG のエンドポイントとして表示されていることを確認します。

IP または MAC ベースの属性を設定する場合は、トラフィックが、新しいマイクロセグメントに配置した VM で動作していることを確認します。

NX-OS スタイル CLI を使用した Cisco ACI でのマイクロセグメンテーションの設定

このセクションでは、アプリケーション EPG 内で VM ベースの属性を使用して Cisco ACI for Cisco ACI Virtual Edge、Cisco AVS, VMware VDS、または Microsoft Hyper-V でマイクロセグメンテーションを設定する方法について説明します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 USeg EPG を作成します。

例：

この例は、アプリケーション EPG のためのものです。

（注） 次の例のマイクロセグメンテーションを許可するコマンドが VMware VDS にのみ必要です。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-baseEPG1
apic1(config-tenant-app-epg)# bridge-domain member cli-bd1
apic1(config-tenant-app-epg)# vmware-domain member cli-vmm1 allow-micro-segmentation
```

例：

（オプション）この例の設定は、uSeg EPG の EPG の優先順位と一致します。:

```
apic1(config)# tenant Coke
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# match-precedence 10
```

例：

この例では、属性 VM 名に基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'vm-name contains <cos1>'
```

例：

この例では、IP アドレスに基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'ip equals <FF:FF:FF:FF:FF:FF>'
```

例：

この例では、MAC アドレスに基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'mac equals
<FF-FF-FF-FF-FF-FF>'
```

例：

この例では、演算子 AND を使用してすべての属性を一致させるか、演算子 OR を使用してすべての属性を一致させます。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# attribute-logical-expression 'hv equals host-123 OR
(guest-os equals "Ubuntu Linux (64-bit)" AND domain contains fex)'
```

例：

この例では、属性 VM カスタム属性に基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'custom <Custom Attribute
Name> equals <Custom Attribute value>'
```

ステップ 3 (Cisco ACI Virtual Edge のみ）：uSeg EPG を Cisco ACI Virtual Edge VMM ドメインに接続し、スイッチングおよびカプセル化モードを指定します。

例：

```
vmware-domain member AVE-CISCO
    switching-mode AVE
    encap-mode vxlan
    exit
```

ステップ 4 USeg EPG の作成を確認します。

例：

次の例は、VM 名属性フィルタを持つ uSeg EPG のためのものです。

```
apic1(config-tenant-app-uepg)# show running-config
# Command: show running-config tenant cli-ten1 application cli-a1 epg cli-uepg1 type
micro-segmented # Time: Thu Oct 8 11:54:32 2015
  tenant cli-ten1
    application cli-a1
      epg cli-uepg1 type micro-segmented
        bridge-domain cli-bd1
        attribute-logical-expression 'vm-name contains cos1 force'
        {vmware-domain | microsoft-domain} member cli-vmm1
        exit
     exit
exit
```

REST API を使用した Cisco ACI でのマイクロセグメンテーションの設定

ここでは、REST API を使用して Cisco ACI for Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、または Microsoft vSwitch でマイクロセグメンテーションを設定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 `Https://apic-ip-address/api/node/mo/.xml.`*`apic-ip-address`*`/api/node/mo/.xml.` にポリシーをポストします。

例：

この例では、すべての属性と EPG 一致設定 1 と一致する状態で、「vm」を含む属性 VM 名と「CentOS」および「Linux」の値を含むオペレーティング システム属性を持つ uSeg EPG を設定します。

```
<fvAEPg name="Security" isAttrBasedEPg="yes" pcEnfPref="unenforced" status="">
      <fvRsBd tnFvBDName="BD1" />
      <fvRsDomAtt tDn="uni/vmmp-VMware/dom-mininet”/>
       <fvCrtrn name="default" match="all” prec="1”>
                  <fvVmAttr name="foo" type="vm-name" operator="contains" value="vm"/>
                <fvSCrtrn name="sub-def" match="any”>
                        <fvVmAttr name="foo1" type="guest-os" operator="contains"
value="CentOS"/>
                        <fvVmAttr name="foo2" type="guest-os" operator="contains"
value="Linux"/>
                    </fvSCrtrn>
       </fvCrtrn>
 </fvAEPg>
```

例：

この例では、アプリケーション EPG のマイクロセグメンテーションが有効になっています。

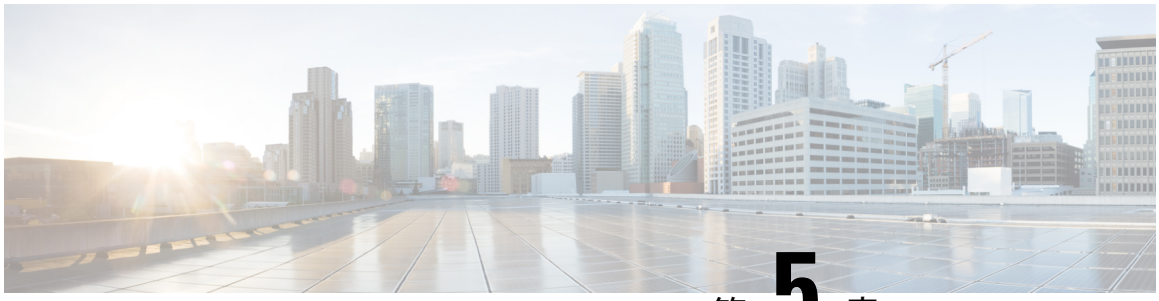
```
<polUni>
  <fvTenant dn="uni/tn-User-T1" name="User-T1">
      <fvAp dn="uni/tn-User-T1/ap-Application-EPG" name="Application-EPG">
          <fvAEPg dn="uni/tn-User-T1/ap-Application-EPG/applicationEPG”
name="applicationEPG” pcEnfPref="enforced” >
               <fvRsBd tnFvBDName="BD1" />
               <fvRsDomAtt tDn="uni/vmmp-VMware/dom-cli-vmm1" classPref="useg”/>
           </fvAEPg>
        </fvAp>
   </fvTenant>
</polUni>
```

上記の例では、文字列 `<fvRsDomAtt tDn="uni/vmmp-VMware/dom-cli-vmm1" classPref="useg”/>` は VMware VDS とのみ関連しており、 Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチとは関連していません。

例：

この例では、uSeg EPG を Cisco ACI Virtual Edge VMM ドメインにアタッチし、スイッチングモードを追加します。

```
<fvRsDomAtt resImedcy="immediate" instrImedcy="immediate" switchingMode="AVE"
encapMode="auto" tDn="uni/vmmp-VMware/dom-AVE-CISCO" primaryEncapInner=""
secondaryEncapInner=""/>
```



第 5 章

EPG 内分離の適用と Cisco ACI

この章の内容は、次のとおりです。

VMware VDS または Microsoft Hyper-V 仮想スイッチの EPG 分離

EPG 内分離は、同じベース EPG または uSeg EPG 内の物理エンドポイント デバイスまたは仮想エンドポイントデバイスが相互に通信しないようにするオプションです。デフォルトでは、同じEPGに含まれるエンドポイントデバイスは互いに通信することができます。しかし、EPG 内のエンドポイント デバイスの別のエンドポイント デバイスからの完全な分離が望ましい状況が存在します。たとえば、同じ EPG 内のエンドポイント VM が複数のテナントに属している場合、またはウイルスが広がるのを防ぐために、EPG内の分離を実行することができます。

Cisco ACI 仮想マシンマネージャ (MM) ドメインは、EPG 内のアイソレーションが有効になっている EPG ごとに、VMware VDS または Microsoft Hyper-V 仮想スイッチに独立した PVLAN ポート グループを作成します。ファブリック管理者がプライマリ カプセル化を指定するか、または EPG と VMM ドメインの関連付け時にファブリックが動的にプライマリ カプセル化を指定します。ファブリック管理者が VLAN pri 値とVLAN-sec 値を静的に選択すると、VMM ドメインによって VLAN-pri と VLAN-sec がドメイン プール内のスタティック ブロックの一部であることが検証されます。

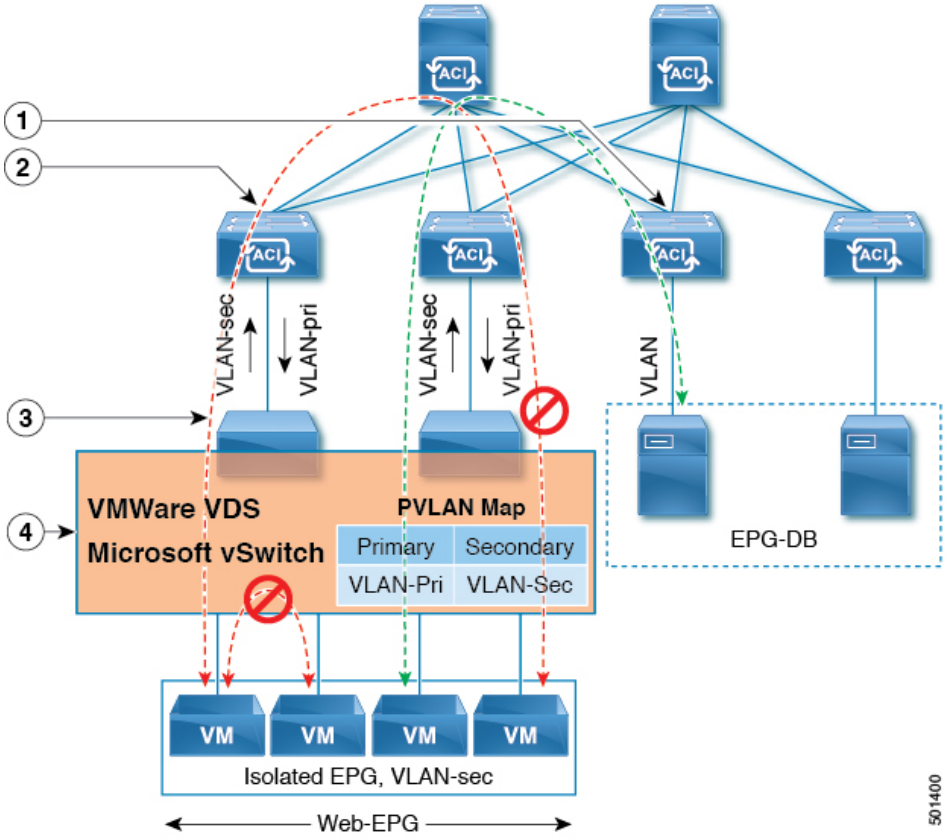
（注） イントラ EPG 隔離が強制されない場合、設定で指定されていても VLAN-pri 値は無視されます。

VMware VDS または Microsoft Hyper-V 仮想スイッチの VLAN-pri/VLAN-sec ペアは、EPG とドメインの関連付け中にVMM ドメインごとに選択されます。EPG内隔離EPGに作成されたポート グループは `PVLAN` に設定されたタイプでタグ付けされた VLAN-sec を使用します。VMware

VDS または Microsoft Hyper-V 仮想スイッチおよびファブリックは、VLAN-pri/VLAN-sec カプセル化をスワップします。

- Cisco ACI ファブリックから VMware VDS または Microsoft Hyper-V 仮想スイッチへの通信は、VLAN-pri を使用します。
- VMware VDS または Microsoft Hyper-V 仮想スイッチから Cisco ACI ファブリックへの通信は、VLAN-sec を使用します。

図 *8 : VMware VDS* または *Microsoft Hyper-V* 仮想スイッチの *EPG* 分離



この図に関する次の詳細に注意してください。

1. EPG-DB は VLAN トラフィックを Cisco ACI リーフ スイッチに送信します。Cisco ACI の出力リーフ スイッチは、プライマリ VLAN (PVLAN) タグでトラフィックをカプセル化し、それを Web-EPG のエンドポイントに転送します。
2. VMware VDS or Microsoft Hyper-V 仮想スイッチは VLAN-sec を使用して ACI リーフ スイッチにトラフィックを送信します。Cisco ACI リーフ スイッチは、Web-EPG 内のすべての VLAN-sec 内トラフィックに分離が適用されているため、すべての EPG 内トラフィックをドロップします。
3. VMware VDS または Microsoft Hyper-V 仮想スイッチ Cisco ACI リーフ へのアップリンク VLAN は、独立型トランク モードです。Cisco ACI リーフスイッチは、VMware VDS また

は Microsoft Hyper-V 仮想スイッチへのダウンリンク トラフィックに VLAN-pri を使用します。

4. PVLAN マップは、VMware VDS または Microsoft Hyper-V 仮想スイッチおよび Cisco ACI リーフ スイッチで設定されます。WEB-EPG からの VM トラフィックは VLAN-sec 内でカプセル化されます。VMware VDS または Microsoft Hyper-V 仮想スイッチは PVLAN タグに従ってローカルの WEB 内 EPG VM トラフィックを拒否します。ESXi 内ホストまたは Microsoft Hyper-V ホストのすべての VM トラフィックは、VLAN-Sec を使用して Cisco ACI リーフに送信されます。

関連項目

Cisco AVS 環境での EPG 内分離の設定については、Cisco AVS の EPG 内分離の適用 （103 ページ）を参照してください。

GUI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Tenants** > ***tenant*** を選択します。

ステップ 3 左側のナビゲーション ウィンドウで、**[アプリケーション プロファイル]** フォルダと適切なアプリケーション プロファイルを展開します。

ステップ 4 **Application EPGs** フォルダを右クリックし、**Create Application EPG** を選択します。

ステップ 5 [Create Application EPG] ダイアログ ボックスで、次の手順を実行します:

a) **Name** フィールドに EPG 名を追加します。

b) [Intra EPG Isolation] 領域で、[Enforced] をクリックします。

c) **Bridge Domain** フィールドで、ドロップダウン リストからブリッジ ドメインを選択します。

d) EPG をベア メタル/物理ドメイン インターフェイスまたは VM ドメインに関連付けます。

- VM ドメインの場合、[Associate to VM Domain Profiles] チェックボックスをオンにします。
- ベア メタルの場合、[Statically Link with Leaves/Paths] チェックボックスをオンにします。

e) [Next] をクリックします。

f) **Associated VM Domain Profiles** エリアで、+ アイコンをクリックします。

g) **Domain Profile** プロファイルのドロップダウン リストから、適切な VMM ドメインを選択します。

スタティックの場合、**Port Encap (or Secondary VLAN for Micro-Seg)** フィールドでセカンダリ VLAN を指定し、**Primary VLAN for Micro-Seg** フィールドで、プライマリ VLAN を指定します。Encap フィールドを空白のままにすると、値が動的に割り当てられます。

（注） スタティックの場合、スタティック VLAN を VLAN プールで使用できる必要があります。

ステップ 6 [Update] をクリックし、[Finish] をクリックします。

NX-OS スタイル CLI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定

手順

ステップ 1 CLI で、EPG 内分離 EPG を作成します。

例：

次の例は VMware VDSの場合です:

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
  tenant Tenant_VMM
    application Web
      epg intraEPGDeny
        bridge-domain member VMM_BD
       vmware-domain member PVLAN encap vlan-2001 primary-encap vlan-2002 push on-demand

        vmware-domain member mininet
          exit
        isolation enforce
        exit
      exit
    exit
apic1(config-tenant-app-epg)#
```

例：

次の例は、Microsoft Hyper-V 仮想スイッチを示します。

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
  tenant Tenant_VMM
    application Web
      epg intraEPGDeny
        bridge-domain member VMM_BD
        microsoft-domain member domain1 encap vlan-2003 primary-encap vlan-2004
        microsoft-domain member domain2
          exit
```

```
        isolation enforce
        exit
      exit
    exit
apic1(config-tenant-app-epg)#
```

ステップ 2 設定を確認します。

例：

```
 show epg StaticEPG detail
Application EPg Data:
Tenant              : Test_Isolation
Application         : PVLAN
AEPg                : StaticEPG
BD                  : VMM_BD
uSeg EPG            : no
Intra EPG Isolation : enforced
Vlan Domains        : VMM
Consumed Contracts  : VMware_vDS-Ext
Provided Contracts  : default,Isolate_EPG
Denied Contracts    :
Qos Class           : unspecified
Tag List            :
VMM Domains:
Domain                 Type       Deployment Immediacy  Resolution Immediacy  State
      Encap       Primary
Encap
 --------------------  ---------  --------------------  --------------------
--------------  ----------  ----------
 DVS1                   VMware     On Demand             immediate             formed
       auto        auto

Static Leaves:
 Node        Encap             Deployment Immediacy  Mode                Modification
Time
----------  ----------------  --------------------  ------------------
------------------------------

Static Paths:
 Node        Interface                       Encap             Modification Time

 ----------  ------------------------------  ----------------
------------------------------
 1018        eth101/1/1                      vlan-100
2016-02-11T18:39:02.337-08:00
 1019        eth1/16                         vlan-101
2016-02-11T18:39:02.337-08:00

Static Endpoints:
 Node        Interface          Encap            End Point MAC      End Point IP Address
          Modification Time
 ----------  ------------------------------  ----------------  ------------------
------------------------------  ------------------------------

Dynamic Endpoints:
Encap: (P):Primary VLAN, (S):Secondary VLAN
 Node        Interface            Encap             End Point MAC      End Point IP
Address         Modification Time
 ----------  ------------------------------  ----------------  ------------------
------------------------------  ------------------------------
1017        eth1/3               vlan-943(P)       00:50:56:B3:64:C4  ---
         2016-02-17T18:35:32.224-08:00
```

```
vlan-944(S)
```

REST API を使用した VMware VDS または Microsoft Hyper-V バーチャル スイッチの EPG 内の分離の設定

手順

ステップ 1 XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。

例：

```
POST https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml
```

ステップ 2 VMware VDS または Microsoft Hyper-V 仮想スイッチデプロイメントの場合は、POST メッセージの本文に次の XML 構造のいずれかを含めます。

例：

次の例は、VMware VDS の場合です。

```
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
          <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
          <fvRsBd tnFvBDName="bd" />
          <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
          <fvRsDomAtt encap="vlan-2001" instrImedcy="lazy" primaryEncap="vlan-2002"
resImedcy="immediate" tDn="uni/vmmp-VMware/dom-DVS1”>
    </fvAEPg>
 </fvAp>
</fvTenant>
```

例：

次の例は、Microsoft Hyper-V の仮想スイッチの場合です。

```
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
          <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
          <fvRsBd tnFvBDName="bd" />
         <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
       <fvRsDomAtt tDn="uni/vmmp-Microsoft/dom-domain1”>
 <fvRsDomAtt encap="vlan-2004" instrImedcy="lazy" primaryEncap="vlan-2003"
 resImedcy="immediate" tDn="uni/vmmp-Microsoft/dom-domain2”>
   </fvAEPg>
 </fvAp>
</fvTenant>
```

Cisco AVS の EPG 内分離の適用

デフォルトでは、EPGに属するエンドポイントは契約が設定されていなくても相互に通信できます。ただし、相互に、EPG 内のエンドポイントを特定できます。EPG 内でエンドポイント分離を適用することで、ウィルスやその他の問題がある VM が EPG 内の他の VM に影響を与えないようにすることができる場合もあります。

アプリケーション内のすべてのエンドポイントに分離を設定することも、いずれにも設定しないこともできます。一部のエンドポイントに分離を設定し、他のエンドポイントに設定しない方法は使用できません。

EPG 内のエンドポイントを分離しても、エンドポイントが別の EPG 内のエンドポイントと通信できるようにするコントラクトには影響しません。

EPG が VLAN モードの Cisco AVS ドメインと関連付けられている場合は、EPG 内のエンドポイントの分離によって障害が発生します。

（注） 内部 EPG で、Cisco AVS microsegment（uSeg）EPG の分離は現在サポートされていません。2 個の EPG 間に存在するすべてのコントラクトに関係なく、内部 EPG 分離いずれかが適用された場合、別の uSeg Epg 内に存在する 2 つのエンドポイント間の通信が可能です。

GUI を使用した Cisco AVS の EPG 内分離の設定

この手順に従って、EPG のエンドポイントが相互に分離されている EPG を作成します。

EPG が使用するポートは VM マネージャ（VMM）のいずれかに属している必要があります。

（注） この手順は、EPG の作成時に EPG 内のエンドポイントを分離することを前提としています。既存の EPG 内のエンドポイントを分離するには、Cisco APIC 内の EPG を選択し、[Properties] ペインの [Intra EPG Isolation] 領域で [Enforced] を選択して [SUBMIT] をクリックします。

始める前に

Cisco AVS が VXLAN モードであることを確認します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 [Tenants] を選択してテナントのフォルダを展開し、[Application Profiles] フォルダを展開します。

ステップ 3 アプリケーション プロファイルを右クリックし、[Create Application EPG] を選択します。

ステップ 4 [Create Application EPG] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに EPG 名を入力します。
b) [Intra EPG Isolation] 領域で、[Enforced] をクリックします。
c) [Bridge Domain] ドロップダウン リストから、ブリッジ ドメインを選択します。
d) [Associate to VM Domain Profiles] チェックボックスをオンにします。
e) [Next] をクリックします。
f) [Associate VM Domain Profiles] 領域で [+] アイコンをクリックし、[Domain Profile] ドロップダウン リストから目的の VMM ドメインを選択します。
g) [Update] をクリックし、[FINISH] をクリックします。

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの「Cisco AVS の分離エンドポイントについて表示する統計情報の選択」の項と「Cisco AV で分離されたエンドポイントの統計情報の表示」の項を参照してください。

NX-OS スタイルの CLI を使用した Cisco AVS の EPG 内分離の設定

始める前に

Cisco AVS が VXLAN モードであることを確認します。

手順

CLI で、EPG 内分離 EPG を作成します。

例：

```
# Command: show running-config
tenant TENANT1
  application APP1
    epg EPG1
      bridge-domain member VMM_BD
      vmware-domain member VMMDOM1
      isolation enforce <---- This enables EPG into isolation mode.
      exit
   exit
exit
```

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの「Cisco AVS の分離エンドポイントについて表示する統計情報の選択」の項と「Cisco AV で分離されたエンドポイントの統計情報の表示」の項を参照してください。

REST API を使用した Cisco AVS の EPG 内分離の設定

始める前に

Cisco AVS が VXLAN モードであることを確認します。

手順

ステップ 1 XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。

例：

```
   POST
https://192.0.20.123/api/mo/uni/tn-ExampleCorp.xml
```

ステップ 2 VMM の導入では、POST メッセージの本文に次の例に示す XML 構造を含めます。

例：

```
Example:
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd" />
      <fvRsDomAtt encap="vlan-2001" tDn="uni/vmmp-VMware/dom-DVS1”>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの「Cisco AVS の分離エンドポイントについて表示する統計情報の選択」の項と「Cisco AV で分離されたエンドポイントの統計情報の表示」の項を参照してください。

Cisco AVS の分離エンドポイントについて表示する統計情報の選択

Cisco AVS で EPG 内分離を設定した場合、拒否された接続数、受信パケット数、送信済みマルチキャストパケット数などのエンドポイントの統計情報を表示する前に、それらを選択する必要があります。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > ***[tenant]*** の順に選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、**[Application Profiles]** > ***[profile]*** > **[Application EPGs]** の順に選択し、エンドポイントの統計情報を含む EPG を選択します。

ステップ 4 EPG の [Properties] 作業ペインで、[Operational] タブをクリックして EPG 内のエンドポイントを表示します。

ステップ 5 エンドポイントをダブルクリックします。

ステップ 6 エンドポイントの [Properties] ダイアログボックスで、[Stats] タブをクリックし、チェック アイコンをクリックします。

ステップ 7 [Select Stats] ダイアログボックスの [Available] ペインで、エンドポイントについて表示する統計情報を選択し、右向き矢印を使用してそれらの情報を [Selected] ペインに移動します。

ステップ 8 [Submit] をクリックします。

Cisco AV で分離されたエンドポイントの統計情報の表示

Cisco AVS での EPG間分離を設定している場合は、エンドポイントの統計情報をいったん選択すると、それらの情報が表示されます。

始める前に

分離エンドポイントについて表示する統計情報を選択しておく必要があります。手順については、このガイドの「Cisco AVS の分離エンドポイントについて表示する統計情報の選択」を参照してください。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > ***[tenant]*** の順に選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、**[Application Profiles]** > ***[profile]*** > **[Application EPGs]** の順に選択し、エンドポイントの統計情報を含む EPG を選択します。

ステップ 4 EPG の **Properties** 作業ウィンドウで、**Stats** タブをクリックして、EPG の統計情報を表示します

中央のウィンドウに、先ほど選択した統計情報を表示します。作業ウィンドウの右上で、テーブル ビュー アイコンやチャート ビュー アイコンをクリックして、ビューを変更できます。

Cisco ACI Virtual Edge での EPG 内分離の適用

デフォルトでは、EPGに属するエンドポイントは契約が設定されていなくても相互に通信できます。ただし、EPG 内のエンドポイントを相互に分離することもできます。たとえば、EPG

内でウイルスや他の問題を持つ VM が EPG の他の VM に影響を及ぼすことがないように、エンドポイント分離を適用するのが望ましい場合があります。

アプリケーション EPG 内のすべてのエンドポイントに分離を設定するか、どれにも設定しないことができます。一部のエンドポイントに分離を設定し、他のエンドポイントには設定しないことはできません。

EPG 内のエンドポイントを分離しても、エンドポイントが別の EPG 内のエンドポイントと通信できるようにする契約には影響しません。

（注） VLAN モードで Cisco ACI Virtual Edge ドメインと関連付けられている EPG での EPG内分離の適用はサポートされていません。このような EPG で EPG 内の分離を適用しようとすると、エラーがトリガーされます。

（注） Cisco ACI Virtual Edge マイクロセグメント (uSeg) EPG で EPG 内分離を使用することは現在のところサポートされていません。

（注） VXLAN カプセル化を使用し、EPG 内分離が適用されている Cisco ACI Virtual Edge EPG では、プロキシ ARP はサポートされていません従って、Cisco ACI Virtual Edge EPG 間で契約が設定されていても、EPG 内分離された EPG 間でサブネット間通信を行うことはできません。(VXLAN)。

GUI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

この手順に従って、EPG のエンドポイントが相互に分離されている EPG を作成します。

EPG が使用するポートは VM マネージャ（VMM）のいずれかに属している必要があります。

（注） この手順は、EPG の作成時に EPG 内のエンドポイントを分離することを前提としています。既存の EPG 内のエンドポイントを分離するには、Cisco APIC 内の EPG を選択し、[Properties] ペインの [Intra EPG Isolation] 領域で [Enforced] を選択して [SUBMIT] をクリックします。

始める前に

VXLAN 関連の設定が Cisco ACI Virtual Edge VMM ドメインに存在すること、特に Cisco ACI Virtual Edge ファブリック全体のマルチキャスト アドレスとマルチキャスト アドレスのプール (EPG ごとに 1 つ) が存在することを確認します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 [Tenants] を選択してテナントのフォルダを展開し、[Application Profiles] フォルダを展開します。

ステップ 3 アプリケーション プロファイルを右クリックし、[Create Application EPG] を選択します。

ステップ 4 [Create Application EPG] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドに EPG 名を入力します。

b) [Intra EPG Isolation] 領域で、[Enforced] をクリックします。

c) [Bridge Domain] ドロップダウン リストから、ブリッジ ドメインを選択します。

d) [Associate to VM Domain Profiles] チェックボックスをオンにします。

e) [Next] をクリックします。

f) **Associate VM Domain Profiles** エリアで、次の手順に従います:

- + (プラス) アイコンをクリックし、**Domain Profile** ドロップダウンリストから、対象とする Cisco ACI Virtual Edge VMM ドメインを選択します。
- **Switching Mode** ドロップダウンリストリストから、**AVE** を選択します。
- **Encap Mode** ドロップダウンリストから **VXLAN** または **Auto** を選択します。

  Auto を選択したら、Cisco ACI Virtual Edge VMM ドメインのカプセル化モードが VXLAN になっていることを確認します。
- (オプション) セットアップに適した他の設定オプションを選択します。

g) [Update] をクリックし、[Finish] をクリックします。

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （110 ページ） と [Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する （111 ページ） を参照してください。

NX-OS スタイルの CLI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

始める前に

Cisco ACI Virtual Edge VMM ドメイン、特に Cisco ACI Virtual Edge ファブリック全体のマルチキャスト アドレスと (EPG ごとに 1 つの) マルチキャスト アドレスのプールに、VXLAN に関連する設定に存在するかどうかを確認します。

手順

CLI で、EPG 内分離 EPG を作成します。

例：

```
# Command: show running-config tenant Tenant2 application AP-1 epg EPG-61
  tenant Tenant2
    application AP-1
      epg EPG-61
        bridge-domain member BD-61
        vmware-domain member D-AVE-SITE-2-3
          switching-mode AVE
          encap-mode vxlan
          exit
        isolation enforce            # This enables EPG into isolation mode.
        exit
      exit
    exit
```

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （110 ページ） と [Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する （111 ページ） を参照してください。

REST API を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

始める前に

VXLAN に関連する設定に存在するかどうかを確認します Cisco ACI Virtual Edge VMM ドメイン、特に、 Cisco ACI Virtual Edge ファブリック全体のマルチキャスト アドレスと (EPG ごとに 1 つ) のマルチキャスト アドレスのプール。

手順

ステップ 1 XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。

例：

```
   POST
https://10.197.139.36/api/mo/uni/tn-Tenant2.xml
```

ステップ 2 VMM の導入では、POST メッセージの本文に次の例に示す XML 構造を含めます。

例：

```
<fvTenant name="Tenant2" >
  <fvAp name="AP-1">
```

```
    <fvAEPg name="EPG-61" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <!-- pcEnfPref="unenforced" DISABLES ISOLATION-->
        <fvRsBd tnFvBDName="BD-61" />
        <fvRsDomAtt switchingMode="AVE" encapMode="vxlan" resImedcy="immediate"
tDn="uni/vmmp-VMware/dom-D-AVE-SITE-1-XXIII" >
        </fvRsDomAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （110 ページ） と [Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する （111 ページ） を参照してください。

[Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する

Cisco ACI Virtual Edge で EPG 内分離を設定した場合、拒否された接続数、受信パケット数、送信済みマルチキャストパケット数などのエンドポイントの統計情報を表示する前に、それらを選択する必要があります。その後、統計情報を表示できます。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > ***[tenant]*** の順に選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、**Application Profiles**、***profile***、および **Application EPGs** フォルダを展開し、表示するエンドポイント統計情報を含む EPG を選択します。

ステップ 4 EPG の [Properties] 作業ペインで、[Operational] タブをクリックして EPG 内のエンドポイントを表示します。

ステップ 5 エンドポイントをダブルクリックします。

ステップ 6 エンドポイントの [Properties] ダイアログボックスで、[Stats] タブをクリックし、チェック アイコンをクリックします。

ステップ 7 **Select Stats** ダイアログボックスの **Available** ペインで、エンドポイントについて表示する統計情報を選択し、右向き矢印を使用してそれらの情報を **Selected** ペインに移動します。

ステップ 8 [Submit] をクリックします。

[Virtual Networking] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する

Cisco ACI Virtual Edge で EPG 内分離を設定した場合、拒否された接続数、受信パケット数、送信済みマルチキャストパケット数などのエンドポイントの統計情報を表示する前に、それらを選択する必要があります。その後、統計情報を表示できます。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM domain*** > **Controllers** > ***controller instance name*** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)*** > を選択します。

ステップ 3 [Stats] タブをクリックします。

ステップ 4 チェック マークが付いたタブをクリックします。

ステップ 5 **Select Stats** ダイアログボックスで、表示する統計情報を **Available**ペインでクリックし、右向き矢印をクリックして、それらを **Selected** ペインに移動します。

ステップ 6 (オプション)サンプリング間隔を選択します。

ステップ 7 [Submit] をクリックします。

[Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する

Cisco ACI Virtual Edge で EPG 内分離を設定していた場合には、エンドポイントの統計情報を選択すると、確認することができるようになります。

始める前に

分離エンドポイントについて表示する統計情報を選択しておく必要があります。手順については、このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （110 ページ） を参照してください。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > ***[tenant]*** の順に選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、**Application Profiles**、***profile***、および **Application EPGs** フォルダを展開し、表示の必要な統計情報があるエンドポイントを含んでいる EPG を選択します。

ステップ 4 EPG の [Properties] 作業ペインで、[Operational] タブをクリックして EPG 内のエンドポイントを表示します。

ステップ 5 統計情報を表示するエンドポイントをダブルクリックします。

ステップ 6 エンドポイントの **Properties** 作業ウィンドウで、**Stats** タブをクリックします。

作業ウィンドウに、先ほど選択した統計情報が表示されます。作業ウィンドウの左上で、テーブル ビュー アイコンやチャート ビュー アイコンをクリックして、ビューを変更できます。

[Virtual Networking] タブで Cisco ACI Virtual Edge の分離エンドポイント統計情報を表示する

Cisco ACI Virtual Edge で EPG 内分離を設定していた場合には、エンドポイントの統計情報を選択すると、確認することができるようになります。

始める前に

分離エンドポイントについて表示する統計情報を選択しておく必要があります。手順については、このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （110 ページ） を参照してください。

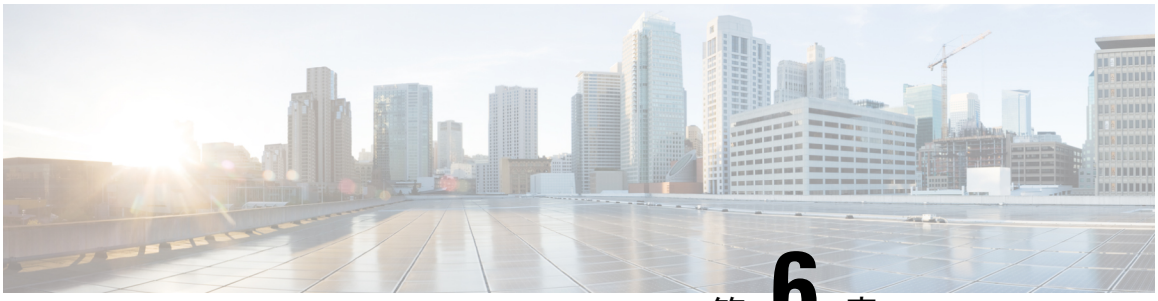
手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM name*** > **Controllers** > **controller instance name** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)*** を選択します。

ステップ 3 [Stats] タブをクリックします。

中央のウィンドウに、先ほど選択した統計情報を表示します。作業ウィンドウの左上で、テーブル ビュー アイコンやチャート ビュー アイコンをクリックして、ビューを変更できます。



第 6 章

Cisco ACI と Cisco ACI vPod

Cisco ACI と Cisco ACI vPod

Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) は、ベアメタル クラウド環境やその他のリモート ロケーションに事実上 Cisco ACI ファブリックを拡張できるようにする、ソフトウェアのみのソリューションです。これは、Cisco APIC リリース 4.0(2) 以降で一般に利用可能です。

Cisco ACI vPod は、ESXi ハイパーバイザを実行できるサーバが少なくとも 2 台存在する任意の場所に展開できます。これにより、物理リーフがない場所で Cisco ACI Virtual Edge を使用できるようになります。

Cisco ACI vPod とそのコンポーネントである仮想スパイン（vSpine）のペアと仮想リーフ（vLeaf）のペア、および Cisco ACI Virtual Edge は、ESXi で実行されます。VSpine と vLeaf はコントロール プレーンの管理を処理し、Cisco ACI Virtual Edge はパケットの転送、ポリシーの適用、およびすべてのデータ プレーンの管理を処理します。

Cisco ACI vPod は、VMware vCenter Server により定義されるデータセンターを管理します。リモート ロケーションの Cisco ACI vPod ごとに Cisco ACI Virtual Edge のインスタンスを最大 8 個使用できます。Cisco APIC を使用して、仮想データセンターで Cisco ACI vPod のノードを管理し、Cisco ACI ポリシーを適用できます。

Cisco ACI vPod は、物理ポッド、オンプレミス ポッド、またはマルチポッドとポッド間ネットワーク経由で通信します。物理ポッドまたはマルチポッド、ポッド間ネットワーク（IPN）接続、および Cisco ACI vPod の設定は、Cisco APIC で行うことができます。 Cisco ACI vPod コンポーネント仮想マシン（VM）の展開には、Cisco ACI vCenter プラグイン、Python スクリプト、または PowerCLI を使用できます。

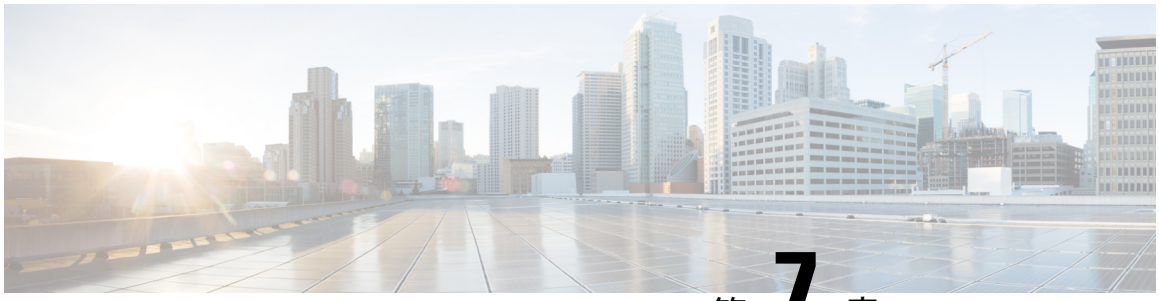
Cisco ACI vPod は、『*VMware Hardware Compatibility Guide*』に記載されているすべてのサーバ ハードウェアと互換性があります。

Cisco ACI vPod に関する情報は、Cisco.com から入手できる次のドキュメントで確認できます。

• *Cisco ACI Virtual Pod* リリース ノート

Cisco ACI と Cisco ACI vPod

- *Cisco ACI Virtual Pod インストール ガイド*
- *Cisco ACI vPod クイック スタート ガイド*



第 7 章

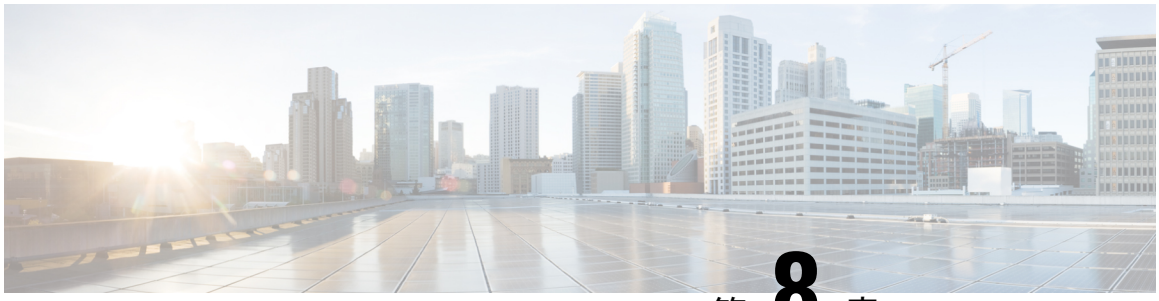
Cisco ACI with Cisco ACI Virtual Edge

Cisco ACI と Cisco ACI Virtual Edge

Cisco APIC リリース 3.1(1) 以降では、シスコ 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) は Cisco ACI Virtual Edge をサポートします。Cisco ACI Virtual Edge は、Cisco ACI 環境向けの次世代 Application Virtual Switch (AVS) です。Cisco ACI Virtual Edge はハイパーバイザに依存しない分散サービス VM で、ハイパーバイザに属しているネイティブな分散仮想スイッチを利用します。Cisco ACI Virtual Edge はユーザ スペースで動作し、仮想リーフとして機能し、Cisco Application Policy Infrastructure Controller （APIC） によって管理されます。

Cisco ACI Virtual Edge に関する情報は、Cisco.com から入手できる、次のドキュメントから得られます:

- Cisco ACI Virtual Edge Release Notes
- Cisco ACI Virtual Edge Installation Guide
- Cisco ACI Virtual Edge Configuration Guide



第 8 章

Cisco ACI with Cisco AVS

Cisco ACI with Cisco AVS

Cisco Application Virtual Switch は、ハイパーバイザに常駐する分散型仮想スイッチです。Cisco Application Centric Infrastructure（ACI）専用に設計されたもので、Application Policy Infrastructure Controller（APIC）によって管理されます。シスコの AVS は、コントロール プレーンと通信するための OpFlex プロトコルを実装しています。

シスコの AVS トラフィック転送モードとして、ローカルスイッチングありとローカルスイッチングなしの 2 つをサポートしています。転送モードは、シスコの AVS のインストール時に選択されます。

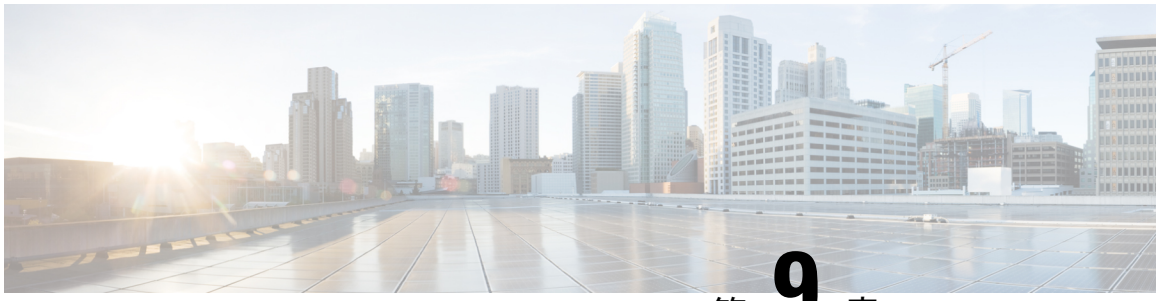
シスコの AVS は、VMware ESXi ハイパーバイザにより、 Cisco APIC 用の vLeaf としてサポートされ、VMware vCenter Server により定義されるデータセンターを管理します。

シスコの AVS は、Cisco Nexus スイッチなどの、イーサネット標準準拠のアップストリーム物理アクセス レイヤ スイッチと互換性があります。シスコの AVS は、『*VMware Hardware Codmpatibility Guide*』に記載されているすべてのサーバ ハードウェアと互換性があります。

シスコの AVS に関する情報は、Cisco.com から入手できる次のドキュメントで確認できます。

- *Cisco AVS* リリース ノート
- *Cisco AVS* インストール ガイド
- *Cisco AVS* コンフィギュレーション ガイド
- *Cisco AVS* トラブルシューティング ガイド

Cisco ACI with Cisco AVS



第 9 章

Cisco ACI with VMware vRealize

この章の内容は、次のとおりです。

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 Application Policy Infrastructure Controller （APIC） リリース 2.0(1) から、vRA と vRO は VMware DVS のほかに Cisco AVS もサポートしています。Cisco APIC リリース 3.1(1) から、vRA と vRO は Cisco Application Centric Infrastructure Virtual Edge (Cisco ACI Virtual Edge) をサポートしています。

（注） Cisco APIC GUI では、 Cisco ACI Virtual Edge は **AVE** という用語で示されています。

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
Shared	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。
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 *9 : vRealize ACI* 統合の論理モデル図

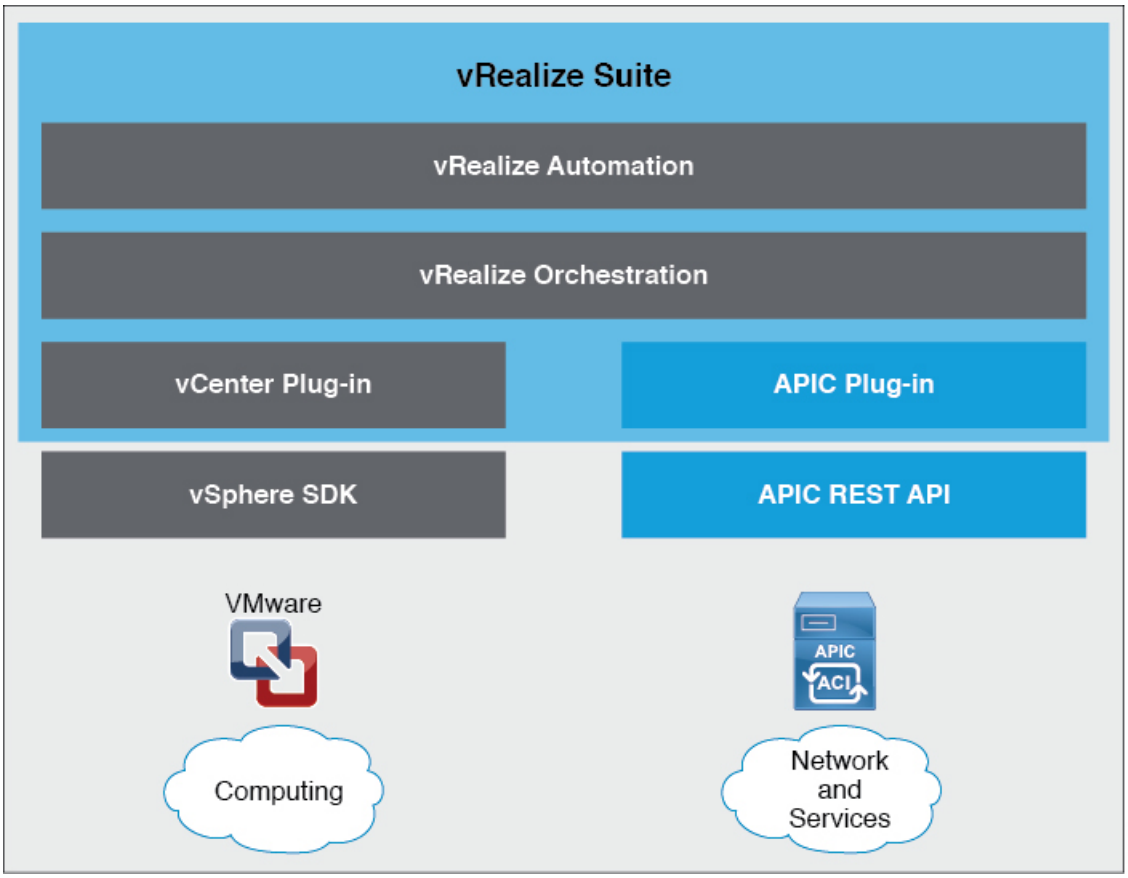
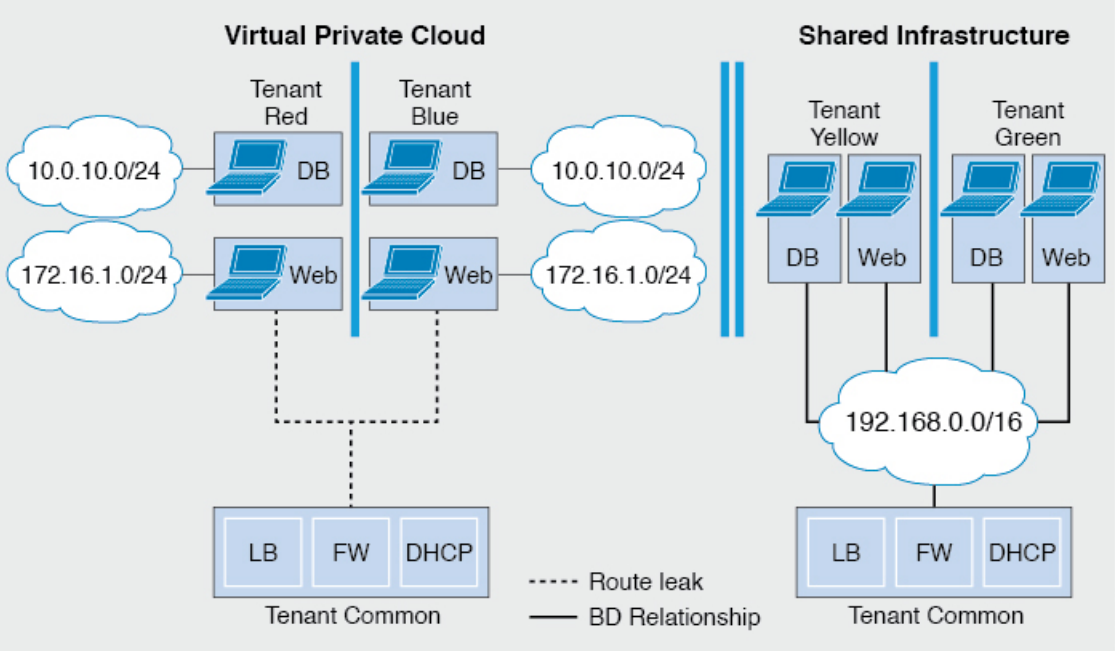


図 *10* : 共有サービス プランと仮想プライベート クラウド プランの比較図



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 （128 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 リリース 7.0 ～ 7.4 をインストール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。

- 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 （126 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 （127 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 （128 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 （162 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 （159 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 （133 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 （128 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 （133 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 （127 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 （128 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 （134 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 （133 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 （128 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 （133 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（135 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（138 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 [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 [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 [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 [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	○	○
ファイアウォール	○	○
プロバイダー DHCP	○	○
共有ロード バランサ	○	○
パブリック インターネット アクセス	○	○
テナント間共有サービス	○	○
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	なし	○

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 （146 ページ）を参照してください。

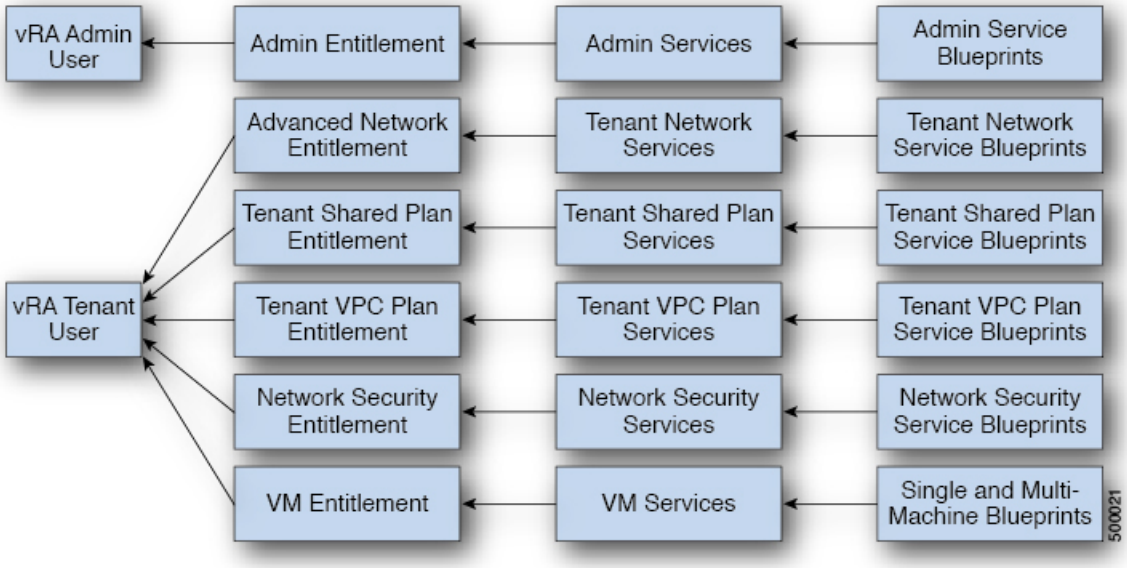
詳細については、vRealize の ACI テナント サービス （149 ページ）を参照してください。

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 （155 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 *11 : 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. 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。
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. vRealize Automation にテナント管理者としてログインし、**[Catalog]** > **[Tenant Network 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。

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. 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。
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. 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。
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. vRealize Automation に管理者としてログインし、**[Administration]** > **[Catalog Management]** > **[Entitlements]** の順に選択します。
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。

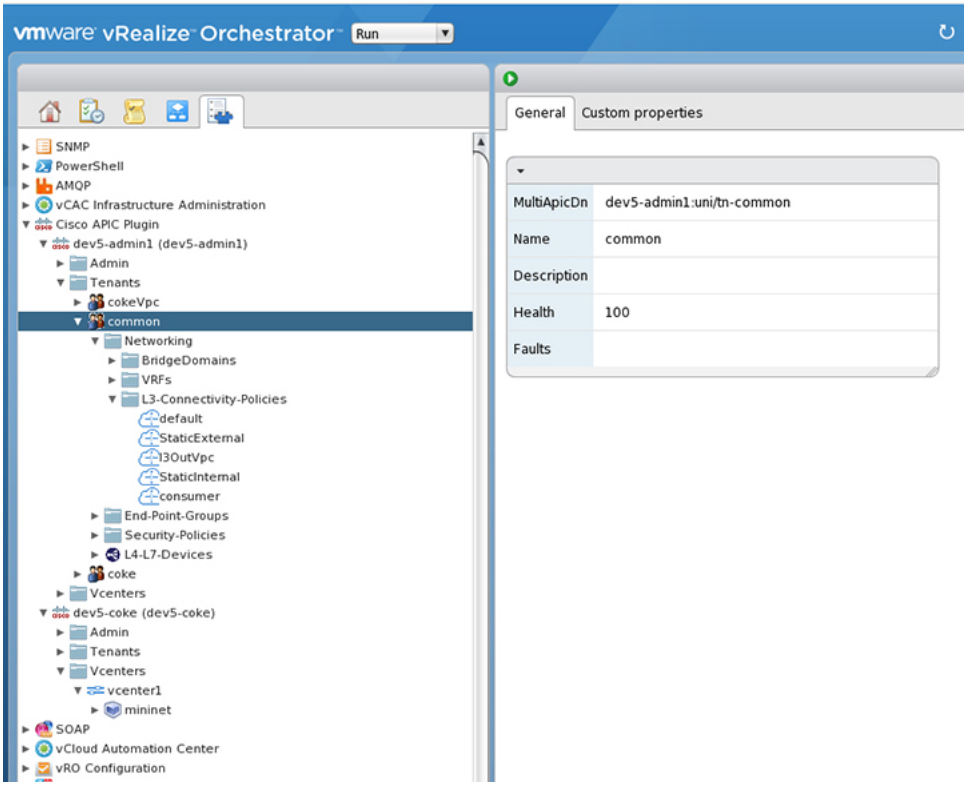
APIC のワークフロー

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 にログインしていることを確認し、メニューバーで **[TENANT]** > **common]** の順に選択します。
  - 「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 にログインしていることを確認し、メニューバーで **[TENANT]** > **common]** の順に選択します。
  - 「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

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 **仮想ネットワーク** > **インベントリ**を選択します。

ステップ 3 **Inventory** ナビゲーション ウィンドウで、**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は、VLAN またはマルチキャスト アドレス プールを更新することができます。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

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 （167 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 **[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 （168 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** 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 **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 （169 ページ）

• Cisco APIC の VMM ドメインの削除の確認 （169 ページ）
• Cisco APIC で VLAN プールの削除を確認する （169 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 （170 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、**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 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 （171 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 **Virtual Networking** > **Inventory** > **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 Configuration Guide, Release 5.2(1)SV3(3.27)』の「Distributed Firewall」の項
- 『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 （172 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 （201 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 **Virtual Networking** > **Inventory** > **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) **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。

f) **EncapMode** ドロップダウンリスト、いずれかを選択します **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 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 ドメインには、VLAN または VXLAN を選択するは、予期しない結果に可能性があります。

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

h) **内通 EPG 拒否** フィールドで、いずれかの値を選択 **はい** または **No** 。

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） **許可"マイクロセグメンテーション"** 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。

- 展開 ***your_apic_user*** > **テナント** > ***your_tenant*** > **ネットワー キング** > **BridgeDomains** > ***your_bridgedomain*** をこのブリッジ 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。

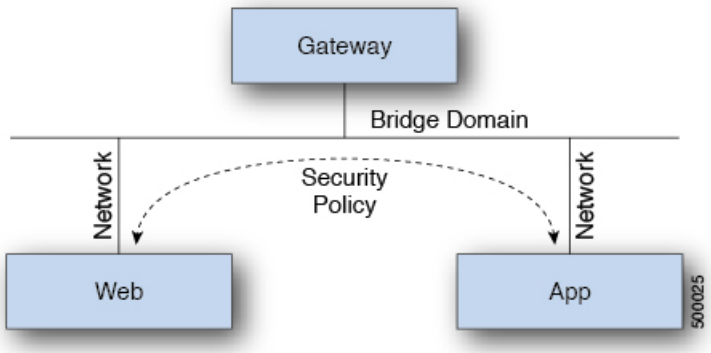
ステップ 7 メニュー バーで、[Virtual Networking] を選択します。

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 [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ー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 [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
protocol	• icmp • icmpv6 • tcp • udp • ブランク

ルール エントリ リスト	値
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) [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) [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) [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。

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 **[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) **[アプリケーション階層番号]** フィールドで、uSeg が所属する階層の番号を入力します。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) EPG 内分離を適用する場合には、**[EPG 内拒否**: ドロップダウンリストから **[はい]** を選択します。EPG 内分離を適用しない場合には、 **[いいえ]** を選択します。

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、**[新規]** をクリックして IP 基準 (または IP 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** : の IP アドレス、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** : の MAC アドレスがアドレス (たとえば、00:50:56:44:44:5 D) を指定します。

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
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。

- **値** ：属性タイプ値を入力します。各属性タイプの例は、上記のタイプのテーブルに表示されます。

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 （193 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 Cisco 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] 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、必要な uSeg をダブルクリックしてプロパティを表示します。

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 （194 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 Cisco APIC として、テナントにログインし、[**テナント** > ***your_tenant*** 。
ステップ 2 ナビゲーション ウィンドウで、**Tenant *your_tenant*** > **Application Profiles** > **default** > **uSeg EPGs** を選択します。
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** : の IP アドレス、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** : の MAC アドレスがアドレス (たとえば、00:50:56:44:44:5 D) を指定します。

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。

- **名前** : VM 条件 (または VM 属性) の名前。
- **Description**— VM 基準の説明です。
- **タイプ** : 次の表は、サポートされている属性のタイプにそれぞれマッピング APIC 、および例です。(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。
- **値** : 属性タイプ値を入力します。各属性タイプの例は、上記のタイプのテーブルに表示されます。

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 （197 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 Cisco APIC へテナントとしてログインして、 **[Tenants]** > ***[your_tenant]*** の順に選択します。

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、必要な uSeg をダブルクリックしてプロパティを表示します。

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 （194 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 （200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 （201 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 ナビゲーション ウィンドウで、**Tenant** ***your_tenant*** > **Application Profiles** > **default** > **uSeg EPGs** > ***your_useg*** > **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 *12* : 共有プラン：ロード バランサの概要

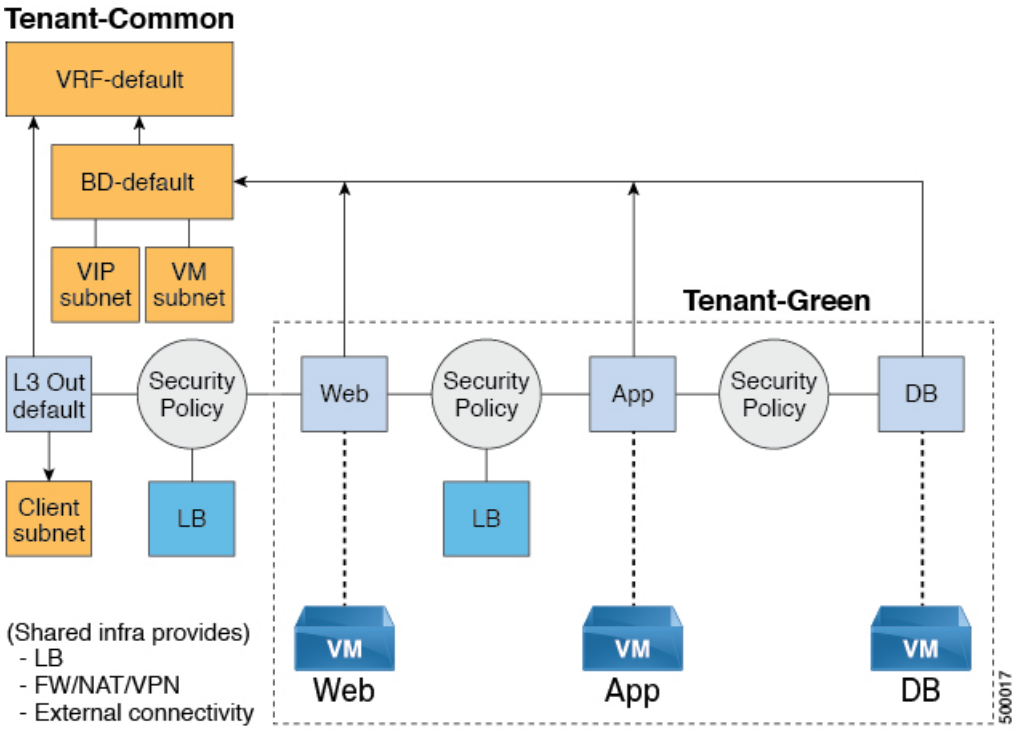
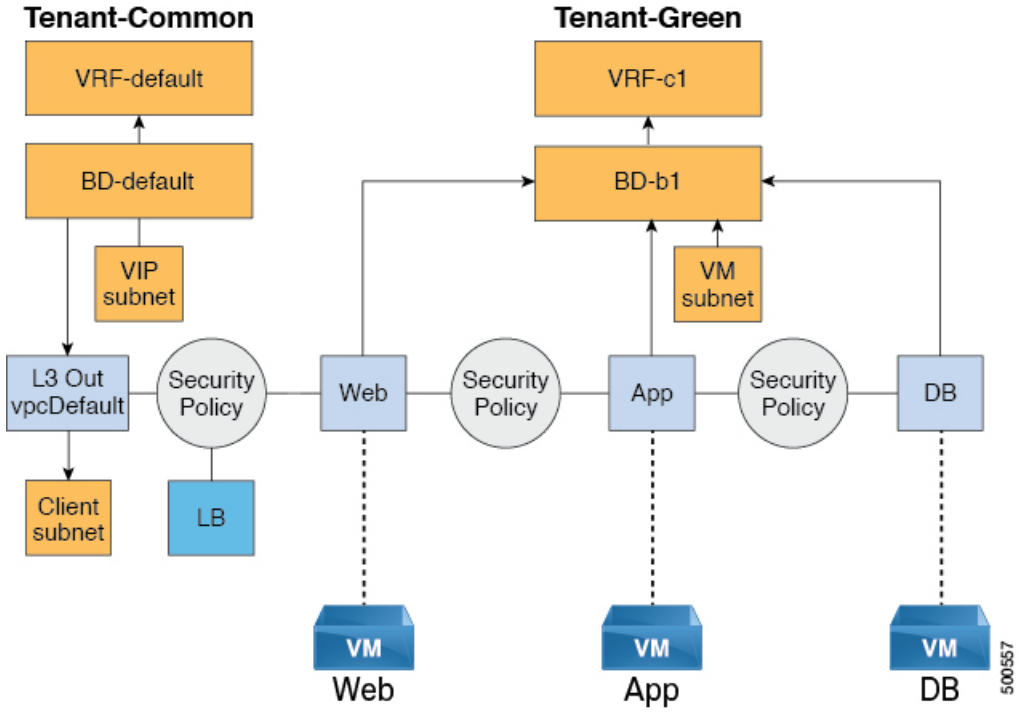


図 *13 : VPC* プラン：ロード バランサのみ



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。

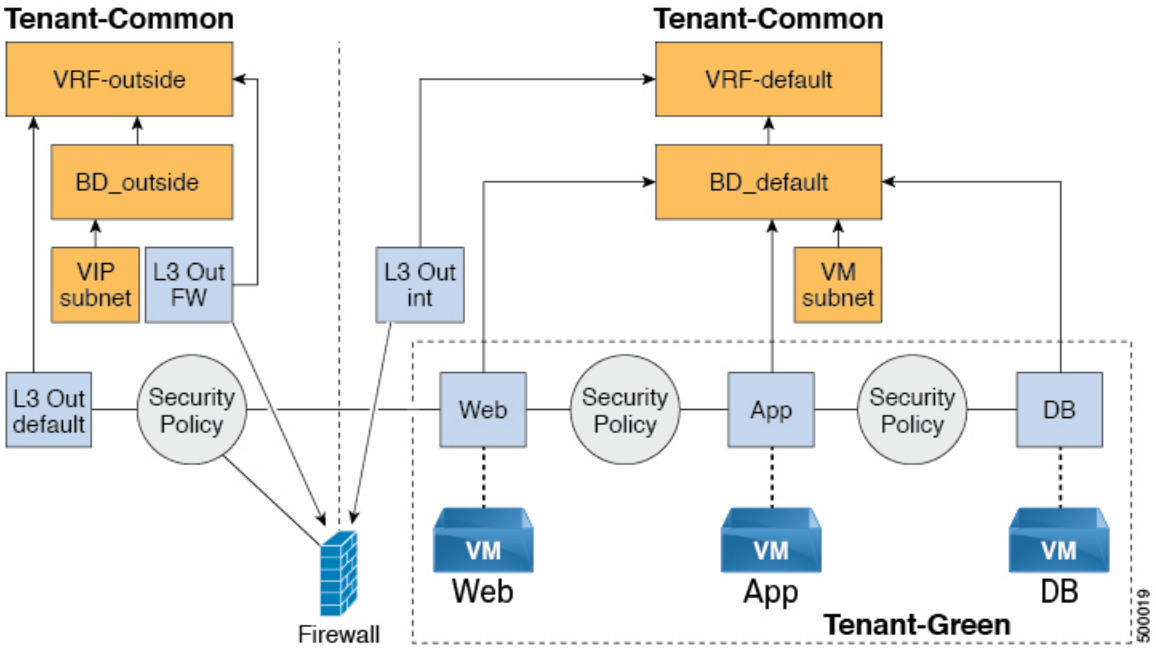
ステップ 3 フィールドに必要な情報を入力します。

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 *14 :* 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 *15 :* 共有プラン：ファイアウォールとロード バランサの概要

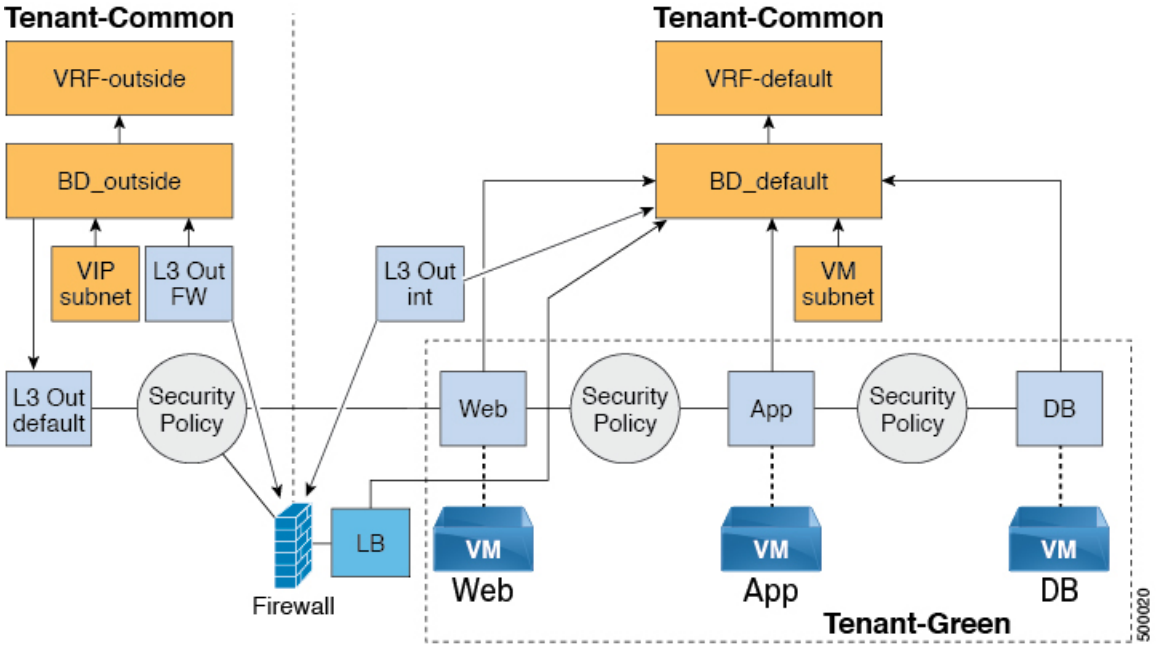
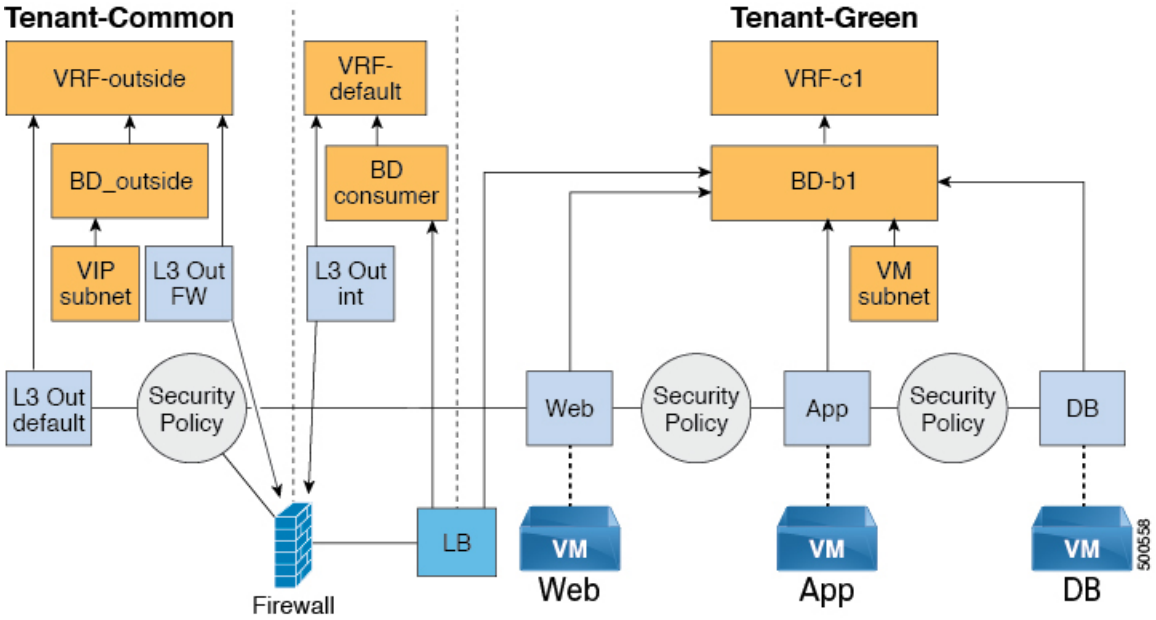


図 *16 : VPC* プラン：境界ファイアウォールとロード バランサ



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 （203 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。

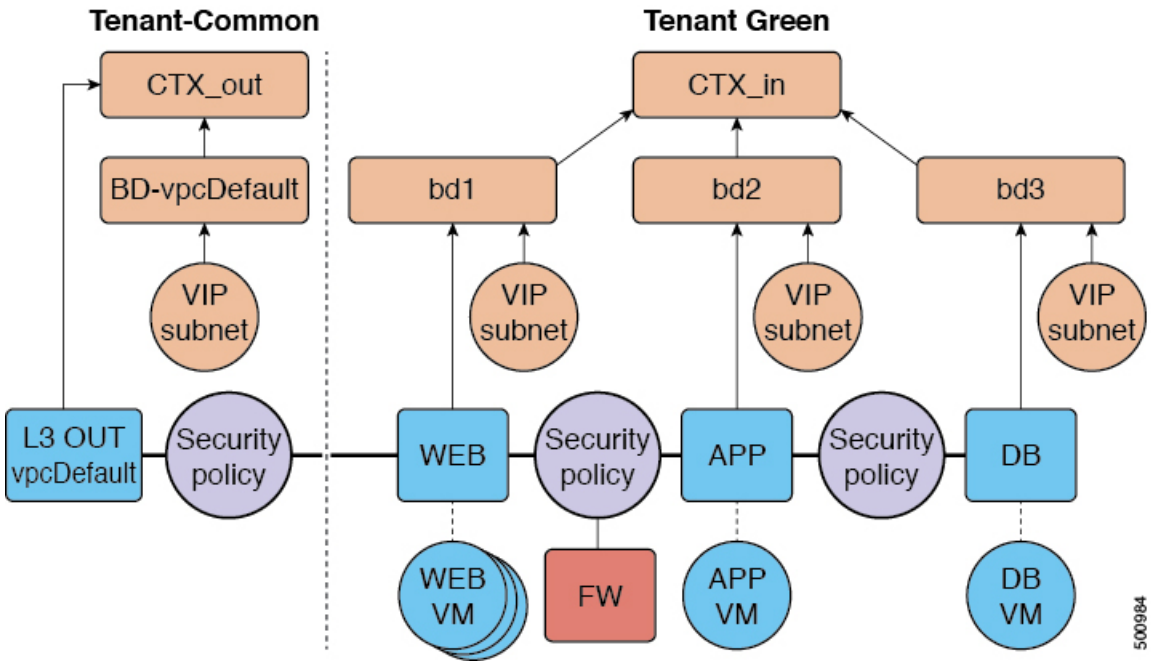
ステップ 3 フィールドに必要な情報を入力します。

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 *17 : 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

ルール エントリ リスト	値
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

導入シナリオ	説明
Web > ロード バランサとファイアウォール > **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
データベース > アプリケーション	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
アプリケーション > ロード バランサ > **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
ロードバランサのみ		○		○	

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、**Tools** > **API Search** の順に選択します。
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 クレデンシャルを使用して APIC にアクセスするには、[Use certificate authentication] を **yes** に設定し、**Certificate Name** と **Private Key** パラメータに入力します。

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 （228 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

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
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。

第 10 章

Cisco ACI vCenter プラグイン

この章の内容は、次のとおりです。

Cisco ACI と VMware vSphere Web クライアントについて

Cisco ACI vCenter プラグインは、vSphere Web クライアント内から ACI ファブリックを管理することを可能にするユーザ インターフェイスです。

これにより、VMware vSphere Web クライアントから VMware vCenter と ACI ファブリックの両方を一括管理することが可能になります。

Cisco ACI vCenter プラグインを使えば、仮想化管理者は、同じインフラストラクチャを共有しながら、ネットワーキングチームから独立して、ネットワークの接続性を定義することが可能になります。

詳細なネットワークの構成は、Cisco ACI vCenter プラグインの対象ではありません。仮想化管理者と直接関連する要素だけが表示されます。

Cisco ACI vCenter プラグインの概要

VMware vSphere Web クライアント用の Cisco Application Centric Infrastructure(ACI) vCenter プラグインは、GUI に Cisco ACI ファブリックと呼ばれる新しいビューを追加します。

Cisco Application Centric Infrastructure(ACI) vCenter プラグインは、ACI と vCenter との既存の統合は変更しませんが、EPG、uSeg EPG、契約、テナント、VRF、および VMware vSphere Web クライアントからのブリッジ ドメインを設定することができます。

Cisco Application Centric Infrastructure(ACI) vCenter プラグインはステートレスで、すべてを Application Policy Infrastructure Controller(APIC) から取得しますが、情報は一切保存しません。

Cisco ACI vCenter プラグインによって提供される機能の簡単な概要を次に示します:

詳細については、Cisco ACI vCenter プラグインの機能と制約事項 （240 ページ）を参照してください。

Cisco ACI vCenter プラグインでは、ACI ファブリックで次のオブジェクトの作成、読み取り、更新および削除 (CRUD) を行うことができます:

- テナント
- アプリケーション プロファイル
- EPG / uSeg EPG
- 契約
- VRF
- ブリッジ ドメイン

Cisco ACI vCenter プラグインは、L2 および L3 Out の使用に関する、より限定された操作も提供します。すべての高度な設定は、APIC でも前もって行っておく必要があります。

- 事前設定された L2 および L3 Out は、契約のプロバイダまたはコンシューマとして使用できます。
- 作成、編集、または削除は行えません。

Cisco ACI vCenter プラグインではまた、契約に既存のグラフ テンプレートを適用して、事前設定された L4 ～ L7 サービスを利用することもできます。

- グラフの既存のテンプレートを使用できませす。作成はできません。
- 機能プロファイルのうち、必須であるのに空のパラメータだけが表示され、設定できます。

Cisco ACI vCenter プラグインには、トラブルシューティングの機能もあります:

- エンドポイントからエンドポイントへのセッション(障害、監査、イベント、統計、契約、Traceroute)

Cisco ACI vCenter プラグインを開始する

Cisco ACI vCenter プラグイン ソフトウェアの要件

Cisco ACI vCenter プラグイン ソフトウェアの要件は次のとおりです:

プラットフォーム シリーズ	推奨リリース
vCenter	Cisco APIC は、VMware がサポートする Linux アプライアンスと Windows サーバの任意のバージョンをサポートします。詳細は、VMware のマニュアルを参照してください。
Application Policy Infrastructure Controller（APIC）	リリース 3.2(2) 以降

必要な APIC の設定

このセクションでは、必要な APIC 設定について説明します。

APIC と、プラグインがインストールされる vCenter の間には、少なくとも 1 つの VMM ドメインがすでに存在している必要があります。

詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

Cisco ACI vCenter プラグインのインストール

このセクションでは、Cisco ACI vCenter プラグインのインストール方法について説明します。vCenter と APIC の間の HTTPS トラフィックを操作する必要があります。vCenter と プラグインを直接 APIC からダウンロードするからです。

vCenter と APIC の間で HTTPS トラフィックを有効にすることはできず、Cisco ACI vCenter プラグイン zip ファイルを自分の Web サーバでホストする場合にはCisco ACI vCenter プラグインの代替インストール （273 ページ）を参照してください。

vCenter 5.5 (アップデート 3e 以降) または vCenter 6.0 (アップデート 2 以降) を使用している場合には、このセクションの手順に従います。vCenter 5.5 または 6.0 より前のリリースを使用している場合は、Cisco ACI vCenter プラグインの代替インストール （273 ページ） を参照してください。

プラグインをインストールするには、vCenter は Web サーバからプラグインをダウンロードする必要があります。次の手順では、APIC をWeb サーバとして使用し、vCenter は APIC から直接プラグインをダウンロードします。

vCenter 5.5 Update 3e または vCenter 6.0 Update 2 より前を使用して理得r場合には、vCenter は HTTPS 通信のために TLSv1 を使用しますが、これは現在では旧式のものとなっています。セキュリティ上の理由から、APIC は TLSv1.1 と TLSv1.2 だけをサポートしています。そのため、vCenter は APIC からプラグインをダウンロードすることはできません。プラグインは、TLSv1 を許可し、または HTTPS を使用しない独立した Web サーバに配置する必要があります。

始める前に

- すべての前提条件を満たしていることを確認します。

  詳細については、Cisco ACI vCenter プラグイン ソフトウェアの要件 （235 ページ）および必要な APIC の設定 （235 ページ）のセクションを参照してください。

- vCenter サーバと APIC の間で HTTPS トラフィックが許可されることを確認します。

手順

ステップ 1 次の URL にアクセスします:

例：

```
https://<APIC>/vcplugin
```

ステップ 2 Web ページの指示に従って作業を行います。

Vcenter プラグインをACI ファブリックに接続する

このセクションでは、ACI ファブリックに VCenter プラグインを接続する方法について説明します。

（注）

- 登録は vCenter全体で行われ、実行するユーザーは考慮されません。実行ユーザーのログインだけではなく、vCenter 全体の設定です。
- Role Based Access Control（RBAC）は、登録時に使用するクレデンシャルに基づくものです。登録に使用される APIC アカウントの権限は、vCenterプラグインの設定の制限を定義します。

次のいずれかの方法を使用して、VCenter プラグインを ACI ファブリックに接続できます。

クレデンシャルを使用して、VCenterプラグインを ACI ファブリックに接続します。	詳細については、クレデンシャルを使用した ACI ファブリックへの VCenter プラグインインの接続 （237ページ）を参照してください。

既存の証明書を使用して、VCenterプラグインを ACI ファブリックに接続します。	詳細については、既存の証明書を使用して vCenterプラグインを ACI ファブリックに接続する （238 ページ）を参照してください。
新しい証明書を作成することで、VCenterプラグインを ACI ファブリックに接続します。	詳細については、新しい証明書の作成により、vCenterプラグインを ACI ファブリックに接続する （239 ページ）を参照してください。

クレデンシャルを使用した ACI ファブリックへの VCenter プラグインインの接続

クレデンシャルを使用して、ACI ファブリックに VCenter プラグインを接続する方法について説明します。

始める前に

isco ACI vCenter プラグインがインストールされていることを確認します。詳細については、Cisco ACI vCenter プラグインのインストール （235 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[Cisco ACI ファブリック]** を選択します。

ステップ 3 **[はじめに]** ペインで、**[vSphere を ACI ファブリックに接続]** を選択します。

ステップ 4 **[新しい ACI ファブリックの登録]** ダイアログ ボックスで **[はい]** をクリックして、新しい ACI ファブリックを登録します。

ステップ 5 **[新しい APIC ノードの登録]** ダイアログ ボックスで、次の操作を実行します:

a) **[IP/FQDN]** フィールドに IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

b) **[証明書を使用する]** フィールドでは、APIC の認証のために [証明書を使用する] チェックボックスをチェックしないでください。

c) **[ユーザー名]** フィールドにユーザー名を入力します（admin）。

d) [Password] フィールドにパスワードを入力します。

e) [OK] をクリックします。

ステップ 6 **[情報]** ダイアログ ボックスで、**[OK]** をクリックします。

APIC ノードが ACI ファブリックに正常に追加されました。

ステップ 7 **[ACI ファブリック]** ペインで、新しく登録された APIC でその他の APIC を検出したことが表示されますs。

Cisco ACI vCenter プラグインは要求に常に 1 個の APIC を使用します。ただし、APIC が現在使用されない場合は APIC に切り替えます。

（注） 非ローカル ログイン ドメインでユーザーを登録するには、**[ユーザー名]** フィールドに ***local domain\user name*** と入力し、*local domain* を適切なローカル ドメイン名に置き換えて、*user name* をユーザー名に置き換えます。

既存の証明書を使用して vCenter プラグインを ACI ファブリックに接続する

このセクションでは、既存の証明書を使用して、vCenter プラグインを ACI ファブリックに接続する方法について説明します。

始める前に

- 証明書はすでに管理者ユーザが使用できるよう APIC で設定されています。
- 証明書の名前と秘密キーを取得しています。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Navigator** ウィンドウで、**Cisco ACI Fabric** を選択します。

ステップ 3 **Getting Started** ペインで、**Connect vSphere to your ACI Fabric** を選択します。

ステップ 4 **Register a new ACI Fabric** ダイアログボックスで **Yes** をクリックして、新しい ACI ファブリックを登録します。

ステップ 5 **Register a new APIC Node** ダイアログボックスで、次の操作を実行します:

a) **IP/FQDN** フィールドに、IP アドレスまたは完全修飾ドメイン名(FQDN) を入力します。

b) **Use Certificate** フィールドで **Use Certificate** チェック ボックスをオンにします。

ステップ 6 **Action** セクションで **Use an existing certificate** を選択します。

ステップ 7 **Name** フィールドに証明書名を入力します。

ステップ 8 **Private Key** セクションに、証明書の秘密キーをペーストします。

ステップ 9 **Check Certificate** をクリックします。

ステータスは [Connection Success] に切り替わります。

（注） 接続エラーが表示された場合には、証明書の名前と秘密キーが正しいか確認して、もう一度やり直してください。

ステップ 10 [OK] をクリックします。

ステップ 11 **Information** ダイアログボックスで、**OK** をクリックします。
APIC ノードは、ACI ファブリックに正常に追加されました。

ステップ 12 **ACI Fabric** ペインでは、新たに登録した APIC が、他の APIC を検出します。

Cisco ACI vCenter プラグインは常に、リクエストのため、単一の APIC を使用します。現在使用中の APIC が利用できなくなった場合には、Cisco ACI vCenter プラグインは APIC を切り替えます。

新しい証明書の作成により、vCenter プラグインを ACI ファブリックに接続する

このセクションでは、新しい証明書を作成することにより、vCenter プラグインを ACI ファブリックに接続する方法について説明します。

始める前に

- プラグインがインストールされていることを確認します。
- APIC 管理者のクレデンシャルに対するアクセス権があります。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[Cisco ACI ファブリック]** を選択します。

ステップ 3 **Getting Started** ペインで、**Connect vSphere to your ACI Fabric** を選択します。

ステップ 4 **Register a new ACI Fabric** ダイアログボックスで **Yes** をクリックして、新しい ACI ファブリックを登録します。

ステップ 5 **Register a new APIC Node** ダイアログボックスで、次の操作を実行します:

a) **IP/FQDN** フィールドに、IP アドレスまたは完全修飾ドメイン名(FQDN) を入力します。
b) **Use Certificate** フィールドで **Use Certificate** チェック ボックスをオンにします。

ステップ 6 **Action** フィールドで、**Generate a new certificate** を選択します。

ステップ 7 [Name] フィールドに新しい証明書の名前を入力します。

ステップ 8 **Generate certificate** ぼたんをクリックします。

ステップ 9 表示された証明書をコピーします。

コピーが必要なのは、-----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- までで、これらの行も含めます。

ステップ 10 この証明書を APIC 内の管理者ユーザに追加します。同じ証明書名を使用していることを確認してください。

a) APIC GUI に admin としてログインします。
b) メニュー バーで、**Admin** を選択します。
c) **Navigation** ペインで、**Security Management** > **Local Users** > **admin** を展開します。
d) **Work** ウィンドウの **User Certificate** セクションで、プラスのアイコンをクリックして証明書を追加します。
e) **Name** フィールドに証明書名を入力します。

f) **Data** フィールドに、手順 8 でコピーした証明書の内容をペーストします。
g) [Submit] をクリックします。

ステップ 11 vCenter プラグインで、**Check Certificate** をクリックします。

ステータスは [Connection Success] に変わります。

（注） 接続エラー メッセージが表示された場合には、証明書が APIC に正しく追加されていること、証明書名が同じであることを確認します。

ステップ 12 [OK] をクリックします。

ステップ 13 **Information dialog** ボックスで、**OK** をクリックします。
APIC ノードは、ACI ファブリックに正常に追加されます。

ステップ 14 **ACI Fabric** ペインでは、新たに登録した APIC が、他の APIC を検出します。

Cisco ACI vCenter プラグインは常に、リクエストのため、単一の APIC を使用します。現在使用中の APIC が利用できなくなった場合には、Cisco ACI vCenter プラグインは APIC を切り替えます。

Cisco ACI vCenter プラグインの機能と制約事項

このセクションでは、管理するすべてのオブジェクト タイプに対して、Cisco ACI vCenter プラグインで提供される可能な操作について説明します。また、意図的な設定制限が課されます。

オブジェクトに関する詳細情報については、「*Cisco Application Centric Infrastructure Fundamentals*」を参照してください。

テナント

Cisco ACI vCenter プラグインは、テナント オブジェクトで CRUD 操作を使用できます。次の属性はプラグインで公開されます。

- [Name]：テナントの名前。
- Description (Optional)：テナントの説明です。

テナントがプラグインで作成される場合、VRF に接続されている VRF *tenant_name*>_default とブリッジ ドメイン< *tenant_name* >_default は、内部で自動的に作成されます。アプリケーション プロファイル <*tenant_name*>_default は、内部で作成されます。

インフラストラクチャテナント（インフラ）および管理テナント（管理）は、プラグインで公開されていません。

（注） プラグインにACIファブリックを登録中、プラグインで表示されるテナントは使用されるアカウントに関連付けられている権限によって異なります。

Application Profiles

Cisco ACI vCenter プラグインは、アプリケーション プロファイル オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：アプリケーション プロファイルの名前。
- Description (Optional)：アプリケーションプロファイルの説明です。

エンドポイント グループ

Cisco ACI vCenter プラグインは、エンドポイント グループ オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：エンドポイント グループの名前。
- Description (Optional)：エンドポイント グループの説明です。
- ブリッジ ドメイン：このエンドポイントのグループに関連付けられているブリッジ ドメイン。
- EPG 内分離：これにより、EPG に接続されている仮想マシン間のすべてのトラフィックを拒否します。デフォルトでは、同じ EPG のすべての仮想マシンは互いに通信できます。
- 分散型スイッチ：EPG が展開されている DVS/Cisco AV。これは、ACI の VMM ドメインの関連付けに対応しています。

  デフォルトでは、プラグインで作成されたすべての EPG は、プラグインが使用されている vCenter を指す VMM ドメインに関連付けられています。同じ vCenter を指す複数の VMM ドメインがある場合は、EPG を展開する DVS で選択された形式で少なくとも 1 つ選択する必要があります。

マイクロセグメンテーションの許可（Cisco AV ではなく DVS のみ)：これにより、「ベース EPG」を作成できます。この EPG に接続されているすべての仮想マシンは、uSeg EPG の「マイクロセグメンテーション」ルールを適用するための候補です。マイクロセグメント EPG ルールは、「ベース EPG」に接続されている仮想マシンにのみ適用されます。

（注） すべて EPG は、分散型のスイッチが Cisco AV の場合ベース EPG として見なされます。

使用されるプラグインが「仮想」として表示される vCenter を指す VMM ドメインに、EPG がリンクされています。その他の EPG は「物理」として表示されます。

アクションの更新と削除は、vCenter（仮想）を指している VMM ドメインにリンクされている EPG にのみ許可されます。他の EPG（物理）は読み取り専用です。VMM ドメインに関係なく、更新は EPG がコントラクトの消費または提供を行うように許可されています。

uSeg EPG

Cisco ACI vCenter プラグインは、マイクロセグメント EPG オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：マイクロセグメント EPG の名前。
- Description (Optional)：マイクロセグメント EPG の説明です。
- ブリッジ ドメイン：このマイクロセグメント EPG に関連付けられているブリッジ ドメイン。
- EPG 内分離：これにより、EPG に接続されている仮想マシン間のすべてのトラフィックを拒否します。デフォルトでは、同じEPGのすべての仮想マシンは互いに通信できます。
- 分散型スイッチ：EPG が展開されている DVS/Cisco AV。これは、ACI の VMM ドメインの関連付けに対応しています。

  デフォルトでは、プラグインで作成されたすべての EPG は、プラグインが使用されている vCenter を指す VMM ドメインに関連付けられています。同じ vCenter を指す複数の VMM ドメインがある場合は、EPG を展開する DVS で選択された形式で少なくとも 1 つ選択する必要があります。
- Miro セグメンテーションの属性：このマイクロセグメントEPGに属数VMを決定するルールのリスト。ルールのオプションには、IP、MAC、VM名、OS、ホスト、VMid、VNic、ドメイン、データ センタ、カスタム属性を含みます。

（注） ドメイン属性（VMM ドメイン）では、ローカル vCenter に VMM ドメインを選択できます。対応する DVS/Cisco AV を選択してドメインを選択します。

カスタム属性のみ選択できます。これらはプラグインでは設定できません。これらは、VMware vSphere クライアントを設定する必要があります。カスタム ラベルを作成するには、次を参照してください。 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005720

L2 および L3 の外部ネットワーク

レイヤ 2 およびレイヤ 3 の外部ネットワークは、ネットワーク管理者によって APIC で作成および設定される必要があります。これらは vCenter プラグインの読み取り専用です。

これらのオブジェクトで許可されるプラグイン操作のみ、コントラクトを消費または提供できます。

L3 外部ネットワークに表示されている情報は次のとおりです。

- Name：L3 外部ネットワークの名前
- Subnets：この L3 外部ネットワークで示される外部サブネット
- VRF：この L3 外部ネットワークに属する VRF
- 接続されたブリッジ ドメイン：この L3 外部ネットワークに接続されているブリッジ ドメイン

L2 外部ネットワークに表示されている情報は次のとおりです。

- Name：L2 外部ネットワークの名前
- ブリッジ ドメイン：このブリッジ ドメインに関連付けられているブリッジ ドメイン
- VLAN ID：この L2 外部ネットワークに関連付けられている VLAN ID

VRF

Cisco ACI vCenter プラグインでは、VRF オブジェクトで CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：VRF の名前。
- Description (Optional)：VRF の説明です。
- ポリシーの適用：コントラクトをこの VRF の EPG に適用する必要があるかどうかを決定します。

ブリッジ ドメイン

Cisco ACI vCenter プラグインでは、ブリッジ ドメインのオブジェクトに CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：ブリッジ ドメインの名前。
- Description (Optional)：ブリッジ ドメインの説明です。
- プライベート サブネット：このブリッジ ドメインのゲートウェイのリスト。

（注）
- 共有およびアドバタイズされるサブネットは読み取り専用です。これらは、プラグインで設定できることはできません。プライベート サブネットのみを追加または削除できます。
- ブリッジ ドメインはが APIC により L3/L2 アウトに接続されていますが、これは削除できません。

契約

Cisco ACI vCenter プラグインでは、コントラクトのオブジェクトに CRUD 操作が可能です。次の属性はプラグインで公開されます。

- Name：コントラクトの名前。
- Description (Optional)：コントラクトの説明です。
- コンシューマ：コントラクト（EPG、uSeg Epg、L2/L3 外部ネットワーク）のコンシューマ
- プロバイダ：コントラクトのプロバイダ（EPG、uSeg Epg、L2/L3 外部ネットワーク）
- フィルタ：コントラクトに関連付けられているフィルタのリスト

- 両方向に適用：指定されたフィルタがコンシューマからプロバイダまたはプロバイダからコンシューマへのみ適用できることを示します。
- L4 L7 グラフ テンプレート：既存のグラフ テンプレートをコントラクトに関連付けることができます。L4 ～ L7 サービス セクションについては以下を参照してください。

（注）

- サブネットは表示されません。プラグインは、単一の件名を持つコントラクトのみ管理します。複数の件名を持つコントラクトが表示されますが、編集できません。
- コンシューマおよびコントラクトが同じテナント内にない場合は、コントラクト インターフェイスが自動的に作成されます（*_Tenant-name_contract-name* という名前）。

Filters

Cisco ACI vCenter プラグインでは、フィルタ オブジェクトの CRUD 操作が可能です。APIC からすべてのパラメータが公開されます。

L4 ～ L7 サービス

- L4 L7 サービスは、単一のプロバイダ契約にのみ追加できます。
- プラグインではグラフ テンプレートを作成できません（既存のグラフ テンプレートのみ消費）
  - グラフ テンプレートには次を含むように設定する必要があります。
    - デバイスとの関連付け
    - 機能プロファイルとの関連付け
  - 最大 2 個のノードを持つグラフ テンプレートのみをサポートします
- プラグインがフォルダ操作を許可していないため、機能プロファイル フォルダの名前つけと階層が有効である必要があります。
  - 機能プロファイルの空の必須パラメータが、プラグインで編集できます。
- グラフ コネクタが設定可能です。
  - APIC からすべてのパラメータが公開されます
  - 必要に応じて、リダイレクト ポリシーを消費のみ可能ですが作成はできません

トラブルシューティング

- エンドポイント間のトラブルシューティング セッションのみがサポートされます。
  - 既存のセッションを選択するか、新規を作成できます。

- 物理トポロジ（スパイン/リーフ）は表示されません。
- トポロジの表示はvNICが接続するホスト、VM、 v NIC、EPGにフォーカスしているVM 中心型です。

- セッションで使用可能な情報：
  - 障害
  - コントラクト：表では2つのEPG間のすべてのコントラクト/フィルタ/エントリを一覧にします（ヒット カウントは表示されません）
  - ドロップ/統計情報
  - 監査/イベント
  - traceroute
- アトミック カウンタおよびSPANは利用できません。
- より基本的なトラブルシューティング ツールは、エンドポイントではないオブジェクト（VM、EPG、L3アウト）間で使用でき、選択された2つのオブジェクト間の設定されたコントラクトのみ表示します。
- VMおよびEPGへの接続のビューが使用可能です。
  - 特定のVMについては、VNICを接続するEPGを表示することができます。
- L4 - L7コネクタがトラブルシューティング セッションの送信元または宛先として使用される場合、トラブルシューティング ウィザードのコントラクト セクションで次のエラーが表示されることが予想されます。

  この機能には、EPGの一部である両方に対して送信元と宛先のエンドポイントが必要です。

  このエラーメッセージは、無視しても問題ありません。

Cisco AVS のインストールとアップグレード

Cisco ACI vCenterプラグインでは、vSphere Webクライアントから Cisco AVをインストール、アンインストール、アップグレード、ダウングレードできます。

- VCenterプラグインを ACI ファブリックに接続すると、Cisco APICのすべての Cisco AVSドメインの親を表示でき、Cisco AVSドメインに関連付けられているデータ センタの一部またはすべてのホストの Cisco AVSをインストール、アンインストール、アップグレード、ダウングレードできます。
- Cisco.comからダウンロードされた Cisco AVSの新しいバージョンは、GUIを使用してvCenterにアップロードできます。これらのバージョンは、特定のドメイン内のホストにインストールできます。

- 特定の Cisco AV ドメインに接続されている場合は、すべてのホストを表示できます。インストールされている場合、ホストの OpFlex エージェントのステータスと Cisco AV の現在のバージョンを表示できます。

Cisco AVS をインストールまたはアップグレードするとき、Cisco AVS は ESXi ホストで次の手順を自動的に実行します。

1. ホストでメンテナンス モードを開始します。
2. ホストのデータ ストアに適した VIB ファイルをアップロードします。
3. Cisco AVS ソフトウェアをインストールまたは再インストールします。
4. ホストのデータ ストアから VIB ファイルを削除します。
5. ホストのメンテナンス モードを終了します。

（注）

- VCenter プラグインはホスト上の Cisco AV VIB をインストールまたはアンインストールのみします。Cisco AVS スイッチに対してホストを接続または切断する必要があります。
- ホストが HA/DRS クラスタの一部である場合、ホストがメンテナンス モードになっているとき、VM は自動的に移行されます。VM が自動的に移行できない場合、インストールまたはアップグレードを正常に行うため、ホストのすべての VM を移行するかオフにする必要があります。

詳細については、『Cisco AVS インストール ガイド』の次のセクションを参照してください。

- 「VMware vCenter プラグインを使用した Cisco AVS のインストール」
- 「VMware vCenter プラグインを使用した Cisco AVS のアップグレードまたはダウングレード」
- 「VMware vCenter プラグインを使用した Cisco AVS のアンインストール」

Cisco ACI vCenter プラグインのためのロールベース アクセス コントロール

Cisco APIC リリース 3.1 (1)から Cisco ACI vCenter プラグインは、 Cisco APIC のユーザ ロールとセキュリティ ドメインに基づいて、拡張されたロールベース アクセス コントロール (RBAC) をサポートしています。

Cisco ACI vCenter プラグインの UI には、Cisco APIC ユーザの読み取りと書き込み権限が反映されます。たとえば、ユーザが契約機能にアクセスしようとしても、契約に対する読み取り権限を持っていない場合、グレーの画面と、ユーザがアクセス権を持っていないことを示すメッセージが表示されます。書き込み権限を持っていないユーザには、無効なリンクまたはアクションが表示されます。

設定の読み取りと書き込みロール

次のテーブルでは、Cisco ACI vCenter プラグインの RBAC のさまざまな機能を有効または無効にするための読み取りと書き込みロールに関し、それぞれの権限を設定する方法について説明しています。

（注） ユーザに対し、セキュリティ ドメインを割り当てる際には、Cisco APICのロールを作成し、割り当てる必要があります。ユーザがアクセスするテナントについても、セキュリティ ドメインを追加する必要があります。

表 *4 : Cisco ACI vCenter* プラグインの *RBAC* 権限

ロール	ワークフロー	限定読み取りロール	書き込みロール
すべてのロールで必須の設定		vmm-connectivity および vmm-ep	
アプリケーションプロファイル	リスト	tenant-network-profile または tenant-epg	
	作成/削除		テナント ネットワーク プロファイル
EPG	List	tenant-epg、tenant-connectivity-l2、および tenant-connectivity-l3	
	作成/削除	tenant-connectivity-l2 および tenant-connectivity-l3	tenant-epg
VRF	List	tenant-connectivity-l2 および tenant-connectivity-l3	
	作成/削除		tenant-connectivity-l2 および tenant-connectivity-l3

ロール	ワークフロー	限定読み取りロール	書き込みロール
ブリッジ ドメイン	BD の一覧	tenant-connectivity-l2 および tenant-connectivity-l3	
	BD の作成/削除		tenant-connectivity-l2 および tenant-connectivity-l3
	BD サブネットの一覧	tenant-connectivity-l2 および tenant-connectivity-l3	
	BD サブネットの作成/削除		tenant-connectivity-l2 および tenant-connectivity-l3
契約	契約の一覧	tenant-security および tenant-epg	
	契約の作成/削除		tenant-security および tenant-epg
	フィルタの一覧	tenant-security および tenant-epg	
	フィルタの作成/削除	tenant-epg	tenant-security
L4L7	一覧	tenant-security、tenant-epg、および nw-svc-policy	
	作成/削除	tenant-epg	tenant-security および nw-svc-policy
トラブルシューティング	セッションの一覧	admin*	
	セッションの作成/削除		admin*
L2 Out	L2Out の一覧	tenant-ext-connectivity-l2	
	契約の作成	tenant-ext-connectivity-l2	tenant-security
L3 Out	L3Out の一覧	tenant-ext-connectivity-l3	
	契約の作成	tenant-ext-connectivity-l3	tenant-security

（注） 上記のテーブルでは、セキュリティ ドメインが「all」になっている場合、アスタリスク (*) が付いているロールを追加する必要があります。

Cisco APIC のユーザ ロールとセキュリティ ドメインの詳細については、『Cisco ACI Fundamentals』の「User Access: Roles, Privileges, and Security Domains」のセクションを参照してください。

Cisco ACI vCenter プラグインで推奨される RBAC 設定

aaaUser のために、APIC 上で権限を持つ 2 つのユーザ ロールを定義することを推奨します:

- vcplugin_read — aaaUser の読み取りアクセス許可を定義します。
- vcplugin_write — aaaUser の書き込みアクセス権を定義します。

Cisco ACI ファブリックは、Cisco APIC 上のローカル ユーザとしてのみ登録できます。デフォルトのログイン ドメインがローカルの場合は、admin または任意のローカル ユーザ名とパスワードでログインできます。

ただし、デフォルトのログイン ドメインがローカルではない場合でも、ユーザ名でローカル ドメインを指定することにより、やはりファブリックを定義することができます:

```
apic# local domain\username
```

ローカル ドメインとユーザ名を入力する場合には、Cisco APIC にローカル ドメイン名が存在する必要があります。

（注） どの RBAC 設定でも、aaaUser のセキュリティ ドメインを Cisco APIC と VMware vCenter の間の VMM ドメインに割り当てることが必要です。

（注） Cisco ACI vCenter プラグインは、このガイドの Cisco ACI vCenter プラグインのためのロールベース アクセス コントロール （246 ページ） の RBAC 権限のテーブルで記述されているアクセス許可に従うものであれば、どのユーザ ロールの組み合わせにでも適応することができます。

CiscoACIvCenterプラグインを使用している場合のVMware vCenter のアップグレード

VMware vCenter をバージョン 6.0 からバージョン 6.5 にアップグレードしようとしており、Cisco ACI vCenter プラグインを使用している場合には、アップグレードに進む前に、追加の手順を実行する必要があります。

手順

vCenter で、`C:\ProgramData\cisco_aci_plugin\` フォルダを削除します。

フォルダを削除しないまま、アップグレード後にファブリックをもう一度登録しようとすると、「Error while saving setting in C:\ProgramData\cisco_aci_plugin*user_domain*.properties」というエラーメッセージが出ます。ここでの user は vSphere Web クライアントにログインしているユーザであり、domain は所属ドメインになります。

それでもファブリックは登録できますが、古い vCenter で作成された設定を上書きすることはできません (権限がありません)。vCenter の再起動後に、これまで加えた APIC 設定の変更をもう一度入力する必要があります。

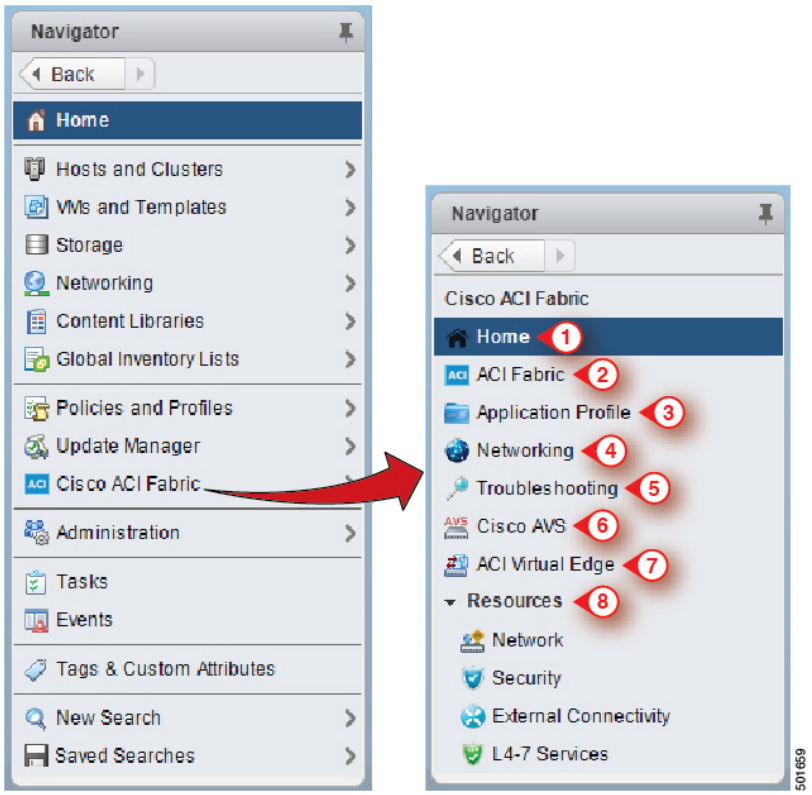
Cisco ACI vCenter プラグイン GUI

Cisco ACI vCenter プラグイン GUI アーキテクチャの概要

ここでは、Cisco ACI vCenter プラグインの GUI アーキテクチャの概要について説明します。

メイン メニュー

図 *18* : メイン メニュー



1	**Home**—Cisco ACI vCenterプラグインホームページを表示し、**[Getting Started]** タブと**[About]**タブがあります。 **[Create a new Tenant]**、**[Create a new Application Profile]**、**[Create a new Endpoint Group]** などの基本的なタスクを実行できる**[Getting Started]**タブ、Cisco Application Centric Infrastructure (ACI) リンクをクリックして、ACI Web サイトを参照してください。 The **[About]** タブには、Cisco ACI vCenter プラグインの現在のバージョンが表示されます。
2	**ACI Fabric**—ACI ファブリックをプラグインに登録し、ファブリックのテナントを管理するために使用されます。
3	**Application Profile**—EPG、uSeg EPG、L2/L3Out、および契約のドラッグアンドドロップインターフェイスでアプリケーションプロファイルを管理するために使用します。アプリケーションの健全性、統計およびフォルトに関する可視性を提供します。
4	**Networking**—VRF およびブリッジ ドメインを管理するためのドラッグ アンド ドロップ インターフェース。

5	**Troubleshooting**—エンティティ、エンドポイントからエンドポイントへのトラブルシューティングセッションの間で定義されたコントラクトを表示し、仮想マシン(VM)をブラウズし、エンドポイント グループ (EPG) への接続を表示します。
6	**Cisco AVS**—Cisco AVS のインストール、アップグレード、またはアンインストール。 ポリシーについては、Cisco Application Virtual Switch Installation Guide を参照してください。
7	**Cisco ACI Virtual Edge**—Cisco ACI Virtual Edge のインストールまたはアンインストール、または Cisco AVS または VMware VDS から ACI Virtual Edge への移行。 ポリシーについては、Cisco ACI Virtual Edge Installation Guide を参照してください。
8	**Resources**—プラグインによって管理されているすべてのオブジェクトの階層型ビューでブラウズすることができます。

（注） **[Application Profile]**、**[Networking]** および **[Resources]** のセクションをナビゲートしている間、各画面の上部にある選択バーでは、アクティブなテナントを選択できます。各セクションに表示されるコンテンツは、そのバーで選択されたテナントに固有です。

Cisco ACI vCenter プラグインの概要

このセクションでは、Cisco ACI vCenter プラグインの GUI 概要について説明します。

（注） すべての障害、統計、イベント、監査の時刻は、ブラウザのローカル タイム ゾーンに表示されます。Cisco APIC のタイム ゾーンがシステムのタイム ゾーンと一致していない場合、タイム スタンプは別のタイム ゾーンのものになる可能性があります。

ホーム

VMware vSphere Web クライアントの [Navigator] ペインで、[Home] を選択します。[Work] ペインには次のタブが表示されます。

- [Getting Started] タブ

  [Getting Started] ペインの下部では、次の操作を実行できます:

  - [Create a new Tenant] をクリックして、新しいテナントを作成します。
  - [Create a new Application Profile] をクリックして、新しいアプリケーション プロファイルを作成します。
  - [Create a new Endpoint Group] をクリックして、新しいエンドポイント グループを作成します。

- Cisco Application Centric Infrastructure (ACI) リンクをクリックして、ACI の Web サイトを閲覧します。

- [About] タブ

  [About] ペインには、Cisco ACI vCenter プラグインのバージョンが表示されます。

ACI ファブリック

VMware vSphere Web クライアントの [Navigator] ペインで、[Cisco ACI Fabric] を選択します。[Work] ペインには次のタブが表示されます。

- [ACI Fabric] タブ

  [ACI Fabric] ペインでは、ペインでは、次の操作を実行できます:

  - [Register a new ACI Fabric / ACI Node] をクリックして、新しい ACI ファブリックまたは ACI ノードを登録します。
  - ファブリックの現在の Cisco APIC 状態に関する情報を表示します。

  （注） プラグインは、Cisco APIC が利用不可であることを検出すると、接続の試行を中止して、ステータスを更新しなくなります。応答しない Cisco APIC に接続しようとしてタイムアウトまで待機するのを避けるには、次の操作を行います。[Reload] をクリックして、Cisco APIC の状態を更新します。これは、利用不可なものも含めて、それぞれの Cisco APIC への再接続を試みます。再び利用可能になっていた場合には、そのステータスは更新されます。

- [Tenants] タブ

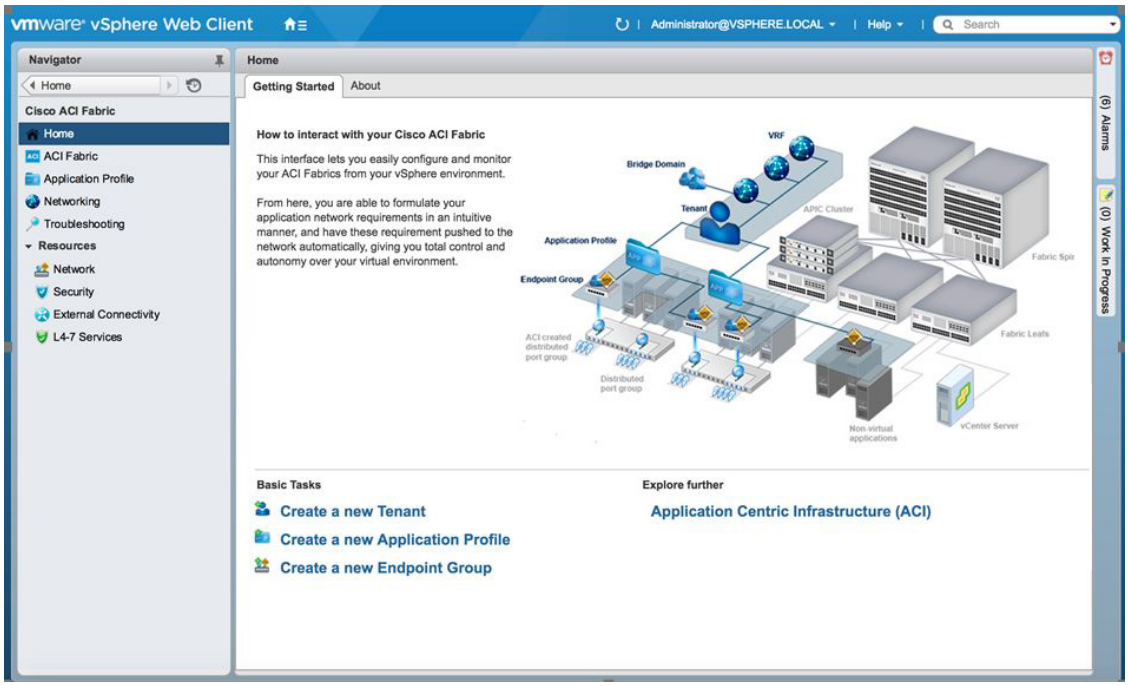
  [Tenants] ペインでは、次の操作を実行できます:

  - 登録済みの ACI ファブリックに存在する別のテナントを管理します。
  - [Create a new Tenant] をクリックして、新しいテナントを作成します。
  - 別のテナントを表示します。

    テーブルでテナントを選択して、[Delete Tenant <テナント名>] をクリックすれば、テナントを削除できます。

    テーブルでテナントを選択して、[<テナント名>] を右クリックし、[Edit settings] を選択すれば、テナントの説明を編集できます。

図 *19 : ACI* ファブリック - ホーム



アプリケーション プロファイル

VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Application Profile]** を選択します。[Work] ペインでは、次の操作を実行できます。

- アクティブなテナントとアプリケーションプロファイルを選択します。
- [Create a new Application Profile] をクリックして、新しいアプリケーション プロファイルを作成します。
- [Drag and drop to configure] セクションで要素をドラッグ アンド ドロップすることにより、アプリケーション プロファイル全体を構成できます。要素は次のとおりです。
  - エンドポイント グループ
  - uSeg
  - L3 外部ネットワーク
  - L2 外部ネットワーク
  - コントラクト
- これらのタブを使用して、ポリシー、トラフィック統計、健全性、障害、監査ログとイベントを表示します。

  [Policy] タブでは、コンシューマとプロバイダ表示またはトラフィック表示に切り替えることができます。

ネットワーキング

VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Networking]** を選択します。[Work] ペインでは、次の操作を実行できます。

- ブリッジ ドメインが設定される分離 VRF を作成することにより、すべてのエンドポイント グループに対する自分独自のアドレッシングをセットアップします。エンドポイント グループは、1 つのブリッジ ドメインに関連付けられます。
- アクティブなテナントを選択します。
- [Drag and drop to configure] セクションで次の要素をドラッグ アンド ドロップします:
  - VRF
  - ブリッジ ドメイン

（注） 使用可能なレイヤ 3 およびレイヤ 2 エンドポイント グループは、ここに表示されますが、構成はできません。

トラブルシューティング

VMware vSphere Web クライアントの [Navigator ペインで、**[Cisco ACI Fabric]** > **[Troubleshooting]** を選択します。[Work] ペインには次のタブが表示されます。

- [Policy Checker] タブ

  [Policy Checker] タブでは、2 つのエンティティ (仮想マシン、エンドポイント グループ、レイヤ 3 の外部ネットワークまたはエンドポイント) を選択して、これら 2 つのエンティティ間で適用される、すべての契約およびレイヤ 4 ～ レイヤ 7 サービスを表示できます。

  2 つのエンドポイント間でトラブルシューティング セッションを開始することもできます。

  - [From]、[To] および [Fix Time] チェック ボックスでセッションのタイム フレームを選択します。
  - [Fix Time] チェック ボックスをオンにして、タイム フレームを設定することができます。
  - [Source Destination] セクションでは、送信元と宛先のエンドポイントを選択できます。[Start Troubleshooting session] をクリックすれば、新しいトラブルシューティング セッションを開始できます。
  - [Troubleshooting Session] では、障害、構成された契約、イベント、監査、およびトラフィック統計を検査することができます。
  - [Traceroute] をクリックすると、2 つのエンドポイント間でのトレース ルートを開始できます。

- 要素の隣にあるアイコンをクリックすると、左ペインで選択した大項目に対応する詳細情報を取得できます。
- エンドポイントごとに、対応する vNIC、VM、およびホスト、および vNIC が接続されている EPG を表すトポロジを取得できます。

- [Virtual Machines] タブ

  このビューでは、仮想マシンのネットワーク インターフェイス カードが、エンドポイントのグループに接続されているかどうかを可視化できます。

  - このリストは、[search] フィールドを使用して制限することができます。
  - VNIC が EPG に接続されている場合は、それぞれの VM を表示できます。
  - 関連付けられている EPG が正常かまたは何らかの問題を抱えているかを迅速に確認し、それが属しているテナントとアプリケーションプロファイルを表示できます。

リソース

- **ネットワーク**

  VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[Network]** を選択します。[Work] ペインには次のタブが表示されます。

  - [Endpoint Groups] タブ

    エンドポイント グループを作成してネットワークインフラストラクチャを設定します。各エンドポイント グループには対応する VMware 分散ポート グループがあり、仮想マシンを接続することができます。異なるエンドポイント グループをアプリケーション プロファイルに編成できます。

    - アクティブなテナントを選択します。
    - [Create a new Application Profile] をクリックして、新しいアプリケーション プロファイルを作成します。
    - テーブルでアプリケーションを選択してから [Create a new Endpoint Group] をクリックして、新しいエンドポイント グループを作成します。
    - テーブルを表示して、アクティブなテナントのアプリケーションプロファイルとエンドポイント グループを確認します。
    - 接続されているすべての VM を表示するには、エンドポイント グループを選択します。

  - [VRFs] タブ

    すべてのエンドポイント グループで、ブリッジ ドメインで設定される分離 VRF を作成することにより、独自のアドレッシングをセットアップできます。エンドポイント グループは、1 つのブリッジ ドメインに関連付けられます。

- アクティブなテナントを選択します。
- [Create a new VRF] をクリックして、新しいVRFを作成します。
- [Create a new Bridge Domain] をクリックして、新しいブリッジ ドメインを作成します。
- VRG を確認するには、テーブルを表示します。

- **セキュリティ**

  VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[Security]** を選択します。[Work] ペインには次のタブが表示されます。

  - [Contracts] タブ

    契約では、異なるエンドポイント グル - プの間、およびエンドポイント グループとレイヤ3およびレイヤ2外部ネットワーク間で、セキュリティ ポリシーを定義できます。

    - アクティブなテナントを選択します。
    - [Create a new Contract] をクリックして、新しい契約を作成します。
    - 契約を確認するには、テーブルを表示します。

  - [Filters] タブ

    フィルタは、(プロトコル、ポートなどに基づく) トラフィックの特定のタイプと一致するエンティティです。これらは、契約により、エンドポイント グループとレイヤ3外部ネットワーク間で承認されるサービスを定義するために用いられます。

    - アクティブなテナントを選択します。
    - [Create a new Filter] をクリックして、新しいフィルタを作成します。
    - フィルタを確認するには、テーブルを表示します。

- **外部接続**

  VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[External Connectivity]** を選択します。[Work] ペインには次のタブが表示されます。

  - [L3 External Networks] タブ

    レイヤ 3 外部ネットワークは、Cisco APIC 管理者が定義します。定義されたネットワークは、自分のインフラストラクチャと外部を接続できるようにするために、自分の契約とレイヤ 4 ～ レイヤ 7 サービスで使用できます。

    - アクティブなテナントを選択します。
    - レイヤ 3 外部ネットワークを確認するには、テーブルを表示します。

- [L2 External Networks] タブ

  レイヤ 2 外部ネットワークは、Cisco APIC 管理者が定義します。定義されたネットワークは、自分のインフラストラクチャと外部を接続できるようにするために、自分の契約とレイヤ 4 ～ レイヤ 7 サービスで使用できます。

  - アクティブなテナントを選択します。
  - レイヤ 2 外部ネットワークを確認するには、テーブルを表示します。

- **L4 ～ 7 サービス**

  VMware vSphere Web クライアントの [Navigator] ペインで、**[Cisco ACI Fabric]** > **[Resources]** > **[External Connectivity]** を選択します。[Work] ペインには次のものが表示されます:

  - レイヤ 4 ～ レイヤ 7 サービスを使えば、エンドポイント グループと外部レイヤ 3 ネットワークの間に、事前プロビジョニングされたファイアウォールとロードバランサを追加できます。
  - アクティブなテナントを選択します。
  - 現在、テナント内に展開されているレイヤ 4 ～ 7 のグラフ インスタンスを確認するには、テーブルを表示します。

GUI のヒント

このセクションでは、GUI のヒントについて説明します。

- テーブルやグラフに表示されている ACI オブジェクトを右クリックすると、関連したアクションが表示されます。
- vCenter プラグインのテーブル内に仮想マシン オブジェクトが表示されている時には、それをダブルクリックすると、vSphere Web クライアントの仮想マシンに移動することができます。

ACI オブジェクトの設定の実行

新しいテナントの作成

この項では、新しいテナントを作成する方法について説明します。

始める前に

ACI ファブリックが登録されていることを確認します。詳細については、クレデンシャルを使用した ACI ファブリックへの VCenter プラグインインの接続 （237 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。
ステップ 2 **Work** ウィンドウで、**Cisco ACI Fabric** を選択します。
ステップ 3 **Navigator** ウィンドウで、**ACI Fabric** を選択します。
ステップ 4 **ACI Fabric** ペインで、**Tenants** タブを選択します。
ステップ 5 **Tenants** ペインで、**Create a new Tenant** をクリックします。
ステップ 6 **New Tenant** ダイアログボックスで、次の操作を実行します:
a) **Enter a name for the Tenant** フィールドに、テナントの名前を入力します。
b) (オプション) **Enter a description for the Tenant** フィールドに、テナントの説明を入力します。
c) [OK] をクリックします。

新しいアプリケーション プロファイルの作成

このセクションでは、新しいアプリケーションプロファイルを作成する方法について説明します。

始める前に

- テナントが作成済みであることを確認します。

  詳細については、新しいテナントの作成 （258 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。
ステップ 2 **[作業]** ペインで、**[Cisco ACI ファブリック]** を選択します。
ステップ 3 **Navigator** ウィンドウで、**Resources** > **Network** を選択します。
ステップ 4 **Network** ウインドウの、**Endpoint Groups** タブの下で、次の操作を実行します:
a) **Tenant** ドロップダウン リストから、テナント名を選択します。
b) **Create a new Application Profile** をクリックします。
ステップ 5 **New Application Profile** ダイアログボックスで、次の操作を実行します:
a) **Name** フィールドに、アプリケーション プロファイルの名前を入力します。
b) (オプション)**Description** フィールドで、アプリケーションプロファイルについての説明を入力します。
c) [OK] をクリックします。

ドラッグ アンド ドロップ方式を使用して EPG を作成する

このセクションでは、ドラッグ アンド ドロップ方式を用いてエンドポイント グループ (EPG) を作成する方法について説明します。

始める前に

- テナントが作成済みであることを確認します。

  詳細については、新しいテナントの作成 （258 ページ）を参照してください。

- アプリケーション プロファイルが作成されたことを確認します。

  詳細については、新しいアプリケーションプロファイルの作成 （259 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Navigator** ウィンドウで、**Application Profile** を選択します。

ステップ 3 **Application Profile** ペインで、次の操作を実行します:

a) **Tenant** フィールドで、ドロップダウン リストからテナントを選択します。

b) **Application Profile** フィールドで、ドロップダウン リストからアプリケーション プロファイルを選択します。

c) **Drag and drop to configure** 要素エリアで、**Endpoint Group** をドラッグ アンド ドロップします。

ステップ 4 **New Endpoint Group** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、エンドポイント グループの名前を入力します。

b) (オプション) **Description** フィールドに、EPGの説明を入力します。

c) **Bridge Domain** フィールドで、一般的なテナントや EPG が作成されたテナントから、ブリッジ ドメインを選択します。デフォルトのブリッジ ドメインは、common/default です。ペンのアイコンをクリックして、別のブリッジ ドメインを選択します。

ステップ 5 **Distributed Switch** フィールドで、次の操作を実行します:

a) 少なくとも 1 つの分散スイッチのチェック ボックスをオンにして、EPG を、センタkした分散 スイッチに接続します。

b) マイクロセグメンテーションを許可するために、**Allow micro-segmentation** チェック ボックスをオンにします。

Allow micro-segmentation チェック ボックスは、分散スイッチが DVS である場合にのみ表示されます。分散スイッチが AVS である場合には、GUI は **Allow micro-segmentation** チェック ボックスを表示しません。分散スイッチが AVS である場合、すべての EPG が基本 EPG であると見なされます。

この方法で基本EPGを作成できます。このEPGに接続されているすべての仮想マシンは、uSeg EPG のマイクロセグメンテーション ルールを適用する候補者となります。マイクロセグメンテーション EPG ルールは、基本 EPG に接続されている仮想マシンにのみ適用されます。

c) EPG を分離する場合には、**Intra EPG isolation** チェック ボックスをオンにします。

これにより、このEPGに接続されている仮想マシン間のすべてのトラフィックを拒否することができます。このルールは、マイクロセグメンテーションEPGの下に表示されるマシンにも適用されます。デフォルトでは、同じEPGのすべての仮想マシンは互いに通信できます。

ステップ 6 **OK** をクリックして、新しい EPG を APIC にプッシュします。

新しい EPG がトポロジ内で作成されたのを確認できます。

ドラッグ アンド ドロップ方式を使用した新規 uSeg EPG の作成

このセクションでは、ドラッグ アンド ドロップ方式を使用して新しい uSeg を作成する方法について説明します。

始める前に

- テナントが作成されたことを確認します。

  詳細については、「新規テナントの作成」を参照してください。

- アプリケーションプロファイルが作成されたことを確認します。

  詳細については、新しいアプリケーション プロファイルの作成（259ページ）を参照してください。

- (Cisco AV ではなく DVS のみ）ベース EPG を作成し、そのベース EPG に対してマイクロ-セグメンテーションに参加する必要があるすべての VM が接続されていることを確認します。詳細については、新しいエンドポイント グループの作成を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。

b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します。

c) **[設定するドラッグ アンド ドロップ]** 要素エリアで、トポロジに uSeg をドラッグ アンド ドロップします。

ステップ 4 **[新しいエンドポイント グループ]** ダイアログ ボックスで、次の操作を実行します。

a) **[名前]** フィールドに、EPG の名前を入力します。
b) **[説明]** フィールドに、EPG の説明を入力します。

ステップ 5 **[分散型スイッチ]** フィールドで、その uSeg EPG に関連付ける必要がある分散型スイッチを選択します。

（注） DVS が 1 個のみ存在する場合、デフォルトで選択されるようにチェック ボックスが表示されません。

ステップ 6 **[ブリッジ ドメイン]** フィールドで、共通または uSeg EPG が作成されるテナントからブリッジ ドメインを選択します。デフォルトのブリッジ ドメインでは、共通/デフォルトです。**[ペン]** アイコンをクリックして、別のブリッジ ドメインを選択します。

ステップ 7 **[EPG 内分離]** チェック ボックスをチェックして、EPG を分離します。

ステップ 8 **[マイクロセグメンテーション]** セクションで、**[+]** アイコンをクリックします。

ステップ 9 **[新しいマイクロセグメンテーション グループ]** ダイアログ ボックスで、次の操作を実行します。

a) **[名前]** フィールドに、新規属性の名前を入力します。
b) （任意） **[説明]** フィールドに、新規属性の説明を入力します。
c) **[タイプ]** セクションで、フィルタ対象のタイプを選択します。
d) **[演算子]** セクションで、**[使用する演算子を含む]** を選択します。
e) 使用可能な場合、手動で値を入力する代わりに、**[参照]** ボタンをクリックして特定のオブジェクトを選択します。
f) **[OK]** をクリックすると、新しい属性が uSeg EPG に追加されます。

ステップ 10 USeg EPG に他の属性を追加するには、ステップ 7 および 8 を繰り返します。

ステップ 11 [OK] をクリックします。

ドラッグ アンド ドロップ方式を使用した 2 つの EPG 間のコントラクトの作成

このセクションでは、ドラッグ アンド ドロップ方式を使用して 2 つのエンドポイント グループ（EPG）間のコントラクトを作成する方法について説明します。

始める前に

- 2 つの EPG が作成されていることを確認します。

  詳細については、ドラッグアンドドロップ方式を使用して EPG を作成する （260 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[作業]** ペインで、**[Cisco ACI ファブリック]** を選択します。

ステップ 3 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 4 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。

b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します。

ステップ 5 **[設定するドラッグ アンド ドロップ方式]** 要素エリアで、送信元 EPG にコントラクトをドラッグ アンド ドロップします。

ステップ 6 宛先 EPG をクリックします。送信元 EPG から宛先 EPG に移動する矢印が表示されます。

ステップ 7 **New Contract** ダイアログボックスで、次の操作を実行します:

a) **[コンシューマ]** フィールドで、正しい EPG が表示されていることを確認します。

b) **[プロバイダ]** フィールドで、正しい EPG が表示されていることを確認します。

c) **[名前]** フィールドに、コントラクトの名前を入力します。

d) （オプション）**[説明]** フィールドにコントラクトの説明を入力します。

e) **[フィルタ]** フィールドで、**[+]** アイコンをクリックして、コントラクトをフィルタします。

f) **[新規]** ダイアログ ボックスで、左のリストから右のリストへ [コントラクト] に追加するすべてのフィルタをドラッグ アンド ドロップして**[OK]** をクリックします。

g) （オプション）**[L4 ～ L7 サービスの設定]** チェック ボックスをオンにして、レイヤ 4 ～ レイヤ 7 サービスを設定します。

h) **[OK]** を選択して、コントラクトを作成します。

ドラッグ アンド ドロップ方式を使用して既存の契約への EPG の追加

このセクションでは、ドラッグ アンド ドロップ方式を使用して、既存のコントラクトに EPG を追加する方法について説明します。

始める前に

- コントラクトが作成されたことを確認します。
- EPG が作成されたことを確認します。

  詳細については、ドラッグ アンド ドロップ方式を使用して EPG を作成する （260 ページ）を参照してください。
- コントラクトが **[アプリケーション プロファイル]** ウィンドウで表示されていることを確認します。たとえば、アプリケーション プロファイルの別の EPG はコントラクトをすで

に使用しています。このケースではない場合、「[Security] タブを使用して既存の契約に EPG を追加する」の手順に従います。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。**[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。

b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します。

ステップ 4 **[設定するドラッグ アンド ドロップ]** 要素エリアで、コントラクトをドラッグ アンド ドロップして、次のいずれかを実行します。

- EPG がコントラクトを消費するには：

  1. **[コントラクト]** をコントラクトが消費する必要がある EPG にドラッグ アンド ドロップします。
  2. 関連するコントラクト（EPG からコントラクトに向かって矢印が表示されます）、EPG がコントラクトを消費するコントラクトをクリックします。

- EPG がコントラクトを提供するには：

  1. 提供する必要があるコントラクトに **[コントラクト]** をドラッグ アンド ドロップします。
  2. 関連するコントラクト（コントラクトから EPG に向かって矢印が表示されます）、EPG がコントラクトを提供する **[コントラクト]** をクリックします。

[Security] タブを使用して既存の契約に EPG を追加する

始める前に

- コントラクトが作成されたことを確認します。
- EPG が作成されたことを確認します。

  詳細については、ドラッグ アンド ドロップ方式を使用して EPG を作成する （260 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Navigator** ペインで、**Resources** > **Security** を選択します。

ステップ 3 **Tenant** ドロップダウン リストから、テナントを選択します。

ステップ 4 契約のリストから、EPG を追加する必要のある契約をクリックします。

ステップ 5 + アイコンを、**Consumers** または **Providers** カラムでクリックします (それぞれ EPG の使用または契約の提供を行います)。

ステップ 6 表示されたオプションで、**Add Endpoint Groups** を選択します。

ステップ 7 ダイアログボックスで、次の操作を実行します。

a) EPG があるテナントを展開します。

b) EPG がある **Application Profile** を展開します。

c) EPG を左側のリストから右側のリストにドラッグ アンド ドロップします。

d) [OK] をクリックします。

L3 外部ネットワークのセット アップ

このセクションでは、レイヤ 3 外部ネットワークに接続する方法について説明します。

（注） レイヤ 3 外部ネットワークのすべての設定を行うことはできません。APIC 内に存在するレイヤ 3 外部ネットワークのみ設定できます。

始める前に

- APIC のレイヤ 3（L3）外部ネットワークが設定されていることを確認します。詳細については、『ACI Basic Configuration』を参照してください。
- EPG が作成されたことを確認します。詳細については、ドラッグ アンド ドロップ方式を使用して EPG を作成する （260 ページ）を参照してください。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します。

b) **[アプリケーション プロファイル]** ドロップダウン リストで、アプリケーション プロファイルを選択します（アプリケーション）。
c) **[設定にドラッグ アンド ドロップ]** 要素エリアで、**[L3 外部ネットワーク]** トポロジにドラッグ アンド ドロップします。

ステップ 4 **[オブジェクトの選択]** ダイアログ ボックスで、テナント<*tenant_name*>（tenant1）を選択し、レイヤ 3 外部ネットワークを選択して、**[OK]** をクリックします。

ステップ 5 **[設定にドラッグ アンド ドロップ]** 要素エリアで、**[コントラクト]** を レイヤ 3 外部ネットワーク上にドラッグ アンド ドロップし、それから EPG (WEB) にドラッグして接続します。

ステップ 6 **New Contract** ダイアログボックスで、次の操作を実行します:

a) **[コンシューマ]** フィールドで、正しい レイヤ 3 外部ネットワーク（l3Ext）が表示されていることを確認します
b) **[プロバイダ]** フィールドで、正しい EPG (WEB) が表示されていることを確認します。
c) **Name** フィールドに、契約の名前 (L3ext-to-WEB) を入力します。
d) （任意） **Description** フィールドに、契約の説明を入力します。
e) **[フィルタ]** フィールドでは、**[+]** アイコンをクリックして、トラフィック フィルタを追加できます。
f) **[新規]** ダイアログ ボックスで、コントラクトに追加するすべてのフィルタを左側のリストから右側のリストにドラッグ アンド ドロップして、**[OK]** をクリックします。
g) （任意） **[L4-7 サービスの設定]** チェック ボックスをオンにして、レイヤ 4 ～ レイヤ 7 サービスを設定します。
h) **[OK]** を選択して、コントラクトを作成します。

コントラクトは、トポロジのレイヤ 3 の外部ネットワークに接続されます。

L2 外部ネットワークの設定

このセクションでは、レイヤ 2 (L2) 外部ネットワークに接続する方法について説明します。

（注） L2 外部ネットワークのすべての設定を行えるわけではありません。APIC 内に存在する L2 外部ネットワークの設定だけを行えます。

始める前に

- APIC で L2 外部ネットワークが設定されていることを確認します。詳細については、『ACI 基本設定ガイド』を参照してください
- EPG が存在することを確認します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[ナビゲータ]** ペインで、**[アプリケーション プロファイル]** を選択します。

ステップ 3 **Application Profile** ペインで、次の手順を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します (tenant1)。

b) **Application Profile** ドロップダウン リストから、[Expenses] を選択します。

c) **Drag and drop to configure** エレメント エリアで、**L2 External Network** をトポロジにドラッグ アンド ドロップします。

d) **Drag and drop to configure** エレメント エリアで、**Contract** を L2 外部ネットワーク上にドラッグ アンド ドロップし、それから EPG (WEB) にドラッグして接続します。

ステップ 4 **New Contract** ダイアログボックスで、次の操作を実行します:

a) **Consumers** フィールドで、正しい L2 外部ネットワーク (L2ext) が表示されていることを確認します

b) **Providers** ィールドで、正しい EPG (WEB) が表示されていることを確認します。

c) **Name** フィールドに、契約の名前 (L2ext-to-WEB) を入力します。

d) **Description** フィールドに、契約の説明を入力します。

e) **[フィルタ]** フィールドでは、**[+]** アイコンをクリックして、トラフィック フィルタを追加できます。

f) **[新規]** ダイアログ ボックスで、コントラクトに追加するすべてのフィルタを左側のリストから右側のリストにドラッグ アンド ドロップして、**[OK]** をクリックします。

g) （任意） **Configure L4-7 service** チェック ボックスをオンにして、Layer 4 to Layer 7 サービスを設定します。

h) [OK] をクリックします。

契約はトポロジの L2 外部ネットワークに接続されます。

ドラッグ アンド ドロップ方式を使用した VRF の作成

このセクションでは、ドラッグ アンド ドロップ方式を使用して VRF を作成する方法について説明します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **[作業]** ウィンドウで **[ネットワーキング]** を選択します。

ステップ 3 **Networking** ペインで、次の操作を実行します:

a) **[テナント]** ドロップダウン リストから、テナントを選択します。

b) **[設定するドラッグ アンド ドロップ]** 要素エリアで VRF をペインにドラッグ アンド ドロップします。

ステップ 4 **[新規 VRF]** ダイアログ ボックスで、次の操作を実行します:

a) **[名前]** フィールドに、VRF の名前を入力します。
b) (オプション)**[説明]** フィールドに、VRF の説明を入力します。
c) **[セキュリティ]** セクションで、[ポリシーの適用] チェック ボックスをオンにします。ポリシーの適用は、セキュリティ ルール（コントラクト）を適用する必要があるか、VRF 用かを決定します。
d) [OK] をクリックします。

ブリッジ ドメインの作成

この項では、ブリッジ ドメインを作成する方法について説明します。

始める前に

- VRF (プライベート ネットワーク) が存在することを確認します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Navigator** ウィンドウで **Networking** を選択します。

ステップ 3 **Networking** ペインで、次の操作を実行します:

a) **Tenant** ドロップダウン リストから、テナントを選択します (tenant1)。
b) **Drag and drop to configure** エレメント エリアで、VRF の上にブリッジ ドメインをドラッグ アンド ドロップします。

ステップ 4 **New Bridge Domain** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、ブリッジ ドメインの名前を入力します (BD2) 。
b) （任意） **Description** フィールドに、論理スイッチの説明を入力します。
c) **Private Subnets** セクションにプライベート サブネット (2.2.2.2/24) を入力し、+ アイコンをクリックしてサブネットをブリッジ ドメインに追加します。
d) （任意） 手順 c と d を繰り返して、必要な数のサブネットをブリッジ ドメインに追加します。
e) [OK] をクリックします。

ブリッジ ドメインは、トポロジ内の VRF に接続します。

エンドポイントの間で新しいトラブルシューティングセッションを開始する

このセクションでは、エンドポイントの間で新しいトラブルシューティングセッションを開始する方法について説明します。

手順

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 **Work** ウィンドウで、**Cisco ACI Fabric** を選択します。

ステップ 3 **Navigator** ウィンドウで、**Troubleshooting** を選択します。

ステップ 4 **Policy Checker** タブの **Session name** セクションに、新しいセッション名を入力します。

ステップ 5 **Source and Destination** セクションで、**Select source** をクリックします。

ステップ 6 表示されるメニューで、**Select Endpoint** をクリックします。

ステップ 7 新たに表示されるダイアログボックスで、送信元として使用するエンドポイントを選択して、**OK** をクリックします。

ステップ 8 **Source and Destination** セクションで、**Select destination** をクリックします。

ステップ 9 表示されるメニューで、**Select Endpoint** をクリックします。

ステップ 10 新たに表示されるダイアログボックスで、宛先として使用するエンドポイントを選択して、OK をクリックします

ステップ 11 **Start Troubleshooting Session** をクリックします。

ステップ 12 **[トラブルシューティング]**ペインでは、障害、構成された契約、イベント、監査、およびトラフィック統計を検査することができます。

トポロジには、各エンドポイント、対応する vNIC、VM、ホスト、および vNIC が接続されている EPG の設定が表示されます。要素の隣にあるアイコンをクリックすると、左ペインで選択した大項目に対応する詳細情報を取得できます。

ステップ 13 **[ナビゲーション]** ウィンドウで、**Traceroute** をクリックして、2 つのエンドポイント間のトレース ルートを開始します。

エンドポイント間の既存のトラブルシューティングセッションの開始

このセクションでは、エンドポイント間の既存のトラブルシューティングセッションを開始する方法について説明します。

始める前に

手順

ステップ 1 VMware vSphere Web クライアントにでログインして、**[作業]** ペインで **[Cisco ACI ファブリック]** を選択します。

ステップ 2 **[ナビゲータ]** ペインで、**[トラブルシューティング]** を選択します。

ステップ 3 **[ポリシー チェッカー]** タブの **[セッション名]** セクションで、**[既存のセッションの選択]** をクリックします。

a) **[セクションの選択]** ダイアログ ボックスで、トラブルシューティング セッション を選択します。

b) [OK] をクリックします。

エンドポイント間のトラブルシューティングのみ実行できます。

ステップ 4 **[トラブルシューティング セッションの開始]** をクリックします。

ステップ 5 **[トラブルシューティング]**ペインでは、障害、構成された契約、イベント、監査、およびトラフィック統計を検査することができます。

トポロジには、各エンドポイント、対応する vNIC、VM、ホスト、および vNIC が接続されている EPG の設定が表示されます。要素の隣にあるアイコンをクリックすると、左ペインで選択した大項目に対応する詳細情報を取得できます。

ステップ 6 **[ナビゲーション]** ウィンドウで、**Traceroute** をクリックして、2つのエンドポイント間のトレース ルートを開始します。

Cisco ACI vCenter プラグインのアンインストール

このセクションでは、VMware vCenter プラグインのアンインストール方法について説明します。

始める前に

- PowerCLI コンソールを利用可能にしておく必要があります。
- `ACIPlugin-Uninstall.ps1` スクリプトを利用可能にしておく必要があります。

  このスクリプトはプラグインアーカイブにあります。次のサイトからダウンロードすることもできます: `https://APIC_IP/vcplugin/ACIPlugin-Uninstall.ps1`.

手順

ステップ 1 PowerCLI コンソールを開きます。

ステップ 2 `ACIPlugin-Uninstall.ps1` スクリプトを実行します。

ステップ 3 要求されたら、**vCenter IP / FQDN** フィールドに、プラグインをアンインストールする vCenter の場所を入力します。

ステップ 4 表示されたダイアログボックスに、vCenter のルート権限のクレデンシャルを入力します。アンインストールが成功した場合、コンソールに次のメッセージが表示されます:

```
[x] Uninstalled ACI vCenter Plugin
```

Cisco ACI vCenter プラグインのアップグレード

このセクションでは、Cisco ACI vCenter プラグインをアップグレードする方法について説明します。

手順

Cisco ACI vCenter プラグインをアップグレードするには、インストールの手順に従う必要があります。

詳細については、Cisco ACI vCenter プラグインのインストール （235 ページ）を参照してください。

Cisco ACI vCenter プラグインのインストールのトラブルシューティング

このセクションでは、Cisco ACI vCenter プラグインのインストールのトラブルシューティングを行う方法について説明します。

VMware vSphere Web クライアント GUI で Cisco ACI vCenter プラグインが表示されない場合は、以下の操作を実行してください:

- vCenter と .zip ファイルをホストしている Web サーバの間で HTTPS/HTTP トラフィックが動作していることを確認して、.zip ファイルが vCenter からダウンロードできるようにします。

- HTTP Web サーバを使用している場合には、HTTP ダウンロードが有効であることを確認します。
- HTTPS を使用している場合には、使用するサムプリントが 正しいことを確認します。
- 次の URL に移動し、登録が行われたかどうかを確認します。

  https://<*VCENTER_IP*>/mob/?moid=ExtensionManager&doPath=extensionList%5b"com%2ecisco%2eaciPlugin"%5d

  Cisco ACI vCenter プラグインの詳細が表示されるはずです。

  そうならず、ページが空白の場合には、登録が成功しなかったことを示します。これは、登録スクリプトの実行中にエラーが発生したことを意味しています。これを解決するには、もう一度インストール手順を実行し、登録スクリプトでエラーが表示されるかどうかに注意する必要があります。
- vSphere Web クライアント ログを確認します。
  - Linux アプライアンス: `/var/log/vmware/vsphere-client/logs/vsphere_client_virgo.log`
  - 5.5 Windows 2008: `C:\ProgramData\VMware\vSphere Web Client\serviceability\logs\vsphere_client_virgo.log`
  - 6.0 Windows 2008: %ALLUSERSPROFILE%\VMware\vCenterServer\logs\vsphere-client\logs\vsphere_client_virgo.log
  - ログで「vcenter-plugin」または「com.cisco.aciPlugin」を検索すると、インストール/アップグレードについての関連情報を見つけられます。

  正常なアップグレードの例:

```
[2016-05-31T19:32:56.780Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004 com.vmware.vise.vim.extension.VcExtensionManager
Downloading plugin package from https://172.23.137.72/vcenter-plugin-2.0.343.6.zip
(no proxy defined)
[2016-05-31T19:32:56.872Z] [INFO ] m-catalog-manager-pool-11128 70002693 100019
200004
com.vmware.vise.vim.cm.CmCatalogManager
Detected service providers (ms):206
[2016-05-31T19:32:56.872Z] [INFO ] m-catalog-manager-pool-11128 70002693 100019
200004
com.vmware.vise.vim.cm.CmCatalogManager
No new locales or service infos to download.
[2016-05-31T19:32:57.678Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004
com.vmware.vise.vim.extension.VcExtensionManager
Done downloading plugin package from https://172.23.137.72/vcenter-plugin-2.0.343.6.zip

[2016-05-31T19:32:58.438Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004
com.vmware.vise.vim.extension.VcExtensionManager
Done expanding plugin package to /etc/vmware/vsphere-client/vc-packages/vsphere-client-
serenity/com.cisco.aciPlugin-2.0.343.6
[2016-05-31T19:32:58.440Z] [INFO ] -extensionmanager-pool-11139 70002693 100019
200004
com.vmware.vise.extensionfw.ExtensionManager
Undeploying plugin package 'com.cisco.aciPlugin:2.0.343.5'.
```

参考資料

Cisco ACI vCenter プラグインの代替インストール

ここでは、Cisco ACI vCenter プラグインのインストール方法について説明します。 vCenter と APIC 間で HTTPS トラフィックをイネーブルにできず、独自の Web サーバを使用して Cisco ACI vCenter プラグイン zip ファイルをホストする場合は、次の手順を実行します。

始める前に

- すべての前提条件が満たされていることを確認してください。

  詳細については、Cisco ACI vCenter プラグイン ソフトウェアの要件 （235 ページ）を参照してください。

  詳細については、必要な APIC の設定 （235 ページ）を参照してください。

- PowerCLI コンソールを用意してください。

  詳細については、VMware のマニュアルを参照してください。

手順

ステップ 1 .zip ファイルを Web サーバーで使用可能にします。

a) Web サーバーが HTTPS でない場合。デフォルトでは、vCenter は HTTPS ソースからのダウンロードのみを許可します。HTTP を許可するには、vCenter の次の構成ファイルを開いて編集します。

- vCenter 5.5 Linux アプライアンス: **/var/lib/vmware/vsphere-client/webclient.properties**
- vCenter 6.0 Linux アプライアンス: **/etc/vmware/vsphere-client/webclient.properties**
- vCenter 5.5 Windows 2008: **%ALLUSERSPROFILE%\VMware\vSphere Web Client\webclient.properties**
- vCenter 6.0 Windows 2008: **C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\webclient.properties**

b) ファイルの最後に **allowHttp=true** を追加します。

c) Web サーバーが HTTPS でない場合は、「**/etc/init.d/vsphere-client restart**」コマンドを使用して vSphere Web Client サービスを再起動します。

ステップ 2 PowerCLI コンソールまたは Python を使用してスクリプトを実行します。

オプション	説明
PowerCLI コンソールを	**1.** PowerCLI コンソールを開きます。

オプション	説明

使用するには	**2.** **ACIPlugin-Install.ps1** スクリプトを実行します。
	プロンプトが表示されたら、次の情報を入力します。
	• **vCenter IP / FQDN** フィールドに、プラグインをインストールする必要のある vCenter を入力します。
	• **Plugin .zip file URL** フィールドに、vCenter でプラグインをダウンロードできる URL を入力します。
	（注） .zip ファイルの名前を変更していないことを確認します。
	• HTTPを使用している場合は、[SHA1 Thumbprint] フィールドを空のままにします。HTTPS を使用している場合は、使用している Web サーバの SHA1 サムプリントを次のいずれかの形式で入力します。
	• コロンで区切る場合：
	`xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx`
	• スペースで区切る場合：
	`xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx`
	（注） Windows の一部のブラウザでは、証明書サムプリントが区切り文字のない単一の文字列（たとえば、xxxxxxxxxxxxxxxxxx）として表示されることがあります。この場合はインストールスクリプトで正しく処理されません。Web サーバの SHA1 サムプリントで、必ずいずれかの正しい形式を使用してください。そうしないと、Cisco ACI vCenter プラグインが見かけ上障害を起こします。
	3. ダイアログボックスで、vCenter のルート権限の資格情報を入力します。

Python を使用するには	（注） Python 2.7.9 以降を使用し、Python 環境に pyvmomi パッケージをインストールする必要があります。 Pythonスクリプトを実行します: **`python deployPlugin.py`** プロンプトが表示されたら、次の情報を入力します。 • **[vCenter IP]** フィールドに、プラグインをインストールする必要のある vCenter を入力します。 • **[vCenter Username & Password]** フィールドに、vCenter のルート権限の資格情報を入力します。 • **Plugin .zip file URL** フィールドに、vCenter でプラグインをダウンロードできる URL を入力します。 .zip ファイルの名前を変更していないことを確認します。

オプション	説明

	• **[Https server thumbprint]** フィールドで、HTTP を使用している場合は、これを空のままにします。それ以外の場合は、使用する Web サーバの SHA1 サムプリントを入力します。フィールドはコロンで区切られています。次に例を示します。
	`D7:9F:07:61:10:B3:92:93:E3:49:AC:89:84:5B:03:80:C1:9E:2F:8B`
	（注） 情報を事前に入力できる **deploy.cfg** ファイルもあります。そのファイルを引数としてスクリプトを実行できます。次に例を示します。
	`$ python deployPlugin.py deploy.cfg`

ステップ 3 登録が完了したら、vSphere Web Client にログインします。

（注） vCenter が Web サーバーからプラグインをダウンロードして展開するため、最初のログインに時間がかかることがあります。

VMware vSphere Web Client がロードされると、**Navigator** ペインに **Cisco ACI Fabric** が表示されます。これにより、ACI ファブリックを管理できます。

（注） プラグインを登録した後、初めて Web クライアントを起動すると、Web クライアントのリロードを要求するエラー メッセージが表示されることがあります。**[Reload]** をクリックしてページを更新すると、エラー メッセージは表示されません。

第 11 章

Cisco ACI with Microsoft SCVMM

この章の内容は、次のとおりです。

Cisco ACI with Microsoft SCVMM について

Application Policy Infrastructure Controller（APIC）は、Microsoft VM 管理システムと統合して、プラットフォームのネットワーク管理機能を拡張します。Cisco Application Centric Infrastructure（ACI）は、Microsoft VM 管理システムの次のレベルで統合されます。

- Cisco ACI with Microsoft System Center Virtual Machine Manager（SCVMM）：Cisco ACI と統合すると、SCVMM はネットワーク管理のために ACI と SCVMM 間の通信を可能にします。

（注） SCVMM から SCVMM HA への移行は、Microsoft ではサポートされません。

- Cisco ACI with Microsoft Windows Azure Pack：Cisco ACI with Microsoft Windows Azure Pack の設定方法については、「Cisco ACI with Microsoft Windows Azure Pack ソリューションの概要 （332 ページ）」を参照してください。

Cisco ACI with Microsoft SCVMM ソリューションの概要

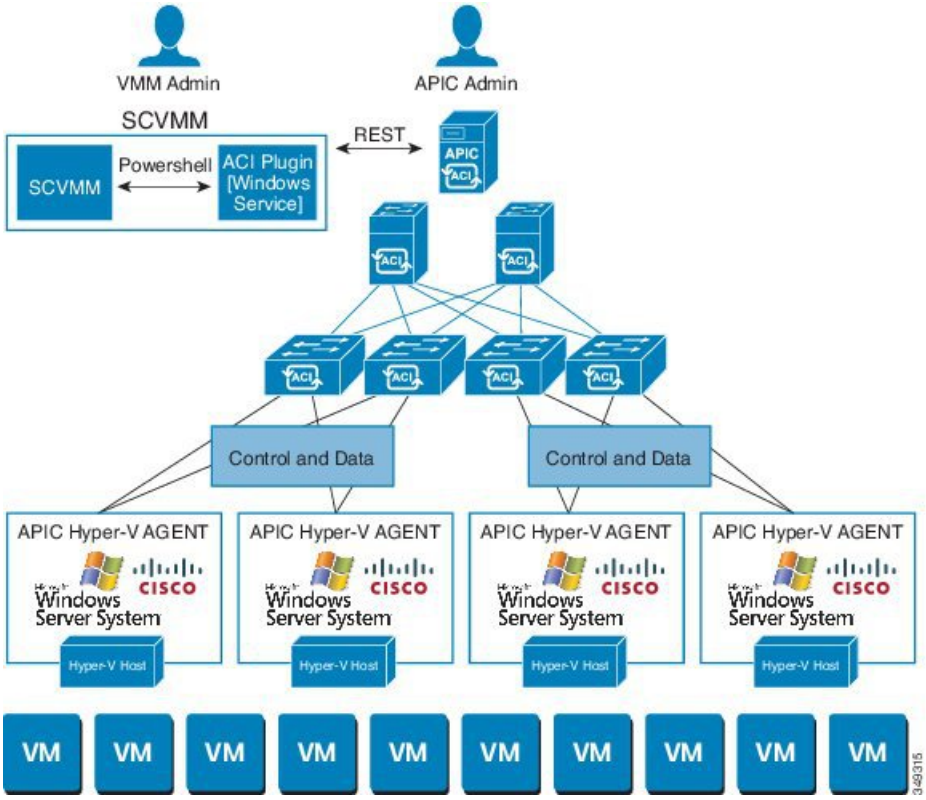
この統合ポイントでは、Application Policy Infrastructure Controller（APIC）と Microsoft System Center Virtual Machine Manager（SCVMM）は、ネットワーク管理のために互いに通信します。エンドポイント グループ（EPG）が APIC で作成され、SCVMM の VM ネットワークとして作成されます。計算は SCVMM でプロビジョニングされ、これらのネットワークを利用できます。

SCVMM の物理トポロジと論理トポロジ

次の図は、Cisco Application Centric Infrastructure（ACI）ファブリックでの一般的な System Center Virtual Machine Manager（SCVMM）導入の典型的なトポロジを示しています。Microsoft SCVMM サービスはスタンドアロン サービスとしてまたは可用性の高いサービスとして、物理ホストや仮想マシンに導入できますが、論理的には APIC と通信する単一の SCVMM インスタンスです。

SCVMM サービスと Application Policy Infrastructure Controller（APIC）との接続は、管理ネットワークを介して行われます。

図 *20 : ACI* ファブリックと *SCVMM* のトポロジ



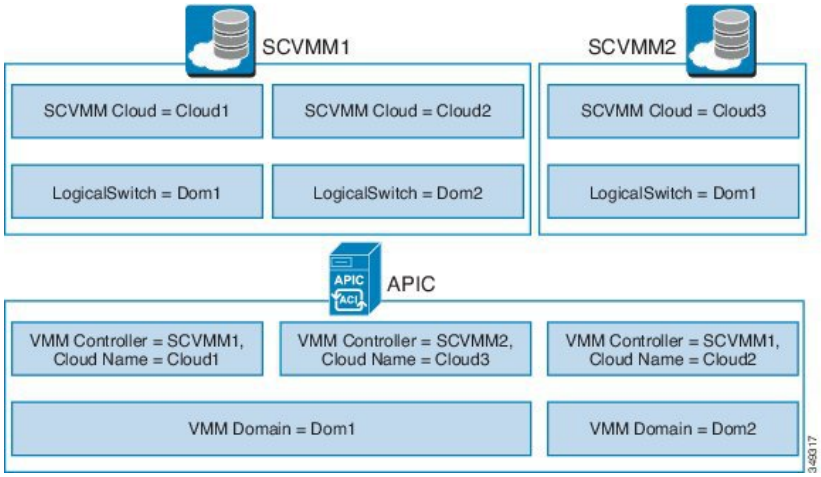
SCVMM での ACI の構造のマッピングについて

ここでは、Microsoft System Center Virtual Machine Manager（SCVMM）での Application Policy Infrastructure Controller（APIC）の構造のマッピングの表と図を示します。

表 *5 : APIC* および *SCVMM* の構造のマッピング

APIC	システム センター
VMM ドメイン	論理スイッチと論理ネットワーク
VMM コントローラ	SCVMM
SCVMM クラウド名	クラウド（ファブリック）
EPG	VM ネットワーク
インフラストラクチャ VLAN	各論理スイッチに1つのインフラストラクチャ VM ネットワーク

図 *21 : ACI* および *SCVMM* の構造のマッピング



マッピングは次のルールに従います。

- 1 つの VMM ドメインを、同じ SCVMM に複数回マッピングすることはできません。

SCVMM ファブリック クラウドとテナント クラウド

Microsoft System Center Virtual Machine Manager（SCVMM）は、論理ファブリックと物理ファブリックのリソース コンテナとして機能する「クラウド」というオブジェクトを提供します。ACI と SCVMM との統合によって、さまざまな論理ネットワークの情報が自動的に作成され、論理ネットワークを指定したクラウドで有効にすることができます。SCVMM との ACI の統合を設定する場合、ファブリック クラウドは Application Policy Infrastructure Controller（APIC）でルート コンテナとして指定するクラウドであり、テナント クラウドはファブリック クラウドに指定されたホスト グループのサブネットを含む SCVMM クラウドです。SCVMM には、論理スイッチの導入に使用するすべてのホスト グループが含まれています。ファブリック クラウドがセットアップされ、論理スイッチがホスト グループ内のホストに導入されると、SCVMM 管理者はテナント クラウドを作成できるようになり、テナント クラウド上で apicLogicalNetwork を有効にして Windows Azure Pack のテナントがファブリック上でテナント ネットワークを作成して導入できるようになります。

例：

```
SCVMM Cloud Name:  Fabric_Cloud
      Host Groups:  All Hosts
            Host Group HumanResources:
                  HyperV Node:  Node-2-24
            Host Group Engineering:
                  HyperV Node:  Node-2-25

SCVMM Cloud Name:  HR_Cloud
      Host Groups: HumanResources

SCVMM Cloud Name:  Engineering_Cloud
      Host Groups:  Engineering
```

Cisco ACI with Microsoft SCVMM の開始

ここでは、Cisco Application Centric Infrastructure（ACI）with Microsoft System Center Virtual Machine Manager（SCVMM）を開始する方法について説明します。

Cisco ACI および 2.2(1) リリース用の Microsoft Integration ファイルをダウンロードして展開します。これは Cisco ACI with Microsoft Windows Azure Pack のインストールの前に実行してください。

1. 次のアドレスのシスコの 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

2. [All Downloads for this Product] を選択します。
3. リリース バージョンと **aci-msft-pkg-2.2.1x.zip** ファイルを選択します。
4. [Download] をクリックします。
5. **aci-msft-pkg-2.2.1x.zip** ファイルを展開します。

（注） Cisco ACI with Microsoft System Center Virtual Machine Manager（SCVMM）は ASCII 文字のみをサポートしています。非 ASCII 文字はサポートしていません。

Windows のシステム ロケールの設定に [English] が設定されていることを確認します。それ以外の場合、ACI with SCVMM はインストールされません。また、システム ロケールのインストール後に英語以外のロケールに変更した場合、APIC および ACI ファブリックと通信すると統合コンポーネントが失敗する場合があります。

Cisco ACI with Microsoft SCVMM の開始の条件

開始する前に、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。

- 管理者コンソールの構築と Microsoft System Center Virtual Machine Manager (SCVMM) バージョンは次のいずれかが満たされていることを確認します。
  - 2016 RTM (ビルド 4.0.1662.0) 以降
  - 更新プログラム ロールアップ 9 (ビルド 3.2.8145.0) と 2012 R2 またはそれ以降
- Windows Server 2016 または 2012 R2 が、Hyper-V ロールが有効化された Hyper-V Server にインストールされていることを確認します。

  Microsoft のマニュアルを参照してください。

- SCVMM でクラウドが設定され、そのクラウドに適切なホストが追加されていることを確認します。

  Microsoft のマニュアルを参照してください。

- インフラストラクチャ VLAN が有効な「default」 AEP が存在することを確認します。
- APIC SCVMM およびホスト エージェント用の Cisco MSI ファイルがあることを確認します。

  Cisco ACI with Microsoft SCVMM の開始 （281 ページ）を参照してください。

- SCVMM のインストールのメンテナンス ウィンドウをスケジュールしたことを確認します。Cisco ACI SCVMM のインストール プロセスにより、現在実行中の SCVMM サービス インスタンスが自動的に再起動されます。

  （注） SCVMM で VM がダイナミック MAC で設定されている場合、SCVMM でこれらの MAC アドレスを認識または検出するのに時間がかかるため、APIC で VM インベントリを更新するのに時間がかかります。

- HYPER-V 管理ツールが HYPER-V ホストとして SCVMM サーバにインストールされていることを確認します。

  HYPER-V 管理ツール機能をインストールするには。

  1. **リモート サーバの管理ツール** 、 **ロールの追加および機能** > **機能** > **リモート サーバの管理ツール** > **ロール Administration Tools** > **HYPER-V 管理ツール** 日と終了しますこの機能をインストールするウィザード。
  2. 各 HYPER-V と SCVMM サーバを繰り返します。

  これは、APIC SCVMM およびホスト エージェントに必要な HYPER-V PowerShell コマンドレットをインストールします。

Cisco ACI with Microsoft SCVMM コンポーネントのインストール、設定、検証

ここでは、Cisco Application Centric Infrastructure（ACI）with Microsoft System Center Virtual Machine Manager（SCVMM）をインストール、設定、および確認する方法を説明します。

コンポーネント	タスク
SCVMM または高可用性 SCVMM への APIC SCVMM エージェントのインストール	SCVMM への APIC SCVMM のエージェントのインストール（284 ページ）を参照してください。 可用性の高い SCVMM への APIC SCVMM エージェントのインストール（285 ページ）を参照してください。 Windows コマンド プロンプトの方法については、Windows のコマンド プロンプトを使用した SCVMM への APIC エージェントのインストール（321 ページ）を参照してください。
OpflexAgent 証明書の生成	APIC OpFlex 証明書の生成（286 ページ）を参照してください。
APIC への OpFlex 証明書ポリシーの追加	APIC への OpFlex 証明書ポリシーの追加（287 ページ）を参照してください。
OpflexAgent 証明書のインストール	OpflexAgent 証明書のインストール（289 ページ）を参照してください。
SCVMM エージェントまたは高可用性 SCVMM の SCVMM エージェントでの APIC クレデンシャルを使用する APIC IP の設定	SCVMM エージェントでの OpflexAgent 証明書を使用した APIC IP 設定の構成（291 ページ）を参照してください。 または 高可用性 SCVMM の SCVMM エージェントでの OpflexAgent 証明書を使用した APIC IP 設定の構成（292 ページ）を参照してください。
Hyper-V サーバへの APIC Hyper-V エージェントのインストール	Hyper-V サーバへの APIC Hyper-V エージェントのインストール（293 ページ）を参照してください。 Windows コマンド プロンプトの方法については、Windows のコマンド プロンプトを使用した Hyper-V Server での APIC Hyper-V エージェントのインストール（322 ページ）を参照してください。

コンポーネント	タスク
SCVMM または高可用性 SCVMM での APIC SCVMM エージェントのインストールの確認	SCVMM での APIC SCVMM エージェントのインストールの確認 （296ページ）を参照してください。 または 高可用性 SCVMM 上の APIC SCVMM エージェントのインストールの確認 （297ページ）を参照してください。
Hyper-V サーバでの APIC Hyper-V エージェントのインストールの確認	Hyper-V サーバでの APIC Hyper-V エージェントのインストールの確認 （298ページ）を参照してください。
SCVMM ドメイン プロファイルの作成	SCVMM ドメイン プロファイルの作成 （299ページ） およびGUI を使用した SCVMM ドメイン プロファイルの作成 （299 ページ） を参照してください。 NX-OS スタイルの CLI を使用する方法については、NX-OS スタイルの CLI を使用した SCVMM ドメイン プロファイルの作成 （323ページ）を参照してください。 REST API を使用する方法については、REST API を使用した SCVMM ドメイン プロファイルの作成 （317ページ）を参照してください。
SCVMM VMM ドメインおよび SCVMM VMM の確認	SCVMM VMM ドメインおよび SCVMM VMM の確認 （302 ページ）を参照してください。
SCVMM のホストへの論理スイッチの導入	SCVMM 上のホストへの論理スイッチの導入 （303 ページ）を参照してください。
テナント クラウドでの論理ネットワークの有効化	テナント クラウドでの論理ネットワークの有効化 （304 ページ）を参照してください。

SCVMM への APIC SCVMM のエージェントのインストール

ここでは、System Center Virtual Machine Manager（SCVMM）に Application Policy Infrastructure Controller（APIC）SCVMM エージェントをインストールする方法を説明します。

手順

ステップ 1 SCVMM サーバに SCVMM 管理者クレデンシャルでログインします。

ステップ 2 SCVMM サーバで、Explorer で **APIC SCVMM Agent.msi** ファイルを見つけます。

ステップ 3 **APIC SCVMM Agent.msi** ファイルを右クリックして [Install] を選択します。

ステップ 4 [Cisco APIC SCVMM Agent Setup] ダイアログボックスで、次の操作を実行します。

a) [Next] をクリックします。

b) [I accept the terms in the License Agreement] チェックボックスにチェックを入れ、[Next] をクリックします。

c) アカウント名とパスワードからなるクレデンシャルを入力します。

SCVMM コンソールに使用したのと同じクレデンシャルを入力します。Cisco APIC SCVMM エージェントで SCVMM 操作を行うには、これらのクレデンシャルが必要です。

インストールプロセスで、入力されたアカウント名とパスワードからなるクレデンシャルが検証されます。インストールが失敗した場合、SCVMM でエラー メッセージが表示され、ユーザは有効なクレデンシャルを再入力する必要があります。

d) アカウント名とパスワードからなるクレデンシャルの検証が成功したら、[Install] をクリックします。

e) [Finish] をクリックします。

可用性の高い SCVMM への APIC SCVMM エージェントのインストール

ここでは、可用性の高い System Center Virtual Machine Manager（SCVMM）に Application Policy Infrastructure Controller（APIC）SCVMM エージェントをインストールする方法について説明します。

手順

ステップ 1 可用性の高い SCVMM インストールの現在の所有者ノードにログインします。

ステップ 2 SCVMM サーバで、File Explorer で **APIC SCVMM Agent.msi** ファイルを見つけます。

ステップ 3 **APIC SCVMM Agent.msi** ファイルを右クリックして [Install] を選択します。

ステップ 4 [Cisco APIC SCVMM Agent Setup] ダイアログボックスで、次の操作を実行します。

a) [Next] をクリックします。

b) [I accept the terms in the License Agreement] チェックボックスにチェックを入れ、[Next] をクリックします。

c) アカウント名とパスワードからなるクレデンシャルを入力します。

SCVMM コンソールに使用したのと同じクレデンシャルを入力します。Cisco APIC SCVMM エージェントで SCVMM 操作を行うには、これらのクレデンシャルが必要です。

インストールプロセスで、入力されたアカウント名とパスワードからなるクレデンシャルが検証されます。インストールが失敗した場合、SCVMM でエラー メッセージが表示され、ユーザは有効なクレデンシャルを再入力する必要があります。

d) アカウント名とパスワードからなるクレデンシャルの検証が成功したら、[Install] をクリックします。

e) [Finish] をクリックします。

ステップ 5 Windows フェールオーバー クラスタのスタンバイ ノードごとに、ステップ 1 から 4 を繰り返します。

APIC OpFlex 証明書の生成

ここでは、Application Policy Infrastructure Controller（APIC）と SCVMM エージェント間の通信をセキュリティで保護する APIC OpFlex 証明書の生成方法について説明します。

（注） これはインストールごとに一度のみ実行してください。

手順

ステップ 1 SCVMM サーバにログインし、**Start** > **Run** > **Windows Powershell** を選択して、アプリケーション バーで **Run as administrator** をクリックします。

ステップ 2 [ACISCVMMPsCmdlets] をロードし、次のコマンドを入力して、新しい OpflexAgent.pfx 証明書ファイルを作成します。

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.INSCISCO> cd \
PS C:\> cd '.\Program Files (x86)\ApicVMMService'
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets

CommandType     Name                       ModuleName
-----------     ----                       ----------
Cmdlet          Get-ACIScvmmOpflexInfo     ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials        ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert         ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert        ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials        ACIScvmmPsCmdlets
```

ステップ 3 次のコマンドを入力して、新しい OpFlex 証明書を生成します。"New-ApicOpflexCert" PowerShell コマンドでは、他のマシンに使用する PFX 証明書のパッケージ ファイルを生成し、ローカル マシンの証明書ストアにこの証明書をインストールします。

```
PS C:\Program Files (x86)\ApicVMMService> $pfxpassword = ConvertTo-SecureString
"MyPassword" -AsPlainText -Force
PS C:\Program Files (x86)\ApicVMMService> New-ApicOpflexCert -ValidNotBefore 1/1/2015
-ValidNotAfter 1/1/2020
-Email t0@domain.com -Country USA -State CA -Locality "San Jose" -Organization MyOrg
-PfxPassword $pfxpassword
Successfully created:
C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx

PS C:\Program Files (x86)\ApicVMMService>
```

ステップ 4 REST API を使用して APIC で使用する証明書情報を表示します。

REST API を使用した、APIC で使用される証明書情報の表示 （287 ページ）を参照してください。

REST API を使用した、APIC で使用される証明書情報の表示

ここでは、REST API を使用して APIC で使用される証明書情報を表示する方法を説明します。

手順

APIC で使用される証明書情報を表示するには、以下を実行します。

```
PS C:\Program Files (x86)\ApicVMMService> $pfxpassword = ConvertTo-SecureString
"MyPassword"
-AsPlainText -Force
PS C:\Program Files (x86)\ApicVMMService> Read-ApicOpflexCert -PfxFile
"C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx" -PfxPassword $pfxpassword
-----BEGIN CERTIFICATE-----
MIIDojCCAoqgAwIBAgIQHz+F2luuOpFKK0p3jxWRfjANBgkqhkiG9w0BAQ0FADBfMRwwGgYJKoZI
hvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkGA1UECAwCQ0ExDDAKBgNV
BAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwHhcNMTUwMTAxMDAwMDAwWhcNMjAwMTAxMDAw
MDAwWjBfMRwwGgYJKoZIhvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkG
A1UECAwCQ0ExDDAKBgNVBAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCzQS3rvrIdxiHfeAUqtX68CdjIL1+nDtqBH8LzDk0RBVb0KU6V
9cYjCAMwW24FJo0PMt4XblvFJDbZUfjWgEY1JmDxqHIAhKIujGsyDoSZdXaKUUv3ig0bzcswEGvx
khGpAJB8BCnODhD3B7Tj0OD8Gl8asd1u24xOy/8MtMDuan/2b32QRmn1uiZhSX3cwjnPI2JQVIif
n68L12yMcp1kJvi6H7RxVOiES33uz00qjxcPbFhsuoFF1eMT1Ng41sTzMTM+xcE6z72zgAYN6wFq
T1pTCLCC+0u/q1yghYu0LBnARCYwDbe2xoa8ClVcL3XYQlEFlp1+HFfd//p1ro+bAgMBAAGjWjBY
MBIGA1UdEwEB/wQIMAYBAf8CAQAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFGuzLCG5
4DEcP+bPiFbiDjMDQ3tMMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQ0FAAOCAQEANc5kKvN4
Q62tIYa1S2HSyiwjaMq7bXoqIH/ICPRqEXu1XE6+VnLnYqpo3TitLmU4G99uz+aS8dySNWaEYghk
8jgLpu39HH6yWxdPiZlcCQ17J5B5vRu3Xjnc/2/ZPqlQDEElobrAOdTko4uAHG4lFBHLwAZA/f72
5fciyb/pjNPhPgpCP0r7svElQ/bjAP1wK8PhCfd7k2rJx5jHr+YX8SCoM2jKyzaQx1BAdufspX3U
7AWH0aF7ExdWy/hW6CduO9NJf+98XNQe0cNH/2oSKYCl9qEK6FesdOBFvCjlRYR9ENqiY4q7xpyB
tqDkBm80V0JslU2xXn+G0yCWGO3VRQ==
-----END CERTIFICATE-----
PS C:\Program Files (x86)\ApicVMMService>
```

APIC への OpFlex 証明書ポリシーの追加

ここでは、Application Policy Infrastructure Controller（APIC）に OpFlex 認証ポリシーを追加する方法について説明します。

手順

AAA ポリシーを追加して、この証明書を APIC サーバで認証できるようにします。GUI または REST Post を使用して、Hyper-V エージェント証明書ポリシーを APIC に追加できます。

- GUI 方式：

1. APIC GUI にログインし、メニュー バーで **[ADMIN]** > **[AAA]** の順に選択します。
2. [Navigation] ペインで、**[Security Management]** > **[Local Users]** の順に選択し、[admin] をクリックします。
3. [PROPERTIES] ペインのドロップダウン リストで **[Actions]** > **[Create X509 Certificate]** の順に選択し、名前とデータを入力します。
4. [Create X509 Certificate] ダイアログボックスで、[Name] フィールドに "**OpflexAgent**" と入力します。
5. SCVMM サーバで、PowerShell の Read-ApicOpflexCert コマンドレットの出力を入力します。
6. Read-ApicOpflexCert コマンドレットを実行するときに、pfx ファイル名の入力を求められたらフル リンク（C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx ）を入力し、パスワードを入力します。
7. 先頭の「-----BEGIN CERTIFICATE-----」から末尾の「-----END CERTIFICATE-----」までコピーして、[DATA] フィールドに貼り付けます。
8. [Submit] をクリックします。
9. [PROPERTIES] ペインの [User Certificates] フィールドの下に、ユーザ証明書が表示されます。

- REST POST 方式 :

```
POST
http://<apic-ip>/api/policymgr/mo/uni/userext/user-admin.json?rsp-subtree=full
{"aaaUserCert":{"attributes":
{"name":"OpflexAgent", "data":"
-----BEGIN CERTIFICATE-----
MIIDojCCAoqgAwIBAgIQHz+F2luuOpFKK0p3jxWRfjANBgkqhkiG9w0BAQ0FADBfMRwwGgYJKoZI
hvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkGA1UECAwCQ0ExDDAKBgNV
BAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwHhcNMTUwMTAxMDAwMDAwWhcNMjAwMTAxMDAw
MDAwWjBfMRwwGgYJKoZIhvcNAQkBFg10MEBkb21haW4uY29tMQ4wDAYDVQQKDAVNeU9yZzELMAkG
A1UECAwCQ0ExDDAKBgNVBAYTA1VTQTEUMBIGA1UEAwwLT3BmbGV4QWdlbnQwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCzQS3rvrIdxiHfeAUqtX68CdjIL1+nDtqBH8LzDk0RBVb0KU6V
9cYjCAMwW24FJo0PMt4XblvFJDbZUfjWgEY1JmDxqHIAhKIujGsyDoSZdXaKUUv3ig0bzcswEGvx
khGpAJB8BCnODhD3B7Tj0OD8Gl8asd1u24xOy/8MtMDuan/2b32QRmn1uiZhSX3cwjnPI2JQVIif
n68L12yMcp1kJvi6H7RxVOiES33uz00qjxcPbFhsuoFF1eMT1Ng41sTzMTM+xcE6z72zgAYN6wFq
T1pTCLCC+0u/q1yghYu0LBnARCYwDbe2xoa8ClVcL3XYQlEFlp1+HFfd//p1ro+bAgMBAAGjWjBY
MBIGA1UdEwEB/wQIMAYBAf8CAQAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFGuzLCG5
4DEcP+bPiFbiDjMDQ3tMMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQ0FAAOCAQEANc5kKvN4
Q62tIYa1S2HSyiwjaMq7bXoqIH/ICPRqEXu1XE6+VnLnYqpo3TitLmU4G99uz+aS8dySNWaEYghk
8jgLpu39HH6yWxdPiZlcCQ17J5B5vRu3Xjnc/2/ZPqlQDEElobrAOdTko4uAHG4lFBHLwAZA/f72
5fciyb/pjNPhPgpCP0r7svElQ/bjAP1wK8PhCfd7k2rJx5jHr+YX8SCoM2jKyzaQx1BAdufspX3U
7AWH0aF7ExdWy/hW6CduO9NJf+98XNQe0cNH/2oSKYCl9qEK6FesdOBFvCjlRYR9ENqiY4q7xpyB
tqDkBm80V0JslU2xXn+G0yCWGO3VRQ==
-----END CERTIFICATE-----
```

OpflexAgent 証明書のインストール

ここでは、OpflexAgent 証明書をインストールする方法について説明します。

手順

ステップ 1 SCVMM サーバに管理者クレデンシャルでログインします。

ステップ 2 次のいずれかの方法を使用します。

- 大規模な展開の場合、グループ ポリシーを使用した証明書の展開について、Microsoft ドキュメントを参照してください。

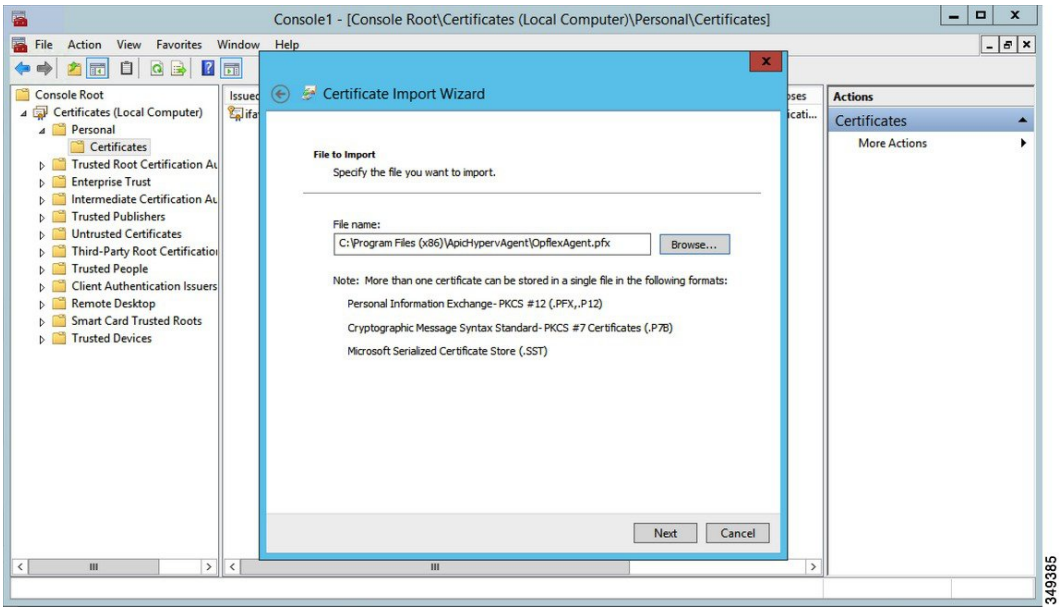
  https://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx。

- 小規模な展開の場合は、次の手順に従います。

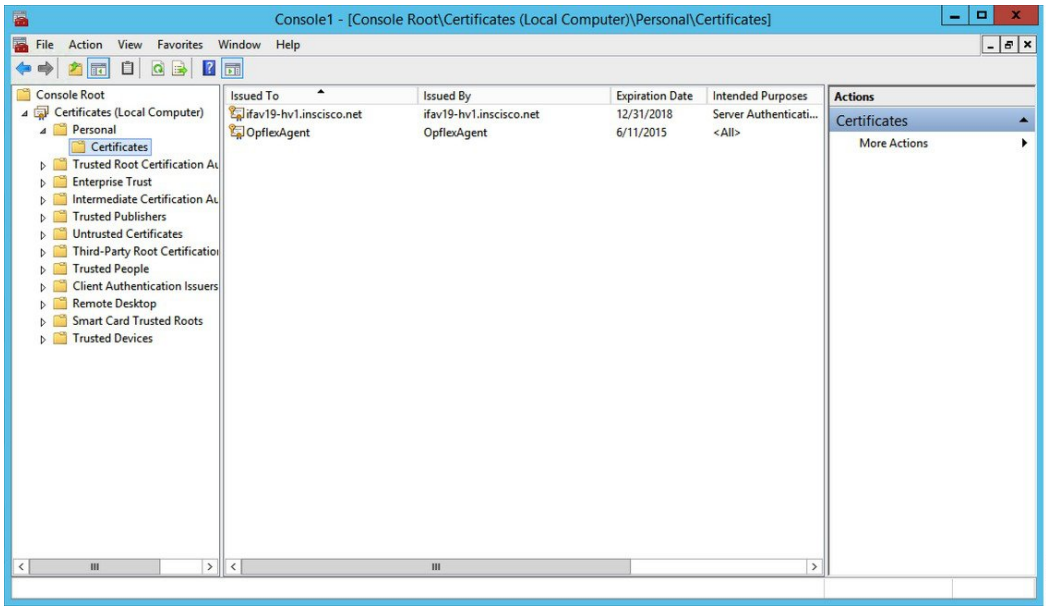
  ローカル マシンに OpFlex セキュリティ証明書を追加する必要があります。Microsoft SCVMM エージェントには **OpflexAgent.pfx** というセキュリティ証明書ファイルがあり、これは SCVMM サーバ上の **C:\Program Files (x86)\ApicVMMService** フォルダにあります。SCVMM サーバで次の手順を実行しない場合、APIC SCVMM エージェントは Application Policy Infrastructure Controller（APIC）と通信できません。

  SCVMM Windows Server 2012 ローカル マシンの証明書リポジトリに、OpFlex セキュリティ証明書をインストールします。各 SCVMM サーバで次の手順を実行して、この証明書をインストールします。

  1. **[Start]** > **[Run]** を選択します。
  2. **mmc** と入力し、**[OK]** をクリックします。
  3. [Console Root] ウィンドウのメニュー バーで、[Add/Remove Snap-in] を選択します。
  4. [Available Snap-ins] フィールドで [Certificates] を選択して [Add] をクリックします。
  5. [Certificates snap-in] ダイアログボックスで [Computer Account] オプション ボタンを選択し、[Next] をクリックします。
  6. [Select Computer] ダイアログボックスで [Local Computer] オプション ボタンを選択し、[Finish] をクリックします。
  7. [OK] をクリックして、[MMC Console] メイン ウィンドウに戻ります。
  8. [MMC Console] ウィンドウで [Certificates (local computer)] をダブルクリックして、ビューを展開します。
  9. [Personal] の下で [Certificates] を右クリックして、**[All Tasks]** > **[Import]** の順に選択します。
  10. [Certificates Import Wizard] ダイアログボックスで、次の操作を実行します。
      1. [Next] をクリックします。
      2. **Opflex Agent** ファイルを参照して [Next] をクリックします。



11. MSI のインストール時に提供された証明書のパスワードを入力します。
12. [Mark this key as exportable.This will allow you to back up or transport your keys at a later time] オプション ボタンを選択する必要があります。
13. [Include all extended properties] オプション ボタンを選択します。
14. [Place all certificates in the following store] オプション ボタンを選択し、[Personal] を見つけて [Next] をクリックします。
15. [Finish] をクリックします。
16. [OK] をクリックします。



ステップ 3 SCVMM サーバごとにステップ 1 ～ 5 を繰り返します。

SCVMM エージェントでの OpflexAgent 証明書を使用した APIC IP 設定の構成

ここでは、System Center Virtual Machine Manager（SCVMM）エージェントで OpflexAgent 証明書を使用して Application Policy Infrastructure Controller（APIC）IP 設定を構成する方法について説明します。

手順

ステップ 1 SCVMM サーバにログインし、**Start** > **Run** > **Windows PowerShell** を選択します。

ステップ 2 次のコマンドを入力して、**ACISCVMMPsCmdlets** をロードします。

例：

（注） GET ApicCredentials と ApicCredentials は現在非推奨であるため、Get-ApicConnInfo と Set-ApicConnInfo を使用します。

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.INSCISCO> cd \
PS C:\> cd '.\Program Files (x86)\ApicVMMService'
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Get-ACIScvmmOpflexInfo                             ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials                                ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert                                 ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert                                ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials                                ACIScvmmPsCmdlets


PS C:\Program Files (x86)\ApicVMMService>
```

ステップ 3 次のコマンドを入力して、APIC 接続パラメータを SCVMM エージェントに設定します。

```
PS C:\Users\administrator.APIC> Set-ApicConnInfo -ApicNameOrIPAddress 172.23.139.224
-CertificateSubjectName OpflexAgent

Apic Credential is successfully set to APIC SCVMM service agent.
```

Set-ApicCredentials に誤った情報を入力した場合、情報を適用できず APIC で検証できません。この情報は保存されません。

```
PS C:\Program Files (x86)\ApicVMMService> Set-ApicConnInfo -ApicNameOrIPAddress
172.23.139.224
-CertificateSubjectName O
pflexAgentWrong
Failed cmdlet with Error: Invalid APIC Connection Settings.
```

```
Set-ApicConnInfo : The remote server returned an error: (400) Bad Request.
At line:1 char:1
+ Set-ApicConnInfo -ApicNameOrIPAddress 172.23.139.224 -CertificateSubjectName Opf ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-ApicConnInfo], WebException
    + FullyQualifiedErrorId : Failed cmdlet with Error: Invalid APIC Connection
Settings.,Cisco.ACI.SCVMM.
    PowerShell.SetApicConnInfo
```

ステップ 4 APIC SCVMM エージェントで APIC 接続パラメータが正しく設定されていることを確認し、次のコマンドを入力します。

```
PS C:\Program Files (x86)\ApicVMMService> Get-ApicConnInfo


EndpointAddress        :
Username               :
Password               :
ApicAddresses          : 172.23.139.224
ConnectionStatus       : Connected
adminSettingsFlags     : 0
certificateSubjectName : OpflexAgent
ExtensionData          :



PS C:\Program Files (x86)\ApicVMMService>
```

高可用性 SCVMM の SCVMM エージェントでの OpflexAgent 証明書を使用した APIC IP 設定の構成

ここでは、System Center Virtual Machine Manager（SCVMM）エージェントで OpflexAgent 証明書を使用して Application Policy Infrastructure Controller（APIC）IP 設定を構成する方法について説明します。

手順

ステップ 1 所有者ノード SCVMM サーバにログインし、**[開始]** > **[実行]** > **[Windows PowerShell]** の順に選択します。

ステップ 2 次のコマンドを入力して、**ACISCVMMPsCmdlets** をロードします。

例：

（注） GET ApicCredentials と ApicCredentials は現在非推奨であるため、Get-ApicConnInfo と Set-ApicConnInfo を使用します。

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.INSCISCO> cd \
PS C:\> cd '.\Program Files (x86)\ApicVMMService'
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets
```

```
CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Get-ACIScvmmOpflexInfo                             ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials                                ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert                                 ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert                                ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo                                   ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials                                ACIScvmmPsCmdlets


PS C:\Program Files (x86)\ApicVMMService>
```

ステップ 3 次のコマンドを入力して、APIC 接続パラメータを SCVMM エージェントに設定します。

```
PS C:\Users\administrator.APIC> Set-ApicConnInfo -ApicNameOrIPAddress 172.23.139.224
-CertificateSubjectName OpflexAgent

Apic Credential is successfully set to APIC SCVMM service agent. 10:25 AM
```

Set-ApicCredentials に誤った情報を入力した場合、情報を適用できず APIC で検証できません。この情報は保存されません。

```
PS C:\Program Files (x86)\ApicVMMService> Set-ApicConnInfo -ApicNameOrIPAddress
172.23.139.224
-CertificateSubjectName O
pflexAgentWrong
Failed cmdlet with Error: Invalid APIC Connection Settings.
Set-ApicConnInfo : The remote server returned an error: (400) Bad Request.
At line:1 char:1
+ Set-ApicConnInfo -ApicNameOrIPAddress 172.23.139.224 -CertificateSubjectName Opf ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-ApicConnInfo], WebException
    + FullyQualifiedErrorId : Failed cmdlet with Error: Invalid APIC Connection
Settings.,Cisco.ACI.SCVMM.
    PowerShell.SetApicConnInfo
```

ステップ 4 APIC SCVMM エージェントで APIC 接続パラメータが正しく設定されていることを確認し、次のコマンドを入力します。

```
PS C:\Program Files (x86)\ApicVMMService> Get-ApicConnInfo


EndpointAddress        :
Username               :
Password               :
ApicAddresses          : 172.23.139.224
ConnectionStatus       : Connected
adminSettingsFlags     : 0
certificateSubjectName : OpflexAgent
ExtensionData
```

Hyper-V サーバへの APIC Hyper-V エージェントのインストール

ここでは、Hyper-V Server に APIC Hyper-V エージェントをインストールする方法を説明します。

始める前に

Hyper-V ノードのダウンタイムをスケジュールしておきます。Hyper-V メンテナンス モードの動作に関する詳細については、https://technet.microsoft.com/en-us/library/hh882398.aspx を参照してください

手順

ステップ 1 SCVMM サーバにログインし、Hyper-V ノードをメンテナンス モードにします。

ステップ 2 管理者クレデンシャルで Hyper-V サーバにログインします。

ステップ 3 Hyper-V Server で、File Explorer で **APIC Hyper-V Agent.msi** ファイルを見つけます。

ステップ 4 **APIC Hyper-V Agent.msi** ファイルを右クリックして、[Install] を選択します。

ステップ 5 [ApicHypervAgent Setup] ダイアログボックスで、次の操作を実行します。

a) [I accept the terms in the License Agreement] チェックボックスをオンにします。

b) [Install] をクリックします。

c) [Finish] をクリックします。

ステップ 6 Microsoft ドキュメントの手順に従って、apicVSwitch 論理スイッチを表示してコンプライアンス状態にします。また、このマニュアルでは、ホスト修復または論理スイッチインスタンス修復も呼ばれています: https://technet.microsoft.com/en-us/library/dn249415.aspx

ステップ 7 次のいずれかの方法を使用します。

- 大規模な展開の場合、グループ ポリシーを使用した証明書の展開について、Microsoft ドキュメントを参照してください。

  https://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx

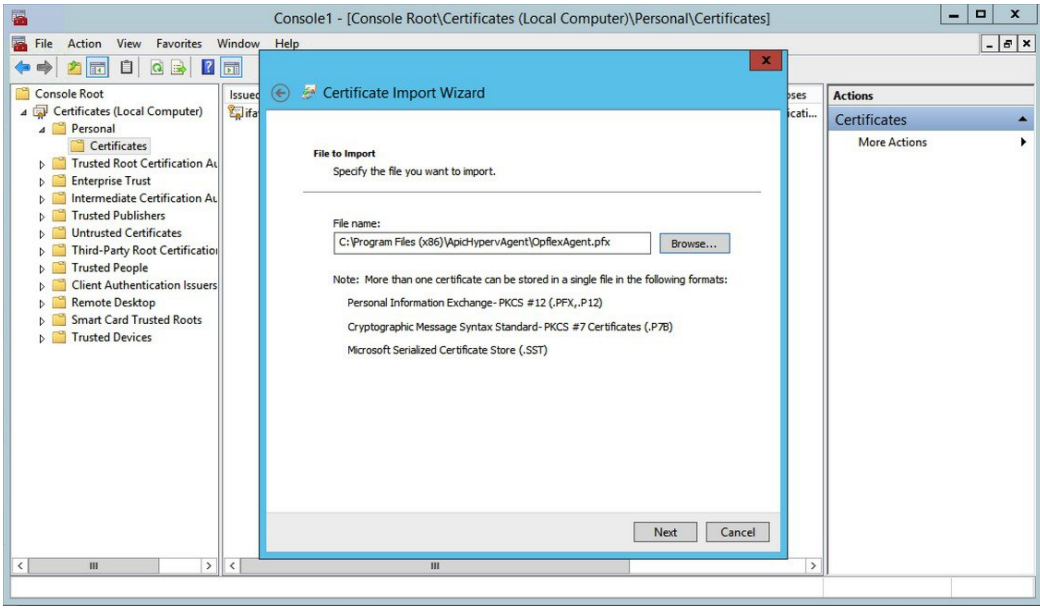
- 小規模な展開の場合は、次の手順に従います。

  ローカル システムに OpFlex セキュリティ証明書を追加する必要があります。Microsoft Hyper-V エージェントには **OpflexAgent.pfx** というセキュリティ証明書ファイルがあり、これは SCVMM サーバ上の **C:\Program Files (x86)\ApicVMMService** フォルダにあります。Hyper-V Server で次の手順を実行しない場合、APIC Hyper-V エージェントは Cisco Application Centric Infrastructure（ACI）ファブリック リーフ スイッチと通信できません。

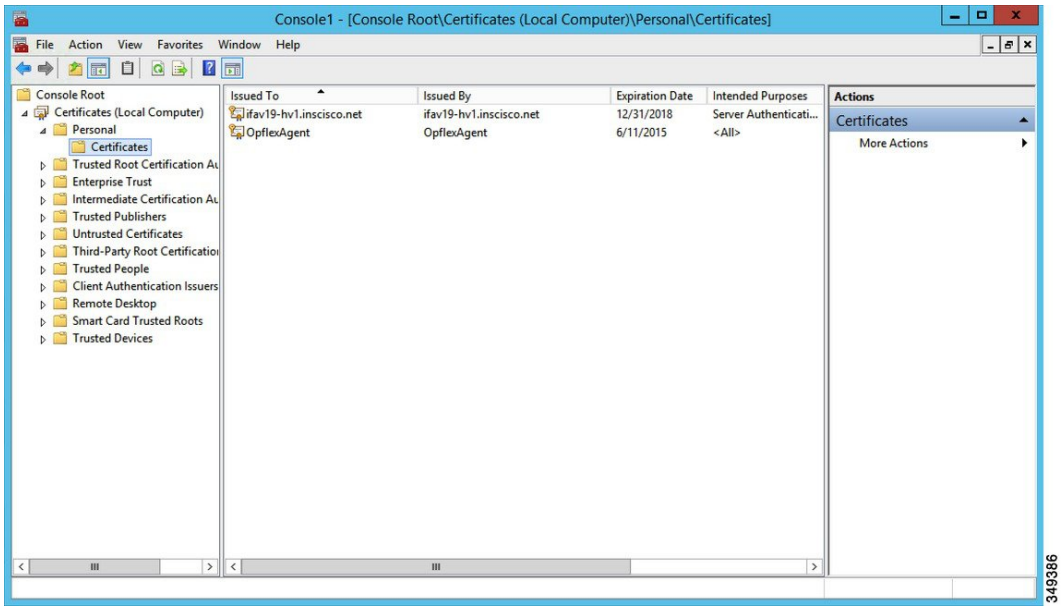
  Hyper-V Windows Server 2012 ローカル マシンの証明書リポジトリに、OpFlex セキュリティ証明書をインストールします。各 Hyper-V Server で次の手順を実行して、この証明書をインストールします。

  1. **[Start]** > **[Run]** を選択します。
  2. **mmc** と入力し、**[OK]** をクリックします。
  3. [Console Root] ウィンドウのメニュー バーで、[Add/Remove Snap-in] を選択します。
  4. [Available Snap-ins] フィールドで [Certificates] を選択して [Add] をクリックします。
  5. [Certificates snap-in] ダイアログボックスで [Computer Account] オプション ボタンを選択し、[Next] をクリックします。

6. [Select Computer] ダイアログボックスで [Local Computer] オプション ボタンを選択し、[Finish] をクリックします。
7. [OK] をクリックして、[MMC Console] メイン ウィンドウに戻ります。
8. [MMC Console] ウィンドウで [Certificates (local computer)] をダブルクリックして、ビューを展開します。
9. [Personal] の下で [Certificates] を右クリックして、**[All Tasks]** > **[Import]** の順に選択します。
10. [Certificates Import Wizard] ダイアログボックスで、次の操作を実行します。
    1. [Next] をクリックします。
    2. **Opflex Agent** ファイルを参照して [Next] をクリックします。



11. MSI のインストール時に提供された証明書のパスワードを入力します。
12. [Mark this key as exportable.This will allow you to back up or transport your keys at a later time] オプション ボタンを選択する必要があります。
13. [Include all extended properties] オプション ボタンを選択します。
14. [Place all certificates in the following store] オプション ボタンを選択し、[Personal] を見つけて [Next] をクリックします。
15. [Finish] をクリックします。
16. [OK] をクリックします。



ステップ 8 SCVMM サーバにログインし、Hyper-V ノードをメンテナンス モードから抜けさせます。

ステップ 9 Hyper-V Server ごとにステップ 1 ～ 8 を繰り返します。

Cisco ACI with Microsoft SCVMM のインストールの確認

SCVMM での APIC SCVMM エージェントのインストールの確認

ここでは、System Center Virtual Machine Manager（SCVMM）上の APIC SCVMM エージェントのインストールを確認する方法を説明します。

手順

ステップ 1 **[Start]** > **[Control Panel]** の順に選択します。

ステップ 2 [Control Panel] ウィンドウで、アドレス バーに [Control Panel\Programs\Programs and Features] と入力します。

ステップ 3 [Cisco APIC SCVMM Agent] を探します。[Cisco APIC SCVMM Agent] が存在する場合、製品はインストールされています。

[Cisco APIC SCVMM Agent] が存在しない場合、製品はインストールされていません。SCVMM への APIC SCVMM のエージェントのインストール （284 ページ）またはWindows のコマンド プロンプトを使用した SCVMM への APIC エージェントのインストール （321 ページ）を参照してください。

ステップ 4 GUI または CLI を使用して、**ApicVMMService** が RUNNING 状態であることを確認します。

- GUI 方式：**[Start]** > **[Run]** の順に選択して **services.msc** を入力します。[Service] ペインで **ApicVMMService** を見つけて、状態が RUNNING であることを確認します。
- CLI 方式：コマンドプロンプトで sc.exe query ApicHypervAgent コマンドを入力し、状態が RUNNING であることを確認します。

```
sc.exe query ApicVMMService

SERVICE_NAME: ApicVMMService
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
```

高可用性 SCVMM 上の APIC SCVMM エージェントのインストールの確認

ここでは、高可用性 System Center Virtual Machine Manager（SCVMM）上の APIC SCVMM エージェントのインストールを確認する方法を説明します。

手順

ステップ 1 **[Start]** > **[Control Panel]** の順に選択します。

ステップ 2 [Control Panel] ウィンドウで、アドレス バーに [Control Panel\Programs\Programs and Features] と入力します。

ステップ 3 [Cisco APIC SCVMM Agent] を探します。[Cisco APIC SCVMM Agent] が存在する場合、製品はインストールされています。

[Cisco APIC SCVMM Agent] が存在しない場合、製品はインストールされていません。SCVMM への APIC SCVMM のエージェントのインストール （284 ページ）またはWindows のコマンドプロンプトを使用した SCVMM への APIC エージェントのインストール （321 ページ）を参照してください。

ステップ 4 GUI または CLI を使用して、**ApicVMMService** が RUNNING 状態であることを確認します。

- GUI 方式：**[Start]** > **[Run]** の順に選択して **services.msc** を入力します。[Service] ペインで **ApicVMMService** を見つけて、状態が RUNNING であることを確認します。
- CLI 方式：コマンドプロンプトで sc.exe query ApicHypervAgent コマンドを入力し、状態が RUNNING であることを確認します。

```
sc.exe query ApicVMMService

SERVICE_NAME: ApicVMMService
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
```

```
    CHECKPOINT : 0x0
    WAIT_HINT : 0x0
```

ステップ 5 **[Start]** > **[PowerShell]** の順に選択して、次のコマンドを入力します。

```
PS C:\Users\administrator.APIC\Downloads> Get-ClusterResource -Name ApicVMMService

Name            State         OwnerGroup          ResourceType
----            -----         ----------          ------------
ApicVMMService  Online        clustervmm07-ha     Generic Service

PS C:\Users\administrator.APIC\Downloads> Get-ClusterCheckpoint -ResourceName
ApicVMMService

Resource        Name
--------        ----
ApicVMMService  SOFTWARE\Wow6432Node\Cisco\Apic

PS C:\Users\administrator.APIC\Downloads> Get-ClusterResourceDependency -Resource
ApicVMMService

Resource        DependencyExpression
--------        --------------------
ApicVMMService  ([VMM Service clustervmm07-ha])
```

Hyper-V サーバでの APIC Hyper-V エージェントのインストールの確認

ここでは、Hyper-V Server 上の APIC Hyper-V エージェントのインストールを確認する方法を説明します。

手順

ステップ 1 **[Start]** > **[Control Panel]** の順に選択します。

ステップ 2 [Control Panel] ウィンドウで、アドレス バーに **[Control Panel\Programs\Programs and Features]** と入力します。

ステップ 3 [Cisco APIC Hyperv Agent] を見つけます。[Cisco APIC Hyperv Agent] が存在する場合、製品はインストールされています。

[Cisco APIC Hyperv Agent] が存在しない場合、製品はインストールされています。Hyper-V サーバへの APIC Hyper-V エージェントのインストール （293 ページ）またはWindows のコマンドプロンプトを使用した Hyper-V Server での APIC Hyper-V エージェントのインストール （322 ページ）を参照してください。

ステップ 4 GUI または CLI を使用して、**ApicHypervAgent** が RUNNING 状態であることを確認します。

- GUI 方式：**[Start]** > **[Run]** の順に選択して **services.msc** を入力します。[Service] ペインで **ApicHypervAgent** を見つけて、状態が RUNNING であることを確認します。
- CLI 方式：コマンドプロンプトで sc.exe query ApicHypervAgent コマンドを入力し、状態が RUNNING であることを確認します。

```
sc.exe query ApicHypervAgent

SERVICE_NAME: ApicHypervAgent
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
```

ACI ポリシーの設定

SCVMM ドメイン プロファイルの作成

ここでは、VMM ドメインの例は、System Center Virtual Machine Manager（SCVMM）ドメインです。タスクの例は次のとおりです。

- VMM ドメイン名と SCVMM コントローラの設定。
- 接続エンティティ プロファイルの作成および VMM ドメインへの関連付け。
- プールの設定。
- すべての設定されたコントローラとそれらの動作状態の確認。

GUI を使用した *SCVMM* ドメイン プロファイルの作成

始める前に

VMM ドメイン プロファイルを作成する前に、Application Policy Infrastructure Controller（APIC）上でインバンドまたはアウトオブバンド管理ネットワークを使用して外部ネットワークへの接続を確立する必要があります。

手順

ステップ 1 ログイン、 APIC GUI のを選択します **仮想ネットワーク** > **インベントリ** 。

ステップ 2 **Navigation** ウィンドウで、**VMM Domains** を展開し、VM プロバイダとして **Microsoft** を右クリックし、**Create SCVMM Domain** を選択します。

ステップ 3 [Create SCVMM domain] ダイアログボックスで、[Name] フィールドに、ドメイン名（productionDC）を入力します。

ステップ 4 オプション: **Delimiter** フィールドに、|、~、**!**、**@**、^、+、または = のいずれかを入力します。記号を入力しなかった場合、ポリシーにシステムのデフォルトのデリミタの|が表示されます。

ステップ 5 [Associated Attachable Entity Profile] フィールドで、ドロップダウン リストから [Create Attachable Entity Profile] を選択し、次の操作を実行して、VMM ドメイン SPAN 間でスイッチ インターフェイスのリストを設定します。

a) [Create Attachable Access Entity Profile] ダイアログボックスの [Profile] 領域で、[Name] フィールドに名前（profile1）を入力し、[Next] をクリックします。
b) [Association to Interfaces] 領域で、[Interface Policy Group] を展開します。
c) [Configured Interface, PC, and VPC] ダイアログボックスの [Configured Interfaces, PC, and VPC] 領域で、[Switch Profile] を展開します。
d) [Switches] フィールドで、ドロップダウン リストから、目的のスイッチ ID（101 および 102）の隣にあるチェックボックスをオンにします。
e) [Switch Profile Name] フィールドに、名前（swprofile1）を入力します。
f) [+] アイコンを展開してインターフェイスを設定します。
g) スイッチのイメージで適切なインターフェイス ポート（インターフェイス 1/1、1/2、1/3）を個別に選択します。
[Interfaces] フィールドに、対応するインターフェイスが自動入力されます。
h) [Interface Selector Name] フィールドに、名前（selector1）を入力します。
i) [Interface Policy Group] フィールドで、ドロップダウン リストから、[Create Interface Policy Group] を選択します。
j) [Create Access Port Policy Group] ダイアログボックスで、[Name] フィールドに、名前（group1）を入力します。
k) [Submit] をクリックします。
l) [Save] をクリックして、もう一度 [Save] をクリックします。
m) [Submit] をクリックします。
n) [Select the interfaces] 領域で、[Select Interfaces] 下の [All] オプション ボタンをクリックします。
o) [vSwitch Policies] フィールドで、[Inherit] オプション ボタンが選択されていることを確認します。
p) [Finish] をクリックします。

[Attach Entity Profile] が選択され、[Associated Attachable Entity Profile] フィールドに表示されます。

ステップ 6 [VLAN Pool] フィールドで、ドロップダウン リストから、[Create VLAN Pool] を選択します。[Create VLAN Pool] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、VLAN プール名（VlanRange）を入力します。
b) [Allocation Mode] フィールドで、[Dynamic Allocation] オプション ボタンが選択されていることを確認します。
c) [Encap Blocks] を展開して、VLAN ブロックを追加します。[Create Ranges] ダイアログボックスで、VLAN の範囲を入力します。

（注） 少なくとも 200 の VLAN 番号の範囲を推奨します。インフラストラクチャ ネットワーク用に予約された VLAN は内部使用が目的のため、この VLAN ID を含む範囲を定義しないでください。

d) [OK] をクリックし、[Submit] をクリックします。

[VLAN Pool] フィールドに、「VlanRange-dynamic」が表示されます。

ステップ 7 [SCVMM] を展開します。[Create SCVMM Controller] ダイアログボックスで、[Type] が [SCVMM] であることを確認して、次の操作を実行します。

a) [Name] フィールドに名前（SCVMM1）を入力します。
b) SCVMM HA クラスタに接続するには、SCVMM HA のインストール時に指定された、SCVMM HA クラスタ IP アドレスまたは SCVMM クラスタ リソース DNS 名を指定します。VMM コンソールを使用して可用性の高い VMM 管理サーバに接続する方法を参照してください。 https://technet.microsoft.com/en-us/library/gg610673.aspx
c) [Host Name (or IP Address)] フィールドに、SCVMM の完全修飾ドメイン名（FQDN）または IP アドレスを入力します。
d) [SCVMM Cloud Name] フィールドに、SCVMM クラウド名（ACI-Cloud）を入力します。
e) [OK] をクリックします。
f) [Create SCVMM Domain] ダイアログボックスで、[Submit] をクリックします。

ステップ 8 次の手順に従って、新しいドメインとプロファイルを確認します。

a) メニュー バーで、**[Virtual Networking]** > **[Inventory]** を選択します。
b) ナビゲーション ウィンドウで、[選択 **VMM ドメイン** > **Microsoft** > **productionDC** > **SCVMM1** 。
c) [Work] ペインで、VMM ドメイン名を表示して、コントローラがオンラインであることを確認します。
d) [Work] ペインに、SCVMM1 のプロパティが動作ステータスとともに表示されます。表示される情報によって、APIC コントローラから SCVMM サーバへの接続が確立され、インベントリが使用できることを確認します。

ポート チャネル ポリシーの設定

ここでは、ポート チャネル ポリシーの設定方法について説明します。

インターフェイス ポート チャネル ポリシーの変更

Cisco ACI SCVMM エージェントは、SCVMM アップリンク ポート プロファイルと集約インターフェイス ポート チャネル ポリシーを同期させ、ポリシーが変更されると自動更新を実行します。

Hyper-V サーバのポリシーを更新するには、次の手順を実行します。

手順

ステップ 1 Cisco APIC GUI にログインし、メニューバーの **[Fabric]** > **[Access Policies]** を選択します。
ステップ 2 [Navigation] ペインで、**[Interfaces]** > **[Leaf Interfaces]** > **[Policy Groups]** を展開します。
ステップ 3 ポリシー グループを選択して、ポリシー グループの名前を確認します。
ステップ 4 ポリシー グループに移動し、要件 (たとえば LACP または MAC Pinning) に基づいて更新します。

ブレード サーバの VMM ドメイン VSwitch ポリシーの上書き

ブレード サーバを ACI ファブリック インターフェイスに接続しているときは、インターフェイスとファブリック インターコネクト間でポート チャネル ポリシーを使用します。ファブリック インターコネクトを LACP 用に設定するときは、MAC Pinning モードの Hyper-V サーバを設定する必要があります。

MAC Pinning モードの Hyper-V サーバを設定するには、次の手順を実行します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで **Virtual Networking** を選択します。

ステップ 2 ナビゲーション ウィンドウで、[展開 **VMM ドメイン** > **Microsoft** > ***Domain_Name*** 。

ステップ 3 [Work] ペインで [ACTIONS] をクリックし、[Create VSwitch Policies] を選択します。

ステップ 4 ポート チャネル ポリシーで、MAC Pinning の既存のポリシーを選択するか、新しいポリシーを作成します。

（注） ホストが論理スイッチにすでに接続されている場合は、SCVMM 管理者は、有効にするアップリンク ポリシーのすべてのホストについて、ホストの修復を行う必要があります。

SCVMM VMM ドメインおよび SCVMM VMM の確認

手順

System Center Virtual Machine Manager コンソール GUI では、新しく作成された SCVMM VMM ドメインおよび VMM コントローラの rootContName（SCVMM クラウド名）に、SCVMM エージェントによって次のオブジェクトが作成されました。

a) 左下のペインで [Fabric] をクリックし、ファブリックの下で次のオブジェクトを確認します。

例：

1. **[Networking]** > **[Logical Switches]** の順に選択し、右側のペインで論理スイッチ名が **apicVSwitch_*VMMdomainName*** であることを確認します。
2. **[Networking]** > **[Logical Networks]** の順に選択し、右側のペインで論理ネットワーク名が **apicLogicalNetwork_*VMMdomainName*** であることを確認します。
3. **[Networking]** > **[Port Profiles]** の順に選択し、右側のペインでポート プロファイル名が **apicUplinkPortProfile_*VMMdomainName*** であることを確認します。

b) 左下のペインで [VMs and Services] をクリックします。

例：

1. [VM Networks] を選択します。
2. 右側のペインで VM ネットワーク名が **apicInfra|10.0.0.30|*SCVMM Controller HostNameORIPAddress filed value|VMMdomainName*** であることを確認します。

   Hyper-V Server で VTEP を作成するには、インフラ VM ネットワークを使用する必要があります。

SCVMM 上のホストへの論理スイッチの導入

ここでは、論理スイッチを System Center Virtual Machine Manager（SCVMM）上のホストに展開する方法を説明します。

（注） SCVMM のアップグレードが実行されてホストがすでに論理スイッチに接続されている場合、ホストからリーフへの接続を確立するには、SCVMM 管理者はすべてのホストに対してホストの修復を行う必要があります。

手順

ステップ 1 SCVMM サーバにログインし、[Navigation] ペインで左下の [Fabric] を選択します。

ステップ 2 [Navigation] ペインで、**[Networking]** > **[Logical Switches]** の順に展開して、論理スイッチが作成されていることを確認します（apicVswitch_cloud1）。

ステップ 3 [Navigation] ペインで左下の [VMs and Services] を選択します。

ステップ 4 [Navigation] ペインで、[All Hosts] を展開します。

ステップ 5 Hyper-V ホスト フォルダ（Dev8）を選択します。

ステップ 6 Hyper-V ホスト（Dev8-HV1）を右クリックして、[Properties] を選択します。

ステップ 7 [Dev8-HV1.inscisco.net Properties] ダイアログボックスで [Virtual Switches] を選択して、次の操作を実行します。

a) [+ New Virtual Switch] を選択します。
b) [New Logical Switch] を選択します。
c) [Logical switch] フィールドで、ドロップダウン リストから論理スイッチ（apicVswitch_cloud1）を選択します。
d) [Adapter] フィールドで、ドロップダウン リストからアダプタ（Leaf1-1-1 - Intel(R) イーサネット サーバ アダプタ X520-2 #2）を選択します。
e) [Uplink Port Profile] フィールドで、ドロップダウン リストからアップリンク ポート プロファイル（apicUplinkPortProfile_Cloud01）を選択します。
f) [New Virtual Network Adapter] をクリックし、名前のない仮想ネットワーク アダプタを選択して、名前（dev8-hv1-infra-vtep）を入力します。
g) [Browse] をクリックします。

h) [Dev8-HV1.inscisco.net Properties] ダイアログボックスで VM ネットワーク（apicInfra| 10.0.0.30 |dev8-scvmm.apic.net|Cloud01）を選択し、[OK] をクリックします。

i) [Virtual Machine Manager] ダイアログボックスで [OK] をクリックします。

ステップ 8 左下で [Job] をクリックします。

ステップ 9 [History] ペインで [Change properties of virtual machine host] ジョブのステータスを調べて、ジョブが完了したことを確認できます。

ステップ 10 Hyper-V Server が SCVMM の適切な Hyper-V ホスト IP アドレスを反映するには、SCVMM 下のホストを更新する必要があります。更新後、APIC GUI には更新された Hyper-V ホスト IP 情報が反映されます。

テナント クラウドでの論理ネットワークの有効化

ここでは、SCVMM テナント クラウドと Cisco ACI を統合できるようにする方法を説明します。詳細については、SCVMM ファブリック クラウドとテナント クラウド（280 ページ）を参照してください。

手順

ステップ 1 SCVMM 管理者クレデンシャルで SCVMM サーバにログインし、SCVMM Admin コンソールを開きます。

ステップ 2 SCVMM Admin コンソールで、[VMs and Services] に移動します。

ステップ 3 [Navigation] ペインで、[Clouds] を展開し、ターゲットのテナント クラウド（HR_Cloud）を右クリックして [Properties] を選択します。

ステップ 4 [Navigation] ペインのポップアップ ウィンドウで、[Logical Networks] を選択します。

a) この SCVMM への VMM ドメインの関連付けの一環として自動的に作成された論理ネットワークを検索します。

b) 論理ネットワーク チェックボックス（apicLogicalNetwork_MyVmmDomain）をクリックします。

c) [OK] をクリックします。

テナント クラウドが [Windows Azure Pack Plan configuration] ページの ACI の統合で使用できるようになりました。

Cisco ACI with Microsoft SCVMM コンポーネントのアップグレード

SCVMM 2016 にアップグレードする場合には、Microsoft の手順を実行してから、Cisco ACI with Microsoft SCVMM コンポーネントをクリーン インストールする必要があります。

前提条件：

SCVMM 2012 R2 にアップグレードする場合には、ACI を 2.2(1) リリースにアップグレードする前に、ACI に統合する Microsoft のサーバーを KB2919355 と KB3000850 更新ロールアップで更新する必要があります。KB2919355 更新ロールアップには 2929781 パッチが含まれています。これは新しい TLS 暗号スイートを追加し、Windows 8.1 および Windows サーバ 2012 R2 での暗号スイートの優先順位を変更します。

次の Microsoft サーバにパッチを適用する必要があります:

- Microsoft Windows Azure パック リソース プロバイダ サーバ
- Microsoft Windows Azure パック テナント サイト サーバ
- Microsoft Windows Azure パック管理サイト サーバ
- Microsoft System Center のサービス プロバイダの基盤/オーケストレーション サーバ
- Microsoft System Center 2012 R2 サーバ
- Microsoft HyperV 2012 R2 サーバ

ACI Microsoft SCVMM コンポーネントのワークフローのアップグレード

ここでは、ACI Microsoft SCVMM コンポーネントのワークフローのアップグレードについて説明します。

手順

ステップ 1 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ます。

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

ステップ 2 SCVMM で APIC SCVMM エージェントをアップグレードするか、高可用性 SCVMM で APIC SCVMM エージェントをアップグレードします。

詳細については、SCVMM での APIC SCVMM エージェントのアップグレード （306 ページ）を参照してください。

詳細については、可用性の高い SCVMM 上の APIC SCVMM エージェントのアップグレード （306 ページ）を参照してください。

ステップ 3 APIC Hyper-V エージェントをアップグレードします。

詳細については、APIC Hyper-V エージェントのアップグレード （307 ページ）を参照してください。

SCVMM での APIC SCVMM エージェントのアップグレード

ここでは、System Center Virtual Machine Manager（SCVMM）で APIC SCVMM エージェントをアップグレードする方法を説明します。

始める前に

Microsoft SCVMM サーバのダウンタイムをスケジュールしておきます。アップグレード プロセスでは Microsoft System Center Virtual Machine Manager サービスが自動的に再起動されるため、SCVMM サービスは一時的に変更またはクエリ要求を処理できなくなります。

手順

SCVMM で APIC SCVMM エージェントをアップグレードします。

リリース 1.1(2x) 以降からアップグレードする場合：

a) SCVMM への APIC SCVMM のエージェントのインストール （284 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

1.1(2x) 以前のリリースからアップグレードする場合：

a) SCVMM への APIC SCVMM のエージェントのインストール （284 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

b) APIC OpFlex 証明書のエクスポート （328 ページ）の手順に従ってください。
c) OpflexAgent 証明書のインストール （289 ページ）の手順に従ってください。
d) SCVMM エージェントでの OpflexAgent 証明書を使用した APIC IP 設定の構成 （291 ページ）または高可用性 SCVMM の SCVMM エージェントでの OpflexAgent 証明書を使用した APIC IP 設定の構成 （292 ページ）の手順に従ってください。

可用性の高い SCVMM 上の APIC SCVMM エージェントのアップグレード

ここでは、高可用性 System Center Virtual Machine Manager（SCVMM）で APIC SCVMM エージェント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 可用性の高い SCVMM インストールのスタンバイ ノードにログインします。

ステップ 2 SCVMM サーバで、File Explorer で **APIC SCVMM Agent.msi** ファイルを見つけます。

ステップ 3 **APIC SCVMM Agent.msi** ファイルを右クリックして [Install] を選択します。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

ステップ 4 [Cisco APIC SCVMM Agent Setup] ダイアログボックスで、次の操作を実行します。

a) [Next] をクリックします。

b) [I accept the terms in the License Agreement] チェックボックスにチェックを入れ、[Next] をクリックします。

c) アカウント名とパスワードからなるクレデンシャルを入力します。

SCVMM コンソールに使用したのと同じクレデンシャルを入力します。Cisco APIC SCVMM エージェントで SCVMM 操作を行うには、これらのクレデンシャルが必要です。

インストールプロセスで、入力されたアカウント名とパスワードからなるクレデンシャルが検証されます。インストールが失敗した場合、SCVMM でエラー メッセージが表示され、ユーザは有効なクレデンシャルを再入力する必要があります。

d) アカウント名とパスワードからなるクレデンシャルの検証が成功したら、[Install] をクリックします。

e) [Finish] をクリックします。

ステップ 5 Windows フェールオーバー クラスタのスタンバイ ノードごとに、ステップ 1 から 4 を繰り返します。

ステップ 6 可用性の高い SCVMM インストールの現在の所有者ノードから、新たなアップグレード スタンバイ ノードの 1 つにフェールオーバーします。

ステップ 7 Windows フェールオーバー クラスタの最終スタンバイ ノードで、ステップ 2 から 4 を繰り返します。

APIC Hyper-V エージェントのアップグレード

ここでは、APIC Hyper-V エージェントをアップグレードする方法について説明します。

始める前に

Hyper-V ノードのダウンタイムをスケジュールしておきます。Hyper-V メンテナンス モードの動作に関する詳細については、https://technet.microsoft.com/en-us/library/hh882398.aspx を参照してください

手順

APIC Hyper-V エージェントをアップグレードします。

リリース 1.1(2x) 以降からアップグレードする場合：

a) Hyper-V サーバへの APIC Hyper-V エージェントのインストール （293 ページ）のステップ 1 ～ 8 に従ってください。ステップ 7 は省略します。OpflexAgent 証明書が Hyper-V ノードにすでにインストールされているため、ステップ 7 はアップグレードには不要です。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

1.1(2x) 以前のリリースからアップグレードする場合：

a) APIC Hyper-V エージェントのアンインストール （390 ページ）の手順に従ってください。
b) Hyper-V サーバへの APIC Hyper-V エージェントのインストール （293 ページ）のステップ 1 ～ 8 に従ってください。ステップ 7 は省略します。OpflexAgent 証明書が Hyper-V ノードにすでにインストールされているため、ステップ 7 はアップグレードには不要です。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

テナントのポリシーの導入

テナント ポリシーの導入の条件

コンピューティング環境が次の条件を満たしていることを確認します。

- APIC SCVMM エージェントがインストールされていることを確認します。

  詳細については、SCVMM への APIC SCVMM のエージェントのインストール （284 ページ）を参照してください。

- APIC Hyper-V エージェントがインストールされていることを確認します。

  詳細については、Hyper-V サーバへの APIC Hyper-V エージェントのインストール （293 ページ）を参照してください。

- 論理スイッチを作成したことを確認します。

  Microsoft のマニュアルを参照してください。

- 仮想スイッチを作成したことを確認します。

  Microsoft のマニュアルを参照してください。

テナントの作成

手順

ステップ 1 メニュー バーで、[TENANTS] を選択し、次の操作を実行します。

a) [Add Tenant] をクリックします。
[Create Tenant] ダイアログボックスが開きます。

b) [Name] フィールドに、テナント名（ExampleCorp）を追加します。

ステップ 2 [Finish] をクリックします。

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。

EPG の作成

ここでは、エンドポイント グループ（EPG）の作成方法について説明します。

手順

ステップ 1 APIC GUI にログインし、メニューバーで **[TENANTS]** > **[Tenant Name]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Tenant Name]** > **[Application Profiles]** > **[Application Profile Name]** の順に展開し、[Application EPGs] を右クリックして [Create Application EPG] を選択します。

ステップ 3 **Create Application EPG** ダイアログボックスで、次の操作を実行します:

a) [Name] フィールドに名前（EPG1）を入力します。

b) [Bridge Domain] フィールドのドロップダウン リストから、ブリッジ ドメインに関連付けるものを選択します。

c) [Associate to VM Domain Profiles] フィールドで、適切なオプション ボタンをクリックし、[Next] をクリックします。

d) [Associated VM Domain Profiles] フィールドの [+] アイコンをクリックし、追加するクラウド（Cloud10）を選択します。

EPG が作成されました。

EPG との Microsoft VMM ドメインの関連付け

ここでは、Microsoft VMM ドメインをエンドポイント グループ（EPG）に関連付けて VM ネットワークを作成する方法を説明します。

始める前に

EPG が作成されていることを確認します。

手順

ステップ 1 APIC GUI にログインし、メニューバーで **[TENANTS]** > **[Tenant Name]** の順に選択します。

ステップ 2 [Navigation] ペインで **[Tenant Name]** > **[Application Profiles]** > **[Application Profile Name]** > **[Application EPGs]** の順に展開して、既存の EPG を選択します。

ステップ 3 [Navigation] ペインで [Domains (VMs and Bare-Metals)] を選択します。

ステップ 4 [Domains (VM and Bare-Metals)] ペインで [ACTIONS] をクリックして、[Add VMM Domain Association] を選択します。

ステップ 5 [Add VMM Domain Association] ダイアログボックスで、[Immediate] または [On Demand] のいずれかについて、[Deploy Immediacy] フィールド オプション ボタンをクリックします。

詳細については、「EPG ポリシーの解決および展開の緊急度 （12 ページ）」を参照してください。

ステップ 6 [Add VMM Domain Association] ダイアログボックスで、[Immediate]、[On Demand] または [Pre-Provision] のいずれかについて、[Resolution Immediacy] フィールド オプション ボタンをクリックします。

詳細については、「EPG ポリシーの解決および展開の緊急度 （12 ページ）」を参照してください。

これで、VM ネットワークが作成されました。

ステップ 7 オプション: **Delimiter** フィールドで、VM ネットワーク名のデリミタに使用する 1 文字として、|、~、!、@、^、+、または = のいずれかを入力します。記号を入力しなかった場合、システムのデフォルトのデリミタである | が使用されます。

APIC で VMM ドメインに関連付けられている EPG の確認

ここでは、Application Policy Infrastructure Controller（APIC）での VMM ドメインとのエンドポイント グループ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 APIC GUI にログインし、メニュー バーで **Virtual Networking** > **Inventory**を選択します。

ステップ 2 ナビゲーション ウィンドウで、**VMM Domains** > **Microsoft** > **Cloud10** > **Controller** > **Controller1** > **Distributed Virtual Switch** > **SCVMM|Tenant|SCVMM|EPG1|Cloud1** を展開します。

新しい VM ネットワーク名の形式は、**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|*Microsoft VMM* ドメイン**です。

ステップ 3 [PROPERTIES] ペインで、VMM ドメインに関連付けられている EPG、VM ネットワーク、および NIC 名、VM 名、IP、MAC、状態などの詳細を確認します。

SCVMM で VMM ドメインに関連付けられている EPG の確認

ここでは、System Center Virtual Machine Manager（SCVMM）で VMM ドメインに関連付けられているエンドポイント グループ（EPG）を確認する方法を説明します。

手順

ステップ 1 デスクトップで [Virual Machine Manager Console] アイコンを開きます。

ステップ 2 左下部ペインで、[VMs and Services] をクリックするか Ctrl+M を押します。

ステップ 3 [VMs and Services] ペインで [VM Networks] をクリックして、VMM ドメインに関連付けられている EPG を確認します。

VMM ドメインに関連付けられている EPG 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| *Microsoft VMM* ドメイン**です。

スタティック IP アドレス プールの作成

スタティック IP アドレス プールは VM テンプレートの導入フェーズ時に Microsoft SCVMM サーバが IP アドレスを仮想マシンに静的に割り当てることができるようにします。この機能によって、DHCP サーバから DHCP アドレスを要求する必要がなくなります。この機能は、ネットワーク内で静的に割り当てられた IP アドレスを必要とするサーバ VM（Windows Active Directory ドメイン コントローラ、DNS サーバ、DHCP サーバ、ネットワーク ゲートウェイなど）の導入によく利用されます。

スタティック IP アドレス プールの詳細については、Microsoft のドキュメント（https://technet.microsoft.com/en-us/library/jj721568.aspx#BKMK_StaticIPAddressPools）を参照してください。

Cisco ACI SCVMM の統合：Cisco APIC は VM ネットワークへのスタティック IP アドレス プールの導入を自動化でき、Microsoft SCVMM サーバ上でのこれらの操作を回避できます。

始める前に

EPG が Microsoft SCVMM VMM ドメインに関連付けられていることを確認します。

手順

ステップ 1 APIC GUI にログインし、メニューバーで **[TENANTS]** > **[Tenant Name]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Tenant Name]** > **[Application Profiles]** > **[Application Profile Name]** > **[Application EPGs]** > ***[Your Target EPG]*** の順に展開し、[Subnets] を右クリックして [Create EPG Subnet] を選択します。

ステップ 3 [Create EPG Subnet] ダイアログボックスで、次の操作を実行します。

a) アドレス/マスクの形式でデフォルトのゲートウェイ IP を入力します。

b) [Submit] をクリックします。

ステップ 4 新しく作成したサブネットを右クリックして [Create Static IP Pool Policy] を選択します。

ステップ 5 [Create Static IP Pool Policy] ダイアログボックスで、次の操作を実行します。

a) [Name (IP)] に入力します。

b) [Start IP] と [End IP] に入力します。

c) オプションの [Static IP Pool policies] に入力します。

[DNS Servers] フィールド、[DNS Search Suffix] フィールド、[Wins Servers] フィールドでは、セミコロンで各エントリを区切ることで、複数のエントリのリストを使用できます。たとえば、[DNS Servers] フィールド内には次のように入力できます。

192.168.1.1;192.168.1.2

（注） 開始IPアドレスと終了IPアドレスを設定するときは、ステップ3で定義したゲートウェイと同じサブネット内にそれらのアドレスがあることを確認します。そうなっていないと、SCVMM へのスタティック IP アドレス プールの導入が失敗します。

指定した EPG に使用されるスタティック IP アドレス プールは 1 つのみです。サブネットの下に複数のスタティック IP プール ポリシーを作成しないでください。他のポリシーが有効になりません。

スタティック IP アドレス プール ポリシーは、VMM ドメインの関連付けに従います。この EPG を同じ VMM ドメイン内の複数の SCVMM コントローラに導入した場合は、同じスタティック IP アドレスが導入されて IP アドレスの重複が発生します。このシナリオでは、重複していないアドレス プールで追加の EPG を導入し、通信に必要なポリシーとコントラクトをエンドポイントに作成します。

NX-OS スタイルの CLI を使用したスタティック IP アドレス プールの作成

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：

```
apic1# config
```

ステップ 2 スタティック IP アドレス プールを作成します。

例：

```
apic1(config)# tenant t0
apic1(config-tenant)# application a0
apic1(config-tenant-app)# epg e0
apic1(config-tenant-app-epg)# mic
microsoft  microsoft-domain
apic1(config-tenant-app-epg)# microsoft static-ip-pool test_pool gateway 1.2.3.4/5
apic1(config-tenant-app-epg-ms-ip-pool)# iprange 1.2.3.4 2.3.4.5
apic1(config-tenant-app-epg-ms-ip-pool)# dns
dnssearchsuffix  dnsservers  dnssuffix
apic1(config-tenant-app-epg-ms-ip-pool)# dnssuffix testsuffix
apic1(config-tenant-app-epg-ms-ip-pool)# exit
apic1(config-tenant-app-epg)# no mi
microsoft  microsoft-domain
apic1(config-tenant-app-epg)# no microsoft static-ip-pool ?
 test_pool
apic1(config-tenant-app-epg)# no microsoft static-ip-pool test_pool gateway ?
 gwAddress  gwAddress
apic1(config-tenant-app-epg)# no microsoft static-ip-pool test_pool gateway 1.2.3.4/5
apic1(config-tenant-app-epg)#
```

ステップ 3 スタティック IP アドレス プールを確認します。

例：

```
apic1(config-tenant-app-epg-ms-ip-pool)# show running-config
# Command: show running-config tenant t0 application a0 epg e0 microsoft static-ip-pool
 test_pool gateway 1.2.3.4/5
# Time: Thu Feb 11 23:08:04 2016
  tenant t0
    application a0
      epg e0
        microsoft static-ip-pool test_pool gateway 1.2.3.4/5
          iprange 1.2.3.4 2.3.4.5
          dnsservers
          dnssuffix testsuffix
          dnssearchsuffix
          winservers
          exit
        exit
      exit
```

仮想マシンの接続および電源投入

ここでは、仮想マシンを接続して電源を入れる方法を説明します。

手順

ステップ 1 SCVMM サーバにログインし、**[VMs and Services]** > **[All Hosts]** の順に選択して、いずれかのホストを選択します。

ステップ 2 [VMs] ペインで、VM ネットワークに関連付ける VM ホストを右クリックして、[Properties] を選択します。

ステップ 3 [Properties] ダイアログボックスで [Hardware Configuration] を選択し、ネットワーク アダプタ（Network Adapter 1）を選択します。

ステップ 4 [Network Adapter 1] ペインで、次の操作を実行して VM ネットワークに接続します。

a) [Connect to a VM network] オプション ボタンをクリックします。
b) [Browse] ボタンをクリックします。
c) ハイパーバイザが関連付けられているすべての VM ネットワークを示す、VM ネットワークのリストを確認します。

ステップ 5 仮想マシンの電源をオンにします。

APIC での関連付けの確認 APIC

ここでは、Application Policy Infrastructure Controller（APIC）で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 APIC GUI にログインし、メニュー バーで **Virtual Networking** > **Inventory**を選択します。

ステップ 2 ナビゲーション ウィンドウで、**VMM Domains** > **Microsoft** > **Cloud10** > **Controller** > **Controller1** > **Hypervisors** > **Hypervisor1** > **Virtual Machines** を展開して、関連づけを確認します。

APIC での EPG の表示 APIC

ここでは、Application Policy Infrastructure Controller（APIC）でエンドポイント グループ（EPG）を表示する方法について説明します。

手順

ステップ 1 APIC GUI にログインし、メニューバーで **[TENANTS]** > **[Tenant Name]** の順に選択します。

ステップ 2 ナビゲーション ウィンドウで、**[Tenant Name]** > **[Application Profiles]** > **[VMM]** > **[Application EPGs]** > **[EPG1]** の順に展開します。

ステップ 3 [Application EPG - EPG1] ペインで [OPERATIONAL] ボタンをクリックし、エンドポイント グループが存在するかどうかを確認します。

Cisco ACI with Microsoft SCVMM のトラブルシューティング

APIC から SCVMM への接続のトラブルシューティング

ApicVMMService ログを使用して、System Center Virtual Machine Manager（SCVMM）サーバをデバッグします。

手順

ステップ 1 SCVMM サーバにログインして、**ApicVMMService** ログに移動します。これは、**C:\Program Files (X86)\ApicVMMService\Logs** にあります。

ステップ 2 **ApicVMMService** ログを確認してデバッグします。

デバッグできない場合は、SCVMM サーバですべての **ApicVMMService** ログを **C:\Program Files (X86)\ApicVMMService\Logs** からコピーして、シスコ テクニカル サポートにお寄せください。

リーフから Hyper-V ホストへの接続のトラブルシューティング

ApicHypervAgent ログを使用して、Hyper-V Server をデバッグします。

手順

ステップ 1 Hyper-V Server にログインして、**ApicHypervAgent** ログに移動します。これは、**C:\Program Files (x86)\ApicHypervAgent\Logs** にあります。

ステップ 2 **ApicHypervAgent** ログを確認してデバッグします。

デバッグできない場合は、Hyper-V Server ですべての **ApicHypervAgent** ログを **C:\Program Files (x86)\ApicHypervAgent\Logs** からコピーして、シスコ テクニカル サポートにお寄せください。

リーフ スイッチを交換した後のトラフィック障害に対応する

SCVMM ホストと統合されたままには、スイッチ リーフ交換はサポートされていません。SCVMM 統合ホストとリーフ スイッチを交換した後、スイッチ内の Vm は Cisco ACI ファブリックを通過するトラフィックを送信できません可能性があります。

SCVMM統合する場合でもホストが置き換えられなかった別のスイッチにVPC、VLANは、交換期間中に一致する Vlan を持たない VPC ピア スイッチがそのスイッチから取得される可能性があります。

これは、新しいシリアル番号を含むこれにより、同じリーフ ID の新しいトンネル エンドポイント (という) の IP アドレスを引き出すためにです。SCVMM ホストは自動的にこの新しい値を更新できません。

リーフ スイッチを交換した後、トラフィックが失敗した場合は、次の手順を実行します。

手順

再起動、 `ApicHypervAgent` すべてのホストにします。

これにより、新しいを再同期し、スイッチを交換した後という IPs を修正するエージェントは可能です。

EPG の設定の問題のトラブルシューティング

エンドポイント グループ（EPG）のライフタイム中、EPG の VLAN ID が APIC で変更された場合、新しい設定を有効にするには、すべての仮想マシンで VLAN 設定を更新する必要があります。

手順

この操作を実行するには、SCVMM サーバで次の PowerShell コマンドを実行します。

例：

```
$VMs = Get-SCVirtualMachine
$VMs | Read-SCVirtualMachine
$NonCompliantAdapters=Get-SCVirtualNetworkAdapter -All | Where-Object
{$_.VirtualNetworkAdapterComplianceStatus -eq "NonCompliant"}
$NonCompliantAdapters | Repair-SCVirtualNetworkAdapter
```

REST API リファレンス

REST API を使用した SCVMM ドメイン プロファイルの作成

ここでは、REST API を使用して SCVMM ドメイン プロファイルを作成する方法を説明します。

手順

ステップ 1 VMM ドメイン名および System Center Virtual Machine Manager（SCVMM）コントローラを設定します。

例：

```
 https://<apic-ip>/api/node/mo/.xml

<polUni>
<vmmProvP vendor="Microsoft">
<!-- VMM Domain -->
<vmmDomP name="productionDC">
<!-- Association to VLAN Namespace -->
<infraRsVlanNs tDn="uni/infra/vlanns-VlanRange-dynamic"/>
<!-- SCVMM IP address information
<vmmCtrlrP name="SCVMM1" hostOrIp="172.21.120.21" rootContName="rootCont01"> -->
</vmmCtrlrP>
</vmmDomP>
</vmmProvP>
```

ステップ 2 VLAN ネームスペースの導入用の接続可能エンティティ プロファイルを作成します。

例：

```
https://<apic-ip>/api/policymgr/mo/uni.xml
<infraInfra>
<infraAttEntityP name="profile1">
<infraRsDomP tDn="uni/vmmp-Microsoft/dom-productionDC"/>
</infraAttEntityP>
</infraInfra>
```

ステップ 3 インターフェイス ポリシー グループおよびセレクタを作成します。

例：

```
https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraAccPortP name="swprofile1ifselector">
        <infraHPortS name="selector1" type="range">
            <infraPortBlk name="blk"
             fromCard="1" toCard="1" fromPort="1" toPort="3">
            </infraPortBlk>
     <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-group1" />
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
```

```
        <infraAccPortGrp name="group1">
            <infraRsAttEntP tDn="uni/infra/attentp-profile1" />
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

ステップ 4 スイッチ プロファイルを作成します。

例：

```
https://<apic-ip>/api/policymgr/mo/uni.xml <infraInfra>
    <infraNodeP name="swprofile1"> <infraLeafS
    name="selectorswprofile11718" type="range"> <infraNodeBlk name="single0"
    from_="101" to_="101"/> <infraNodeBlk name="single1" from_="102"
    to_="102"/> </infraLeafS> <infraRsAccPortP
    tDn="uni/infra/accportprof-swprofile1ifselector"/> </infraNodeP>
    </infraInfra>
```

ステップ 5 VLAN プールを設定します。

例：

```
 https://<apic-ip>/api/node/mo/.xml

<polUni>
<infraInfra>
<fvnsVlanInstP name="VlanRange" allocMode="dynamic">
   <fvnsEncapBlk name="encap" from="vlan-100" to="vlan-400"/>
</fvnsVlanInstP>
</infraInfra>
</polUni>
```

ステップ 6 設定されたすべてのコントローラとそれらの動作状態を検索します。

例：

```
GET:
https://<apic-ip>/api/node/class/vmmAgtStatus.xml

<imdata totalCount="11">
<vmmAgtStatus HbCount="9285" childAction="" dn="uni/vmmp-Microsoft/dom-productionDC
/ctrlr-SCVMM1/AgtStatus-172.21.120.21" lastHandshakeTime="2015-02-24T23:02:51.800+00:00"
 lcOwn="local"
modTs="2015-02-24T23:02:53.695+00:00" monPolDn="uni/infra/moninfra-default"
name="172.21.120.21"
operSt="online" remoteErrMsg="" remoteOperIssues="" status="" uid="15374"/>
</imdata>
```

ステップ 7 1 つのコントローラの下に Hyper-V を取得します。

例：

```
https://<apic-ip>/api/node/class/opflexODev.json?query-target-filter=and(eq(opflexODev.
ctrlrName,'Scale-Scvmm1.inscisco.net'),eq(opflexODev.domName,'Domain1'),ne(opflexODev.isSecondary,'true'))

{"totalCount":"8","subscriptionId":"72057718609018900","imdata":[{"opflexODev":{"attributes":{"childAction"
:"","ctrlrName":"Scale-Scvmm1.inscisco.net","devId":"167807069","devOperIssues":"","devType":"hyperv","dn":"
topology/pod-1/node-191/sys/br-[eth1/43]/odev-167807069","domName":"Domain1","encap":"unknown","features":"0
","hbStatus":"valid-dvs","hostName":"Scale-Hv2.inscisco.net","id":"0","ip":"0.0.0.0","ipAddr":"10.0.136.93",
"isSecondary":"false","lNodeDn":"","lastHandshakeTime":"2015-04-15T17:10:25.684-07:00","lastNumHB":"19772","
lcOwn":"local","mac":"00:00:00:00:00:00","maxMissHb":"0","modTs":"2015-04-15T17:12:09.485-07:00","monPolDn":
"uni/fabric/monfab-default","name":"","numHB":"19772","operSt":"identified","pcIfId":"1","portId":"0","state
":"connected","status":"","transitionStatus":"attached","uid":"15374","updateTs":"0","uuid":"","version":""}
```

}},{"opflexODev":{"attributes":{"childAction":"","ctrlrName":"Scale-Scvmm1.inscisco.net","devId":"167831641"
,"devOperIssues":"","devType":"hyperv","dn":"topology/pod-1/node-191/sys/br-[eth1/43]/odev-167831641","domNa
me":"Domain1","encap":"unknown","features":"0","hbStatus":"valid-dvs","hostName":"Scale-Hv6.inscisco.net","i
d":"0","ip":"0.0.0.0","ipAddr":"10.0.232.89","isSecondary":"false","lNodeDn":"","lastHandshakeTime":"2015-04
-15T17:10:26.492-07:00","lastNumHB":"15544","lcOwn":"local","mac":"00:00:00:00:00:00","maxMissHb":"0","modTs
":"2015-04-15T17:12:10.292-07:00","monPolDn":"uni/fabric/monfab-default","name":"","numHB":"15544","operSt":
"identified","pcIfId":"1","portId":"0","state":"connected","status":"","transitionStatus":"attached","uid":"
15374","updateTs":"0","uuid":"","version":""}}},{"opflexODev":{"attributes":{"childAction":"","ctrlrName":"S
cale-Scvmm1.inscisco.net","devId":"167831643","devOperIssues":"","devType":"hyperv","dn":"topology/pod-1/nod
e-191/sys/br-[eth1/43]/odev-167831643","domName":"Domain1","encap":"unknown","features":"0","hbStatus":"vali
d-dvs","hostName":"Scale-Hv3.inscisco.net","id":"0","ip":"0.0.0.0","ipAddr":"10.0.232.91","isSecondary":"fal
se","lNodeDn":"","lastHandshakeTime":"2015-04-15T17:10:23.268-07:00","lastNumHB":"15982","lcOwn":"local","ma
c":"00:00:00:00:00:00","maxMissHb":"0","modTs":"2015-04-15T17:12:07.068-07:00","monPolDn":"uni/fabric/monfab
-default","name":"","numHB":"15982","operSt":"identified","pcIfId":"1","portId":"0","state":"connected","sta
tus":"","transitionStatus":"attached","uid":"15374","updateTs":"0","uuid":"","version":""}}},{"opflexODev":{
"attributes":{"childAction":"","ctrlrName":"Scale-Scvmm1.inscisco.net","devId":"167807070","devOperIssues":"
","devType":"hyperv","dn":"topology/pod-1/node-191/sys/br-[eth1/43]/odev-167807070","domName":"Domain1","enc
ap":"unknown","features":"0","hbStatus":"valid-dvs","hostName":"Scale-Hv8.inscisco.net","id":"0","ip":"0.0.0
.0","ipAddr":"10.0.136.94","isSecondary":"false","lNodeDn":"","lastHandshakeTime":"2015-04-15T17:10:26.563-0
7:00","lastNumHB":"14219","lcOwn":"local","mac":"00:00:00:00:00:00","maxMissHb":"0","modTs":"2015-04-15T17:1
2:10.364-07:00","monPolDn":"uni/fabric/monfab-default","name":"","numHB":"14219","operSt":"identified","pcIf
Id":"1","portId":"0","state":"connected","status":"","transitionStatus":"attached","uid":"15374","updateTs":
"0","uuid":"","version":""}}},{"opflexODev":{"attributes":{"childAction":"","ctrlrName":"Scale-Scvmm1.inscis
co.net","devId":"167831642","devOperIssues":"","devType":"hyperv","dn":"topology/pod-1/node-191/sys/br-[eth1
/43]/odev-167831642","domName":"Domain1","encap":"unknown","features":"0","hbStatus":"valid-dvs","hostName":
"Scale-Hv4.inscisco.net","id":"0","ip":"0.0.0.0","ipAddr":"10.0.232.90","isSecondary":"false","lNodeDn":"","
lastHandshakeTime":"2015-04-15T17:10:24.978-07:00","lastNumHB":"13947","lcOwn":"local","mac":"00:00:00:00:00
:00","maxMissHb":"0","modTs":"2015-04-15T17:12:08.778-07:00","monPolDn":"uni/fabric/monfab-default","name":"
","numHB":"13947","operSt":"identified","pcIfId":"1","portId":"0","state":"connected","status":"","transitio
nStatus":"attached","uid":"15374","updateTs":"0","uuid":"","version":""}}},{"opflexODev":{"attributes":{"chi
ldAction":"","ctrlrName":"Scale-Scvmm1.inscisco.net","devId":"167807071","devOperIssues":"","devType":"hyper
v","dn":"topology/pod-1/node-190/sys/br-[eth1/43]/odev-167807071","domName":"Domain1","encap":"unknown","fea
tures":"0","hbStatus":"valid-dvs","hostName":"Scale-Hv7.inscisco.net","id":"0","ip":"0.0.0.0","ipAddr":"10.0
.136.95","isSecondary":"false","lNodeDn":"","lastHandshakeTime":"2015-04-15T17:12:10.057-07:00","lastNumHB":
"5708","lcOwn":"local","mac":"00:00:00:00:00:00","maxMissHb":"0","modTs":"2015-04-15T17:12:09.659-07:00","mo
nPolDn":"uni/fabric/monfab-default","name":"","numHB":"5708","operSt":"identified","pcIfId":"1","portId":"0"
,"state":"connected","status":"","transitionStatus":"attached","uid":"15374","updateTs":"0","uuid":"","versi
on":""}}},{"opflexODev":{"attributes":{"childAction":"","ctrlrName":"Scale-Scvmm1.inscisco.net","devId":"167
807067","devOperIssues":"","devType":"hyperv","dn":"topology/pod-1/node-190/sys/br-[eth1/43]/odev-167807067"
,"domName":"Domain1","encap":"unknown","features":"0","hbStatus":"valid-dvs","hostName":"Scale-Hv1.inscisco.
net","id":"0","ip":"0.0.0.0","ipAddr":"10.0.136.91","isSecondary":"false","lNodeDn":"","lastHandshakeTime":"
2015-04-15T17:12:08.637-07:00","lastNumHB":"17659","lcOwn":"local","mac":"00:00:00:00:00:00","maxMissHb":"0"
,"modTs":"2015-04-15T17:12:08.240-07:00","monPolDn":"uni/fabric/monfab-default","name":"","numHB":"17659","o
perSt":"identified","pcIfId":"1","portId":"0","state":"connected","status":"","transitionStatus":"attached",
"uid":"15374","updateTs":"0","uuid":"","version":""}}},{"opflexODev":{"attributes":{"childAction":"","ctrlrN
ame":"Scale-Scvmm1.inscisco.net","devId":"167831644","devOperIssues":"","devType":"hyperv","dn":"topology/po
d-1/node-190/sys/br-[eth1/43]/odev-167831644","domName":"Domain1","encap":"unknown","features":"0","hbStatus
":"valid-dvs","hostName":"Scale-Hv5.inscisco.net","id":"0","ip":"0.0.0.0","ipAddr":"10.0.232.92","isSecondar
y":"false","lNodeDn":"","lastHandshakeTime":"2015-04-15T17:12:09.093-07:00","lastNumHB":"15433","lcOwn":"loc
al","mac":"00:00:00:00:00:00","maxMissHb":"0","modTs":"2015-04-15T17:12:08.695-07:00","monPolDn":"uni/fabric
/monfab-default","name":"","numHB":"15433","operSt":"identified","pcIfId":"1","portId":"0","state":"connecte
d","status":"","transitionStatus":"attached","uid":"15374","updateTs":"0","uuid":"","version":""}}}]}

ステップ 8 1 つの Hyper-V の下に VM を取得します。

例：

```
https://<apic-ip>/api/node/mo/topology/pod-1/node-190/sys/br-[eth1/43]/odev-167807067.
json?query-target=children&target-subtree-class=opflexOVm&subscription=yes
```

{"totalCount":"1","subscriptionId":"72057718609018947","imdata":[{"opflexOVm":{"attributes":{"childAction":"
","ctrlrName":"Scale-Scvmm1.inscisco.net","dn":"topology/pod-1/node-190/sys/br-[eth1/43]/odev-167807067/ovm-

ExtConn_1002_EPG17_003","domName":"Domain1","id":"0","lcOwn":"local","modTs":"2015-04-14T17:36:51.512-07:00"
,"name":"ExtConn_1002_EPG17_003","state":"Powered On","status":"","uid":"15374"}}}]}

ステップ 9 1 つの VM の下に VNIC を取得します。

例：

```
https://<apic-ip>/api/node/class/opflexIDEp.json?query-target-filter=eq(opflexIDEp.
containerName,'ExtConn_1002_EPG17_003')
```

{"totalCount":"4","subscriptionId":"72057718609018983","imdata":[{"opflexIDEp":{"attributes":{"brIfId":"eth1
/43","childAction":"","compHvDn":"","compVmDn":"","containerName":"ExtConn_1002_EPG17_003","ctrlrName":"Scal
e-Scvmm1.inscisco.net","dn":"topology/pod-1/node-190/sys/br-[eth1/43]/idep-00:15:5D:D2:14:84-encap-[vlan-139
8]","domName":"Domain1","domPDn":"","dpAttr":"0","encap":"vlan-1398","epHostAddr":"http://10.0.136.91:17000/
Vleaf/policies/setpolicies","epPolDownloadHint":"all","epgID":"","eppDownloadHint":"always","eppdn":"uni/epp
/fv-[uni/tn-ExtConn_1002/ap-SCVMM/epg-EPG17]","gtag":"0","handle":"0","hypervisorName":"Scale-Hv1.inscisco.n
et","id":"0","instType":"unknown","ip":"0.0.0.0","lcC":"","lcOwn":"local","mac":"00:15:5D:D2:14:84","mcastAd
dr":"0.0.0.0","modTs":"2015-04-14T17:36:50.838-07:00","monPolDn":"uni/fabric/monfab-default","name":"00155DD
21484","pcIfId":"1","portId":"0","scopeId":"0","state":"up","status":"","transitionStatus":"attached","uuid"
:"","vendorId":"Microsoft","vmAttr":"vm-name","vmAttrDn":"","vmAttrOp":"equals","vmAttrOverride":"0","vmmSrc
":"msft"}}},{"opflexIDEp":{"attributes":{"brIfId":"eth1/43","childAction":"","compHvDn":"","compVmDn":"","co
ntainerName":"ExtConn_1002_EPG17_003","ctrlrName":"Scale-Scvmm1.inscisco.net","dn":"topology/pod-1/node-190/
sys/br-[eth1/43]/idep-00:15:5D:D2:14:85-encap-[vlan-1438]","domName":"Domain1","domPDn":"","dpAttr":"0","enc
ap":"vlan-1438","epHostAddr":"http://10.0.136.91:17000/Vleaf/policies/setpolicies","epPolDownloadHint":"all"
,"epgID":"","eppDownloadHint":"always","eppdn":"uni/epp/fv-[uni/tn-ExtConn_1002/ap-SCVMM-Domain1/epg-EPG1]",
"gtag":"0","handle":"0","hypervisorName":"Scale-Hv1.inscisco.net","id":"0","instType":"unknown","ip":"0.0.0.
0","lcC":"","lcOwn":"local","mac":"00:15:5D:D2:14:85","mcastAddr":"0.0.0.0","modTs":"2015-04-14T17:36:51.025
-07:00","monPolDn":"uni/fabric/monfab-default","name":"00155DD21485","pcIfId":"1","portId":"0","scopeId":"0"
,"state":"up","status":"","transitionStatus":"attached","uuid":"","vendorId":"Microsoft","vmAttr":"vm-name",
"vmAttrDn":"","vmAttrOp":"equals","vmAttrOverride":"0","vmmSrc":"msft"}}},{"opflexIDEp":{"attributes":{"brIf
Id":"eth1/43","childAction":"","compHvDn":"","compVmDn":"","containerName":"ExtConn_1002_EPG17_003","ctrlrNa
me":"Scale-Scvmm1.inscisco.net","dn":"topology/pod-1/node-191/sys/br-[eth1/43]/idep-00:15:5D:D2:14:84-encap-
[vlan-1398]","domName":"Domain1","domPDn":"","dpAttr":"0","encap":"vlan-1398","epHostAddr":"http://10.0.136.
91:17000/Vleaf/policies/setpolicies","epPolDownloadHint":"all","epgID":"","eppDownloadHint":"always","eppdn"
:"uni/epp/fv-[uni/tn-ExtConn_1002/ap-SCVMM/epg-EPG17]","gtag":"0","handle":"0","hypervisorName":"Scale-Hv1.i
nscisco.net","id":"0","instType":"unknown","ip":"0.0.0.0","lcC":"","lcOwn":"local","mac":"00:15:5D:D2:14:84"
,"mcastAddr":"0.0.0.0","modTs":"2015-04-14T17:36:50.731-07:00","monPolDn":"uni/fabric/monfab-default","name"
:"00155DD21484","pcIfId":"1","portId":"0","scopeId":"0","state":"up","status":"","transitionStatus":"attache
d","uuid":"","vendorId":"Microsoft","vmAttr":"vm-name","vmAttrDn":"","vmAttrOp":"equals","vmAttrOverride":"0
","vmmSrc":"msft"}}},{"opflexIDEp":{"attributes":{"brIfId":"eth1/43","childAction":"","compHvDn":"","compVmD
n":"","containerName":"ExtConn_1002_EPG17_003","ctrlrName":"Scale-Scvmm1.inscisco.net","dn":"topology/pod-1/
node-191/sys/br-[eth1/43]/idep-00:15:5D:D2:14:85-encap-[vlan-1438]","domName":"Domain1","domPDn":"","dpAttr"
:"0","encap":"vlan-1438","epHostAddr":"http://10.0.136.91:17000/Vleaf/policies/setpolicies","epPolDownloadHi
nt":"all","epgID":"","eppDownloadHint":"always","eppdn":"uni/epp/fv-[uni/tn-ExtConn_1002/ap-SCVMM-Domain1/ep
g-EPG1]","gtag":"0","handle":"0","hypervisorName":"Scale-Hv1.inscisco.net","id":"0","instType":"unknown","ip
":"0.0.0.0","lcC":"","lcOwn":"local","mac":"00:15:5D:D2:14:85","mcastAddr":"0.0.0.0","modTs":"2015-04-14T17:
36:50.932-07:00","monPolDn":"uni/fabric/monfab-default","name":"00155DD21485","pcIfId":"1","portId":"0","sco
peId":"0","state":"up","status":"","transitionStatus":"attached","uuid":"","vendorId":"Microsoft","vmAttr":"
vm-name","vmAttrDn":"","vmAttrOp":"equals","vmAttrOverride":"0","vmmSrc":"msft"}}}]}

参考資料

Windowsのコマンドプロンプトを使用したSCVMMへのAPICエージェントのインストール

ここでは、Windows のコマンド プロンプトを使用して、System Center Virtual Machine Manager（SCVMM）に APIC エージェントをインストールする方法を説明します。

手順

ステップ 1 SCVMM サーバに SCVMM 管理者クレデンシャルでログインします。

ステップ 2 コマンド プロンプトを起動し、**APIC SCVMM Agent.msi** ファイルをコピーしたフォルダを変更し、以下のコマンドを実行します。

例：

```
C:\>cd MSIPackage

C:\MSIPackage>dir
Volume in drive C has no label.
Volume Serial Number is 726F-5AE6

Directory of C:\MSIPackage

02/24/2015  01:11 PM    <DIR>          .
02/24/2015  01:11 PM    <DIR>          ..
02/24/2015  05:47 AM         3,428,352 APIC SCVMM Agent.msi
               1 File(s)      3,428,352 bytes
               2 Dir(s)  37,857,198,080 bytes free

C:\MSIPackage>msiexec.exe /I "APIC SCVMM Agent.msi" /Qn ACCOUNT="inscisco\Administrator"

PASSWORD="MyPassword" /log "C:\InstallLog.txt"
C:\MSIPackage>sc.exe query ApicVMMService

     SERVICE_NAME: ApicVMMService
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

ステップ 3 **msiexec.exe** インストーラ パッケージが成功した場合、警告またはエラー メッセージなしで終了します。失敗した場合、適切な警告またはエラー メッセージが表示されます。

Windows のコマンド プロンプトを使用した Hyper-V Server での APIC Hyper-V エージェントのインストール

ここでは、Windows のコマンド プロンプトを使用して Hyper-V サーバに APIC Hyper-V エージェントをインストールする方法を説明します。

手順

ステップ 1 管理者クレデンシャルで Hyper-V サーバにログインします。

ステップ 2 コマンド プロンプトを起動し、APIC Hyper-V Agent.msi ファイルをコピーしたフォルダに変更し、以下のコマンドを実行します。

例：

```
C:\>cd MSIPackage

C:\MSIPackage>dir
Volume in drive C has no label.
Volume Serial Number is C065-FB79

Directory of C:\MSIPackage

02/24/2015  01:11 PM    <DIR>          .
02/24/2015  01:11 PM    <DIR>          ..
02/24/2015  05:44 AM           958,464 APIC Hyper-V Agent.msi
               1 File(s)        958,464 bytes
               2 Dir(s)  749,486,202,880 bytes free

C:\MSIPackage>msiexec.exe /I "APIC Hyper-V Agent.msi" /log "C:\InstallLog.txt"

C:\MSIPackage>msiexec.exe /I "APIC Hyper-V Agent.msi" /Qn /log "C:\InstallLog.txt"

C:\MSIPackage>sc.exe query ApicHyperVAgent

SERVICE_NAME: ApicHyperVAgent
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

ステップ 3 各 Hyper-V サーバについてステップ 1 ～ 2 を繰り返します。

msiexec.exe インストーラ パッケージが成功した場合、警告またはエラー メッセージなしで終了します。失敗した場合、適切な警告またはエラー メッセージが表示されます。

NX-OS スタイルの CLI を使用した SCVMM ドメイン プロファイルの作成

ここでは、コマンドライン インターフェイス（CLI）を使用して SCVMM ドメイン プロファイルを作成する方法を説明します。

手順

ステップ 1 NX-OS スタイルの CLI で、vlan-domain を設定して VLAN 範囲を追加します。

例：

```
apic1# configure
apic1(config)# vlan-domain vmm_test_1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
```

ステップ 2 vlan-domain にインターフェイスを追加します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# vlan-domain member vmm_test_1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 3 Microsoft SCVMM ドメインを作成し、事前に作成した vlan-domain をそのドメインに関連付けます。このドメインに SCVMM コントローラを作成します。

例：

```
apic1(config)# microsoft-domain mstest
apic1(config-microsoft)# vlan-domain member vmm_test_1
apic1(config-microsoft)# scvmm 134.5.6.7 cloud test
apic1#
```

プログラマビリティのリファレンス

ACI SCVMM PowerShell コマンドレット

ここでは、Cisco Application Centric Infrastructure（ACI）System Center Virtual Machine Manager（SCVMM）PowerShell のコマンドレット、ヘルプ、および例を示します。

手順

ステップ 1 SCVMM サーバにログインし、**Start** > **Run** > **Windows PowerShell** を選択します。

ステップ 2 次のコマンドを入力します。

例：

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\ApicVMMService> cd C:\Program Files (x86)\ApicVMMService>
PS C:\Program Files (x86)\ApicVMMService> Import-Module .\ACIScvmmPsCmdlets.dll
PS C:\Program Files (x86)\ApicVMMService> Add-Type -Path .\Newtonsoft.Json.dll
PS C:\Program Files (x86)\ApicVMMService> Get-Command -Module ACIScvmmPsCmdlets

CommandType     Name                       ModuleName
-----------     ----                       ----------
Cmdlet          Get-ACIScvmmOpflexInfo     ACIScvmmPsCmdlets
Cmdlet          Get-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Get-ApicCredentials        ACIScvmmPsCmdlets
Cmdlet          New-ApicOpflexCert         ACIScvmmPsCmdlets
Cmdlet          Read-ApicOpflexCert        ACIScvmmPsCmdlets
Cmdlet          Set-ApicConnInfo           ACIScvmmPsCmdlets
Cmdlet          Set-ApicCredentials        ACIScvmmPsCmdlets
```

ステップ 3 ヘルプを生成します。

例：

```
commandname -?
```

ステップ 4 例を生成します。

例：

```
get-help commandname -examples
```

設定リファレンス

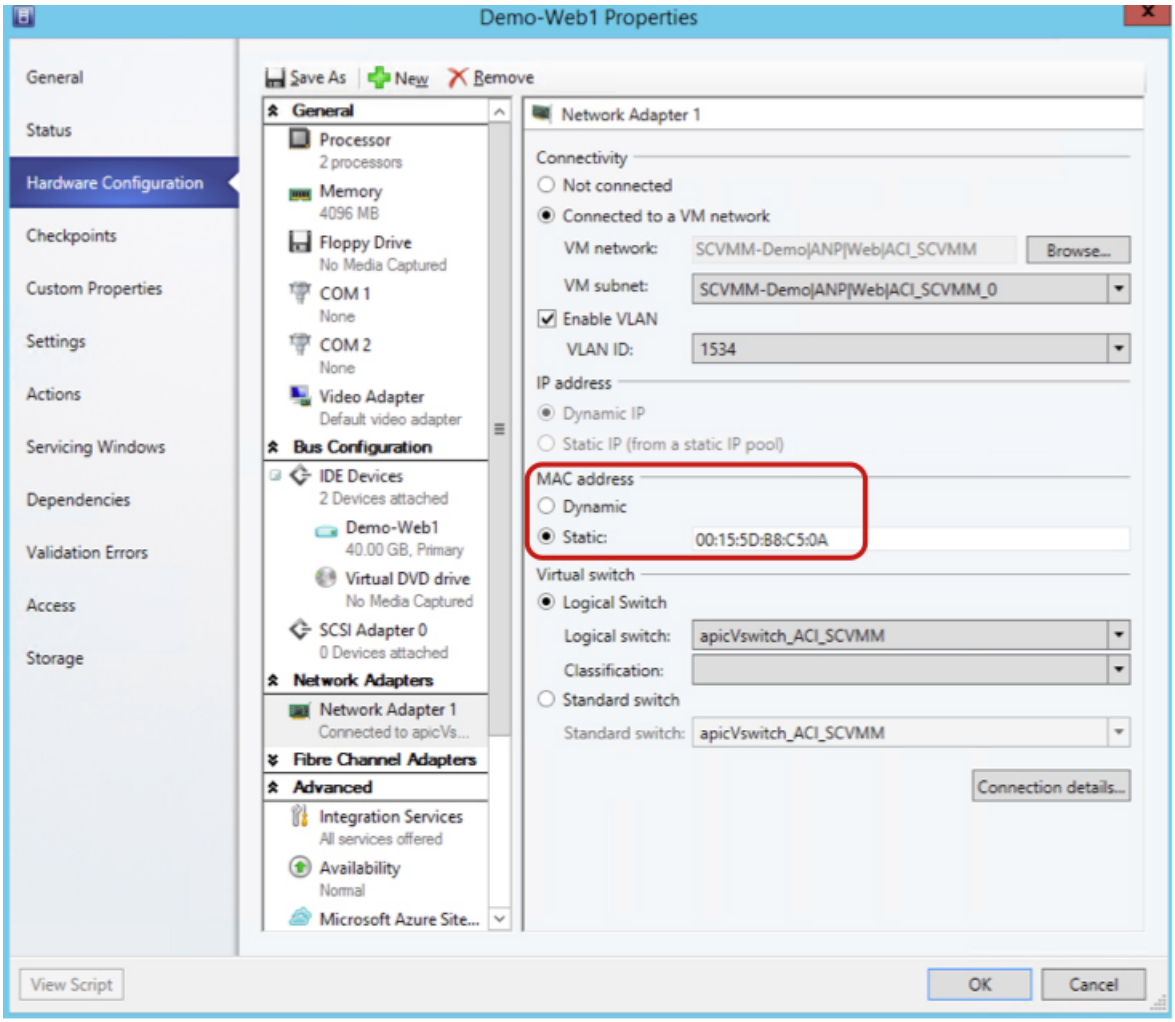
MAC アドレス設定の推奨事項

ここでは、MAC アドレス設定の推奨事項について説明します。

- ダイナミック MAC とスタティック MAC の両方がサポートされます。
- APIC で迅速に VM インベントリを表示する場合、VM ネットワーク アダプタには**スタティック** MAC が推奨されます。
- **ダイナミック** MAC を選択した場合、APIC での VM インベントリの表示に遅延が生じます。遅延は、ダイナミック MAC が SCVMM でただちに認識されないためです。

（注） VM インベントリが表示されなくても、データ プレーンは有効に機能します。

図 *22 : [Properties]* ペインに *[MAC address]* セクションを表示



Cisco ACI with Microsoft SCVMM コンポーネントのアンインストール

ここでは、Cisco Application Centric Infrastructure（ACI）with Microsoft System Center Virtual Machine Manager（SCVMM）コンポーネントをアンインストールする方法について説明します。

手順

ステップ 1 VM ネットワークからすべての仮想マシンをデタッチします。

Microsoft のマニュアルを参照してください。

ステップ 2 すべての Hyper-V で、インフラ VLAN トンネル エンドポイント（VTEP）および APIC 論理スイッチを削除します。

Microsoft のマニュアルを参照してください。

ステップ 3 APIC GUI で、すべての VM およびホストが切断されていることを確認します。

ステップ 4 Application Policy Infrastructure Controller（APIC）から VMM ドメインを削除します。

VMM ドメインを削除するためのガイドライン （14 ページ）を参照してください。

ステップ 5 論理スイッチと論理ネットワークが SCVMM から削除されたことを確認します。

ステップ 6 SCVMM または高可用性 SCVMM で APIC SCVMM エージェントをアンインストールします。

APIC SCVMM エージェントのアンインストール （326 ページ）を参照してください。

高可用性 SCVMM 上の APIC SCVMM エージェントのアンインストール （327 ページ）を参照してください

APIC SCVMM エージェントのアンインストール

ここでは、APIC SCVMM エージェントをアンインストールする方法について説明します。

手順

ステップ 1 SCVMM サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [ApicVMMService] を右クリックして、[Uninstall] を選択します。
これで、APIC SCVMM エージェントがアンインストールされます。

ステップ 4 APIC SCVMM エージェントがアンインストールされたかどうかを確認するには、[プログラムと機能] ウィンドウで [ApicVMMService] が表示されていないことを確認します。

高可用性 SCVMM 上の APIC SCVMM エージェントのアンインストール

ここでは、高可用性 System Center Virtual Machine Manager（SCVMM）で Application Policy Infrastructure Controller（APIC）SCVMM エージェントをアンインストールする方法について説明します。

手順

ステップ 1 可用性の高い SCVMM フェールオーバー クラスタ内の任意のノードにログインします。

ステップ 2 [Failover Cluster Manager Application] を開きます。

ステップ 3 [Windows Failover Cluster Manager] ウィンドウの [Highly Available SCVMM Roles/Resources] タブで、[ApicVMMService] を選択します。

ステップ 4 [ApicVMMService Role] を右クリックして [Take Offline] を選択します。

ステップ 5 ロールがオフラインになったら、[ApicVMMService Role] を右クリックして [Remove] を選択します。

ステップ 6 可用性の高い SCVMM フェールオーバー クラスタ内の各ノードで次の操作を実行して、APIC SCVMM エージェントをアンインストールします。

a) SCVMM サーバにログインします。

b) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

c) [Programs and Features] ウィンドウで [ApicVMMService] を右クリックして、[Uninstall] を選択します。
これで、APIC SCVMM エージェントがアンインストールされます。

d) APIC SCVMM エージェントがアンインストールされたかどうかを確認するには、[プログラムと機能] ウィンドウで [ApicVMMService] が表示されていないことを確認します。

Cisco ACI および Microsoft SCVMM コンポーネントでの CiscoAPIC コントローラおよびスイッチ ソフトウェアをダウングレードする

ここでは、Cisco ACI および Microsoft System Center Virtual Machine Manager（SCVMM）コンポーネントでの Cisco APIC とスイッチ ソフトウェアをダウングレードする方法について説明します。

手順

ステップ 1 SCVMM または高可用性の SCVMM 上の CiscoAPIC SCVMM エージェントをアンインストールします。

APIC SCVMM エージェントのアンインストール （326 ページ）を参照してください。

高可用性 SCVMM 上の APIC SCVMM エージェントのアンインストール （327 ページ）を参照してください。

ステップ 2 次の手順を実行して、Cisco APIC HYPER-V エージェントのダウン グレードします。

a) SCVMM サーバにログインし、Hyper-V ノードをメンテナンス モードにします。
b) 管理者クレデンシャルで Hyper-V サーバにログインします。
c) Cisco APIC HYPER-V エージェントをアンインストールします。
d) バージョンにダウン グレードされている Cisco ACI ファブリックを Cisco APIC HYPER-V エージェントをインストールします。

ステップ 3 スイッチ ソフトウェアをダウングレードします。

ステップ 4 シスコのダウン グレード APIC 。

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

ステップ 5 SCVMM サーバでは、Cisco ACI ファブリックにダウン グレードがされているバージョン SCVMM エージェントをインストールします。

SCVMM への APIC SCVMM のエージェントのインストール （284 ページ）を参照してください

可用性の高い SCVMM への APIC SCVMM エージェントのインストール （285 ページ）を参照してください

ステップ 6 Microsoft のドキュメンテーションの手順に従って、Cisco APIC vSwitch 論理スイッチを表示し、コンプライアンス状態にします。

参照してください ホスト ネットワーク アダプタの設定と *VMM* で論理スイッチ設定が増加コンプライアンスを方法 。

APIC OpFlex 証明書のエクスポート

ここでは、元の OpFlex 証明書を検出できない場合に、新しい Hyper-V ノード、System Center Virtual Machine Manager（SCVMM）および Windows Azure Pack のリソース プロバイダー サーバの ACI ファブリックへの展開に使用できるファイルに、APIC OpFlex 証明書をバックアップする方法を説明します。

手順

ステップ 1 現在 ACI ファブリックのメンバーである Hyper-V ノードにログインします。

ステップ 2 次の操作を実行して、Hyper-V ノードから証明書をエクスポートします。

a) **[Start]** > **[Run]** の順に選択し、**certlm.msc** と入力して証明書マネージャを起動します。

b) [navigation] ペインで、[Certificates - Local Computer] を右クリックして [Find Certificates] を選択します。

c) [Find Certificate] ダイアログボックスで、次の操作を実行します。

- [Find in] フィールドで、ドロップダウン リストから [All certificate stores] を選択します。
- [Contains] フィールドに **OpflexAgent** と入力します。
- [Look in Field] フィールドで、ドロップダウン リストから [Issued By] を選択します。
- [Find Now] をクリックします。

  結果のリストとして、リストに 1 つの証明書が表示されます。

d) 新たに見つかった [OpflexAgent] 証明書を右クリックして、[Export] を選択します。

証明書エクスポート ウィザードが表示されます。

ステップ 3 [Certificate Export Wizard] ダイアログボックスで、次の操作を実行します。

a) [Welcome to the Certificate Export Wizard] ダイアログボックスで [Next] をクリックします。

b) [Export Private Key] ダイアログボックスで [Yes, export the private key] オプション ボタンを選択し、[Next] をクリックします。

c) [Export File Format] ダイアログボックスで [Personal Information Exchange - PKCS #12 (.PFX)] オプション ボタンを選択し、[Include all certificates in the certificate path if possible] および [Export all extended properties] チェックボックスをオンにします。[Next] をクリックします。

d) [Security] ダイアログボックスで [Password] チェックボックスをオンにして、PFX パスワードを入力し、もう一度 PFX パスワードを入力して確認します。[Next] をクリックします。

PFX パスワードは、ターゲット マシンで PFX ファイルをインポートするために後で使用されます。

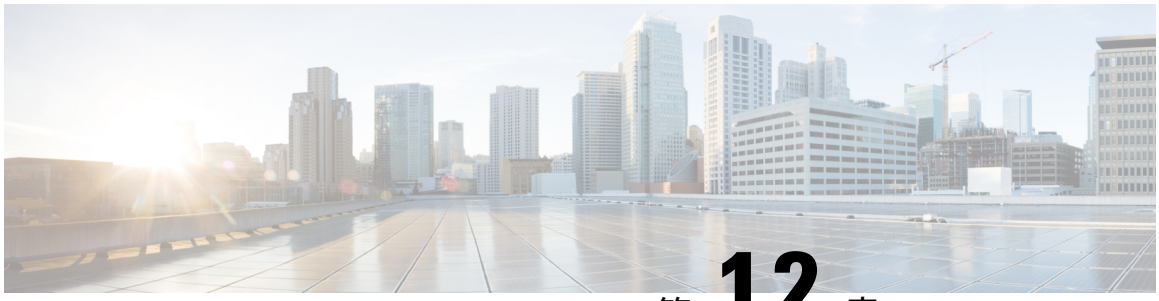
e) [File to Export] ダイアログボックスで、エクスポートしたファイル（C:\OpflexAgent.pfx）を保存する任意のファイル名を入力して、[Next] をクリックします。

f) [Completing the Certificate Export Wizard] ダイアログボックスで、指定した設定がすべて適切であることを確認して [Finish] をクリックします。

g) [Certificate Export Wizard] ダイアログボックスに [The export was successful] と表示されます。[Ok] をクリックします。

ステップ 4 PFX ファイルを既知の場所にコピーします。

ACI ファブリックへの統合のために、Active Directory グループ ポリシーで証明書を展開したり、SCVMM、Windows Azure Pack のリソース プロバイダー、Hyper-V サービスをホストする各種の Microsoft サーバにファイルをコピーできます。



第 12 章

Cisco ACI with Microsoft Windows Azure Pack

この章の内容は、次のとおりです。

Cisco ACI with Microsoft Windows Azure Pack について

Cisco Application Centric Infrastructure（ACI）と Microsoft Windows Azure Pack の統合によって、テナントにセルフサービス エクスペリエンスが提供されます。

ACI によってプラットフォームのネットワーク管理機能が拡張されます。Microsoft Windows Azure Pack は、既存の Microsoft System Center Virtual Machine Manager（SCVMM）インストールの最上位に構築されます。Cisco ACI はこれらの各レイヤに統合ポイントを備えています。そのため、SCVMM 環境で実行した作業を活用でき、Microsoft Windows Azure Pack のインストールで使用することができます。

- Cisco ACI with Microsoft Windows Azure Pack（Microsoft Windows Azure Pack for Windows Server）は、次の機能を含む Microsoft Azure テクノロジーのコレクションです。
  - テナント用の管理ポータル
  - 管理者用の管理ポータル
  - サービス管理 API

- Cisco ACI with Microsoft System Center Virtual Machine Manager：Cisco ACI with Microsoft System Center Virtual Machine Manager（SCVMM）を設定する方法の詳細については、「Cisco ACI with Microsoft SCVMM ソリューションの概要 （278 ページ）」を参照してください。

（注） Windows Azure パックで直接サーバ リターン (DSR) を設定することはできません。DSR を設定する場合は、Cisco APIC で行う必要があります。詳細については、『*Cisco APIC レイヤ 4 ～レイヤ 7 サービス導入ガイド*』の「直接サーバ リターンの設定」の章を参照してください。

Cisco ACI with Microsoft Windows Azure Pack ソリューションの概要

Cisco Application Centric Infrastructure（ACI）と Microsoft Windows Azure Pack の統合によって、テナントにセルフサービス エクスペリエンスが提供されます。Windows Azure Pack の ACI リソース プロバイダーによって Application Policy Infrastructure Controller（APIC）が動作し、ネットワーク管理機能がもたらされます。ネットワークは、System Center Virtual Machine Manager（SCVMM）で作成され、それぞれのテナントのために Windows Azure Pack で使用可能になります。ACI の F5 のレイヤ 4 ～レイヤ 7 機能、Citrix ロード バランサ、およびステートレスのファイアウォールがテナントに提供されます。詳細については、ロード バランシングの概要（359 ページ）を参照してください。

Windows Server 向けの Windows Azure Pack は、Microsoft の顧客が使用可能な Microsoft Azure テクノロジーのコレクションで、データセンターへのインストールに追加コストはかかりません。Windows Server 2012 R2 および System Center 2012 R2 で動作し、Windows Azure テクノロジーを使用することで、Windows Azure エクスペリエンスとともに、豊富なセルフサービス、マルチテナント クラウド、一貫性の提供を実現します。

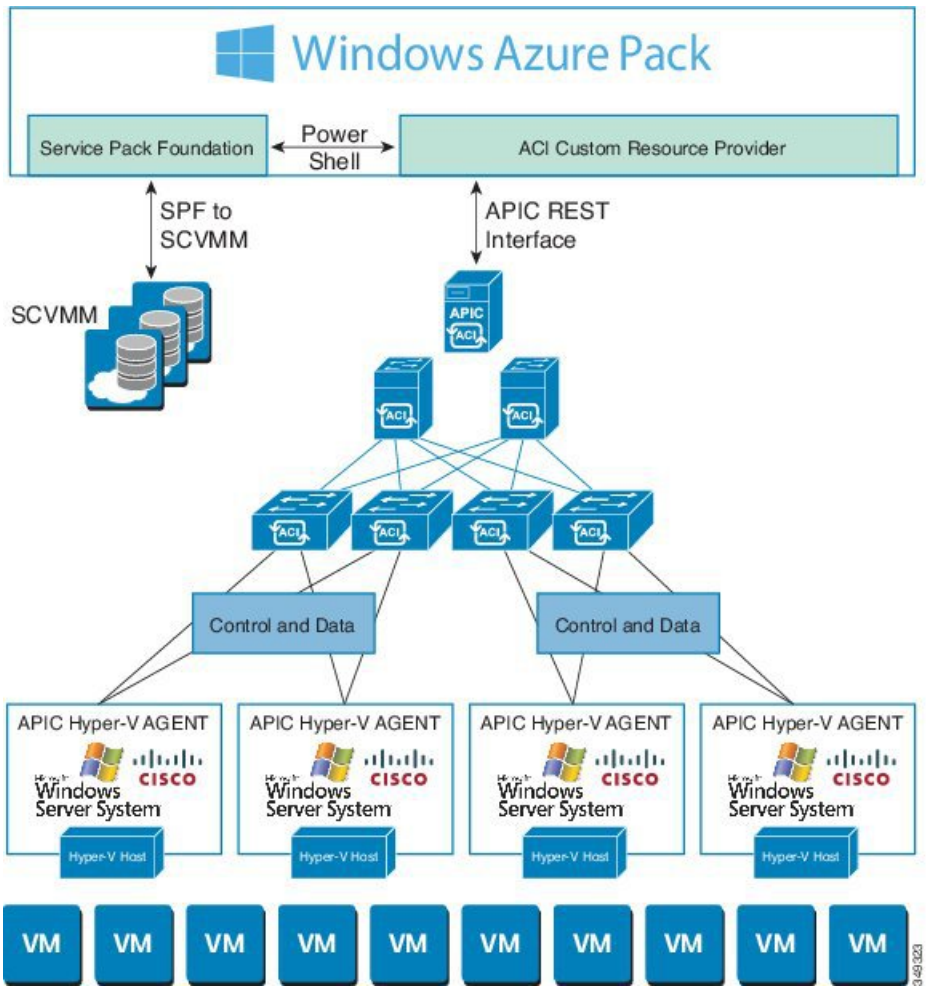
Windows Azure Pack には次の機能があります。

- テナントの管理ポータル：ネットワーク、ブリッジ ドメイン、VM、ファイアウォール、ロードバランサ、外部接続、共有サービスなどのサービスをプロビジョニング、監視、および管理するためのカスタマイズ可能なセルフサービス ポータル。ユーザ ポータルの GUI を参照してください。
- 管理者の管理ポータル：リソース クラウド、ユーザ アカウント、テナントのオファー、クォータ、価格設定、Web サイトのクラウド、仮想マシンのクラウド、およびサービス バスのクラウドを設定し管理する管理者のためのポータル。
- サービス管理 API：カスタム ポータルや課金システムなどのさまざまな統合シナリオの実現に役立つ REST API。

詳細については、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 （346 ページ）を参照してください。

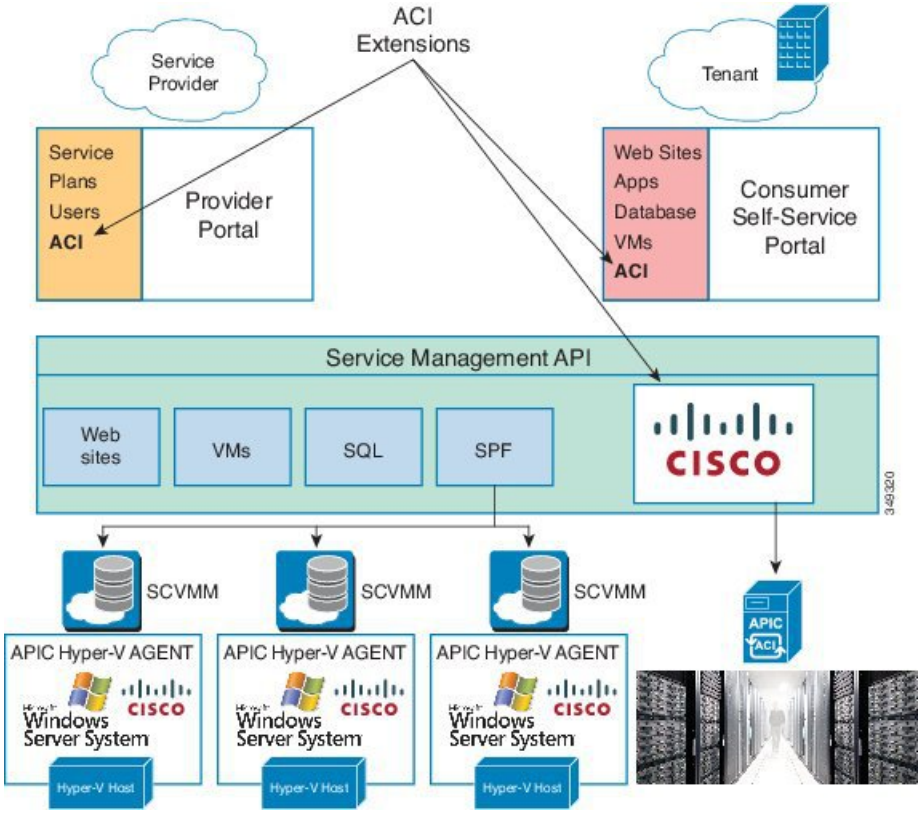
物理トポロジと論理トポロジ

図 *23 : ACI* ファブリックを使用した標準的な *Windows Azure Pack* 導入トポロジ



前の図は、Cisco Application Centric Infrastructure（ACI）ファブリックを使用した標準的な Windows Azure Pack 導入の代表的なトポロジを示しています。Windows Azure Pack と Application Policy Infrastructure Controller（APIC）間の接続は管理ネットワークを経由します。テナントインターフェイスは、GUI または REST API のどちらかを介して Windows Azure Pack のみを対象とします。テナントからは APIC に直接アクセスすることはできません。

図 *24 : ACI* リソース プロバイダー フレームワークにおける *ACI*



Microsoft Windows Azure Pack での ACI 構造のマッピングについて

ここでは、Microsoft Windows Azure Pack での Cisco Application Centric Infrastructure（ACI）のマッピングの表を示します。

表 *6 : ACI* および *Windows Azure Pack* の構造のマッピング

Windows Azure Pack	ACI
サブスクリプション	テナント
ネットワーク	EPG
ファイアウォール ルール	テナント内の契約
共有サービス	テナント間の契約
SCVMM クラウド	VM ドメイン

Cisco ACI with Microsoft Windows Azure Pack の開始

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

Cisco をインストールする前に ACI 、Microsoft Windows Azure Pack をダウンロードして、Cisco が入っているフォルダを解凍 ACI Cisco APIC リリースの Microsoft 統合ファイルに一致するとします。

1. Cisco's Application Policy Infrastructure Controller (APIC) website に移動します。
2. **All Downloads for this Product** > **APIC Software** を選択します。
3. リリースのバージョンと、それに適合する zip 圧縮フォルダを選択します。
4. [Download] をクリックします。
5. Zip 圧縮のフォルダに解凍します。

（注） Cisco ACI with Microsoft Windows Azure Pack 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。

Windows のシステム ロケールとして **English** が設定されていることを確認します。それ以外の場合、CiscoACI with Windows Azure Pack はインストールされません。また、インストールの後にシステム ロケールを英語以外に変更した場合、Cisco APIC および Cisco ACI ファブリックとの通信の際に、統合コンポーネントがエラーを生じる場合があります。

Cisco ACI with Microsoft Windows Azure Pack を開始するための前提条件

開始する前に、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。

- Cisco Application Centric Infrastructure（ACI）with Microsoft System Center Virtual Machine Manager（SCVMM）の設定が完了していることを確認します。

  詳細については、Cisco ACI with Microsoft SCVMM の開始 （281 ページ）を参照してください。

- Microsoft Windows Azure Pack の更新ロールアップ 5、6、7、9、10 または 11 がインストールされていることを確認します。

  Microsoft のマニュアルを参照してください。

- Windows Server 2016 がインストールされていることを確認します。

  Microsoft のマニュアルを参照してください。

- Hyper-V ホストがインストールされていることを確認します。

  Microsoft のマニュアルを参照してください。

- クラウドが SCVMM で設定されていることを確認します。

  Microsoft のマニュアルを参照してください。

- VM クラウドが Windows Azure Pack で設定されていることを確認します。

  Microsoft のマニュアルを参照してください。

- インフラストラクチャ VLAN が有効な「default」 AEP が存在することを確認します。
- 「default」および「vpcDefault」ブリッジ ドメイン と、対応する「default」および「vpcDefault」EPG がテナントに共通して存在することを確認します。
- APIC Windows Azure Pack リソースおよびホスト エージェント用の Cisco MSI ファイルがあることを確認します。

  詳細については、Cisco ACI with Microsoft SCVMM の開始 （281 ページ）を参照してください。

（注） 症状：プランを作成または更新するときに、エラーメッセージが表示されて失敗することがあります。

条件：FQDN を使用せずに Microsoft の Windows Azure Pack を設定している場合に、次のエラーメッセージが表示されます。

```
Cannot validate the new quota settings because one of the underlying services failed to
respond. Details: An error has occurred.
```

回避策：VM クラウドを設定するときは、SCVMM サーバに FQDN を使用するよう通知する Microsoft の Windows Azure Pack UI の指示に従います。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのインストール、設定および確認

ここでは、Cisco ACI with Microsoft Windows Azure Pack コンポーネントをインストール、設定および確認する方法を説明します。

コンポーネント	タスク
ACI Azure Pack のリソース プロバイダーのインストール	ACI Azure Pack リソース プロバイダーのインストール （337ページ）を参照してください。
OpflexAgent 証明書のインストール	OpflexAgent 証明書のインストール （337 ページ）を参照してください。
ACI Azure Pack のリソース プロバイダー サイトの設定	ACI Azure Pack のリソース プロバイダー サイトの設定 （340ページ）を参照してください。

コンポーネント	タスク
ACI Azure Pack の管理者サイト拡張のインストール	ACI Azure Pack の管理者サイト拡張のインストール （341 ページ）を参照してください。
ACI Azure Pack のテナント サイト拡張のインストール	ACI Azure Pack のテナント サイト拡張のインストール （341 ページ）を参照してください。
ACI の設定	ACI のセットアップ （341 ページ）を参照してください。
Windows Azure Pack のリソース プロバイダーの確認	Windows Azure Pack のリソース プロバイダーの確認 （342 ページ）を参照してください。

ACI Azure Pack リソース プロバイダーのインストール

ここでは、Windows Azure Pack サーバに ACI Azure Pack リソース プロバイダーをインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack 環境に VM クラウドを提供する Microsoft Service Provider Foundation サーバにログインします。ACI Azure Pack - Resource Provider Site.msi ファイルを見つけてコピーします。

ステップ 2 ACI Azure Pack - Resource Provider Site.msi ファイルをダブルクリックします。

ステップ 3 [Setup] ダイアログボックスで以下の操作を実行し、ACI Azure Pack - リソース プロバイダーをインストールします。

a) [I accept the terms in the License Agreement] チェックボックスをオンにします。
b) [Install] をクリックします。
c) [Install] をクリックします。
d) [Finish] をクリックします。

OpflexAgent 証明書のインストール

ここでは、OpflexAgent 証明書をインストールする方法について説明します。

手順

ステップ 1 管理者クレデンシャルで Windows Azure Pack サーバにログインします。

ステップ 2 次のいずれかの方法を使用します。

- 大規模な展開の場合、グループ ポリシーを使用した証明書の展開について、Microsoft ドキュメントを参照してください。

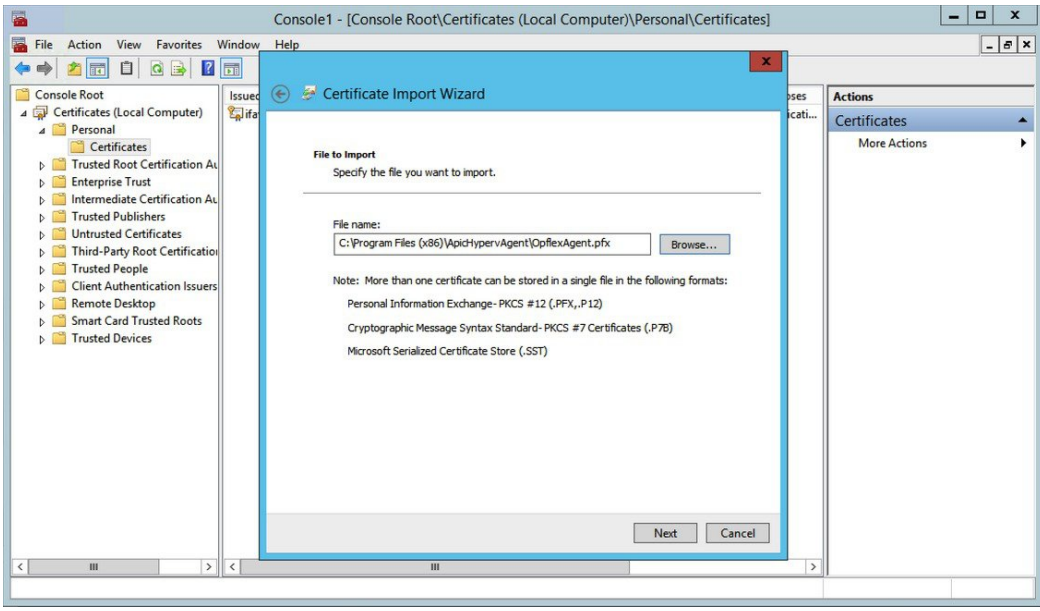
  https://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx。

- 小規模な展開の場合は、次の手順に従います。

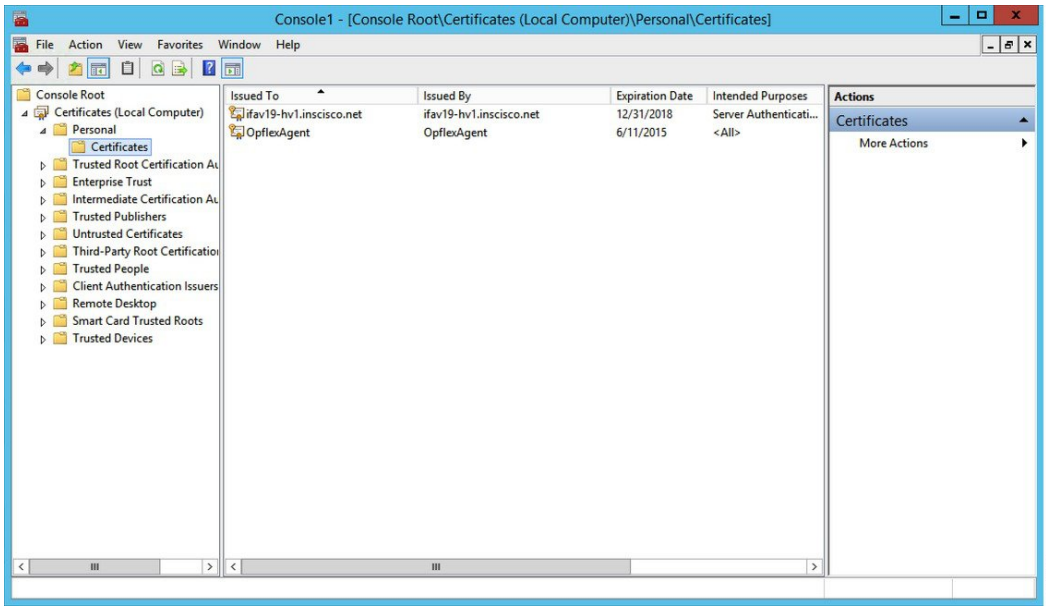
  ローカル システムに OpFlex セキュリティ証明書を追加する必要があります。ACI Windows Azure Pack のリソース プロバイダーは、SCVMM サーバ上にある（**C:\Program Files (x86)\ApicVMMService\OpflexAgent.pfx**）、Cisco ACI SCVMM インストール プロセスからの同じセキュリティ証明書ファイルを使用します。このファイルを Windows Azure Pack のリソース プロバイダー サーバにコピーします。ACI Windows Azure Pack のリソース プロバイダー サーバで次の手順を実行しない場合、APIC ACI Windows Azure Pack のリソース プロバイダーは Application Policy Infrastructure Controller（APIC）と通信できません。

  ACI Windows Azure Pack のリソース プロバイダーの Windows Server 2012 ローカル マシンの証明書リポジトリに、OpFlex セキュリティ証明書をインストールします。各 ACI Windows Azure Pack のリソース プロバイダー サーバで次の手順を実行して、この証明書をインストールします。

  1. **[Start]** > **[Run]** を選択します。
  2. **mmc** と入力し、**[OK]** をクリックします。
  3. [Console Root] ウィンドウのメニュー バーで、[Add/Remove Snap-in] を選択します。
  4. [Available Snap-ins] フィールドで [Certificates] を選択して [Add] をクリックします。
  5. [Certificates snap-in] ダイアログボックスで [Computer Account] オプション ボタンを選択し、[Next] をクリックします。
  6. [Select Computer] ダイアログボックスで [Local Computer] オプション ボタンを選択し、[Finish] をクリックします。
  7. [OK] をクリックして、[MMC Console] メイン ウィンドウに戻ります。
  8. [MMC Console] ウィンドウで [Certificates (local computer)] をダブルクリックして、ビューを展開します。
  9. [Personal] の下で [Certificates] を右クリックして、**[All Tasks]** > **[Import]** の順に選択します。
  10. [Certificates Import Wizard] ダイアログボックスで、次の操作を実行します。
      1. [Next] をクリックします。
      2. **Opflex Agent** ファイルを参照して [Next] をクリックします。



11. MSI のインストール時に提供された証明書のパスワードを入力します。
12. [Mark this key as exportable.This will allow you to back up or transport your keys at a later time] オプション ボタンを選択する必要があります。
13. [Include all extended properties] オプション ボタンを選択します。
14. [Place all certificates in the following store] オプション ボタンを選択し、[Personal] を見つけて [Next] をクリックします。
15. [Finish] をクリックします。
16. [OK] をクリックします。



ACI Azure Pack のリソース プロバイダー サイトの設定

ここでは、Windows Azure Pack サーバで ACI Azure Pack のリソース プロバイダー IIS サイトを設定する方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、[Internet Information Services Manager Application] を開きます。

ステップ 2 **[Application Pools]** > **[Cisco-ACI]** に移動します。

ステップ 3 [Actions] タブで [Advanced Settings] をクリックします。

a) ID フィールドを見つけて、スクロール バーの左側の省略記号をクリックします。

b) カスタム アカウントを選択し、Service Provider Foundation 管理者のアカウント名とパスワードからなるクレデンシャルを入力します。Service Provider Foundation 管理者のユーザ アカウントには、Administrator、SPF_Admin のグループ メンバーシップが必要です。このユーザ アカウントが必要なのは、リソース プロバイダーが接続された SCVMM サーバを問い合わせるためです。また、ユーザ クレデンシャルには、ローカル マシンのレジストリへの書き込み権限、リソース プロバイダーのロギング用に次のディレクトリへの読み取り/書き込みアクセス権が必要です。

C:\Windows\System32\config\systemprofile\AppData\Local

c) [OK] をクリックして、アプリケーション プール ID を終了します。

ステップ 4 [OK] をクリックして、拡張設定を終了します。

ACI Azure Pack の管理者サイト拡張のインストール

ここでは、Windows Azure Pack サーバに ACI Azure Pack の管理者サイト拡張をインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、**ACI Azure Pack - Admin Site Extension.msi** ファイルを見つけます。

ステップ 2 **ACI Azure Pack - Admin Site Extension.msi** ファイルをダブルクリックします。

ステップ 3 [Setup] ダイアログボックスで、次の操作を実行して ACI Azure Pack の管理者サイト拡張をインストールします。

a) [I accept the terms in the License Agreement] チェックボックスをオンにします。
b) [Install] をクリックします。
c) [Finish] をクリックします。

ACI Azure Pack のテナント サイト拡張のインストール

ここでは、Windows Azure Pack サーバに ACI Azure Pack のテナント サイト拡張をインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、**ACI Azure Pack - Tenant Site Extension.msi** ファイルを見つけます。

ステップ 2 **ACI Azure Pack - Tenant Site Extension.msi** ファイルをダブルクリックします。

ステップ 3 [Setup] ダイアログボックスで、次の操作を実行して ACI Azure Pack のテナント サイト拡張をインストールします。

a) [I accept the terms in the License Agreement] チェックボックスをオンにします。
b) [Install] をクリックします。
c) [Finish] をクリックします。

ACI のセットアップ

ここでは、ACI の設定方法について説明します。

手順

ステップ 1 サービス管理ポータルにログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

[ACI] がない場合、[Refresh] をクリックします。

ステップ 3 QuickStart アイコンをクリックします。

ステップ 4 [QuickStart] ペインで、次の操作を順序どおりに実行します。

a) [Register your ACI REST endpoint] をクリックします。
b) [ENDPOINT URL] フィールドに、リソース プロバイダー アドレスである Cisco-ACI ポート（http://*resource_provider_address*:50030）を入力します。
c) [USERSNAME] フィールドに、ユーザ名（ドメイン管理者）を入力します。
d) [PASSWORD] フィールドに、パスワード（ドメイン管理者のパスワード）を入力します。

ステップ 5 **[ACI]** > **[Setup]** タブを選択し、次の操作を実行します。

a) [APIC ADDRESS] フィールドに、APIC IP アドレスを入力します。
b) [CERTIFICATE NAME] フィールドに OpflexAgent と入力します。

Windows Azure Pack のリソース プロバイダーの確認

ここでは、Windows Azure Pack のリソースプロバイダーを確認する方法について説明します。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [aci] ペインで QuickStart Cloud アイコンを選択します。

[Register your ACI REST Endpoint] リンクがグレー表示になっていることを確認します。

ステップ 4 [aci] ペインで [SETUP] を選択します。

APIC アドレスに有効な apic アドレスがあり、証明書名が OpflexAgent であることを確認します。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアップグレード

前提条件：

ACI に統合する Microsoft サーバは、ACI を 2.0(1) リリースにアップグレードする前に、KB2919355 と KB3000850 の更新ロールアップで更新する必要があります。KB2919355 更新ロールアップには、2929781 のパッチが含まれており、新しい TLS 暗号スイートを追加し、Windows 8.1 および Windows サーバ 2012 R2 で暗号スイートの優先順位を変更します。

次の Microsoft サーバにパッチを適用する必要があります:

- Microsoft Windows Azure パック リソース プロバイダ サーバ
- Microsoft Windows Azure パック テナント サイト サーバ
- Microsoft Windows Azure パック管理サイト サーバ
- Microsoft System Center のサービス プロバイダの基盤/オーケストレーション サーバ
- Microsoft System Center 2012 R2 サーバ
- Microsoft HyperV 2012 R2 サーバ

各 Cisco ACI with Windows Azure Pack 統合の `.msi` ファイルをアップグレードするには、更新プログラム ロールアップごとにリストされる Windows Azure Pack コンポーネントをアップグレードするための Microsoft の全般的なガイドラインに従います。全般的なガイドラインは次のとおりです。

- システムが現在稼働中（顧客のトラフィックを処理中）の場合は、Azure サーバのダウンタイムをスケジュールします。Windows Azure Pack は現在ローリング アップグレードをサポートしていません。
- 顧客のトラフィックを停止するか、適切と思われるサイトにリダイレクトします。
- コンピュータのバックアップを作成します。

（注） 仮想マシン（VM）を使用している場合は、現在の状態のスナップショットを撮ります。

VM を使用していない場合は、Windows Azure Pack コンポーネントがインストールされている各マシンの `inetpub` ディレクトリの各 `MgmtSvc-*` フォルダのバックアップを作成します。

証明書、ホスト ヘッダーなどのポートの変更に関連するファイルと情報を収集します。

アップグレードが完了し確認したら、VM スナップショットの管理に関する Hyper-V のベストプラクティス（https://technet.microsoft.com/en-us/library/dd560637(v=ws.10).aspx）に従います。

ACI Windows Azure Pack ワークフローのアップグレード

ここでは、ACI Windows Azure Pack のワークフローをアップグレードする方法を説明します。

手順

ステップ 1 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ます。

『*Cisco APIC Firmware Management Guide*』を参照してください。

ステップ 2 ACI Windows Azure Pack をアップグレードします。

1.1(2x) 以前のリリースからアップグレードする場合：

a) APIC Windows Azure Pack のリソース プロバイダーをアンインストールする必要があります。「APIC Windows Azure Pack のリソース プロバイダーのアンインストール （388 ページ）」を参照してください。

b) Cisco ACI with Microsoft Windows Azure Pack コンポーネントのインストール、設定および確認 （336 ページ）の手順に従います。

c) ステップ 6 に進み、SCVMM で APIC SCVMM エージェントをアップグレードするか、高可用性 SCVMM で APIC SCVMM エージェントをアップグレードします。

リリース 1.1(2x) 以降からアップグレードする場合：

a) ステップ 3 に進みます。

ステップ 3 ACI Windows Azure Pack のリソース プロバイダーをアップグレードします。

詳細については、ACI Windows Azure Pack リソース プロバイダーのアップグレード （345 ページ）を参照してください。

ステップ 4 ACI Azure Pack の管理者サイト拡張をアップグレードします。

詳細については、ACI Azure Pack 管理者サイト拡張のアップグレード （345 ページ）を参照してください。

ステップ 5 ACI Azure Pack のテナント サイト拡張をアップグレードします。

詳細については、ACI Azure Pack テナント サイト拡張のアップグレード （346 ページ）を参照してください。

ステップ 6 SCVMM で APIC SCVMM エージェントをアップグレードするか、高可用性 SCVMM で APIC SCVMM エージェントをアップグレードします。

詳細については、SCVMM での APIC SCVMM エージェントのアップグレード （306 ページ）を参照してください。

詳細については、可用性の高い SCVMM 上の APIC SCVMM エージェントのアップグレード （306 ページ）を参照してください。

ステップ 7 APIC Hyper-V エージェントをアップグレードします。

詳細については、APIC Hyper-V エージェントのアップグレード （307 ページ）を参照してください。

ACI Windows Azure Pack リソース プロバイダーのアップグレード

ここでは、ACI Windows Azure Pack のリソース プロバイダーをアップグレードする方法を説明します。

手順

ACI Windows Azure Pack のリソース プロバイダーをアップグレードします。

リリース 1.1(2x) 以降からアップグレードする場合：

a) ACI Azure Pack リソース プロバイダーのインストール （337 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

b) ACI Azure Pack のリソース プロバイダー サイトの設定 （340 ページ）の手順に従ってください。

1.1(2x) 以前のリリースからアップグレードする場合：

a) APIC Windows Azure Pack のリソース プロバイダーのアンインストール （388 ページ）の手順に従ってください。

b) ACI Azure Pack リソース プロバイダーのインストール （337 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

c) ACI Azure Pack のリソース プロバイダー サイトの設定 （340 ページ）の手順に従ってください。

ACI Azure Pack 管理者サイト拡張のアップグレード

ここでは、ACI Azure Pack の管理者サイト拡張をアップグレードする方法を説明します。

手順

ACI Azure Pack の管理者サイト拡張をアップグレードします。

a) ACI Azure Pack の管理者サイト拡張のインストール （341 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

ACI Azure Pack テナント サイト拡張のアップグレード

ここでは、ACI Azure Pack のテナント サイト拡張をアップグレードする方法を説明します。

手順

ACI Azure Pack のテナント サイト拡張をアップグレードします。

a) ACI Azure Pack のテナント サイト拡張のインストール （341 ページ）の手順に従ってください。

MSI パッケージでは、以前のバージョンをアンインストールし、アップグレードの一環として新しいバージョンをインストールします。

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。

（注） 共有サービス コンシューマは、プロバイダーよりも異なる VRF では、ルート漏出、Vrf 間では、通信を有効にするには自動的に発生します。

Use case	共有プラン	VPC プラン	ユーザ	タスク
プランの作成 これにより、管理者は独自の制限値を使用してプランを作成できます。	○	○	Admin	1.プラン タイプについて （351 ページ）を参照してください。
			Admin	2.プランの作成 （353 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
テナントの作成 これにより、管理者はテナントを作成できます。	○	○	Admin	テナントの作成（354ページ）を参照してください。
共有プランでのネットワークの作成と検証 これにより、テナントは共有プランのネットワークを作成し検証できます。	○	なし	テナント	1.共有プランでのネットワークの作成（370ページ）を参照してください。
			テナント	2.APIC の Microsoft Windows Azure Pack で作成されたネットワークの確認（370ページ）を参照してください。
VPCプランでのネットワークの構築 これにより、テナントは VPC プランでネットワークを作成できます。	なし	○	テナント	VPC プランでのネットワークの構築（372ページ）を参照してください。
VPC プランのブリッジ ドメインの作成、ネットワークの作成、およびブリッジ ドメインの関連付け 仮想プライベートクラウド（VPC）プランのみに適用されます。これにより、テナントはネットワークに対する独自の IP アドレス空間を取得できます。	なし	○	テナント	1.VPC プランでのブリッジ ドメインの作成（370ページ）を参照してください。
			テナント	2.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（371ページ）を参照してください。
同一サブスクリプション内のファイアウォールの作成 これにより、テナントは同一サブスクリプション内にファイアウォールを作成できます。	○	○	テナント	同一サブスクリプション内のファイアウォールの作成（371ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
テナントによる共有サービス提供の許可 これにより、テナントはネットワークを作成し、作成したネットワークにコンピューティング サービス（サーバ）を接続し、他のテナントにこれらのサービスへの接続を提供できます。管理者は、プランで明示的にこの機能を有効にする必要があります。	○	○	Admin	1.テナントによる共有サービス提供の許可（355ページ）を参照してください。
			テナント	2.共有サービスの提供（374ページ）を参照してください。
			テナント	3.アクセス コントロール リストの追加（376ページ）またはアクセス コントロール リストの削除（376ページ）を参照してください。
			Admin	4.テナントによる共有サービス消費の許可（356ページ）を参照してください。
			テナント	5.消費される共有サービスの設定（374ページ）を参照してください。
			Admin	6.共有サービス プロバイダーとコンシューマの表示（357ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
NAT を消費するためにテナントを許可するファイアウォールと ADC ロード バランサ サービス	なし	○	Admin	1.NAT ファイアウォールおよび ADC ロードバランサ サービスを消費するテナントを許可する（356 ページ）を参照してください。
			テナント	2.VM ネットワークに NAT ファイアウォール レイヤ 4 ～ レイヤ 7 サービスを追加する（380 ページ）を参照してください。
			テナント	3.NAT ファイアウォール ポート転送ルールを VM ネットワークに追加する（381 ページ）を参照してください。
			テナント	4.プライベート ADC ロードバランサ レイヤ 4 ～ レイヤ 7 サービスを伴う NAT ファイアウォールを VM ネットワークに追加する（381 ページ）を参照してください。
			テナント	5.パブリック ADC ロードバランサ レイヤ 4 ～ レイヤ 7 サービスを VM ネットワークに追加する（383 ページ）を参照してください。
			テナント	6.VM ネットワークに ADC ロードバランサの設定を追加する（384 ページ）を参照してください。
共有サービスの管理 これにより、管理者は新しいテナントの共有サービスを廃止し、共有サービスからのテナントアクセスを取り消すことができます。	○	○	Admin	新しいテナントからの共有サービスの廃止（358 ページ）を参照してください。 共有サービスからのテナントの取り消し（358 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
VM の作成とネットワークへの接続	○	○	テナント	VM の作成とネットワークへの接続（373 ページ）を参照してください。
ロード バランサの作成	○	○	Admin	1.ロード バランシングの概要（359 ページ）を参照してください。
			Admin	2.APIC でのデバイス パッケージのインポート（359 ページ）を参照してください。
			Admin	3.XML POST を使用した APIC でのロード バランサ デバイスの設定（360 ページ）を参照してください。
			Admin	4.プランに合わせたロード バランサの作成（366 ページ）を参照してください。
			テナント	5.ロード バランサの設定（375 ページ）を参照してください。

Use case	共有プラン	VPC プラン	ユーザ	タスク
外部接続の作成 これにより、テナントネットワークでファブリックの外部宛てに送信される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。	○	○	APIC 管理者	1.L3 外部接続について （367 ページ）を参照してください。
			APIC 管理者	2.Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （367 ページ）を参照してください。
			APIC 管理者	3.l3extinstP「default」で提供される契約の作成 （368 ページ）を参照してください。
			APIC 管理者	4.l3extinstP「vpcDefault」で提供される契約の作成 （369 ページ）を参照してください。
			テナント	5.外部接続用ネットワークの作成 （378 ページ）を参照してください。
			テナント	6.外部接続用のファイアウォールの作成 （378 ページ）を参照してください。
			APIC 管理者	7.APIC でのテナントの L3 外部接続の確認 （379 ページ）を参照してください。

管理タスク

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
分離ネットワーク	○	○
ファイアウォール	○	○
プロバイダー DHCP	Yes	あり *
共有ロード バランサ	Yes	あり *

	共有インフラストラクチャ	仮想プライベート クラウド
パブリック インターネット アクセス	○	○
テナント間共有サービス	○	○
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	なし	○

*仮想プライベート クラウド（VPC）プランでは、プライベート アドレス空間に対するロードバランサと DHCP はサポートされません。いずれの機能もテナントには提供されますが、共有インフラストラクチャによって所有されます。

プラン オプションについて

このセクションでは、プラン オプションについて説明します。

- APIC テナント:APIC テナントの自動作成を無効にする
  - デフォルト: 選択されていません。

    選択されていない: Cisco ACI Azure Pack リソースプロバイダは自動的に APIC テナントを作成/削除します。APIC テナント名は、Windows Azure Pack テナントのサブスクリプション ID (GUID) になります。リソース プロバイダが必要なすべてのマッピングを処理するため、APIC 管理者による手動の介入は不要です。

    選択: Cisco ACI Azure Pack リソース プロバイダは、APIC テナントを自動的に作成/削除しません。APIC テナントは Windows Azure Pack サブスクリプション ID に明示的にマップする必要があります。このマッピングが APIC で確立されると、Azure Pack テナントは、ネットワーク、ファイアウォール、ロードバランサなどとの通常の操作を実行できます。

- APIC テナントの自動作成を無効にすることで有効になる機能
  - SCVMM と Windows Azure Pack VM のネットワーク名は、GUID ではなく APIC テナント名を使用します。これにより、SCVMM 管理者および Azure Pack テナントの可読性が向上します。VM ネットワークは GUID ではなくフレンドリーな名前を持つためです。

- プラン クォータ: Azure Pack プラン管理者は、Azure Pack テナントが作成できる EPG、BD、および VRF の数を制限するプランを作成できるようになりました。
  - APIC 管理者が APIC の下で作成した EPG、BD、および VRF は、Azure Pack プランの割り当て量にカウントされます。
    - 例 1: プラン管理者は、EPG の上限が 5 つの Azure Pack プランを作成します。Azure Pack テナントは 4 つの EPG を作成し、APIC 管理者は Azure Pack テナントの EPG

を作成します。Azure Packテナントは現在、プラン クォータに達しており、プラン クォータ以下になるまで EPG を作成することはできません。

- 例 2: プラン管理者は、EPG の上限が 5 つの Azure Pack プランを作成します。Azure Pack テナントは 5 つの EPG を作成します。APIC 管理者が Azure Pack テナントの EPG を作成します。Azure Packのテナントは現在、プラン クォータに達しており、プラン クォータ以下になるまで EPG を作成することはできません。
- これらのクォータは、Azure Pack テナントに適用されますが、APIC 管理者には適用されません。APIC 管理者は、テナントが自分のクォータを超えた場合でも Azure Pack テナントの EPG、BD、VRF を作成し続けることができます。

- すべてのプラン タイプ: EPG の公開
  - APIC 管理者が EPG を Windows Azure Pack テナントにプッシュできるようになりました。
  - APIC 管理者は、APIC に EPG を作成し、それをテナントプランに関連付けられた VMM ドメイン (SCVMM Cloud) に関連付けることで、Azure Pack テナント用の EPG を作成できるようになりました。
  - テナントの下の「デフォルト」のアプリケーションプロファイルは、Azure Packテナントの所有スペースとみなされます。これはAzure Packテナントが契約を結んで削除できることを意味します。
  - 他のすべてのアプリケーション プロファイルは、APIC 管理者が所有するスペースと見なされます。これらの EPG は、Azure Pack テナントが使用できるようになりますが、Azure Packテナントは、仮想マシンネットワーク アダプタとの関連付け以外で、EPG の変更、削除、または操作を行うことはできません。

プランの作成

これにより、管理者は独自の値でプランを作成できます。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 [Navigation] ペインで [PLANS] を選択します。

ステップ 3 [NEW] を選択します。

ステップ 4 [NEW] ペインで [CREATE PLAN] を選択します。

ステップ 5 [Let's Create a Hosting Plan] ダイアログボックスで、プラン（ブロンズ）の名前を入力し、矢印をクリックして次に進みます。

ステップ 6 [Select services for a Hosting Plan] ダイアログボックスで機能を選択します。[VIRTUAL MACHINE CLOUDS] および [NETWORKING (ACI)] チェックボックスをオンにし、矢印をクリックして次に進みます。

ステップ 7 [Select add-ons for the plan] ダイアログボックスで、チェックマークをクリックして次に進みます。

ステップ 8 [plans] ペインで、プラン（ブロンズ）が作成されるのを待って、（ブロンズ）プラン矢印を選択して設定します。

ステップ 9 プランのサービスの [Bronze] ペインで、[Virtual Machine Clouds] 矢印を選択します。

ステップ 10 [virtual machine clouds] ペインで、次の操作を実行します。

a) [VMM MANAGEMENT SERVER] フィールドで、VMM 管理サーバ（172.23.142.63）を選択します。
b) [VIRTUAL MACHINE CLOUD] フィールドで、クラウド名（Cloud01）を入力します。
c) 下にスクロールして、[Add templates] を選択します。
d) [Select templates to add to this plan] ダイアログボックスで、テンプレートのチェックボックスをオンにし、チェックマークをクリックして次に進みます。
e) [Custom Settings] まで下にスクロールして、SCVMM について [Disable built-in network extensions for tenants] チェックボックスをオンにします。
f) 下部で [SAVE] をクリックします。
g) 終了したら、[OK] をクリックします。

ステップ 11 サービス管理ポータルで、戻る矢印をクリックすると、[Bronze] ペインに戻ります。

ステップ 12 プランのサービスの [Bronze] ペインで、[Networking (ACI)] をクリックして、次の操作を実行します。

a) [PLAN TYPE] フィールドで、ドロップダウン リストからプラン タイプを選択します。
b) 仮想プライベートクラウドプランタイプでは、「テナントごとに許可される最大EPG」、「テナントごとに許可される最大 Bd」、「テナントごとに許可される最大 CTX」に 1 ～ 4000 の間の有効な値を入力します。

   共有インフラストラクチャ プラン タイプでは、「テナントごとに許可される最大 EPG」に 1 ～ 4000 の間の有効な値を入力します。

c) [SAVE] をクリックします。

ステップ 13 [OK] をクリックします。
プランが作成されました。

テナントの作成

これにより、管理者はテナントを作成できます。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで、[USER ACCOUNTS] を選択します。

ステップ 3 [NEW] を選択します。

ステップ 4 [NEW] ペインで下にスクロールし、[USER ACCOUNTS] を選択します。

ステップ 5 [NEW] ペインで、[QUICK CREATE] を選択し、以下の操作を実行します。

a) [ENTER EMAIL ADDRESS] フィールドに電子メール アドレス（tenant@domain.com）を入力します。
b) [ENTER PASSWORD] フィールドにパスワードを入力します。
c) [CONFIRM PASSWORD] フィールドに同じパスワードをもう一度入力します。
d) [CHOOSE PLAN] フィールドでプラン（BRONZE）を選択します。
e) [CREATE] をクリックします。
f) [OK] をクリックします。
テナントが作成されました。

ステップ 6 「APIC テナントの自動作成を無効にする」というプランに関連付けられている Windows Azure パック テナントの場合、Azure パック テナントのログイン情報とサブスクリプション ID をメモしておいてください。

a) APIC GUI にログインし、メニューバーで **TENANTS** > **Tenant Name** を選択します。このテナントは、Azure パック サブスクリプション マッピングをターゲットとする APIC テナントを対象にしています。
b) **Policy** タブを選択します。
c) [GUID] セクションで、+ アイコンをクリックして、新しい Azure パック サブスクリプション マッピングを追加します。
d) Azure パック テナントのサブスクリプション ID を持つ GUID と、Azure パックのログイン アカウントを持つアカウント名を入力します。
e) **Submit** をクリックして変更を保存します。

（注） APIC テナントがマッピングできるのは、ただ 1 つの Azure パック テナント サブスクリプション ID だけです。

テナントによる共有サービス提供の許可

このオプションにより、テナントはネットワークを作成し、コンピューティング サービス（サーバ）をこれらのネットワークに接続し、他のテナントにこれらのサービスへの接続を提供することができます。管理者は、プランで明示的にこの機能を有効にする必要があります。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 [Navigation] ペインで [PLANS] を選択します。

a) プランを選択します。
b) プランのサービスで、[Networking (ACI)] をクリックします。

ステップ 3 [networking (aci)] ペインで [allow tenants to provide shared services] チェックボックスをオンにして、[SAVE] をクリックします。

テナントによる共有サービス消費の許可

テナントが他のテナントで使用される共有サービスを作成できる場合であっても、管理者はテナント間で共有できるサービスを選択する必要があります。この手順では、Windows Azure Pack の管理者がプラン用に共有サービスを選択する方法を示します。

始める前に

- 管理者がテナントによる共有サービスの提供を許可していることを確認します。
- テナントが共有サービスを提供していることを確認します。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[PLANS]** を選択します。

ステップ 3 **[plans]** ペインで **[PLANS]** を選択します。

a) プラン (ゴールド) をクリックします。

ステップ 4 **[Gold]** ペインで **[Networking (ACI)]** を選択します。

ステップ 5 **[networking (aci)]** ペインで、アクセス権を与える共有サービスのチェックボックスをオンにします (DBSrv) 。

ステップ 6 **[SAVE]** をクリックします。

NAT ファイアウォールおよび ADC ロード バランサ サービスを消費するテナントを許可する

Cisco Application Centric Infrastructure（ACI）にはサービス グラフの概念があり、テナントがサービス ノードを挿入してファブリック内の 2 つのエンドポイント グループ（EPG）間でさまざまなレイヤ 4 ～レイヤ 7 機能を実行できます。

ACI と連携した Windows Azure Packには、共有スペース内に外部 NAT ファイアウォール IP および外部 ADC ロード バランサが存在している場合、仮想プライベート クラウド（VPC）でサービスを簡単かつシームレスにプロビジョニングおよび展開できる機能が含まれます。この機能の最も一般的な使用例は、EPG のさまざまなポート転送技術またはロード バランシングが外部 IP に対して行われる場合に、IP アドレスが外部からのアクセスを制限されているサービス プロバイダ モデルが使用できます。

テナント仮想ルーティングおよび転送（VPC）内にすべてのネットワークが含まれている場合や、ACI ファブリックを使用するすべてのテナントでアクセス可能な一連の L3Out を APIC 管理者が設定できる VRF モデルを分割する場合、Azure Pack 内のテナントがストリクト VPCモデルを利用きます。Azure Pack テナントがレイヤ 4 ～ レイヤ 7 サービス デバイスを消費し、テナント VRF 内から提供される提供されたサービスのパブリック アドレスを割り当て可能な、VRF ワークフローの分割に関する指示を提供します。

始める前に

- Application Policy Infrastructure Controller（APIC）管理者が、共通テナントの少なくともレイヤ 4 ～ レイヤ 7 リソース プールで設定されていることを確認します。「*Cisco APIC レイヤ 4 ～ レイヤ 7 サービス展開ガイド*」の「レイヤ 4 ～レイヤ 7 のリソース プールの設定」章を参照してください。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[PLANS]** を選択します。

ステップ 3 **[plans]** ペインで **[PLANS]** を選択します。

a) プラン (ゴールド) をクリックします。

ステップ 4 **[Gold]** ペインで **[Networking (ACI)]** を選択します。

ステップ 5 **[ネットワー キング（aci）]** ペインで、Azure Pack 消費の APIC 管理者によりプロビジョニングされたレイヤ 4 ～ レイヤ 7 サービス プールを選択します。

ステップ 6 [SAVE] をクリックします。

共有サービス プロバイダーとコンシューマの表示

これにより、管理者は共有サービス プロバイダーとコンシューマを表示できます。

始める前に

- 管理者がテナントによる共有サービスの提供を許可していることを確認します。
- テナントが共有サービスを提供していることを確認します。
- 管理者がプランで共有サービスを有効化していることを確認します。
- 消費される共有サービスがテナントに設定されていることを確認します。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [ACI] ペインで、[SHARED SERVICES] を選択して共有サービス プロバイダーを表示します。

ステップ 4 プロバイダーをクリックします。

ステップ 5 [INFO] をクリックして、この共有サービスを消費しているすべてのユーザを表示します。

共有サービスの管理

新しいテナントからの共有サービスの廃止

これにより、管理者は新しいテナントから共有サービスを廃止できます。

手順

ステップ 1 サービス管理ポータル (管理者ポータル) にログインします。
ステップ 2 [Navigation] ペインで [PLANS] を選択します。
ステップ 3 [plans] ペインで、プラン（ゴールド）を選択します。
ステップ 4 [gold] ペインで [Networking (ACI)] を選択します。
ステップ 5 [networking (aci)] ペインで、プランからサービスのマークを外して [SAVE] をクリックします。テナントから共有サービスを廃止しました。

共有サービスからのテナントの取り消し

これにより、管理者は共有サービスからテナントを取り消すことができます。

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。
ステップ 2 [Navigation] ペインで [ACI] を選択します。
ステップ 3 [aci] ペインで、共有サービス（DBSrv）を選択します。
ステップ 4 [INFO] をクリックして、取り消すユーザがその共有サービスに存在することを確認します。
ステップ 5 [Navigation] ペインで [PLANS] を選択します。
ステップ 6 [plans] ペインで、プラン（ゴールド）を選択します。
ステップ 7 [gold] ペインで [Networking (ACI)] を選択します。
ステップ 8 [networking (aci)] ペインで、プランからサービスのマークを外して [SAVE] をクリックします。
ステップ 9 [Navigation] ペインで [ACI] を選択します。
ステップ 10 [aci] ペインで [SHARED SERVICES] を選択します。
ステップ 11 [aci] ペインで、共有サービス（DBSrv）を選択して [INFO] クリックします。
ステップ 12 [Revoke Consumers of DBSrv] ダイアログボックスで、取り消すユーザのチェックボックスをオンにします。
ステップ 13 チェックマークをクリックします。

ロード バランシングの概要

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。

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

APIC GUI を使用してレイヤ 4 ～ 7 のサービスを導入するには、以下のタスクを実行する必要があります。

デバイス パッケージのインポート 管理者のみがデバイス パッケージをインポートできます。	APIC でのデバイス パッケージのインポート（359 ページ）を参照してください。
XML POST の設定と Application Policy Infrastructure Controller（APIC）へのポスト デバイス パッケージについては、Microsoft の Windows Azure Pack サービスに関する項を参照してください。 管理者のみが XML POST を設定して送信できます。	XML POST を使用した APIC でのロード バランサ デバイスの設定 （360 ページ）を参照してください。
プランに合わせたロード バランサの作成 Windows Azure Pack に対する VIP 範囲が設定されています。 管理者のみがプランに合わせたロード バランサを作成できます。	プランに合わせたロードバランサの作成 （366 ページ）を参照してください。
ロード バランサの設定 テナントのみがロード バランサを設定できます。	ロード バランサの設定 （375 ページ）を参照してください。

APIC でのデバイス パッケージのインポート

管理者のみがデバイス パッケージをインポートできます。管理者がデバイス パッケージを Application Policy Infrastructure Controller（APIC）にインポートすると、APIC はユーザが持っているデバイス、およびそのデバイスで何ができるかを知ることができます。

始める前に

デバイス パッケージがダウンロードされていることを確認します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで **[L4-L7 SERVICES]** > **[PACKAGES]** の順に選択します。

ステップ 2 [navigation] ペインで、[Quick Start] を選択します。

ステップ 3 [Quick Start] ペインで、[Import a Device Package] を選択します。

ステップ 4 [Import Device Package] ダイアログボックスで、次の操作を実行します。

a) [BROWSE] をクリックして、F5 や Citrix デバイス パッケージなどのデバイス パッケージを探します。

b) [Submit] をクリックします。

XML POST を使用した APIC でのロード バランサ デバイスの設定

管理者のみが XML POST を設定して送信できます。

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。ロードバランサを消費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、Windows Azure Pack 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 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。

- ロード バランサの VIP インターフェイスは、外部にリンクする必要がある任意の EPG に配置する必要があります。

  ファブリック外部の L3 extOut 外部接続については、『*Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*』を参照してください。

- （オプション）必要に応じて、VIP サブネットが L3 または L2 extOut にリンクされていることを確認してください。EPG あたり 1 つの VIP が割り当てられます。

手順

ステップ 1 次に、Citrix および F5 の XML POST の例を示します。

a) Citrix の XML POST の例：

例：

```
<polUni dn="uni">
    <fvTenant dn="uni/tn-common" name="common">

        <vnsLDevVip name="MyLB" devtype="VIRTUAL">

                                            <!-- Device Package -->
            <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScaler-1.0"/>

                                            <!-- VmmDomain -->
            <vnsRsALDevToDomP tDn="uni/vmmp-VMware/dom-mininet"/>

            <vnsCMgmt name="devMgmt" host="172.31.208.179" port="80"/>
            <vnsCCred name="username" value="nsroot"/>
            <vnsCCredSecret name="password" value="nsroot"/>

            <vnsDevFolder key="enableFeature" name="EnableFeature">
                    <vnsDevParam key="LB" name="lb_1" value="ENABLE"/>
                    <vnsDevParam key="CS" name="cs_1" value="ENABLE"/>
                    <vnsDevParam key="SSL" name="ssl_1" value="ENABLE"/>
            </vnsDevFolder>
            <vnsDevFolder key="enableMode" name="EnableMode_1">
                    <vnsDevParam key="USIP" name="usip_1" value="DISABLE"/>
                    <vnsDevParam key="USNIP" name="usnip_1" value="ENABLE"/>
            </vnsDevFolder>

            <vnsCDev name="ADC1" devCtxLbl="C1">
                <vnsCIf name="1_1"/>
                <vnsCIf name="mgmt"/>

                <vnsCMgmt name="devMgmt" host="172.31.208.179" port="80"/>
                <vnsCCred name="username" value="nsroot"/>
                <vnsCCredSecret name="password" value="nsroot"/>
            </vnsCDev>

            <vnsLIf name="C5">
              <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mIfLbl-outside"/>

                <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-ADC1/cIf-[1_1]"/>
            </vnsLIf>
            <vnsLIf name="C4">
              <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mIfLbl-inside"/>

                <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-ADC1/cIf-[1_1]"/>
            </vnsLIf>

        </vnsLDevVip>

        <vnsAbsGraph name ="MyLB">

            <!-- Node2 Provides SLB functionality -->
            <vnsAbsNode name = "Node2" funcType="GoTo" >

                <vnsRsDefaultScopeToTerm
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeProv-Output1/outtmnl"/>

                <vnsAbsFuncConn name = "C4">
                    <vnsRsMConnAtt
tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mFunc-LoadBalancing/mConn-external" />
                </vnsAbsFuncConn>
```

```
                <vnsAbsFuncConn name = "C5" attNotify="true">
                    <vnsRsMConnAtt
tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mFunc-LoadBalancing/mConn-internal" />
                </vnsAbsFuncConn>

                <vnsAbsDevCfg>
                    <vnsAbsFolder key="Network"
                                  name="network"
                                  scopedBy="epg">
                        <vnsAbsFolder key="nsip" name="snip1">
                         <vnsAbsParam key="ipaddress" name="ip1" value="5.5.5.251"/>

                            <vnsAbsParam key="netmask" name="netmask1"
value="255.255.255.0"/>
                            <vnsAbsParam key="hostroute" name="hostroute"
value="DISABLED"/>
                            <vnsAbsParam key="dynamicrouting" name="dynamicrouting"
 value="ENABLED"/>
                            <vnsAbsParam key="type" name="type" value="SNIP"/>
                        </vnsAbsFolder>
                    </vnsAbsFolder>

                </vnsAbsDevCfg>

                <vnsAbsFuncCfg>
                    <vnsAbsFolder key="internal_network"
                                  name="internal_network"
                                  scopedBy="epg">
                        <vnsAbsCfgRel name="internal_network_key"
                                      key="internal_network_key"
                                      targetName="network/snip1"/>
                    </vnsAbsFolder>
                </vnsAbsFuncCfg>

                <vnsRsNodeToMFunc
tDn="uni/infra/mDev-Citrix-NetScaler-1.0/mFunc-LoadBalancing"/>
            </vnsAbsNode>

            <vnsAbsTermNodeCon name = "Input1">
                <vnsAbsTermConn name = "C1"/>
            </vnsAbsTermNodeCon>

            <vnsAbsTermNodeProv name = "Output1">
                <vnsAbsTermConn name = "C6"/>
            </vnsAbsTermNodeProv>

            <vnsAbsConnection name = "CON1" adjType="L2">
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeCon-Input1/AbsTConn" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Node2/AbsFConn-C4" />
            </vnsAbsConnection>

            <vnsAbsConnection name = "CON3" adjType="L2">
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Node2/AbsFConn-C5" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeProv-Output1/AbsTConn" />
            </vnsAbsConnection>

        </vnsAbsGraph>

    </fvTenant>
</polUni>
```

b) F5 の XML POST の例：

例：

```
<polUni dn="uni">
    <fvTenant name="common">

      <fvBD name="MyLB">
        <fvSubnet ip="6.6.6.254/24" />
        <fvRsCtx tnFvCtxName="default"/>
      </fvBD>

      <vnsLDevVip name="MyLB" devtype="VIRTUAL">
          <vnsRsMDevAtt tDn="uni/infra/mDev-F5-BIGIP-1.1.1"/>
          <vnsRsALDevToDomP tDn="uni/vmmp-VMware/dom-mininet"/>
          <vnsCMgmt name="devMgmt" host="172.31.210.88" port="443"/>
          <vnsCCred name="username" value="admin"/>
          <vnsCCredSecret name="password" value="admin"/>

          <vnsLIf name="internal">
              <vnsRsMetaIf tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mIfLbl-internal"/>
             <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-BIGIP-1/cIf-[1_1]"/>

          </vnsLIf>

          <vnsLIf name="external">
              <vnsRsMetaIf tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mIfLbl-external"/>
             <vnsRsCIfAtt tDn="uni/tn-common/lDevVip-MyLB/cDev-BIGIP-1/cIf-[1_2]"/>

          </vnsLIf>

      <vnsCDev name="BIGIP-1">
          <vnsCIf name="1_1"/>
          <vnsCIf name="1_2"/>

          <vnsCMgmt name="devMgmt" host="172.31.210.88" port="443"/>
          <vnsCCred name="username" value="admin"/>
          <vnsCCredSecret name="password" value="admin"/>

          <vnsDevFolder key="HostConfig" name="HostConfig">
            <vnsDevParam key="HostName" name="HostName"
value="example22-bigip1.ins.local"/>
            <vnsDevParam key="NTPServer" name="NTPServer" value="172.23.48.1"/>
        </vnsDevFolder>

      </vnsCDev>

    </vnsLDevVip>
    <vnsAbsGraph name = "MyLB">
    <vnsAbsTermNodeCon name = "Consumer">
        <vnsAbsTermConn name = "Consumer">
        </vnsAbsTermConn>
    </vnsAbsTermNodeCon>
      <!-- Node1 Provides Virtual-Server functionality -->
      <vnsAbsNode name = "Virtual-Server" funcType="GoTo">

        <vnsAbsFuncConn name = "internal" attNotify="yes">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mFunc-Virtual-Server/mConn-internal"
 />
        </vnsAbsFuncConn>
        <vnsAbsFuncConn name = "external">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mFunc-Virtual-Server/mConn-external"
```

```
/>
        </vnsAbsFuncConn>
        <vnsRsNodeToMFunc
            tDn="uni/infra/mDev-F5-BIGIP-1.1.1/mFunc-Virtual-Server"/>
        <vnsAbsDevCfg>
          <vnsAbsFolder key="Network" name="webNetwork">

            <!-- Active Bigip SelfIP -->
            <vnsAbsFolder key="ExternalSelfIP" name="External1" devCtxLbl="ADC1">
              <vnsAbsParam key="SelfIPAddress" name="seflfipaddress"
                           value="6.6.6.251"/>
              <vnsAbsParam key="SelfIPNetmask" name="selfipnetmask"
                           value="255.255.255.0"/>
              <vnsAbsParam key="Floating" name="floating"
                           value="NO"/>
            </vnsAbsFolder>
            <vnsAbsFolder key="InternalSelfIP" name="Internal1" devCtxLbl="ADC1">
              <vnsAbsParam key="SelfIPAddress" name="seflfipaddress"
                           value="12.0.251.251"/>
              <vnsAbsParam key="SelfIPNetmask" name="selfipnetmask"
                           value="255.255.0.0"/>
              <vnsAbsParam key="Floating" name="floating"
                           value="NO"/>
            </vnsAbsFolder>
            <vnsAbsFolder key="Route" name="Route">
              <vnsAbsParam key="DestinationIPAddress" name="DestinationIPAddress"
                           value="0.0.0.0" />
              <vnsAbsParam key="DestinationNetmask" name="DestinationNetmask"
                           value="0.0.0.0"/>
              <vnsAbsParam key="NextHopIPAddress" name="NextHopIP"
                           value="6.6.6.254"/>
            </vnsAbsFolder>
          </vnsAbsFolder>
        </vnsAbsDevCfg>
        <vnsAbsFuncCfg>
          <vnsAbsFolder key="NetworkRelation" name="webNetwork">
            <vnsAbsCfgRel key="NetworkRel" name="webNetworkRel"
                          targetName="webNetwork"/>
          </vnsAbsFolder>
        </vnsAbsFuncCfg>
      </vnsAbsNode>
    <vnsAbsTermNodeProv name = "Provider">
         <vnsAbsTermConn name = "Provider" >
         </vnsAbsTermConn>
    </vnsAbsTermNodeProv>
    <vnsAbsConnection name = "CON3" adjType="L3">
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeCon-Consumer/AbsTConn" />
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Virtual-Server/AbsFConn-external" />
    </vnsAbsConnection>
    <vnsAbsConnection name = "CON1" adjType="L2">
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsNode-Virtual-Server/AbsFConn-internal" />
        <vnsRsAbsConnectionConns
tDn="uni/tn-common/AbsGraph-MyLB/AbsTermNodeProv-Provider/AbsTConn" />
    </vnsAbsConnection>
    </vnsAbsGraph>
  </fvTenant>

</polUni>
```

ステップ 2 次に、Citrix および F5 の設定可能なパラメータを示します。

a) Citrix の設定可能なパラメータ：

パラメータ	サンプル値	説明
vnsLDevVip name	「MyLB」	この値はロード バランサの ID で、ロード バランサ選択のプラン セクションの、Windows Azure Pack の管理者ポータルに表示されます。これは、同じ代替値を持つ XML POST 全体でグローバルに変更できます。
vnsRsALDevToDomP tDn	「uni/vmmp-VMware/dom-mininet」	これは、ロードバランサ VM が置かれている VMM ドメインです。たとえば、仮想ロード バランサがある場合、vCenter VMM ドメイン、SCVMM、または物理ドメインに関連付けることができます。 （注） どのドメインを指定する場合でも、VLAN 範囲が関連付けられている必要があります。
vnsCMgmt name="devMgmt" host	「172.31.208.179」	これは、Cisco Application Centric Infrastructure（ACI）ファブリックに通信されるロード バランサの IP アドレスです。
vnsCCred name	「username」	ユーザ名。
vnsCCredSecret name	「password」	パスワード。
vnsAbsParam key	「ipaddress」	これは、ファブリックがこのデバイスを識別する IP アドレスです。
vnsAbsParam key="ipaddress" name="ip1" value	「5.5.5.251」	この IP アドレスは、ブリッジ ドメインの 1 つである必要があります。

b) F5 の設定可能なパラメータ：

パラメータ	サンプル値	説明
fvBD name	「MyLB」	この値はロード バランサの ID で、ロード バランサ選択のプラン セクションの、Windows Azure Pack の管理者ポータルに表示されます。これは、同じ代替値を持つ XML POST 全体でグローバルに変更できます。
vnsRsALDevToDomP tDn	「uni/vmmp-VMware/dom-mininet」	これは、有効な VLAN ENCAP ブロックを持つ任意の VMM ドメインです。 （注） この Windows Azure Pack のロード バランサ設定では、この VMM ドメインに LB 構成との関連性はほかにありません。これは、後方互換性のために使用されます。
vnsCMgmt name="devMgmt" host	「172.31.210.88」	これは、ACI ファブリックに通信されるロード バランサの IP アドレスです。
vnsCCred name	「username」	ユーザ名。
vnsCCredSecret name	「password」	パスワード。

ステップ 3 F5 または Citrix のいずれかのデバイス パッケージを POST します。

プランに合わせたロード バランサの作成

管理者のみがデバイス パッケージをインポートできます。

始める前に

- デバイス パッケージをインポートします。
- XML POST の設定と Application Policy Infrastructure Controller（APIC）へのポスト

手順

ステップ 1 サービス管理ポータル（管理者ポータル）にログインします。

ステップ 2 [Navigation] ペインで [PLANS] を選択します。

ステップ 3 [plans] ペインで、ロード バランサを追加するプランを選択します（shareplan）。

ステップ 4 [shareplan] ペインで **[Networking (ACI)]** を選択します。

ステップ 5 [networking (aci)] ペインで、次の操作を実行して共有ロード バランサを追加します。

a) [shared load balancer] チェックボックスをオンにします。

b) [LB DEVICE ID IN APIC] フィールドで、ドロップダウン リストからロード バランサ（MyLB）を選択します。

c) [VIP RANGE] フィールドで、VIP 範囲（5.5.5.1 ～ 5.5.5.100）を指定します。

d) [SAVE] をクリックします。

（注） VIP 範囲が重複しない限り、異なるプラン間で共有される、単一のロード バランサを使用できます。

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。Microsoft Windows Azure Pack 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。

Windows Azure Pack 用に L3 外部接続を設定するための前提条件

Windows Azure Pack 用にレイヤ 3（L3）外部接続を設定するには、次の前提条件を満たす必要があります。

- Application Policy Infrastructure Controller（APIC）GUI にログインしていることを確認し、メニューバーで **[TENANT]** > **common]** の順に選択します。
  - 「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 にログインしていることを確認し、メニューバーで **[TENANT]** > **common]** の順に選択します。

- 「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。

Windows Azure Pack は、上で強調表示した命名規則以外の特別な要件なしで、共通 l3ExtOut 構成を利用します。

l3extinstP「default」で提供される契約の作成

ここでは、l3extinstP「default」で提供される契約の作成方法を説明します。

Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （367 ページ）を参照してください。

スコープが「グローバル」であることを確認します。この契約では、コンシューマからプロバイダーへのすべてのトラフィックを許可し、プロバイダーからコンシューマへ確立された TCP のみを許可します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

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

ステップ 3 [ACTION] をクリックし、ドロップダウン リストから [Create Contract] を選択します。

ステップ 4 [Create Contract] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに名前（L3_DefaultOut）を入力します。
b) [Scope] タブで、ドロップダウン リストから [Global] を選択します。
c) [Subjects] フィールドで、[+] アイコンをクリックします。
d) [Create Contract Subject] ダイアログボックスで、次の操作を実行します。
e) [Name] フィールドに、任意の名前を入力します。
f) [Apply Both direction] をオフにします。
g) **[Filter Chain For Consumer to Provider]** フィールドで **[+]**アイコンをクリックし、ドロップダウン リストから **[default/common]** を選択して、**[Update]** をクリックします。
h) **[Filter Chain For Provider to Consumer]** フィールドで [+] アイコンをクリックし、ドロップダウン リストから **[est/common]**を選択して、**[Update]** をクリックします。
i) **[OK]**をクリックして **[Create Contract Subject]**ダイアログボックスを閉じます。
j) [OK] をクリックして [Create Contract] ダイアログボックスを閉じます。

これで、l3extinstP「default」で提供される契約が作成されました。

l3extinstP「vpcDefault」で提供される契約の作成

ここでは、l3extinstP「vpcDefault」で提供される契約の作成方法を説明します。

Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （367 ページ）を参照してください。

スコープが「グローバル」であることを確認します。この契約では、コンシューマからプロバイダーへのすべてのトラフィックを許可し、プロバイダーからコンシューマへ確立された TCP のみを許可します。

手順

ステップ 1 APIC GUI にログインし、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

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

ステップ 3 [ACTION] をクリックし、ドロップダウン リストから [Create Contract] を選択します。

ステップ 4 [Create Contract] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに名前（L3_VpcDefaultOut）を入力します。
b) [Scope] タブで、ドロップダウン リストから [Global] を選択します。
c) [Subjects] フィールドで、[+] アイコンをクリックします。
d) [Create Contract Subject] ダイアログボックスで、次の操作を実行します。
e) [Name] フィールドに、任意の名前を入力します。
f) [Apply Both direction] をオフにします。
g) **[Filter Chain For Consumer to Provider]** フィールドで **[+]**アイコンをクリックし、ドロップダウン リストから **[default/common]** を選択して、**[Update]** をクリックします。
h) **[Filter Chain For Provider to Consumer]** フィールドで [+] アイコンをクリックし、ドロップダウン リストから **[est/common]**を選択して、**[Update]** をクリックします。
i) **[OK]**をクリックして **[Create Contract Subject]**ダイアログボックスを閉じます。
j) [OK] をクリックして [Create Contract] ダイアログボックスを閉じます。

これで、l3extinstP「vpcDefault」で提供される契約が作成されました。

テナントのタスク

ここでは、テナントのタスクについて説明します。

（注） 共有サービスのコンシューマがプロバイダとは異なる VRF に属している場合には、通信を可能にするため、VRF 間のルート リーキングが自動的に生じます。

共有または仮想プライベート クラウド プランのエクスペリエンス

これは、共有または仮想プライベートクラウド（VPC）プランでのテナントのエクスペリエンスです。

共有プランでのネットワークの作成

これにより、管理者は共有プランのネットワークを作成できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **[ACI]** ペインで、**[NETWORKS]** を選択します。

ステップ 4 **[New]** をクリックします。

ステップ 5 **[NEW]** ペインで、**[NETWORKS]** を選択し、以下の操作を実行します。

a) **[NETWORK NAME]** フィールドに、ネットワークの名前 (S01) を入力します。

b) **[CREATE]** をクリックします。

c) **[REFRESH]** をクリックします。

APIC の *Microsoft Windows Azure Pack* で作成されたネットワークの確認

ここでは、APIC の Microsoft Windows Azure Pack で作成し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 APIC GUI にログインし、メニュー バーで [TENANTS] を選択します。

ステップ 2 **Navigation**ペインで、**Tenant 018b2f7d-9e80-43f0-abff-7559c026bad5** > **Application Profiles** > **default** > **Application EPGs** > **EPG Network01** の順に展開し、Microsoft Windows Azure Pack で作成したネットワークがAPIC で作成されたことを確認します。

VPC プランでのブリッジ ドメインの作成

仮想プライベートクラウド（VPC）プランのみに適用されます。これにより、テナントはネットワークに対する独自の IP アドレス空間を取得できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、[BRIDGE DOMAIN] を選択します。

ステップ 5 [BRIDGE DOMAIN] フィールドにブリッジ ドメイン名（BD01）を入力します。

ステップ 6 現在のテナントが複数の Azure Pack プランをサブスクライブしている場合は [Subscription] を選択し、対象のブリッジ ドメインを作成します。

ステップ 7 オプション：[SUBNET'S GATEWAY] フィールドにサブネットのゲートウェイ（192.168.1.1/24）を入力します。

ステップ 8 **[コンテキスト]** フィールドで、すでにサブスクリプションの一部になっているコンテキストを選択するか、または **[新規作成]** を選択して、ブリッジ ドメインに新規コンテキストを作成します。

ステップ 9 [CREATE] をクリックします。

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

これにより、テナントは VPC プランでネットワークを作成し、ブリッジ ドメインに関連付けることができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで [NETWORK] を選択します。

ステップ 5 [NETWORK NAME] フィールドに、ネットワーク名（S01）を入力します。

ステップ 6 [BRIDGE NAME] フィールドに、ブリッジ名（BD01）を入力します。

ステップ 7 [CREATE] をクリックします。

ステップ 8 [aci] ペインで、[NETWORKS] を選択します。

ネットワークがブリッジ ドメインに関連付けられていることがわかります。

同一サブスクリプション内のファイアウォールの作成

これにより、テナントは同一サブスクリプション内にファイアウォールを作成できます。

始める前に

2 つのネットワークが作成されていることを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、[FIREWALL] を選択します。

ステップ 5 [FROM NETWORK] フィールドで、ドロップダウン リストから、ネットワーク名（WEB01）を選択します。

ステップ 6 [TO NETWORK] フィールドで、ドロップダウン リストから、もう 1 つのネットワーク名（WEB02）を選択します。

ステップ 7 [PROTOCOL] フィールドにプロトコル（tcp）を入力します。

ステップ 8 [PORT RANGE BEGIN] フィールドに開始ポート範囲（50）を入力します。

ステップ 9 [PORT RANGE END] フィールドに終了ポート範囲（150）を入力します。

ステップ 10 [CREATE] をクリックします。
同一サブスクリプション内にファイアウォールが追加されました。

VPC プランでのネットワークの構築

これにより、テナントは VPC プランでネットワークを作成できます。

手順

ステップ 1 サービス管理ポータル（テナント ポータル）にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 **[New]** をクリックします。

ステップ 4 [NEW] ペインで **[ACI]** > **[NETWORK]** の順に選択して、次の操作を実行します。

a) [NETWORK NAME] フィールドに、ネットワーク名（Network01）を入力します。

b) オプション 1：共有ブリッジ ドメインにネットワークを作成します。

- [BRIDGE DOMAIN] フィールドで、ドロップダウン リストからブリッジ ドメインを選択します。（デフォルト）。
- [CREATE] をクリックします。

  このプロセスが完了するには、数分かかることがあります。

c) オプション 2：テナント ブリッジ ドメインにネットワークを作成します。

- [BRIDGE DOMAIN] フィールドで、ドロップダウン リストからブリッジ ドメイン（myBridgeDomain）を選択します。

d) オプション：スタティック IP アドレス プールを使用してネットワークを導入するには、次の操作を実行します。

- アドレス/マスクの形式でゲートウェイを入力します（192.168.1.1/24）。結果のスタティック IP アドレス プールはゲートウェイ サブネットの全範囲を使用します。
- DNS サーバを入力します。複数のサーバが必要な場合は、セミコロンを使用してリストを区切ります（192.168.1.2;192.168.1.3）。

（注） サブネットは、コンテキスト内の他のすべてのサブネットと照合して検証されます。ネットワークの作成では、重複が検出された場合はエラーが返されます。

- [CREATE] をクリックします。

このプロセスが完了するには、数分かかることがあります。

VM の作成とネットワークへの接続

これにより、テナントは VM を作成し、ネットワークに接続することができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、**[STANDALONE VIRTUAL MACHINE]** > **[FROM GALLERY]** の順に選択します。

ステップ 5 [Virtual Machine Configuration] ダイアログボックスで、設定（LinuxCentOS）を選択します。

ステップ 6 次に進む矢印をクリックします。

ステップ 7 [Portal Virtual Machine Settings] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに VM 名（SVM01）を入力します。
b) [ADMINISTRATOR ACCOUNT] フィールドに root が表示されます。
c) [New Password] フィールドに新しいパスワードを入力します。
d) 確認のために [CONFIRM] フィールドにもう一度パスワードを入力します。
e) 次に進む矢印をクリックします。

ステップ 8 [Provide Virtual Machine Hardware Information] ダイアログボックスで、次の操作を実行します。

a) [NETWORK ADAPTER 1] フィールドのドロップダウン リストから、関連付けて計算するネットワーク アダプタ（6C6DB302-aObb-4d49-a22c-151f2fbad0e9|default|S01）を選択します。
b) チェックマークをクリックします。

ステップ 9 [Navigation] ペインで、[Virtual Machines] を選択して VM（SVM01）のステータスを確認します。

共有サービスの提供

これにより、テナントは共有サービスを提供することができます。

始める前に

管理者がテナントによる共有サービスの提供を許可していることを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [ACI] ペインで [SHARED SERVICE] を選択します。

ステップ 4 [SHARED SERVICES] ダイアログボックスで、次の操作を実行します。

a) [ACTION] フィールドで、ドロップダウン リストから、[PROVIDE A SHARED SERVICE CONTRACT] を選択します。
b) [NETWORK] フィールドで、ドロップダウン リストから、ネットワーク（WEB01）を選択します。
c) [SERVICE NAME] フィールドに、サービス名（DBSrv）を入力します。
d) [DESCRIPTION] フィールドに、説明を入力します。
e) [PROTOCOL] フィールドにプロトコル（tcp）を入力します。
f) [PORT RANGE BEGIN] フィールドに、ポート範囲の開始（139）を入力します。
g) [PORT RANGE END] フィールドに、終了ポート範囲（139）を入力します。
h) チェックマークをクリックします。

消費される共有サービスの設定

これにより、テナントは消費される共有サービスを設定できます。

始める前に

- 管理者がテナントによる共有サービスの提供を許可していることを確認します。
- テナントが共有サービスを提供していることを確認します。
- 管理者がプランで共有サービスを有効化していることを確認します。
- 共有サービス コンシューマは、プロバイダーよりも異なる VRF では、ルート漏出、Vrf 間では、通信を有効にするには自動的に発生します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 ナビゲーション ウィンドウで、**[ACI]** > **[SHARED SERVICE]** の順に選択します。

ステップ 3 **[SHARED SERVICE]** ダイアログボックスで、次の操作を実行します。

a) **[Network]** フィールドで、ネットワーク (V1) を選択します。

b) **[Consumed Services]** フィールドで、サービスのチェックボックス (DBSrv) をオンにします。

c) チェックマークを付けます。

ステップ 4 **[aci]** ペインで **[SHARED SERVICES]** を選択して、プランのコンシューマをチェックします。

ロード バランサの設定

これにより、テナントはロード バランサを設定することができます。

始める前に

- 管理者がデバイス パッケージをインポートしたことを確認します。
- 管理者が XML POST を設定し、Application Policy Infrastructure Controller（APIC）にポストしたことを確認します。
- 管理者がプランにロード バランサを追加したことを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、[LOAD BALANCER] を選択します。

ステップ 5 [NETWORK NAME] フィールドに、ネットワーク名（WEB01）を入力します。

ステップ 6 [PORT] フィールドにポート（80）を入力します。

ステップ 7 [PROTOCOL] フィールドにプロトコル（tcp）を入力します。

ステップ 8 [CREATE] をクリックします。

ステップ 9 [ACI] ペインで、[LOAD BALANCER] を選択し、ロード バランサのネットワーク、仮想サーバ、アプリケーション サーバ、ポート、およびプロトコルを確認します。

ブリッジ ドメインには次のサブネットを設定してください。

- SNIP のサブネット
- ホストのサブネット

- VIP のサブネット

VIP のサブネットが必要な場合は、L3 または L2 extOut にリンクする必要があります。

アクセス コントロール リストの追加

これにより、テナントは共有サービスにアクセス コントロール リスト（ACL）を追加することができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [aci] ペインで [SHARED SERVICES] を選択します。

ステップ 4 [aci] ペインで、ACL（DBSrv）をさらに追加する共有サービスを選択します。

ステップ 5 [+ACL] をクリックして ACL を追加します。

ステップ 6 [Add ACL for DBSrv] ダイアログボックスで、次の操作を実行します。

a) [PROTOCOL] フィールドにプロトコル（tcp）を入力します。
b) [PORT NUMBER BEGIN] フィールドに、開始ポート番号（301）を入力します。
c) [PORT NUMBER END] フィールドに、終了ポート番号（400）を入力します。
d) チェックマークをクリックします。

アクセス コントロール リストの削除

これにより、テナントは共有サービスからアクセス コントロール リスト（ACL）を削除することができます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **[aci]** ペインで、次の操作を実行します。

a) **[SHARED SERVICES]** を選択します。
b) ACL を削除する共有サービス（DBSrv）を選択します。
c) **[Trash ACL]** をクリックして ACL を削除します。

ステップ 4 **[Delete ACL from DBSrv]** ダイアログボックスで、削除する ACL のチェック ボックスをオンにし、チェックマークをクリックします。

Windows Azure Pack で使用する APIC 上でのテナント L3 外部発信の準備

ここでは、Windows Azure Pack で使用するためにテナント L3 外部発信を APIC でどのように準備するかについて説明します。

手順

ステップ 1 APIC GUI にログインし、メニューバーで **[TENANTS]** > **[Tenant Name]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[External Routed Networks]** の順に展開し、[External Routed Networks] を右クリックして [Create Routed Outside] を選択します。

ステップ 3 [Create Route Outside] ダイアログボックスで、次の操作を実行します。

a) 名前（myRouteOut）を入力します。

b) VRF（3b4efb29-f66e-4c93-aed4-dc88ed4be8f2/CTX_01）を選択します。

c) ネットワーク設定の要件に従って現在のダイアログ ボックスを設定します。次の Web サイトには、ACI ファブリック レイヤ 3 Outside 接続の詳細が示されています。http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/basic-config/b_ACI_Config_Guide/b_ACI_Config_Guide_chapter_0110.html

d) [Next] をクリックします。

e) [Finish] をクリックします。

ステップ 4 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[External Routed Networks]** > **[Route Outside Name]** の順に展開し、[Logical Node Profiles] を右クリックして [Create Node Profile] を選択します。

ステップ 5 L3ExtOut のガイドに従って、ノード プロファイルの作成を実行します。次の Web サイトには、ACI ファブリック レイヤ 3 Outside 接続の詳細が示されています。 http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/basic-config/b_ACI_Config_Guide/b_ACI_Config_Guide_chapter_0110.html

ステップ 6 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[External Routed Networks]** > **[Route Outside Name]** の順に展開し、[Networks] を右クリックして [Create External Network] を選択します。

ステップ 7 [Create External Network] ダイアログボックスで、次の操作を実行します。

a) **<RouteOutsideName>InstP** の形式で名前を入力します。たとえば、[Route Outside Name] に **myRoutOut** と入力し、[my External Network Name] に **myRoutOutInstP** を入力します。

b) [Subnet] セクションで、[+] アイコンをクリックします。

c) ネットワーク設計ごとに、[Create Subnet] ダイアログボックスに外部サブネットの詳細を入力します。

d) [Subnet] ダイアログボックスで、[OK] をクリックして完了します。

e) [Create External Network] ダイアログボックスで、[Submit] をクリックします。

ステップ 8 [Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[Bridge Domains]** > **[Bridge Domain Name]** の順に展開し、[L3 Configurations] タブを選択して次の操作を実行します。

a) [Associated L3 Outs] の右側の + アイコンをクリックします。

b) ドロップダウンリストで、[L3 Out (3b4efb29-f66e-4c93-aed4-dc88ed4be8f2/myRouteOut)] を選択します。

c) [UPDATE] をクリックします。
d) [Bridge Domain - <Name>] ページで [Submit] をクリックします。

ステップ 9 オプション：ACI Integrated Windows Azure Pack の統合されたスタティック IP アドレス プール機能を使用しないテナント ネットワークの場合は、次の手順を実行します。

[Navigation] ペインで、**[Tenant Name]** > **[Networking]** > **[Bridge Domains]** > **[Bridge Domain Name]** の順に展開し、[L3 Configurations] タブを選択して次の操作を実行します。

a) [Subnets] の右側の + アイコンをクリックします。
b) [Create Subnet] ダイアログボックスで、次の操作を実行します。
- アドレス/マスクの形式でゲートウェイ IP を入力します。
- [Advertised Externally] チェックボックスをオンにします。
- [Submit] をクリックします。

外部接続用ネットワークの作成

これにより、テナントは外部接続用のネットワークを作成することができます。

外部接続は ACI 共通 L3ExtOut またはユーザ定義の L3ExtOut のいずれかで確立できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 [Navigation] ペインで [ACI] を選択します。
ステップ 3 [New] をクリックします。
ステップ 4 [NEW] ペインで [NETWORK] を選択します。
ステップ 5 [NETWORK NAME] フィールドに、ネットワーク名（wapL3test）を入力します。
ステップ 6 オプション 1：ルート アドバタイズメントにブリッジ ドメインのサブネットを使用します。

[CREATE] をクリックします。

ステップ 7 オプション 2：ルート アドバタイズメントに EPG のサブネットを使用します。

アドレス/マスクの形式でゲートウェイを入力します（192.168.1.1/24）。

a) [CREATE] をクリックします。

外部接続用のファイアウォールの作成

これにより、テナントは外部接続用のファイアウォールを作成することができます。

外部接続は ACI 共通 L3ExtOut またはユーザ定義の L3ExtOut のいずれかで確立できます。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 [Navigation] ペインで [ACI] を選択します。

ステップ 3 [New] をクリックします。

ステップ 4 [NEW] ペインで、[FIREWALL] を選択します。

ステップ 5 オプション 1：ACI 共通の L3ExtOut *External:default を使用した共有 Windows Azure Pack プランまたは VPC Windows Azure Pack プランの場合は、次の手順を実行します。

a) [FROM NETWORK] フィールドで、ドロップダウン リストからネットワーク名（*External:default）を選択します。

オプション 2：ユーザ定義の外部ネットワークを使用した VPC Windows Azure Pack プランの場合は、次の手順を実行します。

a) [FROM NETWORK] フィールドで、ドロップダウン リストからネットワーク名（External:myRouteOut）を選択します。

ステップ 6 [TO NETWORK] フィールドで、ドロップダウン リストから別のネットワーク名（wapL3test）を選択します。

ステップ 7 [PROTOCOL] フィールドにプロトコル（tcp）を入力します。

ステップ 8 [PORT RANGE BEGIN] フィールドに、ポート範囲の開始（12345）を入力します。

ステップ 9 [PORT RANGE END] フィールドに、ポート範囲の終了（45678）を入力します。

ステップ 10 [CREATE] をクリックします。
外部接続用のファイアウォールが追加されました。

APIC でのテナントの L3 外部接続の確認

ここでは、APIC 上のテナントの L3 外部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 APIC GUI にログインし、メニュー バーで [TENANTS] 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 b81b7a5b-7ab8-4d75-a217-fee3bb23f427]** > **[Application Profiles]** > **[Application EPG]** の順に展開し、外部接続用ネットワークの作成 （378 ページ）で作成したネットワークが存在することを確認します（wapL3test）。

ステップ 3 ナビゲーション ウィンドウで、**[EPG wapL3test]** > **[Contracts]** の順に展開し、契約名が L3+EPG 名+プロトコル+ポート範囲（L3wapL3testtcp1234545678）の形式で存在し、契約が EPG によって提供され、STATE が [formed] であることを確認します。

ステップ 4 オプション 1：*External:default で契約を作成した共有 L3 Out 導入では、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

オプション 2：テナント所有の L3 Out 導入では、メニュー バーで **[TENANTS]** > ***<your tenant-id>*** を選択します。

ステップ 5 ナビゲーション ウィンドウで、**[Security Policies]** > **[Imported Contracts]** の順に展開し、ステップ 3 で確認した契約が契約インターフェイスとしてインポートされていることを確認します。

ステップ 6 オプション 1：*External:default で契約を作成した共有 L3 Out 導入では、メニュー バーで **[TENANTS]** > **[common]** の順に選択します。

オプション 2：テナント所有の L3 Out 導入では、**[TENANTS]** > ***<your tenant-id>*** を選択します。

ステップ 7 [External Network Instance Profile -defaultInstP] ペインの [Consumed Contracts] フィールドで、ステップ 5 で確認した契約インターフェイスを探し、それが存在することおよび STATE が [formed] であることを確認します。

ステップ 8 メニュー バーで、**[TENANTS]** を選択します。

ステップ 9 ナビゲーション ウィンドウで、**[Tenant b81b7a5b-7ab8-4d75-a217-fee3bb23f427]** > **[Application Profiles]** > **[Application EPG]** > **[EPG wapL3test]** > **[Contracts]** の順に展開します。

ステップ 10 [Contracts] ペインの [Consumed Contracts] フィールドで、Windows Azure Pack 用に L3 外部接続を設定するための前提条件 （367 ページ）で共有サービスのテナントまたは VPC のテナントのために定義したデフォルトの契約がこの EPG によって消費され、STATE が [formed] であることを確認します。

ステップ 11 オプション 2：ユーザ定義の外部ネットワークとゲートウェイを指定したテナント ネットワークを使用する VPC Windows Azure Pack プランの場合は、次の手順に従います。

[Navigation] ペインで、**[Tenant Name]** > **[Application Profiles]** > **[Application EPG]** > **[EPG *wapL3test*]** > **[Subnets]** > **[Subnet Address]** の順に選択し、[Scope] が [Advertised Externally] とマークされていることを確認します。

VM ネットワークに NAT ファイアウォール レイヤ 4 ～ レイヤ 7 サービスを追加する

これにより、適応型セキュリティ アプライアンス (ASA) ファイアウォールまたはファイアウォール コンテキストがプロビジョニングされ、外部 IP アドレス プールからネットワーク アドレス変換（NAT） IP がダイナミックに割り当てられ、ASA 上にダイナミックな PAT が構成されてアウトバウンド トラフィックが可能になり、サービス グラフの残りの部分のプロビジョニングが容易に行えるようになります。

始める前に

- Azure パック プランがレイヤ 4 ～ レイヤ 7 サービス プールにアクセスできるように構成されていることを確認します。
- ACI VM ネットワークがゲートウェイまたはサブネットを持つように作成されていることを確認します。
- レイヤ 4 ～ レイヤ 7 リソース プールのプライベート サブネットが APIC 管理者から提供されていない場合、サブネットとオーバーラップする状態で レイヤ 4 ～ レイヤ 7 サービ

スを追加しようとすると、エラーが発生し、設定はプッシュされません。この場合、VM ネットワークを削除して、別のサブネットとともに再度作成してください。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。
ステップ 3 **aci** ペインで、**NETWORKS** を選択し、さらにネットワーク設定を入力します。
ステップ 4 **Enable direct internet access using NAT** チェック ボックスをオンにします。
ステップ 5 **SAVE** をクリックします。

NAT ファイアウォール ポート転送ルールを VM ネットワークに追加する

これは、ネットワークアドレス変換（NAT）ファイアウォールを設定し、VMネットワーク内で NAT IP から内部 IP にトラフィックを転送します。

始める前に

- Cisco Application Centric Infrastructure（ACI）VM ネットワークが NAT に設定されていることを確認します。.

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。
ステップ 3 **[aci]** ペインで、**[ネットワーク]** を選択し、さらにネットワーク設定を入力します。
ステップ 4 **[ネットワーク]** ペインで、**[ルール]** を選択します。
ステップ 5 パネル下部の **[追加]** をクリックします。
ステップ 6 ポート転送ルールに必要な情報を入力します。

（注） 宛先 IP アドレスは、VM ネットワークのサブネット範囲内の IP アドレスである必要があります。

ステップ 7 **[保存]** チェックマークをチェックします。

プライベート ADC ロード バランサ レイヤ 4 ～ レイヤ 7 サービスを伴う NAT ファイアウォールを VM ネットワークに追加する

NAT ファイアウォールを展開することに加えて、この設定では内部ロード バランサが展開されます。このシナリオでは、ロード バランサの VIP は、レイヤ 4 ～ レイヤ 7 のプライベート IP アドレス サブネットから (テナント VRF ごとに) 動的に割り当てられます。この 2 ノード

サービス グラフの展開では、テナントが、トラフィックのロード バランシングのために、内部ロードバランサへトラフィックを転送するポート転送規則を作成していることを前提としています。

始める前に

- Azure パック プランがレイヤ 4 ～ レイヤ 7 サービス プールにアクセスするように設定されていることを確認します。
- ACI VM ネットワークが、ゲートウェイまたはサブネットを持つように作成されていることを確認します。
- レイヤ 4 ～ レイヤ 7 リソース プールのプライベート サブネットが APIC 管理者から提供されていない場合、サブネットとオーバーラップする状態で レイヤ 4 ～ レイヤ 7 サービスを追加しようとすると、エラーが発生し、設定はプッシュされません。このような場合には、VM ネットワークを削除し、代わりのサブネットを用意して再度作成してください。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。
ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。
ステップ 3 **aci** ペインで、**NETWORKS** を選択し、さらにネットワーク設定を入力します。
ステップ 4 **Enable direct internet access using NAT** チェック ボックスをクリックします。
ステップ 5 **Enable internal load balancer (internal)** チェック ボックスをクリックします。
ステップ 6 **SAVE** をクリックします。

VRF の追加の NAT ファイアウォールのパブリック IP アドレスを要求します。

NAT ルールを使用するため、追加のパブリック IP アドレスを割り当てるには、次の手順を使用します。NAT が有効になっているすべての EPG からこのパブリック IP アドレスを要求できます。したがって、VRF 内のすべての Epg の使用可能です。

NAT ルールは、各 EPG に保存されます。したがってことをお勧め NAT ルールのポイントの宛先 IP、EPG 内およびしない、VRF に別の場所にエンドポイントにのみ。

始める前に

NAT ファイアウォールの Cisco ACI VM 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 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **Aci**] ペインを選択します **ネットワーク** 、矢印をクリックしてさらにネットワーク構成を入力します。

ステップ 4 **ネットワーク**] ペインで、選択 **IP アドレス** 。

ステップ 5 下部のパネルでをクリックして **IP アドレスを要求** 。

ステップ 6 [OK] をクリックします。

L4 L7 リソース プールで使用可能なパブリック IP アドレスがある場合は、IP アドレスが割り当てられ、このテーブルに存在します。この IP アドレスもに存在するが、 **ルール**] タブの [着信の NAT ルールを設定します。

パブリック ADC ロード バランサ レイヤ 4 ～ レイヤ 7 サービスを VM ネットワークに追加する

これにより、ロード バランサが提供され、外部 IP アドレス プールから VIP が動的に割り当てられ、必要なルートとプロビジョニングがサービス グラフの残りの部分に追加されるので、導入が容易になります。

始める前に

- Azure パック プランがレイヤ 4 ～ レイヤ 7 サービス プールにアクセスするように設定されていることを確認します。
- ACI VM ネットワークが、ゲートウェイまたはサブネットを持つように作成されていることを確認します。
- レイヤ 4 ～ レイヤ 7 リソース プールのプライベート サブネットが APIC 管理者から提供されていない場合、サブネットとオーバーラップする状態で レイヤ 4 ～ レイヤ 7 サービスを追加しようとすると、エラーが発生し、設定はプッシュされません。このような場合には、VM ネットワークを削除し、代わりのサブネットで VM ネットワークを再度作成してください。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **aci** ペインで、 **NETWORKS** を追加し、矢印をクリックして残りのネットワーク設定を入力します。

ステップ 4 **Enable load balancer (public)** チェック ボックスをオンにします。

ステップ 5 (オプション) **Allow Outbound Connections** チェック ボックスをオンにします。

（注） このオプションを使用できるのは、この VM ネットワークで NAT が設定されていない場合だけです。

ステップ 6 **SAVE** をクリックします。

VM ネットワークに ADC ロード バランサの設定を追加する

これにより、パブリックかプライベートの ADC ロード バランサが設定されます。VM ネットワークに割り当てられた VIP 上でリッスンし、ロード バランシングの行われるトラフィックを、接続数の最も少ない実サーバに転送します。VM ネットワーク全体が負荷分散されることになります。VM または VNIC がオンラインになると、それらは自動的にロード バランサに追加されます。VM ネットワーク全体で負荷分散が行われるため、VM ネットワークのすべてのエンドポイントが同一であり、定義されているロードバランサのサービスを行えると想定されます。

始める前に

- ACI VM ネットワークが、パブリックまたはプライベートのロードバランシングに合わせて設定されていることを確認します。

手順

ステップ 1 サービス管理ポータル (テナント ポータル) にログインします。

ステップ 2 **[Navigation]** ペインで **[ACI]** を選択します。

ステップ 3 **aci** ペインで、 **NETWORKS** を追加し、矢印をクリックして残りのネットワーク設定を入力します。

ステップ 4 **NETWORKS** ペインで、**LOAD BALANCERS** を選択します。

ステップ 5 下部パネルの **ADD** をクリックします。

ステップ 6 ロード バランサに必要な情報を入力します (名称: HTTP、プロトコル: TCP、ポート: 80)。

ステップ 7 **SAVE** チェックマークをクリックします。

Cisco ACI with Microsoft Windows Azure Pack のトラブルシューティング

管理者としてのトラブルシューティング

手順

Windows Azure Pack の管理者は管理者ポータルで、テナントによって導入されたすべてのネットワークを表示できます。問題が発生した場合は、APIC GUI を使用して、次のオブジェクトのエラーを探します。

a) VMM ドメイン
b) Windows Azure Pack のテナント ネットワークに対応するテナントおよび EPG

テナントとしてトラブルシューティング

エラー メッセージがある場合、エラー メッセージとともにワークフローの説明および管理者に対するアクションを提供してください。

EPG の設定の問題のトラブルシューティング

エンドポイント グループ（EPG）のライフタイム中、EPG の VLAN ID が APIC で変更された場合、新しい設定を有効にするには、すべての仮想マシンで VLAN 設定を更新する必要があります。

手順

この操作を実行するには、SCVMM サーバで次の PowerShell コマンドを実行します。

例：

```
$VMs = Get-SCVirtualMachine
$VMs | Read-SCVirtualMachine
$NonCompliantAdapters=Get-SCVirtualNetworkAdapter -All | Where-Object
{$_.VirtualNetworkAdapterComplianceStatus -eq "NonCompliant"}
$NonCompliantAdapters | Repair-SCVirtualNetworkAdapter
```

プログラマビリティのリファレンス

ACI Windows Azure Pack の PowerShell コマンドレット

ここでは、Cisco Application Centric Infrastructure（ACI）Windows Azure Pack の PowerShell コマンドレット、ヘルプおよび例をリストする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインし、**[開始]** > **[実行]** > **[Windows PowerShell]** の順に選択します。

ステップ 2 次のコマンドを入力します。

例：

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator> cd C:\inetpub\Cisco-ACI\bin
PS C:\inetpub\Cisco-ACI\bin> Import-Module .\ACIWapPsCmdlets.dll
PS C:\inetpub\Cisco-ACI\bin> Add-Type -Path .\Newtonsoft.Json.dll
PS C:\inetpub\Cisco-ACI\bin> Get-Command -Module ACIWapPsCmdlets

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Add-ACIWAPEndpointGroup                            ACIWapPsCmdlets
Cmdlet          Get-ACIWAPAdminObjects                             ACIWapPsCmdlets
Cmdlet          Get-ACIWAPAllEndpointGroups                        ACIWapPsCmdlets
Cmdlet          Get-ACIWAPBDSubnets                                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPConsumersForSharedService                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPEndpointGroups                           ACIWapPsCmdlets
Cmdlet          Get-ACIWAPEndpoints                                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPLBConfiguration                          ACIWapPsCmdlets
Cmdlet          Get-ACIWAPOpflexInfo                               ACIWapPsCmdlets
Cmdlet          Get-ACIWAPPlans                                    ACIWapPsCmdlets
Cmdlet          Get-ACIWAPStatelessFirewall                        ACIWapPsCmdlets
Cmdlet          Get-ACIWAPSubscriptions                            ACIWapPsCmdlets
Cmdlet          Get-ACIWAPTenantCtx                                ACIWapPsCmdlets
Cmdlet          Get-ACIWAPTenantPlan                               ACIWapPsCmdlets
Cmdlet          Get-ACIWAPTenantSharedService                      ACIWapPsCmdlets
Cmdlet          Get-ACIWAPVlanNamespace                            ACIWapPsCmdlets
Cmdlet          New-ApicOpflexCert                                 ACIWapPsCmdlets
Cmdlet          Read-ApicOpflexCert                                ACIWapPsCmdlets
Cmdlet          Remove-ACIWAPEndpointGroup                         ACIWapPsCmdlets
Cmdlet          Remove-ACIWAPPlan                                  ACIWapPsCmdlets
Cmdlet          Remove-ACIWAPTenantCtx                             ACIWapPsCmdlets
Cmdlet          Set-ACIWAPAdminLogin                               ACIWapPsCmdlets
Cmdlet          Set-ACIWAPBDSubnets                                ACIWapPsCmdlets
Cmdlet          Set-ACIWAPLBConfiguration                          ACIWapPsCmdlets
Cmdlet          Set-ACIWAPLogin                                    ACIWapPsCmdlets
Cmdlet          Set-ACIWAPOpflexOperation                          ACIWapPsCmdlets
Cmdlet          Set-ACIWAPPlan                                     ACIWapPsCmdlets
Cmdlet          Set-ACIWAPStatelessFirewall                        ACIWapPsCmdlets
Cmdlet          Set-ACIWAPTenantSharedService                      ACIWapPsCmdlets
```

```
Cmdlet          Set-ACIWAPUpdateShareServiceConsumption   ACIWapPsCmdlets
Cmdlet          Set-ACIWAPVlanNamespace                   ACIWapPsCmdlets
```

ステップ 3 ヘルプを生成します。

例：

```
commandname -?
```

ステップ 4 例を生成します。

例：

```
get-help commandname -examples
```

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアンインストール

ここでは、Cisco Application Centric Infrastructure（ACI）with Microsoft Windows Azure Pack コンポーネントをアンインストールする方法について説明します。

（注） アンインストールでは、VM や論理ネットワークのようなアーティファクトが削除されます。アンインストールは、VM やホストなどの他のリソースが、これらを使用していないときにのみ成功します。

コンポーネント	タスク
VM ネットワークからのすべての仮想マシンの切断	Microsoft のマニュアルを参照してください。
すべての Hyper-V からの VXLAN トンネル エンドポイント（VTEP）の論理スイッチの削除	Microsoft のマニュアルを参照してください。
System Center Virtual Machine Manager（SCVMM）からのクラウドの削除	Microsoft のマニュアルを参照してください。
ACI with Microsoft Windows Azure Service Pack 1.1(1j) リリースをアンインストールするために APIC Windows Azure Pack リソース プロバイダーをアンインストール	APIC Windows Azure Pack のリソース プロバイダーのアンインストール（388 ページ）を参照してください。

コンポーネント	タスク
このリリースの ACI with Microsoft Windows Azure Pack をアンインストールするために以下をアンインストール • ACI Azure Pack リソース プロバイダー • ACI Azure Pack 管理者サイト拡張 • ACI Azure Pack テナント サイト拡張	ACI Azure Pack リソース プロバイダーのアンインストール （388ページ）を参照してください。 ACI Azure Pack 管理者サイト拡張のアンインストール （389ページ）を参照してください。 ACI Azure Pack テナント サイト拡張のアンインストール （389 ページ）を参照してください。
APIC Hyper-V エージェントのアンインストール	APIC Hyper-V エージェントのアンインストール （390 ページ）を参照してください。

APIC Windows Azure Pack のリソース プロバイダーのアンインストール

ここでは、APIC Windows Azure Pack のリソース プロバイダーをアンインストールする方法について説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [APIC Windows Azure Pack Resource Provider] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから APIC Windows Azure Pack のリソース プロバイダーがアンインストールされます。

ステップ 4 APIC Windows Azure Pack のリソース プロバイダーがアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。
b) [Programs and Features] ウィンドウで [APIC Windows Azure Pack Resource Provider] が表示されていないことを確認します。

ACI Azure Pack リソース プロバイダーのアンインストール

ここでは、ACI Azure Pack のリソース プロバイダーをアンインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [ACI Azure Pack Resource Provider] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから ACI Azure Pack のリソース プロバイダーがアンインストールされます。

ステップ 4 ACI Azure Pack のリソース プロバイダーがアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

b) [Programs and Features] ウィンドウで [ACI Azure Pack Resource Provider] が表示されていないことを確認します。

ACI Azure Pack 管理者サイト拡張のアンインストール

ここでは、ACI Azure Pack の管理者サイト拡張をアンインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [ACI Azure Pack Admin Site Extension] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから ACI Azure Pack の管理者サイト拡張がアンインストールされます。

ステップ 4 ACI Azure Pack の管理者サイト拡張がアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[プログラムのアンインストール]** の順に選択します。

b) [プログラムと機能] ウィンドウで [ACI Azure Pack Admin Site Extension] が表示されていないことを確認します。

ACI Azure Pack テナント サイト拡張のアンインストール

ここでは、ACI Azure Pack のテナント サイト拡張をアンインストールする方法を説明します。

手順

ステップ 1 Windows Azure Pack サーバにログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [ACI Azure Pack Tenant Site Extension] を右クリックして、[Uninstall] を選択します。
これにより、Windows Azure Pack サーバから ACI Azure Pack のテナント サイト拡張がアンインストールされます。

ステップ 4 ACI Azure Pack のテナント サイト拡張がアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

b) [Programs and Features] ウィンドウで [ACI Azure Pack Tenant Site Extension] が表示されていないことを確認します。

APIC Hyper-V エージェントのアンインストール

ここでは、APIC Hyper-V エージェントをアンインストールする方法について説明します。

手順

ステップ 1 Hyper-V Server にログインします。

ステップ 2 **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

ステップ 3 [Programs and Features] ウィンドウで [Cisco APIC HyperV Agent] を右クリックして、[Uninstall] を選択します。
これで、Hyper-V Server から APIC Hyper-V エージェントがアンインストールされます。

ステップ 4 APIC Hyper-V エージェントがアンインストールされたかどうかを確認するには、次の操作を実行します。

a) **[Start]** > **[Control Panel]** > **[Uninstall a Program]** の順に選択します。

b) [Programs and Features] ウィンドウで [Cisco APIC HyperV Agent] が表示されていないことを確認します。

ステップ 5 Hyper-V Server ごとにステップ 1 ～ -4 を繰り返します。

Cisco ACI および Microsoft Windows Azure Pack コンポーネントでの Cisco APIC およびスイッチ ソフトウェアのダウングレード

ここでは、Cisco ACI with Microsoft Windows Azure Pack コンポーネントで Cisco APIC とスイッチ ソフトウェアをダウングレードする方法について説明します。

（注） Cisco APIC 3.1 (1) 以降で作成し使用しているレイヤ 4 ～ レイヤ 7 のリソース プール設定は、古いビルドの Cisco APIC/Windows Azure Pack と互換性がありません。ステップ 1 ～ 3 は、Cisco APIC 3.1(1) 以降のバージョンをそれより前のバージョンにダウングレードする場合に適用されます。

手順

ステップ 1 Cisco APIC でレイヤ 4 ～ レイヤ 7 のリソース プールのリストを確認します。

Cisco APIC 3.1(1) 以降で作成したリソース プールのリストを控えておきます。これらのリソース プールでは、GUI に [Function Profiles] タブがあり、NX-OS スタイル CLI の設定に「version normalized」があります。

ステップ 2 Windows Azure Pack テナント ポータル：レイヤ 4 ～ レイヤ 7 クラウド オーケストレータ モードのリソース プール（Cisco APIC 3.1(1) 以降で作成したリソース プール）を使用して、仮想プライベート クラウドのある Cisco ACI VM ネットワークごとに、次の手順を実行します。

a) サービス管理ポータル (テナント ポータル) にログインします。
b) [Navigation] ペインで [ACI] を選択します。
c) [aci] ペインで [NETWORKS] を選択し、矢印をクリックして、さらにネットワーク設定を入力します。
d) [Enable direct internet access using NAT] チェックボックスがオンの場合はオフにします。
e) [Enable internal load balancer（internal）] チェックボックスがオンの場合はオフにします。
f) [Enable load balancer（public）] チェックボックスがオンの場合はオフにします。
g) [SAVE] をクリックします。

ステップ 3 Windows Azure Pack 管理者：プラン サービスとして ACI ネットワー キングを追加し、レイヤ 4 ～ レイヤ 7 クラウド オーケストレータ モードのリソース プールを使用している Windows Azure Pack プランごとに、次の手順を実行します。

a) サービス管理ポータル (管理者ポータル) にログインします。
b) [Navigation] ペインで [PLANS] を選択します。
c) [Plans] ペインで、[PLANS] を選択し、プラン（ゴールド）をクリックします。
d) [Gold] ペインで、[Networking（ACI）] を選択します。

e) [Networking] ペインで、次のいずれかの操作を実行します。

- Cisco APIC 管理者が Cisco APIC 3.0(x) またはそれ以前で Azure Pack を使用するためにプロビジョニングしたレイヤ 4 ～ レイヤ 7 リソース プールを選択します。
- [Choose one…] を選択して、Azure Pack テナント用の仮想プライベート クラウド NAT ファイアウォール サービスおよび ADC ロード バランサ サービスを無効にします。

f) [SAVE] をクリックします。

ステップ 4 Cisco ACI with Microsoft Windows Azure Pack コンポーネントをアンインストールします。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのアンインストール （387 ページ）を参照してください。

ステップ 5 APIC コントローラとスイッチ ソフトウェアをダウングレードします。

『Cisco APIC ファームウェアの管理、インストール、アップグレード、およびダウングレード ガイド』を参照してください。

ステップ 6 ダウングレード バージョンの Cisco ACI with Microsoft Windows Azure Pack コンポーネントをインストールします。

Cisco ACI with Microsoft Windows Azure Pack コンポーネントのインストール、設定および確認（336 ページ）を参照してください。