



## Cisco ACI 仮想エッジインストールガイド、リリース 3.2(x)

初版：2021年6月8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/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ [www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/) ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



## 目次

---

第 1 章	<b>新機能および変更された機能に関する情報 1</b>
	新機能および変更された機能に関する情報 1

---

第 2 章	<b>Cisco ACI Virtual Edge 3</b>
	Cisco ACI Virtual Edge とは 3
	Cisco ACI Virtual Edge および VMware vCenter 5
	マルチポッド環境での Cisco ACI Virtual Edge 6
	必要なソフトウェア 7
	Cisco ACI vPod : Cisco ACI ファブリックを拡張する 7

---

第 3 章	<b>Cisco ACI Virtual Edge のインストール 9</b>
	Cisco ACI Virtual Edge のインストールについて 9
	デフォルトのポートグループ 11
	Cisco ACI Virtual Edge のインストール ワークフロー 11
	Cisco ACI Virtual Edge をインストールするための前提条件 12
	Cisco APIC の設定の構成 14
	vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの作成 14
	インターフェイスとスイッチのプロファイルのガイドラインと前提条件 15
	vCenter ドメイン プロファイルのガイドラインと前提条件 17
	GUI を使用した vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの作成 18
	VMware vSphere Client HTML5 GUI を使用して ESXi ホストと PNIC を追加する 24
	Cisco ACI vCenter プラグインの Flash バージョンを使用した ESXi ホストおよび PNIC の追加 26

vCenter を使用した Cisco ACI Virtual Edge のインストール	27
Cisco ACI 仮想エッジ VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードする	27
Cisco ACI vCenter プラグインの HTML5 バージョンを使用して OVF ファイルをアップロードする	28
Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードする	29
Cisco ACI vCenter プラグインの HTML5 バージョンを使用して Cisco ACI 仮想エッジを展開する	30
Cisco ACI vCenter プラグインを使用した ESXi ホストでの Cisco ACI Virtual Edge のデプロイ	31
VMware PowerCLI を使用した Cisco ACI Virtual Edge のインストール	33
PowerCLI 環境の設定	33
VMware PowerCLI を使用した VMware vCenter コンテンツ ライブラリの管理	34
VMware PowerCLI を使用した Cisco ACI Virtual Edge の展開	35
Python を使用した Cisco ACI Virtual Edge のインストール	37
Python 環境の設定	38
Python を使用した VMware vCenter コンテンツ ライブラリの管理	39
Python を使用して Cisco ACI Virtual Edge を展開する	41
Cisco ACI Virtual Edge 展開の確認	43
GUI を使用した Cisco ACI 仮想エッジ ライセンスの表示	44
VMware vCenter でスタティック IP アドレスを設定する	45
VMware vSphere クライアントの HTML5 バージョンを使用したスタティック IP アドレスの設定	45
VMware vSphere Web クライアントの Flash バージョンを使用したスタティック IP アドレスの設定	46
インストール後の設定	47
<hr/>	
第 4 章	<b>Cisco AV から移行する Cisco ACI Virtual Edge</b> 49
Cisco AVS から Cisco ACI Virtual Edge 移行する	49
Cisco AV から移行するための方法を Cisco ACI Virtual Edge	49
Cisco AVS から Cisco ACI Virtual Edge に移行するための前提条件	52

	GUI を使用して Cisco AVS VMM ドメインを Cisco ACI Virtual Edge に移行する	53
	Cisco ACI vCenter プラグイン を使用して Cisco AVS から Cisco ACI Virtual Edge に移行する	55
<b>第 5 章</b>	<b>VMware VDS からの移行 Cisco ACI Virtual Edge</b>	<b>57</b>
	Cisco ACI Virtual Edge への VDS ドメインの移行について	57
	VDS ドメインへの移行 Cisco ACI Virtual Edge GUI を使用して	58
<b>第 6 章</b>	<b>Cisco ACI Virtual Edge のアップグレード</b>	<b>61</b>
	Cisco ACI 仮想エッジのアップグレードについて	61
	Cisco APIC、ファブリック スイッチ、および Cisco ACI Virtual Edge での推奨アップグレード手順	63
	Cisco ACI Virtual Edge アップグレードのワークフロー	64
	Cisco ACI Virtual Edge のアップグレードのための前提条件	64
	Cisco ACI Virtual Edge のアップグレード	65
	Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードする	65
	Cisco ACI vCenter プラグインを使用した ESXi ホストでの Cisco ACI Virtual Edge のデプロイ	66
<b>第 7 章</b>	<b>Cisco ACI Virtual Edge のアンインストール</b>	<b>69</b>
	Cisco ACI Virtual Edge のアンインストールについて	69
	Cisco ACI Virtual Edge のアンインストールのワークフロー	69
	Cisco ACI vCenter プラグインを使用して、Cisco ACI Virtual Edge をアンインストールする	70
	VMware PowerCLI を使用した Cisco ACI Virtual Edge のアンインストール	72
	Python を使用した Cisco ACI Virtual Edge のアンインストール	73
<b>付録 A :</b>	<b>サポートされるトポロジ</b>	<b>75</b>
	直接接続	75
	シスコ ファブリック エクステンダ	77
	Cisco UCS ファブリック インターコネクトでの VPC	77
	Cisco Nexus 5000 および MAC ピン接続によるデュアルサイド VPC	78
	Cisco Nexus 5000 および VPC によるデュアルサイド VPC	79

Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトを使用したシングルサイド VPC 80

Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトによるデュアルサイド VPC 81

---

付録 B :	作成 vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの代替手順 83
	ポート チャネル スイッチおよびインターフェイスのプロファイルの作成 83
	GUI を使用した VPC インターフェイスとスイッチ プロファイルの作成 85
	GUI を使用して FEX ノードのインターフェイスとスイッチ プロファイルを作成する 88
	インターフェイス ポリシー グループを変更して vSwitch 側のポリシーをオーバーライドする 90
	Cisco ACI Virtual Edge の VMM ドメイン プロファイルの作成 92

---

付録 C :	VMware vSphere Proactive HA を使用して Cisco ACI 仮想エッジ可用性を改善する 97
	Cisco ACI 仮想エッジ可用性の改善 97
	vSphere Proactive HA を使用する利点 99
	vSphere Proactive HA の仕組み 100
	VMware vSphere Proactive HA を設定するための前提条件 102
	vSphere Proactive HA in Cisco APIC で vSphere Proactive HA を有効にする 102
	VMware vCenter で vSphere Proactive HA を有効にする 103
	ESXi ホストのヘルス レベルの手動設定 104
	Cisco APIC GUI を使用して Cisco ACI 仮想エッジ ホストの状態を表示して設定する 104
	VMware vCenter のホスト向けヘルス アップデートのトラッキング 105
	VM グループ検疫保護 105
	Cisco APIC GUI を使用した VM グループ保護の設定 106

---

付録 D :	NX-OS Style CLI を使用してタスクを実行する 107
	Cisco ACI 仮想エッジへの移行 107
	NX-OS スタイルの CLI を使用して VDS ドメインを Cisco ACI Virtual Edge へ移行する 107
	VMware vSphere Proactive HA を使用して Cisco ACI 仮想エッジの可用性の向上 108
	NX-OS Style CLI を使用して vSphere Proactive HA を有効にする 108
	NX-OS Style CLI を使用して Cisco ACI 仮想エッジ ホストで状態を設定する 109

NX-OS Style CLI を使用して VM グループ保護を設定する 110

---

付録 E :

**REST API を使用してタスクを実行する 111**

Cisco ACI 仮想エッジへの移行 111

REST API を使用して Cisco AVS VMM ドメインを Cisco ACI Virtual Edge に移行する 111

REST API を使用して VDS ドメインを Cisco ACI Virtual Edge へ移行する 112

VMware vSphere Proactive HA による Cisco ACI 仮想エッジの可用性の向上 113

REST API を使用して vSphere Proactive HA を有効にする 113

REST API を使用して REST API 仮想エッジで状態を設定する 114

REST API を使用して VM グループ保護を設定する 114





# 第 1 章

## 新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

## 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。

機能	説明	参照先
このリリースでは、Cisco ACI 仮想エッジのインストール関連の新機能はありません。	このドキュメントには、以前のリリースからの変更はありません。	該当なし





## 第 2 章

# Cisco ACI Virtual Edge

この章は、次の項で構成されています。

- [Cisco ACI Virtual Edge とは \(3 ページ\)](#)
- [Cisco ACI Virtual Edge および VMware vCenter \(5 ページ\)](#)
- [マルチポッド環境での Cisco ACI Virtual Edge \(6 ページ\)](#)
- [必要なソフトウェア \(7 ページ\)](#)
- [Cisco ACI vPod : Cisco ACI ファブリックを拡張する \(7 ページ\)](#)

## Cisco ACI Virtual Edge とは

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は Cisco ACI 仮想エッジをサポートします。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 AVS を使用する場合には、Cisco ACI Virtual Edge に移行することができます。VMware VDS を使用する場合には、その上で Cisco ACI Virtual Edge を実行できます。Cisco ACI Virtual Edge をカーネル スペースから分離したため、ソリューションはさまざまなハイパーバイザに適応できます。また、単純なアップグレードも容易になります。Cisco ACI Virtual Edge はハイパーバイザ アップグレードに関連付けられていないからです。Cisco ACI 仮想エッジでは、コントロールプレーンの通信に OpFlex プロトコルを実装しています。トラフィックの転送では、ローカルスイッチングおよびローカルスイッチングなしの 2 つのモードをサポートしています。

Cisco ACI Virtual Edge リリース 1.1(1a) は、VMware ハイパーバイザのみをサポートしています。これは、プライベート VLAN (PVLAN) モードで設定された vSphere 分散スイッチ (VDS) を活用します。

ネットワーク管理者が Cisco APIC 上で Cisco ACI Virtual Edge VMM ドメインを作成する場合には、ドメインを、DVS 上のポート グループの PVLAN ペア関連付けで使用される一定範囲の VLAN に関連付ける必要があります。サーバ管理者の場合は、PVLAN を vCenter のポート グ

ループに関連付ける必要はありません。Cisco APIC が自動的に PVLAN ペアをエンドポイントグループ (EPG) に関連付けるからです。



(注) Cisco APIC の EPG は、vCenter のポートグループに相当します。

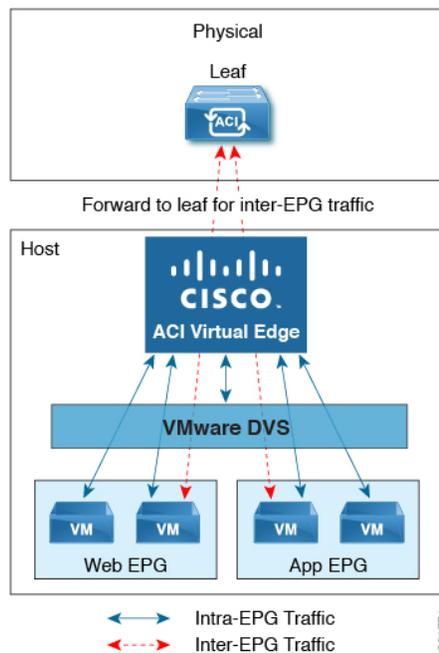
### ローカルスイッチングモード

ローカルスイッチングモードでは、Cisco ACI Virtual Edge は、EPG 内のすべてのトラフィックをリーフを経由せずローカルに転送します。すべての EPG 間トラフィックはリーフを通じて転送されます。このモードでは、Cisco ACI Virtual Edge は VLAN または VXLAN カプセル化、あるいはその両方を使用してトラフィックをリーフとバックに転送できます。カプセル化のタイプは、Cisco ACI Virtual Edge VMM ドメインの作成時に選択できます。

単一の VMM ドメインは、ローカルスイッチングモードで VLAN と VXLAN カプセル化を使用するように設定できます。

VLAN カプセル化を選択する場合は、一連の VLAN の範囲が Cisco ACI 仮想エッジによって使用可能である必要があります。これらの VLAN には、Cisco ACI Virtual Edge とリーフ間のレイヤ2 ネットワーク内でのみ意味があるローカルスコープがあります。VXLAN カプセル化を選択する場合は、Cisco ACI Virtual Edge とリーフの間で使用できる必要があるのはインフラ VLAN のみです。これにより、設定が簡素化されます。Cisco ACI Virtual Edge と物理リーフ間に1つ以上のスイッチがある場合に推奨されるカプセル化タイプです。

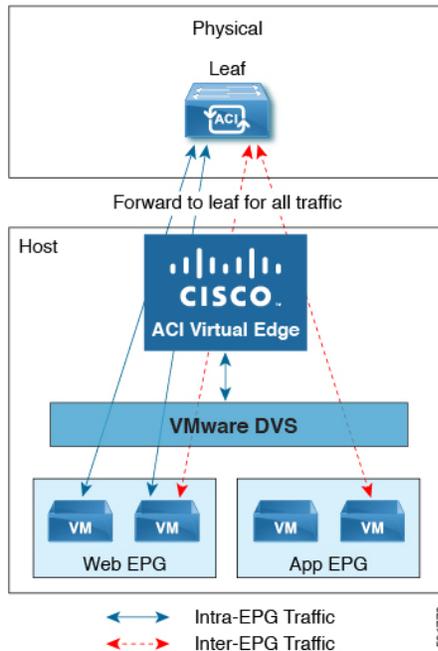
図 1: ローカルスイッチングモードの Cisco ACI Virtual Edge



### ローカルスイッチングモードなし

ローカルスイッチングモードなしの場合、リーフはすべてのトラフィックを転送します。このモードでは、VXLAN が唯一許可されるカプセル化タイプです。

図 2: ローカルスイッチングなしモードの *Cisco ACI Virtual Edge*



### Statistics Collection

Cisco ACI Virtual Edge での統計収集はデフォルトで有効になっています。Cisco APIC GUI 内では、VM リソースの使用に関連して Cisco ACI Virtual Edge の障害が出る場合があります。

これらの障害のトラブルシューティングは VMware vCenter で行ってください。Cisco ACI はこれらの障害を VMware vCenter から受信した情報だけに基いて生成するからです。

## Cisco ACI Virtual Edge および VMware vCenter

Cisco ACI Virtual Edge は、多数の仮想ホストにまたがって広がる分散仮想スイッチです。vCenter Server により定義されるデータセンターを管理します。

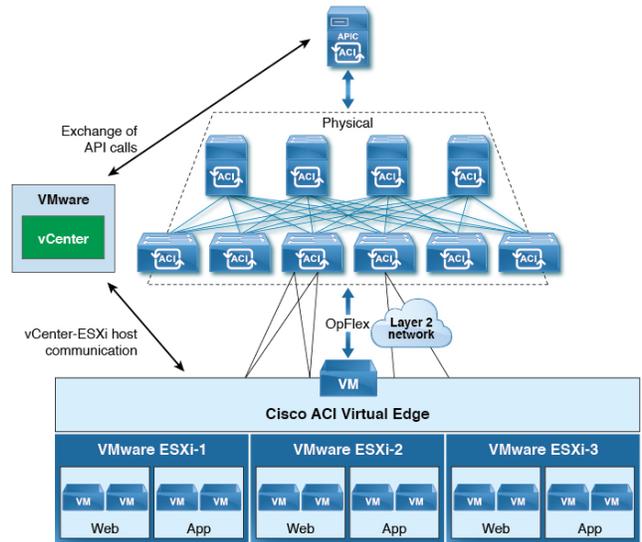
Cisco ACI Virtual Edge は、Cisco Nexus スイッチなどの、イーサネット標準準拠のアップストリーム物理アクセスレイヤスイッチと互換性があります。Cisco ACI Virtual Edge は *VMware Hardware Compatibility List* (HCL) に記載されているすべてのサーバハードウェアと互換性があります。

Cisco ACI Virtual Edge は、VMware 仮想インフラストラクチャ内に完全に統合される、分散仮想スイッチソリューションです。このインフラストラクチャには、仮想化管理者のための VMware vCenter も含まれます。このソリューションにより、ネットワーク管理者は一貫した

データセンター ネットワーク ポリシーを確立するために仮想スイッチやポート グループを設定することができます。

次の図は、Cisco ACI Virtual Edge と Cisco APIC および VMware vCenter を含むトポロジを示しています。

図 3: Cisco ACI Virtual Edge トポロジの例



(注) 1つのCisco ACI ファブリックに接続された複数のvCentersがある場合、デフォルトのOUI割り当てではなくvCentersを展開するには、複数のvCentersにわたるMACアドレス割り当てスキーマにオーバーラップがないことを確認してください。オーバーラップがあると、重複したMACアドレスが生成される可能性があります。詳細については、VMwareのマニュアルを参照してください。

## マルチポッド環境での Cisco ACI Virtual Edge

Cisco ACI Virtual Edge はマルチポッド環境の一部である可能性があります。マルチポッド環境はすべてのポッドに単一のCisco APIC クラスタを使用します。そのため、すべてのポッドが単一のファブリックとして機能します。

マルチポッド環境は、独立した制御プレーンプロトコルを有する複数のポッドで構成された、障害耐性の高いファブリックのプロビジョニングを可能にします。また、リーフスイッチとスパインスイッチ間のフルメッシュケーブル配線にも柔軟性があります。

Cisco ACI Virtual Edge はマルチポッド環境で動作するための追加の設定を必要としません。

マルチポッド環境の詳細については、Cisco.com の次のマニュアルを参照してください。

- 『Cisco Application Centric Infrastructure Fundamentals』

- 『Cisco APIC Getting Started Guide』
- 『Cisco APIC NX-OS Style Command-Line Interface Configuration Guide』

次の機能は、Cisco APIC リリース 3.1(1) ~ 4.0(1) のマルチポッドを使用した Cisco ACI Virtual Edge ではサポートされていません。

- 2つの個別の POD に2つの個別の NFS を搭載したストレージ vMotion
- 異なる POD の ERSPAN 宛先
- 異なる POD の分散型ファイアウォール syslog サーバ

## 必要なソフトウェア

次の表に必要なソフトウェアのバージョンを示しています Cisco ACI Virtual Edge Cisco APIC、VMware vCenter と VMware ESXi ハイパーバイザで動作します。

コンポーネント	説明
Cisco ACI Virtual Edge ソフトウェア	Cisco ACI Virtual Edge リリース 1.1(1) で始まるはサポートされています。
Cisco APIC	Cisco ACI Virtual Edge Cisco APIC リリース 3.1 (1) 以降でサポートされます。
VMware vCenter	Cisco ACI Virtual Edge は、VMware vCenter サーバのリリース 6.0 以降と互換性があります。
VMware vSphere のベア メタル	Cisco ACI Virtual Edge は、VMware ESXi ハイパーバイザのリリース 6.0 以降で、Cisco APIC 用の vLeaf としてサポートされます。

## Cisco ACI vPod : Cisco ACI ファブリックを拡張する

インフラストラクチャの要求、柔軟性、コスト削減を達成するために、ハイブリッドデータセンター モデルを採用する組織が増えてきています。こうした組織では、仮想プライベートクラウドやその他の社内 IT リソースを含めたさまざまなテクノロジーを、リモート ロケーションと組み合わせて利用しています。リモート ロケーションには、ホステッドデータセンター、サテライト データセンター、マルチクラウド環境などがあります。

しかし、ハイブリッドを導入するためには、ロケーションに関係なく、ワークロードの一貫した管理とポリシーが必要になります。また、ディザスタリカバリのサポートや、データセンター間で負荷を軽減するための機能も必要です。その一方で、互換性のあるハードウェアや、新しい機器を追加するためのスペースが不足している組織もあります。

Cisco Application Centric Infrastructure (ACI) 仮想ポッド (vPod)を導入すれば、こうした課題を克服して、Cisco ACI のファブリックを仮想的にさまざまなリモート ロケーションに拡張することができます。

### Cisco ACI vPod とは

Cisco ACI vPod は、Cisco APIC リリース 4.0(2) で一般に利用可能です。これはソフトウェアのみのソリューションであり、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台存在する場所に展開することができます。Cisco ACI vPod と、そのコンポーネントである仮想スパイン (vSpine)、仮想リーフ (vLeaf)、およびCisco ACI Virtual Edge は、ESXi ハイパーバイザ上で実行されます。

Cisco ACI vPod 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。オンプレミスデータセンターの場合と同様に、リモートロケーションにある各 Cisco ACI vPod で Cisco ACI Virtual Edge のインスタンスを最大 8 個使用できます。

Cisco ACI vPod は、ポッド間ネットワーク (IPN) を介して物理的なオンプレミスポッドまたはマルチポッドと通信します。物理ポッドまたはマルチポッド、IPN 接続、および Cisco ACI vPod (APIC) の Cisco Application Policy Infrastructure Controller を設定します。Cisco ACI vPod のコンポーネントの展開には、Cisco ACI vCenter プラグイン、スクリプト、または PowerCLI を使用できます。

### の利点 Cisco ACI vPod

Cisco ACI vPod をインストールすると、それを Cisco APIC と組み合わせて使用することで、リモートロケーションに Cisco ACI ファブリック ポリシーを適用することができます。

Cisco APIC により、オンプレミスデータセンターとリモートロケーションに、ワークロードの一元管理機能が提供されます。オンプレミスとリモートの両方のロケーションで、ポリシーを簡単に、かつ矛盾なく適用することができます。

Cisco ACI vPod ソリューションがもたらす柔軟性、拡張性、一元管理により、次のような使用事例のシナリオを活用できるようになります。

- Cisco ACI ファブリックをベアメタルクラウドに拡張する
- Cisco ACI ファブリックをブラウンフィールドの展開に拡張する
- Cisco ACI ファブリックをコロケーションデータセンターに拡張する
- シスコ以外のハードウェアから Cisco ACI ファブリックにワークロードを移行する

### 詳細情報の入手先

詳細については、Cisco.com で『Cisco ACI Virtual Pod Release Notes』を参照してください。



## 第 3 章

# Cisco ACI Virtual Edgeのインストール

この章では、前提条件とインストール方法を含む Cisco ACI Virtual Edge のインストールについて説明します。

- [Cisco ACI Virtual Edge のインストールについて \(9 ページ\)](#)
- [デフォルトのポートグループ \(11 ページ\)](#)
- [Cisco ACI Virtual Edge のインストールワークフロー \(11 ページ\)](#)
- [Cisco ACI Virtual Edge をインストールするための前提条件 \(12 ページ\)](#)
- [vCenter を使用した Cisco ACI Virtual Edge のインストール \(27 ページ\)](#)
- [VMware PowerCLI を使用した Cisco ACI Virtual Edge のインストール \(33 ページ\)](#)
- [Python を使用した Cisco ACI Virtual Edge のインストール \(37 ページ\)](#)
- [Cisco ACI Virtual Edge 展開の確認 \(43 ページ\)](#)
- [GUI を使用した Cisco ACI 仮想エッジ ライセンスの表示 \(44 ページ\)](#)
- [VMware vCenter でスタティック IP アドレスを設定する \(45 ページ\)](#)
- [インストール後の設定 \(47 ページ\)](#)

## Cisco ACI Virtual Edge のインストールについて

Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge のインストールは、Cisco Application Policy Infrastructure Controller (APIC) と VMware vCenter で実施される一連のタスクで構成されています。ESXi ホストを Cisco ACI Virtual Edge に展開するには、3 つの方法のいずれかを使用することができます:

- VMware vCenter 用 Cisco ACI プラグイン
- VMware PowerCLI (Windows プラットフォームで)

VMware vCenter 用 Cisco ACI プラグインは、元々 Adobe Flash で動作するように設計されていました。ただし、2020 年の終わりに、Adobe は Flash の更新を停止します。VMware vSphere 6.7 リリース以降、プラグインの新しいバージョンである Cisco ACI HTML5 vCenter プラグインは、Flash ではなく HTML5 で動作するように設計されています。プラグインは、HTML5 VMware vSphere クライアント内で動作します。

新しい Cisco ACI プラグインを使用して、Cisco ACI Virtual Edge を展開および設定するための主要なタスクのほとんどを実行できます。Cisco ACI vCenter プラグイン手順は、使用するプラグインのバージョンを示します。



(注) The name of the VMware vSphere クライアントの名前は、Flash または HTML5 バージョンを使用しているかどうかで異なります。Flash バージョンは、VMware vSphere Web クライアントと呼ばれます。HTML バージョンは、VMware vSphere Client と呼ばれません。

- Python スクリプト

以下のセクションでは、前提条件とインストールの方法について説明します。Cisco AVS から Cisco ACI Virtual Edge に移行する方法については、本ガイドの [Cisco AV から移行する Cisco ACI Virtual Edge \(49 ページ\)](#) の章を参照してください。VMware VDS から Cisco ACI Virtual Edge に移行する方法については、本ガイドの [VMware VDS から移行する Cisco ACI Virtual Edge \(57 ページ\)](#) の章を参照してください。



- (注)
- Cisco ACI Virtual Edge をインストールする、またはそのプロパティを変更する場合には、vSphere (シック) クライアントは使用しないでください。Cisco ACI Virtual Edge をインストールするには、Cisco ACI プラグイン、VMware Power CLI または Python スクリプトのみを使用してください。Cisco ACI Virtual Edge vApp プロパティを変更するには、vSphere Web クライアントのみを使用してください。
  - ESXi ホスト上に Cisco ACI Virtual Edge VM を展開すると、OpFlex 自動的にオンラインになります。VMkernel ポートをインフラ ポート グループには割り当てないでください。これは Cisco AVS の OpFlex で行われているからです。
  - 同じホストに複数の Cisco ACI Virtual Edge VM をインストールすることもできますが (Cisco ACI Virtual Edge VMM ドメインごとに 1 つ)、ホストごとに 1 つの Cisco ACI Virtual Edge VM だけをインストールすることを推奨します。

### Cisco ACI 仮想エッジ導入のベスト プラクティス

次のベストプラクティスに従って、トラフィック損失を最小限に抑え、ハードウェア障害による可用性を高めます。

- ACI 仮想エッジ展開の場合は、vCenter のクラスターと APIC の VMM ドメインで ProActive HA を設定します。
- ACI 仮想エッジの ProActive HA 展開の場合は、vCenter の DRS 設定で [可用性についてホスト間で多数の仮想マシンを分散する] オプションを無効にするようにしてください。

vSphere Proactive HA の有効化の詳細については、[VMware vSphere Proactive HA を使用して Cisco ACI 仮想エッジ可用性を改善する \(97 ページ\)](#) を参照してください。

## デフォルトのポートグループ

Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge を作成すると、VMware vCenter は自動的に複数のポートグループを作成します。

- **ave-external-vxlan-1** および **ave-external-vxlan-2** : Cisco ACI Virtual Edge 仮想マシン (VM) はこれらのポートグループを使用して、ホストの外部の間で VXLAN トラフィックを送受信します。VXLAN トラフィックは、着信 VM インターフェイスに基づいて、これら 2 つのポート間で分散されます。
- **ave-internal-1** および **ave-internal-2** : Cisco ACI Virtual Edge VM は、これらのポートグループを使用して、分散仮想スイッチ (DVS) 内の VM との間で PVLAN トラフィックを送受信します。内部 VLAN ブロックは、内部トラフィックをロードバランシングするために、これら 2 つのポートグループ間で均等に分散されます。
- **ave-external-vlan** : Cisco ACI Virtual Edge VM はこのポートグループを使用して、ホストの外部の間で VLAN トラフィックを送受信します。VMM ドメインに関連付けられた VLAN モードエンドポイントグループ (EPG) に使用される VLAN を有効にします。VLAN モードの場合、VLAN には「ave-ctrl」 EPG に割り当てられた VLAN が含まれる場合があります。
- **infra** : VM はこの特別なポートグループを使用して、別の Cisco ACI Virtual Edge から発信された ERSPAN トラフィックを受信します。ポートグループはネイティブ モードで、着信 Encapsulated Remote Switched Port Analyzer (ERSPAN) トラフィックは Cisco ACI Virtual Edge をバイパスし、DVS によって転送されます。

## Cisco ACI Virtual Edge のインストール ワークフロー

このセクションでは、Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge をインストールするのに必要な高レベルなタスクを説明します。

1. Cisco Application Policy Infrastructure Controller (APIC) と VMware vCenter のタスクを含む、すべての前提条件を満たします。[Cisco ACI Virtual Edge をインストールするための前提条件 \(12 ページ\)](#) の項を参照してください。
2. Cisco.com から Cisco ACI Virtual Edge Open Virtualization Format (OVF) ファイルをダウンロードし、vCenter コンテンツ ライブラリにアップロードします。VMware vCenter、vCenter 電源 CLI、または Python スクリプトに Cisco ACI プラグインを使用することができます。説明については、次のいずれかのセクションを参照してください。
  - [Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードする \(29 ページ\)](#)

- [PowerCLI 環境の設定 \(33 ページ\)](#)  
および [VMware PowerCLI を使用した VMware vCenter コンテンツ ライブラリの管理 \(34 ページ\)](#)
  - [Python 環境の設定 \(38 ページ\)](#)  
および [Python を使用した VMware vCenter コンテンツ ライブラリの管理 \(39 ページ\)](#)
3. ESXi ホストに Cisco ACI Virtual Edge を展開します。次の 4 つのうちいずれかの方法を使用できます。説明については、次のセクションを参照してください。
    - [Cisco ACI vCenter プラグインの HTML5 バージョンを使用して Cisco ACI 仮想エッジを展開する \(30 ページ\)](#)
    - [Cisco ACI vCenter プラグインを使用した ESXi ホストでの Cisco ACI Virtual Edge のデプロイ \(31 ページ\)](#)
    - [VMware PowerCLI を使用した Cisco ACI Virtual Edge の展開 \(35 ページ\)](#)
    - [Python を使用して Cisco ACI Virtual Edge を展開する \(41 ページ\)](#)
  4. Cisco ACI Virtual Edge と通信するために使用されるインターフェイス (kni0) に仮想トンネルエンドポイント (VTEP) の IP アドレスがあることを確認し、OpFlex が稼働していることを確認します。  
  
このガイドの[Cisco ACI Virtual Edge 展開の確認 \(43 ページ\)](#) セクションを参照してください。



(注) より高いレベルの可用性を確保するために、ローカルデータストアに Cisco ACI Virtual Edge を展開することを推奨します。

## Cisco ACI Virtual Edge をインストールするための前提条件

インストールする前に、次のタスクを実行 Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge :

### ストレージおよびメモリ

少なくとも 30 GB のストレージと 4 GB のメモリが必要です。

### Cisco ACI ファブリックおよび Cisco APIC

- Cisco Application Policy Infrastructure Controller (APIC) が正常にセットアップされていることを確認します。参照してください、[『Cisco APIC Getting Started guide』](#) および [Cisco APIC の基本的なコンフィギュレーションガイド](#)、最初の Cisco APIC を設定する方法については、[Cisco.com](#) にします。

- すべてのスイッチが登録されており、Cisco ACI ファブリックが最新であることを確認します。手順については、Cisco.com の『*Cisco Application Centric Infrastructure Fundamentals*』および『*Cisco APIC Getting Started Guide*』を参照してください。
- VMware vCenter プラグイン内部 Cisco ACI ファブリックが登録されていることを確認します。「*Cisco ACI 仮想化ガイド*」の「Cisco ACI vCenter プラグイン」章にある「vCenter プラグインを ACI ファブリックに接続する」を参照してください。

## VMM ドメイン

新しい vCenter の VMM ドメインとインターフェイスおよび Cisco ACI Virtual Edge 用スイッチのプロファイルを作成します。

これらのタスクを実行する unified 設定ウィザードを使用することをお勧めします。このガイドの GUI を使用した vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの作成 (18 ページ) の手順を参照してください。ただし、別の詳細なポリシーを設定する必要がある場合があります。その場合は、本ガイドの付録 [作成 vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの代替手順 \(83 ページ\)](#) を参照してください。

## Hosts

- VMware vCenter の vSphere Web クライアントを使用して、新しい Cisco ACI Virtual Edge 分散仮想スイッチ (DVS) に 1 つ以上の ESXi ホストとその PNIC を追加します。
- ホストがすでに実行されている Vm を分散リソース スケジューラ (DRS) クラスタに属している場合は Cisco ACI Virtual Edge を追加する前に、メンテナンス モードで、ホストを配置、Cisco ACI Virtual Edge を DVS にします。移行から、DRS をにより、メンテナンスモードで、ホストにインストールを開始する前に、他のホストに Vm、Cisco ACI Virtual Edge VM が完全に対応します。
- 場合は、ホストは、DRS クラスタに属している、Nehalem 以上、DRS クラスタの拡張 VMotion 互換性 (EVC) モードが設定されていることを確認します。
- VMware vSphere Hypervisor (ESXi) 6.5 U1 を使用している場合は、Cisco Discovery Protocol (CPD) が有効になっている VXLAN モードで、Cisco ACI Virtual Edge にホストを追加する前に、Intel X710 ポートアダプタ ドライバをファームウェア 6.01 搭載の 1.8.6 以降に更新します。ポートアダプタ ドライバを更新しないと、VMware の紫色の診断画面が表示されることがあります。

## VXLAN カプセル化

VXLAN カプセル化を使用して Cisco ACI Virtual Edge を接続する場合、Cisco ACI ファブリックと Cisco ACI Virtual Edge 間のパス上のすべての中間デバイスで、最大伝送単位 (MTU) の値を 1600 以上に設定します。これらには FI スイッチや UCS-B などがあります。ただし、パフォーマンスを最適化するには、MTU を、Cisco ACI ファブリックのパス上のすべての中間デバイスと Cisco ACI Virtual Edge がサポートする、最大サポート サイズに設定します。

## VMware vCenter

- Cisco ACI Virtual Edge 管理ツールを使用するには、Cisco ACI VMware vCenter プラグインの Flash バージョンを使用している場合は、VMware vCenter 6.0 Update 3 以降を使用することをお勧めします。HTML5 バージョンを使用している場合は、Cisco ACI HTML5 vCenter プラグイン VMware vCenter 6.7 Update 2 または VMware vCenter 7.0 を使用することをお勧めします。これらのツールには、VMware vCenter プラグイン、VMware PowerCLI、および Python スクリプトが含まれます。
- インストールする場合は Cisco ACI Virtual Edge、Active Directory ドメイン コントローラとシングルサインオン接続要求を作成するホストの VMware vCenter Server のクロック同期、VMware PowerCLI を使用しています。展開する際に問題が発生する可能性があります。クロックが同期されていない場合 Cisco ACI Virtual Edge VMware PowerCLI ツールを使用します。

詳細については、「ナレッジ ベース記事」例外を報告 SSOConnection SDK を発信: クライアントはサーバから SOAP 障害を受信:<timestamp>が要求ライフタイム間隔に含まれていないので、時間が 600000 ミリ秒 (2125193) のクロック許容度を拡張」で、VMware Web サイト</timestamp>。

## リモート リーフ展開

リモート リーフ展開に Cisco ACI Virtual Edge をインストールする場合は、Cisco.com の「[Cisco ACI リモート リーフ アーキテクチャ ホワイト ペーパー](#)」の「[リモート リーフ向けに推奨される QOS 設定](#)」の項で推奨されているように、L3 トラフィックの DSCP class-cos 変換ポリシーを有効にします。

# Cisco APIC の設定の構成

次のセクションでは、Cisco APIC で Cisco ACI Virtual Edge および VMware ESXi Hypervisor を設定する方法について説明します。

1. [vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの作成 \(14 ページ\)](#)
2. [インターフェイスとスイッチのプロファイルのガイドラインと前提条件 \(15 ページ\)](#)
3. [vCenter ドメイン プロファイルのガイドラインと前提条件 \(17 ページ\)](#)
4. [GUI を使用した vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの作成 \(18 ページ\)](#)

## vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの作成

インストールする前に、Cisco ACI Virtual Edge、vCenter を作成する必要があります。ドメイン、インターフェイス、およびスイッチのプロファイル。Cisco APIC の統合設定ウィザードで次のタスクを実行することを推奨します。このガイドの [GUI を使用した vCenter ドメイン、イン](#)

[インターフェイス、およびスイッチのプロファイルの作成 \(18 ページ\)](#) の手順を参照してください。

このタスクを実行する前に、このセクションのガイドラインを理解して、それに従う必要があります。

### 代替手順

手順を検索できます [FEX プロファイル](#) または [詳細なインターフェイス、スイッチ、または vCenter ドメインプロファイルを設定する場合は、作成 vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの代替手順 \(83 ページ\)](#) このガイドで。

### ファイアウォールの考慮事項

推奨される統合構成ウィザードを使用すると、後で変更できるファイアウォールポリシーが Cisco APIC によって自動で作成されます。代わりに代替手順を使用してインターフェイス、スイッチ、または vCenter ドメインのプロファイルを作成すると、ファイアウォールポリシーを手動で作成しなければならなくなります。指示に従っての分散型ファイアウォールのセクションで、[Cisco ACI 仮想エッジ Configuration guide](#) 。

## インターフェイスとスイッチのプロファイルのガイドラインと前提条件

Cisco ACI Virtual Edge 用のインターフェイスとスイッチのプロファイルを作成する場合は、次のガイドラインに従って前提条件を満たしてください。

### インターフェイスおよびスイッチのプロファイルを作成するガイドライン

Cisco ACI Virtual Edge は、ポートチャネル (PC)、仮想ポートチャネル (VPC)、MAC の固定、および FEX インターフェイスポリシーをサポートしています。

- リーフスイッチと Cisco ACI Virtual Edge vSphere ホスト間にレイヤ 2 ネットワークがある場合は、レイヤ 2 ネットワークに接続されているインターフェイス上でインターフェイスポリシーを設定します。
- 使用するリンク数とリーフ数によって、Cisco ACI Virtual Edge に対し PC または VPC ポリシーを設定する必要があるかどうか判断できます。
  - リーフと ESXi ホスト間で複数のリンクを使用している場合は、PC ポリシーを設定する必要があります。
  - 複数のリーフと ESXi ホスト間で複数のリンクを使用している場合は、VPC ポリシーを設定する必要があります。
- LACP ポリシーを選択するには、以下のガイドラインに従います。
  - Cisco ACI Virtual Edge (vSphere ホスト) からのアップリンクがリーフスイッチに直接接続されており、LACP チャンネルプロトコルを使用するかオンにする場合は、[LACP (Active or Passive)] を選択します。

- Cisco ACI Virtual Edge からのアップリンクがリーフスイッチに直接接続されている一方で、LACP チャンネルプロトコルを使用しない場合は、[Static Channel - Mode On] を選択します。
- Cisco ACI Virtual Edge からのアップリンクを1つのチャンネルにまとめることができず、個別のリンクとして動作する場合は、[MAC Pinning] を選択します。



---

(注) VPC リーフ ペアへの直接接続で MAC ピニングを使用しないでください。代わりに、Link Aggregation Control Protocol (LACP) または拡張 LACP を使用して、冗長性と信頼性を提供します。直接接続で MAC ピニングを使用すると、ピアリーフスイッチの再起動時にトラフィックが失われます。MAC ピニングは、サウスバウンドインターフェイスを使用する Cisco UCS ファブリック インターコネクトなど、仮想ポートチャンネル(VPC)をサポートできない場合にのみ使用してください。

---

- 管理インターフェイスの vSwitch ポートグループを選択するには、次のガイドラインに従います。

Cisco ACI Virtual Edge 管理インターフェイス用に作成した vSwitch ポートグループが、DHCP または vCenter IP プールによって、少なくとも IPv4 アドレスを提供できることを確認します。管理インターフェイス用の vSwitch ポートグループに対して、追加の IPv6 アドレスを設定することができます。ただし、IPv6 アドレスのみで設定することはできません。



---

(注) Cisco ACI vCenter プラグインは、スタティック IP アドレスの設定をサポートしていません。ただし、VMware PowerCLI または Python スクリプトを使用してスタティック IP アドレスを設定できます。このガイドの [VMware PowerCLI を使用した Cisco ACI Virtual Edge のインストール \(33 ページ\)](#) と [Python を使用した Cisco ACI Virtual Edge のインストール \(37 ページ\)](#) を参照してください。または、VMware vCenter でスタティック IP アドレスを設定できます。本ガイドの [VMware vSphere Web クライアントの Flash バージョンを使用したスタティック IP アドレスの設定 \(46 ページ\)](#) または [VMware vSphere クライアントの HTML5 バージョンを使用したスタティック IP アドレスの設定 \(45 ページ\)](#) セクションを参照してください。

---

### インターフェイスおよびスイッチ プロファイルを作成する前提条件

リーフスイッチインターフェイスがESXiハイパーバイザーに物理的に接続されていることを確認します。または、レイヤ2デバイスを使用している場合には、リーフがレイヤ2のデバイスに物理的に接続されていることを確認します。

## vCenter ドメイン プロファイルのガイドラインと前提条件

Cisco ACI Virtual Edge をインストールする前に、新しい vCenter ドメイン プロファイルを作成する必要があります。既存の vCenter ドメイン プロファイルを変換することはできません。

### VMware vCenter ドメイン プロファイルの作成のガイドライン

単一のドメイン下に、複数のデータセンターとDVSエントリを作成できます。ただし、各データセンターに割り当てることができる Cisco ACI Virtual Edge は1つだけです。

vCenterおよびESXiホスト管理でIPv6が有効な場合は、VMMドメインを作成するときにIPv6を使用できます。

### VMware vCenter ドメイン プロファイルの作成の前提条件

マルチキャスト IP アドレス プールが十分なマルチキャスト IP アドレスがあることを確認します。VMware vCenter ドメインに発行する EPG の数に対応する必要があります。VMware vCenter ドメインにすでに関連付けられているマルチキャストアドレス プールに IP アドレスをいつでも追加できます。

十分な VLAN ID があることを確認します。これを行わないと、エンドポイント グループ (EPG) 上のポートがカプセル化を使用できないと報告することがあります。

vCenter がインストールおよび設定されており、インバンド/アウトオブバンド管理ネットワークを介して到達可能である必要があります。

vCenter に対する管理者/ルートのクレデンシヤルが必要です。

## GUIを使用したvCenterドメイン、インターフェイス、およびスイッチのプロファイルの作成



(注) vCenterドメインを作成する際にVMware PortGroup名でデリミタを選択していた場合でも、この手順では使用できません。VMware vSphere Proactive HA機能を利用する場合も、この手順では使用できません。この手順では、vCenterドメイン、インターフェイス、およびスイッチプロファイルを設定できるようにする設定ウィザードを使用します。

代わりに、vCenterドメインを個別に作成する必要があります。**[vCenterドメインの作成 (Create vCenter Domain)]**ダイアログボックスにデリミタオプションが表示されます。**[vCenterドメインの作成 (Create vCenter Domain)]**ダイアログボックスには、VMware vCenterでVMware Proactive HAオブジェクトを作成するオプションもあります。また、Proactive HAがトリガーされるまでの期間を設定するオプションも含まれています。このガイドの手順[Cisco ACI Virtual EdgeのVMMドメインプロファイルの作成 \(92ページ\)](#)を参照してください。

### 始める前に

vCenterドメインプロファイルを作成する前に、Cisco APICでイン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 Cisco APIC にログインします。
- ステップ 2 メニューバーで、**[Fabric] > [Access Policies]** の順にクリックします。
- ステップ 3 **[ナビゲーション (Navigation)]** ナビゲーション ペインで**[クイック スタート (Quick Start)]** をクリックし、中央ペインで**[インターフェイス、PC、および VPC (Configure an interface, PC, and VPC)]** をクリックします。
- ステップ 4 **[Configure Interfaces, PC, and VPC]** ダイアログ ボックスで、**[Configured Switch Interfaces]** を展開し、緑色の **[+]** アイコンをクリックしてから、次の手順を実行します。
  - a) **[Select Switches to Configure Interfaces]** エリアで **[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。
  - b) **[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表示されます。
  - c) 緑色の **[+]** アイコンをもう一度クリックします。

**Configure Interfaces, PC, and VPC** ダイアログボックスはウィザードを表示します。これを使用すれば、vCenterドメイン、インターフェイス、およびスイッチプロファイルを設定できます。
- ステップ 5 このウィザードで、次の手順を実行します。
  - a) **Interface Type** エリアで、適切なオプション ボタンを選択します。

Cisco ACI Virtual Edge の展開で有効なオプションは PC、VPC のみです。このガイドのセクション [インターフェイスとスイッチのプロファイルのガイドラインと前提条件 \(15 ページ\)](#) を参照してください。

- b) **[Interfaces]** フィールドで、vSphere ホストのインターフェイスまたはインターフェイスの範囲を入力します。
- インターフェイスまたはインターフェイスの範囲を入力すると、ウィザードは **[Interface Selector Name]** フィールドに名前を入力します。
- c) **Interface Policy Group** エリアで、**Create One** ラジオ ボタンを選択します。
- (注) この手順は、インターフェイスおよびスイッチのポリシーを作成する場合であり、vCenter のドメインを最初から作成すると想定しています (既存のものを使用するものではありません)。**Choose One** ラジオ ボタンを選択すると、ウィザードではポリシーを作成できなくなります。
- d) **CDP Policy** または **LLDP Policy** ドロップダウン リストから、ポリシーを作成します。
- (注)
- Cisco Unified Computing System (UCS) サーバを使用する場合は、2つのポリシーを作成します。最初のポリシーは Cisco Discovery Protocol (CDP) ポリシーを有効にし、2 番目のポリシーは Link Layer Discovery Protocol (LLDP) を無効にします。
  - CDP および LLDP ポリシーは、デフォルトでは無効にされています。これらは構成ウィザードで有効にできます。**Interface Policy Group** エリアで CDP ポリシーまたは LLDP ポリシーを有効にして、ファブリック内の Cisco ACI Virtual Edge と他のスイッチ上でそれらを有効にします。Cisco ACI Virtual Edge で CDP または LLDP のみを有効にする場合は、構成ウィザードの **vSwitch Policy** エリアでそれらを有効にします。
- e) **Link Level Policy** ドロップダウン リストで、目的のリンク レベル ポリシーを選択するか、作成します。
- リンク レベル ポリシーは物理インターフェイスの速度を指定します。リンク レベル ポリシーを選択しない場合、速度はデフォルトの 10 Gbps になります。
- f) **Port Channel Policy** ドロップダウン リストで、**Create Port Channel Policy** を選択します。
- g) **Create Port Channel Policy** ダイアログボックスで、ポリシーの名前を入力し、モードを選択し、**Submit** をクリックします。
- ESXi サーバ上で同じポリシーモードを選択します。たとえば、サーバが LACP をサポートしていない場合は、**Static Channel - Mode On** または **MAC Pinning** を選択できます。ダイアログボックスの他のフィールドはオプションです。
- h) **Attached Device Type** エリアで、**AVE VLAN Hosts** または **AVE VXLAN Hosts** を選択します。

(注) ハイパーバイザがリーフスイッチに直接接続されている場合は、VLANまたはVXLANを使用できます(ファブリックインターコネクがファブリックに接続されているCisco UCSブレードサーバは、直接接続されていると見なされます)。ただし、ハイパーバイザがリーフスイッチに直接接続されていない場合は、VXLANを使用する必要があります。詳細については、[Cisco ACI Virtual Edge \(3 ページ\)](#) を参照してください。

- i) **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。

[1 個作成 (Create One)] オプションを使用して、この手順と同様に、インターフェイスまたはスイッチプロファイルに新しいVMMドメインを作成します。[1 個選択 (Choose One)] ボタンを使用して、既存のVMMドメインの一部にする新しいホスト用のインターフェイスまたはスイッチのプロファイルを作成するときに使用します。

- j) [Domain Name] フィールドに、ドメイン名を入力します

(注) VMMドメインを作成する際に、ステップ 5 h で選択したアタッチデバイスのタイプに応じて、VLAN または VXLAN カプセル化を選択できます。ただし、VLAN および VXLAN カプセル化を使用するように設定できるのは1つのVMMドメインだけです。Cisco ACI Virtual Edge のインストールが完了したら、混合カプセル化をモードを有効にすることができます。『[Cisco ACI Virtual Edge Configuration Guide](#)』の「Mixed-Mode Encapsulation Configuration」のセクションを参照してください。

- k) 次のいずれかの手順を実行します。

**必須** : Cisco ACI Virtual Edge を使用し、混合モードまたは VLAN モードで展開する場合は、2つのVLANカプセル化ブロックを持つ単一のVLANプールを作成します。1つはプライマリのカプセル化のため、もう1つはプライベートVLANの実装のためです。

手順5 h での選択内容	次の操作
AVE VLAN のホスト	<ol style="list-style-type: none"> <li>1. [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。</li> <li>2. [VLANRange] フィールドに、必要に応じて VLAN の範囲を入力します。   (注) インフラストラクチャネットワークの予約 VLAN ID を含む範囲を定義しないでください。この VLAN は内部使用のためのものだからです。   VLAN の範囲は、外部またはオンザワイヤカプセル化のためのものです。これは、ドメインに割り当てられる EPG ごとに VLAN を割り当てるために使用されます。VLAN は、リーフとの間でパケットを送受信する際に使用されます。   3. <b>Internal VLAN Range</b> フィールドに、範囲を入力します。   内部 VLAN の範囲は、Cisco ACI 仮想エッジにより、内部 vSwitch のプライベート VLAN の割り当てに使用されます。VLAN は ESX ホストの外部またはオンザワイヤからは表示されません。   (注) Cisco ACI Virtual Edge を使用し、混合モードまたは VLAN モードで展開する場合は、2 つの VLAN カプセル化ブロックを持つ単一の VLAN プールを作成します。1 つはプライマリのカプセル化のため、もう 1 つはプライベート VLAN の実装のためです。</li> </ol>

手順5 h での選択内容	次の操作
AVE VXLAN ホスト	<ol style="list-style-type: none"> <li>1. <b>VLAN</b> エリアで、<b>Create One</b> ラジオボタンが選択されていることを確認します。</li> <li>2. <b>Internal VLAN Range</b> フィールドに、範囲を入力します。</li> <li>3. <b>Fabric Multicast Address</b> フィールドに、225.1.1.1 のようなマルチキャストアドレスを入力します。</li> <li>4. <b>Pool of Multicast Address Ranges</b> フィールドで、新しいマルチキャストプールを作成するか、既存のものを選択します。  (注) ステップ3でマルチキャストアドレスを設定していた場合、ステップ4で設定する範囲がオーバーラップしないようにしてください。</li> <li>5. <b>Local Switching</b> エリアで、<b>True</b> または <b>False</b> を選択します。  ローカルスイッチングでは、EPG内のトラフィックはリーフは行きません。それで、ローカルスイッチングを選択した場合、一部のトラフィックカウンタが表示されない可能性があります。すべてのEPG内トラフィックを表示するには、<b>False</b> を選択する必要があります。ローカルスイッチングモードとローカルスイッチングなしモードの詳細については、<a href="#">Cisco ACI Virtual Edge とは (3 ページ)</a> のセクションを参照してください。</li> </ol>

- l) (任意) **[Security Domains]** ドロップダウンリストから、セキュリティドメインを選択するか、作成します。
- m) **[vCenter Login Name]** フィールドに、vCenterの管理者またはルートユーザ名を入力します。
- n) **[Password]** フィールドに、vCenterの管理者またはルートのパスワードを入力します。
- o) **[Confirm Password]** フィールドにパスワードを再入力します。

**ステップ 6** [+] アイコンをクリックして **[vCenter]** を展開し、**[Create vCenter Controller]** ダイアログボックスで、次のアクションを実行します。

(注) 同じドメインに複数の vCenter コントローラを作成できます。さらに vCenter コントローラを作成する場合は、新しい vCenter コントローラごとにステップ 6 のサブステップを繰り返します。

a) **[Name]** フィールドに、vCenter ドメインを参照する名前を入力します。

この名前は vCenter ドメイン名と同じである必要はなく、vCenter ホスト名を使用できます。

b) **[Host Name (or IP Address)]** 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必要があります。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。

c) **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。

選択した DVS バージョンは、仮想スイッチに追加できるホストの最小 ESXi バージョンを表します。したがって DVS バージョン 6.0 を選択すれば、ESXi バージョン 6.0 以降のホストを追加または管理できます。

(注) Cisco ACI 仮想エッジは、DVS および ESXi のバージョン 6.0 以降をサポートしています。

d) **[Datacenter]** フィールドで、データセンター名を入力します。

**[Datacenter]** に入力する名前は、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。

e) **[OK]** をクリックします。

(注) 次の3つの手順で、ポートチャネル、vSwitch、またはインターフェイス制御ポリシーを指定しない場合は、この手順の前半で設定したものと同一インターフェイスポリシーが vSwitch に適用されます。

**ステップ 7** **[インターフェイス、PC、および VPC を設定する (Configure Interface, PC, And VPC)]** ダイアログボックスで、**[ポートチャネルモード (Port Channel Mode)]** ドロップダウンリストからモードを選択します。

- (注)
- **MAC Pinning** は、トップオブラックスイッチと Cisco ACI Virtual Edge の間にユニファイドコンピューティングシステム (UCS) ファブリックインターコネクト (FI) がある倍に選択します。
  - **VPC** リーフペアへの直接接続で MAC ピニングを使用しないでください。代わりに、Link Aggregation Control Protocol (LACP) または拡張 LACP を使用して、冗長性と信頼性を提供します。直接接続で MAC ピニングを使用すると、ピアリーフスイッチの再起動時にトラフィックが失われます。MAC ピニングは、サウスバウンドインターフェイスを使用する Cisco UCS ファブリックインターコネクトなど、仮想ポートチャネル (VPC) をサポートできない場合にのみ使用してください。

- ステップ 8** **vSwitch Policy** エリアで、ポリシーを選択します。
- ステップ 9** **Interface Controls** エリアで、**BPDU Guard**、**BPDU Filter**、または両方を選択します。
- BPDU ガードおよび BPDU フィルタの詳細については、『[Cisco ACI Virtual Edge Configuration Guide](#)』の「BPDU Features」のセクションを参照してください。
- ステップ 10** **Firewall** ドロップダウン リストから、**Learning**、**Enabled** または **Disabled** モードを選択します。
- [Learning] モードがデフォルトになっていますが、これは分散ファイアウォールをサポートしていない Cisco AVS のバージョンから Cisco ACI Virtual Edge にアップロードする場合にのみ使用してください。それ以外の場合、分散ファイアウォールは [Enabled] モードである必要があります。分散ファイアウォール モードは後で変更できます。『[Cisco ACI 仮想エッジ構成ガイド](#)』の「分散ファイアウォール」の章を参照してください。
- ステップ 11** [NetFlow Exporter Policy] オプションは無視します。
- ステップ 12** [保存 (Save)] をクリックし、[保存 (Save)] を再度クリックし、[送信 (Submit)] をクリックします。
- ステップ 13** 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。
- メニューバーで、[Virtual Networking] > [Inventory] を選択します。
  - ナビゲーションウィンドウで、[VMM Domains] > [VMware] > [Domain\_name] > [Controllers] を展開し、vCenter を選択します。
- 作業ウィンドウの [Properties] の下で、仮想マシンマネージャ (VMM) ドメイン名を参照して、コントローラがオンラインであることを確認します。作業ウィンドウに、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、Cisco APIC 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。

## VMware vSphere Client HTML5 GUI を使用して ESXi ホストと PNIC を追加する

Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge をインストールする前に、1つ以上の ESXi ホストと、それらに対応する物理 NIC (PNIC) を Cisco ACI Virtual Edge を展開する DVS に追加します。



- (注) Proactive HA がすでに設定されている状態でクラスタにホストを追加し、Cisco ACI Virtual Edge VMM ドメインにホストを追加またはホストをアタッチするとき、それらのホストはある状況かでは適切に動作しない可能性があります。Cisco ACI Virtual Edge または OpFlex がダウンしたとき、Proactive HA でホストが適切に動作しない可能性があります。ホストのヘルスステータスが Cisco Cisco Application Policy Infrastructure Controller (APIC) で黄色に適切に設定されているにもかかわらず、ホストが検疫モードにならない可能性もあります。

この問題を修正するには、クラスタの Proactive HA を無効にして、再度有効にします。

## 始める前に

- Cisco ACI Virtual Edge のためのVMM ドメインを作成します。このガイドの手順 [Cisco ACI Virtual Edge の VMM ドメイン プロファイルの作成 \(92 ページ\)](#) を参照してください。
- ホストで使用可能な PNIC を少なくとも 1 つ用意します。

## 手順

**ステップ 1** VMware vSphere Client にログインします。

**ステップ 2** [ホーム (Home)] ページから、[ネットワークング (Networking)] に移動し、ホストと PNIC を追加する Cisco ACI Virtual Edge DVS に移動します。

**ステップ 3** 左側のナビゲーションペインで、ホストを右クリックし、ドロップダウンリストから [ホストの追加と管理 (Add and Manage Hosts)] を選択します。

または、[作業 (Work)] ペインの上部にある [アクション (ACTIONS)] ドロップダウンリストから [ホストの追加と管理 (Add and Manage Hosts)] を選択できます。

**ステップ 4** [DVS]/[ホストの追加と管理 (Add and Manage Hosts)] ダイアログ ボックスで、次のステップを完了します。

- a) [タスクの選択 (Select Task)] ペインで、[ホストの追加 (Add Hosts)] オプション ボタンをクリックし、[次へ (NEXT)] をクリックします。
- b) [ホストの選択 (Select Hosts)] ペインで、[ホストの追加 (Add hosts)] の横にある緑色のプラス記号 (+) をクリックします。
- c) [新しいホストの選択 (Select New Hosts)] ダイアログ ボックスで、追加するホストの隣にあるチェック ボックスをチェックし、[OK] をクリックします。

複数のホストを選択できます。

- d) [部地理アダプタの管理 (Manage Physical Adapters)] ペインで、追加するホストの PNIC を選択し、[アップリンクの割り当て (Assign uplink)] をクリックします。
- e) [アップリンクの選択 (Select an uplink)] ダイアログ ボックスで、アダプタのアップリンクを選択し、[OK] をクリックします。

そのホストからアップリンクに割り当てる追加の PNIC ごとに、ステップ 4d および 4e を繰り返します。

[物理アダプタの管理 (Manage Physical Adapters)] ペインに、PNIC がホストに割り当てられていることが表示されます。

- f) [NEXT] をクリックします。
- g) [VMkernel アダプタの管理 (Manage VMkernel adapter)] ペインで設定を表示し、[次へ (Next)] をクリックします。
- h) [VM ネットワーキングの移行 (Migrate VM networking)] ペインで、[次へ (NEXT)] をクリックします。
- i) [終了準備の完了 (Ready to complete)] ペインで、[完了 (FINISH)] をクリックします。

## Cisco ACI vCenter プラグインの Flash バージョンを使用した ESXi ホストおよび PNIC の追加

Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge をインストールする前に、1 つ以上の ESXi ホストと、それらに対応する PNIC を新しい Cisco ACI Virtual Edge DVS に追加します。



(注) Proactive HA がすでに設定されている状態でクラスタにホストを追加し、Cisco ACI Virtual Edge VMM ドメインにホストを追加またはホストをアタッチするとき、それらのホストはある状況かでは適切に動作しない可能性があります。Cisco ACI Virtual Edge または OpFlex がダウンしたとき、Proactive HA でホストが適切に動作しない可能性があります。ホストのヘルスステータスが Cisco Application Policy Infrastructure Controller (APIC) で黄色に適切に設定されているにもかかわらず、ホストが検疫モードにならない可能性もあります。

この問題を修正するには、クラスタの Proactive HA を無効にして、再度有効にします。

### 始める前に

- Cisco ACI Virtual Edge のための VMM ドメインを作成します。このガイドの手順 [Cisco ACI Virtual Edge の VMM ドメイン プロファイルの作成 \(92 ページ\)](#) を参照してください。
- ホストで使用可能な PNIC を少なくとも 1 つ用意します。

### 手順

- ステップ 1 VMware vCenter Web クライアントにログインします。
- ステップ 2 **Networking** に移動します。
- ステップ 3 左側のナビゲーションウィンドウで、Cisco ACI Virtual Edge フォルダと、新しく作成した Cisco ACI Virtual Edge VMM ドメインのためのフォルダを展開します。
- ステップ 4 Cisco ACI Virtual Edge ドメインを右クリックして、**Add and Manage Hosts** を選択します。
- ステップ 5 **Add and Manage Hosts** ダイアログの **Select task** ペインで、**Add hosts** ラジオ ボタンをクリックして、**Next** をクリックします。
- ステップ 6 **Select hosts** ペインで、**New hosts** を選択します。
- ステップ 7 **Select new hosts** ダイアログで、Cisco ACI Virtual Edge DVS に追加するすべてのホストを選択して、**OK** をクリックします。
- ステップ 8 **Add and Manage Hosts** ダイアログボックスで、**Next** をクリックします。
- ステップ 9 **Manage physical adapters** チェック ボックスをオンにして、**Next** をクリックします。
- ステップ 10 **Manage physical network adapters** ペインで PNIC を選択し、**Assign uplink** をクリックします。
- ステップ 11 **Select an Uplink** ダイアログボックスで、アダプタのアップリンクを選択して、[OK] をクリックします。

**ステップ 12** 追加する PNIC ごとに、手順10 と手順 11 を繰り返します。

**ステップ 13** **Next** をクリックし、**Next** をもう一度クリックし、**Finish** をクリックします。

手順 6 で選択した各ホストが、Cisco ACI Virtual Edge ドメインの作業ウィンドウに表示されます。

#### 次のタスク

Cisco ACI Virtual Edge VMの OVF ファイルを vCenter にアップロードします。

## vCenter を使用した Cisco ACI Virtual Edge のインストール

インストールの前提条件を満たしたら、vCenter を使用して Cisco ACI Virtual Edge をインストールすることができます。プロセスを自動化する Cisco ACI vCenter プラグインを使用します。

最初に、Cisco ACI Virtual Edge VM オープン仮想化フォーマット (OVF) ファイルを vCenter コンテンツ ライブラリにアップロードします。それから、Cisco ACI Virtual Edge を ESXi ホストに展開することができます。



(注) コンテンツ ライブラリとしてローカル データ ストアを使用する場合には、ホストを削除してからコンテンツ ライブラリを再度作成し、vCenter に再アタッチします。ホストを再アタッチするとデータ ストアの ID が変更されるため、コンテンツ ライブラリとデータ ストアの間の関連づけが解除されるからです。



(注) Cisco ACI Virtual Edge を展開した後に、vCenter インベントリから削除し、追加し直してはなりません。これを行うと、導入時に加えたすべての設定が削除されます。既存のものをインベントリに戻すのではなく、Cisco ACI Virtual Edge を新しく追加してください。

## Cisco ACI 仮想エッジ VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードする

ESXi ホストで Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge を展開する間に、Cisco ACI Virtual Edge 仮想マシン (VM) OVF ファイルを VMware vCenter にアップロードします。次の 2 つの方式のいずれかを使用できます。

- [Cisco ACI vCenter プラグインの HTML5 バージョンを使用して OVF ファイルをアップロードする \(28 ページ\)](#)
- [Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードする \(29 ページ\)](#)

## Cisco ACI vCenter プラグインの HTML5 バージョンを使用して OVF ファイルをアップロードする

Cisco ACI vCenter プラグインの HTML5 バージョンを使用して、Cisco アプリケーション セン トリック インフラストラクチャ (ACI) 仮想 Edge VM OVF ファイルを VMware vCenter にアップ ロードします。

### 始める前に

次のことを既に実行済みである必要があります。

- Cisco Application Policy Infrastructure Controller の Cisco ACI Virtual Edge 用の VMM ドメ インを作成済み。
- 自分のコンピュータに OVF ファイルの入ったフォルダをダウンロードします。
- OVF ファイルが Cisco APIC のバージョンと互換性があることを確認。
- Cisco ACI vCenter プラグインの使用を予定している場合は、ファブリックがプラグインに 登録されていることを確認します。

プラグインをインストールして使用するための手順については、『[Cisco ACI Virtualization Guide](#)』の「Cisco ACI vCenter Plug-in」の章を参照してください。

### 手順

**ステップ 1** VMware vSphere Client にログインします。

**ステップ 2** [メニュー (Menu)] ドロップダウンリストから、[コンテンツライブラリ (Content Library)] を選択します。

Cisco ACI Virtual Edge VM OVF をアップロードしたものを受け取るため、既存のコンテンツ ライブラリを使用するか、作成します。コンテンツ ライブラリの作成手順については、VMware のドキュメンテーションを参照してください。

**ステップ 3** 左側のナビゲーションペインで、ライブラリを右クリックし、ドロップダウンリストから [項 目のインポート (Import Item)] を選択します。

**ステップ 4** [ライブラリ項目のインポート (Import Library Item)] ダイアログ ボックスの [ソース ファイ ル (Source file)] 領域で、次のいずれかの手順を実行します。

- URL を使用して OVF ファイルをアップロードするには、[URL] オプション ボタンをク リックし、ファイルの URL を入力します。
- ローカルファイルから OVF ファイルをアップロードするには、[ローカルファイル (Local file)] オプション ボタンをクリックし、[ファイルのアップロード (UPLOAD FILE)] を クリックします。ポップアップウィンドウでファイルを選択し、[開く (Open)] をクリッ クします。

**ステップ 5** [宛先 (Destination)] 領域で、[項目名 (Item name)] フィールドのファイルに名前を入力し ます。

ステップ 6 [インポート (Import)] をクリックします。

OVFファイルがコンテンツ ライブラリにアップロードされると、[テンプレート (Templates)] タブのコンテンツ ライブラリ作業ウィンドウに表示されます。

---

## Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードする

Cisco ACI Virtual Edge VM OVF ファイル を vCenter にアップロード済み。これは ESXi ホストに Cisco ACI Virtual Edge を展開する前に行っておく必要があります。

### 始める前に

次のことは実行済みであることを前提に説明します：

- Cisco APIC の Cisco ACI Virtual Edge 用の VMM ドメインを作成済み。
- 自分のコンピュータに OVF ファイルの含まれているフォルダをダウンロード。
- OVF ファイルが Cisco APIC のバージョンと互換性があることを確認。
- Cisco ACI vCenter プラグインの使用を予定している場合は、ファブリックがプラグインに登録されていることを確認します。

プラグインのインストールと使用に関する詳細は、「[Cisco ACI 仮想ガイド](#)」の「Cisco ACI vCenter プラグイン」の章を参照してください。

### 手順

ステップ 1 vSphere Web クライアントにログインします。

ステップ 2 [Content Libraries] を選択します。

Cisco ACI Virtual Edge VM OVF をアップロードしたものを受け取るため、既存のコンテンツ ライブラリを使用するか、作成します。手順については、VMware のドキュメンテーションを参照してください。

ステップ 3 ライブラリを選択し、[Import item] をクリックします。

ステップ 4 [Import library item] ダイアログボックスで、[Browse] ボタンをクリックします。

ステップ 5 ポップアップ ダイアログボックスで、OVF ファイルを選択し、[Open] をクリックします。

別のポップアップ ダイアログ ボックスが表示され、OVF フォルダ内の仮想マシンディスク (VMDK) ファイルと XML ファイルを選択するように求められます。

ステップ 6 VMDK ファイルと XML ファイルを選択し、[OK] をクリックします。

OVF ファイルをコンテンツ ライブラリにアップロードすると、**Templates** タブの下の作業ウィンドウに表示されます。

---

### 次のタスク

ESXi ホストに Cisco ACI Virtual Edge を展開します。

## Cisco ACI vCenter プラグインの HTML5 バージョンを使用して Cisco ACI 仮想エッジを展開する

Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge VM OVF ファイルを VMware vCenter にアップロードした後、ESXi ホストに Cisco ACI Virtual Edge をデプロイします。

### 始める前に

次のことを既に実行済みである必要があります。

- Cisco APIC の Cisco ACI Virtual Edge 用の VMM ドメインを作成済み。
- vCenter の新しい Cisco ACI Virtual Edge DVS に 1 つ以上の ESXi ホストと PNIC を追加済み。
- Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードした。

### 手順

---

- ステップ 1 VMware vSphere Client にログインします。
- ステップ 2 [ホーム (Home)] ページの左側のナビゲーション ペインで、[Cisco ACI ファブリック (Cisco ACI Fabric)] をクリックします。
- ステップ 3 [Cisco ACI ファブリック (Cisco ACI Fabric)] ナビゲーション ペインで、[ファブリック (Fabric)] ドロップダウン リストからファブリックを選択します。
- ステップ 4 左側のナビゲーション ペインで、[AVE] をクリックしてファブリックに関連付けられたドメインのリストを表示し、Cisco ACI Virtual Edge VM を展開するドメインをダブルクリックします。
- ステップ 5 [AVE] 作業ウィンドウで、[AVE] タブをクリックします。
- ステップ 6 (オプション) [作業 (Work)] ペインの右上にある [同時に実行できるタスクの最大数 (Max concurrent Tasks)] 鉛筆アイコンをクリックして、同時に実行する展開の数を選択します。

複数のホストに Cisco ACI Virtual Edge VM を展開する場合、同時タスクの数を指定すると、VM は指定した数のホストに導入されます。たとえば、5 つのホストに VM を展開し、同時に実行する 3 つのタスクを選択すると、他の 2 つのホストへの展開がキューに入れられている間に、同時に 3 つのホストで展開が進行します。

- ステップ7 [データセンター (Datacenter)] テーブルで、Cisco ACI Virtual Edge VM を展開する各ホストのチェックボックスをオンにします。
- ステップ8 [AVE を展開 (DEPLOY AVE)] をクリックします。
- ステップ9 ポップアップ ウィンドウで [続行 (CONTINUE)] をクリックします。  
[新規 AVE ウィザード (New AVE Wizard)] が表示されます。
- ステップ10 [バージョン (Version)] ペインで、使用する Cisco ACI Virtual Edge バージョンのオプションボタンをクリックし、[次へ (Next)] をクリックします。
- ステップ11 [ネットワーキング (Networking)] ペインで、Cisco ACI Virtual Edge VM で使用する管理ポートグループのオプションボタンをクリックし、[次へ (Next)] をクリックします。
- ステップ12 [ストレージ (Storage)] ペインで、以下のアクションのうちいずれかを完了します。
- [vCenter でデータストアを自動的に選択する (Let vCenter select the Datastore Automatically)] のチェックボックスをオンのままにして、[次へ (Next)] をクリックします。
  - [vCenter でデータストアを自動的に選択する (Let vCenter select the Datastore Automatic)] のチェックボックスをオフにし、ホストのドロップダウンリストからデータストアを選択して、[次へ (Next)] をクリックします。
- ステップ13 [設定 (Settings)] ペインの [管理者パスワード (Admin Password)] および [管理者パスワードの確認 (Confirm Admin Password)] フィールドに、VMware vCenter のパスワードを入力し、[次へ (Next)] をクリックします。
- ステップ14 [概要 (Summary)] ペインで、新しく展開された VM に関する情報を表示し、[完了 (FINISH)] をクリックします。

#### 次のタスク

展開が進行中であることを確認します。[AVE] 作業ウィンドウで、VM を展開したホストに [新規 AVE (New AVE)] ポップアップ ウィンドウが表示されます。ホストには、展開が完了した割合が表示されます。また、作業ペインの右上にあるクリップボードアイコンをクリックし、[ACI タスクと設定 (ACI Tasks & Settings)] で新しい AVE タスクに関する情報を表示することもできます。

## Cisco ACI vCenter プラグインを使用した ESXi ホストでの Cisco ACI Virtual Edge のデプロイ

Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードした後、ESXi ホストに Cisco ACI Virtual Edge をデプロイします。リモートサイトで Cisco Application Centric Infrastructure (ACI) 仮想ポッド (vPod) のコンポーネントとして Cisco ACI Virtual Edge を展開できます。または、Cisco ACI vPod の一部にせずに Cisco ACI Virtual Edge を展開することもできます。詳細については、Cisco ACI vPod 製品のマニュアルを参照してください。

## 始める前に

次のことを既に実行済みである必要があります。

- Cisco APIC の Cisco ACI Virtual Edge 用の VMM ドメインを作成済み。
- VMware vCenter の新しい Cisco ACI Virtual Edge DVS に 1 つ以上の ESXi ホストと PNIC を追加済み。
- Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードした。



(注) VMware vCenter 6.0 Web Client を使用している場合は、OVF ファイルを参照するポップアップウィンドウが表示されないことがあります。この場合、OVF ファイル、仮想マシン ディスク ファイル (VMDK)、VMware を HTTP サーバーにアップロードします。その後、サーバーから OVF ファイル URL を使用して、OVF ファイルをコンテンツ ライブラリにダウンロードします。

## 手順

- ステップ 1 vSphere Web クライアントにログインします。
- ステップ 2 [Home] 作業ウィンドウで、[Cisco ACI Fabric] アイコンをクリックします。
- ステップ 3 Cisco ACI Fabric ナビゲーション ウィンドウで、**ACI Virtual Edge** をクリックします。
- ステップ 4 [ACI 仮想エッジ (ACI Virtual Edge)] 作業ウィンドウで、複数の仮想ドメインがある場合は、[ACI 仮想エッジ ドメインの選択 (Select an ACI Virtual Edge Domain)] ドロップダウン リストからドメインを選択します。仮想ドメインが 1 つしかない場合は、次の手順に進みます。
- ステップ 5 Cisco ACI Virtual Edge をデプロイするホストを選択します。
- ステップ 6 [ACI Virtual Edge version] ドロップダウン リストから、デプロイするバージョンを選択します。
- ステップ 7 [Management PortGroup] ドロップダウン リストから、管理ポート グループを選択します。
- ステップ 8 [Datastore] ドロップダウン リストから [Custom] を選択し、[Edit] をクリックします。
- ステップ 9 [カスタム AVE データストア選択 (Custom AVE Datastore selection)] ダイアログ ボックスで、各 Cisco ACI Virtual Edge のローカルまたはリモート データ ストアを選択します。

(注) 高レベルの可用性を確保するには、存在する場合ローカル データ ストアを選択することをお勧めします。

(注) VMware vCenter では、すべてのタイプのローカルストレージが表示されない場合があります。ただし、[ローカル データストアのみ使用する (Use local datastore only)] チェックボックスをオフにすると、VMware vCenter はすべてのローカル データ ストアを表示します。詳細については、詳細については、「When installing ESX/ESXi 4.x or 5.x to a physical server, the local SAS drive appears as a remote storage (1027819)」を参照してください。

- ステップ 10 [VM Admin Password] フィールドに、Cisco ACI Virtual Edge VM の新しいパスワードを入力します。
- ステップ 11 Cisco ACI Virtual Edge を Cisco ACI vPod の一部として展開する場合は、次の手順を実行します。
- [vPod モード (vPod Mode) ] チェック ボックスをオンにします。
  - [vPod] ドロップダウンリストから、Cisco ACI Virtual Edge を関連付ける Cisco ACI vPod を選択します。
- ステップ 12 [Install/Upgrade ACI Virtual Edge] をクリックします。
- ステップ 13 [Install] ダイアログボックスで、[Yes] をクリックします。

作業ウィンドウで、インストールされたホストに OpFlex ステータス、Cisco ACI Virtual Edge VM、および管理 IP が表示されます。OpFlex が登場するまで少し時間がかかるかもしれません。

#### 次のタスク

- 正しい EPG を Cisco APIC コントローラの VMM ドメインに接続するか、または Cisco ACI vCenter プラグインを使用して VMware vCenter 経由で接続します。
- VM を vCenter の正しいポートグループに配置します。

## VMware PowerCLI を使用した Cisco ACI Virtual Edge のインストール

プレインストールの前提条件を満たした後に、VMware PowerCLI を使用して Cisco ACI Virtual Edge をインストールすることができます。

最初に VMware Power CLI 環境を設定します。最初に、VMware PowerCLI ファイルを含む zip ファイルをダウンロードし、Cisco ACI Virtual Edge モジュールをインポートし、vCenter コンテンツ ライブラリから新しい Cisco ACI Virtual Edge VM を展開します。

### PowerCLI 環境の設定

PowerCLI を使用して Cisco Application Centric Infrastructure (ACI) 仮想ポッド (vPod) または Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge の仮想マシン (VM) を展開する前に、Cisco AVE PowerCLI モジュールをインポートし、VMware vCenter への接続を確立します。

#### 始める前に

PowerCLI 6.0 リリース 3 以降があることを確認します。

## 手順

**ステップ 1** Cisco ACI vPod または Cisco ACI Virtual Edge の高次の設定ファイルが含まれている CiscoAVE.zip ファイルをダウンロードします。

zip ファイルには次のものが含まれています。

- CiscoAVE.psm1 : CiscoAVE VMware PowerCLI モジュール ファイル
- lib/ : モジュール ライブラリ

**ステップ 2** **Import-Module** コマンドを使用して、CiscoAVE PowerCLI モジュールをインポートします。

例 :

```
PowerCLI C:\> Import-Module CiscoAVE.psm1
```

**ステップ 3** 標準の PowerCLI コマンド (**Connect-VIServer** および **Connect-CisServer**) を使用して VMware vCenter に接続します。

**Connect-CisServer** コマンドは、VMware vCenter コンテンツ ライブラリのタグ付けや管理などの機能に必要です。

例 :

```
PowerCLI C:\> Connect-VIServer -Server 172.23.143.235 -User admin -Password lab
```

Name	Port	User
----	----	----
172.23.143.235	443	admin

例 :

```
PowerCLI C:\> Connect-CisServer -Server 172.23.143.235 -User admin -Password lab
```

Name	User	Port
----	----	----
172.23.143.235	admin@localos	443

## VMware PowerCLI を使用した VMware vCenter コンテンツ ライブラリの管理

オープン仮想化フォーマット (OVF) ファイルを VMware vCenter コンテンツ ライブラリにアップロードします。これで、ファイル内のスクリプトで仮想マシン (VM) を展開できます。

既存のコンテンツ ライブラリを使用するか、コンテンツ ライブラリを作成します。VMware vSphere Web クライアント UI で、またはこの項に記載している PowerCLI コマンドを使用して、新しいコンテンツ ライブラリを作成します。

## 手順

- ステップ 1 New-LocalContentLibrary** コマンドを使用して新しい VMware vCenter コンテンツ ライブラリを作成します。

次のテキストはコマンドの構文です。

```
New-LocalContentLibrary [-Name] Object [-Datastore] Object [-Datacenter] Object
[CommonParameters]
```

例 :

```
PowerCLI C:\> New-LocalContentLibrary -Name ave-lib -Datastore 129-local -Datacenter
mininet
Connecting to vCenter.....[ok]
Creating content library 'ave-lib'.....[ok]
```

- ステップ 2 New-ContentLibraryItem** コマンドを使用して OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードします。

コマンドを実行するローカルマシンで OVF (.ova) ファイルを利用可能にする必要があります。

次のテキストはコマンドの構文です。

```
New-ContentLibraryItem [-Name] Object [-ContentLibrary] Object [-Ovf] Object
[CommonParameters]
```

例 :

```
PowerCLI C:\> New-ContentLibraryItem -Name vpod-ova -ContentLibrary ave-lib -Ovf
L:\ova\aci-vpod.14.0.0.84.ova
Connecting to vCenter.....[ok]
Extracting OVA.....[ok]
Validating.....[ok]
Uploading aci-vpod.14.0.0.84-disk1.vmdk.....[ok]
Uploading aci-vpod.14.0.0.84.ovf.....[ok]
Finishing up.....[ok]
```

- ステップ 3 Remove-LocalContentLibraryItem** コマンドを使用して VMware vCenter コンテンツ ライブラリから項目を削除します。

次のテキストはコマンドの構文です。

```
Remove-LocalContentLibraryItem [-Name] Object [-ContentLibrary] Object [CommonParameters]
```

例 :

```
PowerCLI C:\> Remove-LocalContentLibraryItem -Name vpod-14.0.0.84 -ContentLibrary vpod-ova
Connecting to vCenter.....[ok]
Deleting content library item 'vpod-14.0.0.84'.....[ok]
```

## VMware PowerCLI を使用した Cisco ACI Virtual Edge の展開

Windows プラットフォームを用いている場合には、Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge をインストールするために VMware PowerCLI を使用することができます。リモートサイトで Cisco Application Centric Infrastructure (ACI) 仮想ポッド

(vPod) のコンポーネントとして Cisco ACI Virtual Edge を展開できます。または Cisco ACI vPod の一部にせず展開できます。詳細については、Cisco ACI vPod を参照してください。



(注) パラメータのヘルプを参照するには、コマンドで「Get-Help」を使用します。たとえば、**Get-Help New-LocalContentLibrary** のように入力します。

## 手順

**ステップ 1** Cisco ACI Virtual Edge をどれくらい使用したいかによって、次のアクションのいずれかを実行します。

オプション	説明
Cisco ACI Virtual Edge を展開する場合...	結果
Cisco ACI vPod の一部として	ステップ 2 に進みます。
Cisco ACI vPod の一部とせず	ステップ 3 に進みます。

**ステップ 2** **New-VPodAveVM** コマンドを使用して Cisco ACI vPod の一部として Cisco ACI Virtual Edge を展開します。

次のテキストはコマンドの構文です。

```
New-VPodAveVM [-HostName] Object [-DomainName] Object [-MgmtPortgroupName] Object
[-AdminPassword] SecureString [-InfraVlan]
Object [-OvfItem] Object [-ApicVersion] Object [-VpodId] Object [[-Vtor1Ip] String]
[[ -Vtor2Ip] String] [[-VtepIp]
String] [[-VtepNetmask] String] [[-VtepGateway] String] [[-Library] String]
[[ -DatastoreName] String] [[-Ip] String]
[[ -Netmask] String] [[-Gateway] String] [[-Nameserver] String] [[-VmHostname] String]
[CommonParameters]
```

例 :

```
PowerCLI C:\> $pass = Read-Host -AsSecureString
*****
PowerCLI C:\> New-VPodAveVM -HostName 198.51.100.15 -DomainName mininet -MgmtPortgroupName
"VM Network"
-AdminPassword $pass -InfraVlan 4 -OvfItem cisco-ave-build312 -ApicVersion "4.0(1.0)"
-VpodId 2

Connecting to vCenter.....[ok]
Validating configuration.....[ok]
Deploying OVF (this might take several minutes).....[ok]
Applying Cluster configuration.....[ok]
Applying Cluster configuration.....[ok]
Applying VM configuration.....[ok]
Applying Host configuration.....[ok]
Powering On VM.....[ok]
```

**ステップ 3** **New-AveVM** コマンドを使用して Cisco ACI vPod の一部としてではなく Cisco ACI Virtual Edge を展開します。

次のテキストはコマンドの構文です。

```
New-AveVM [-HostName] Object [-DomainName] Object [-MgmtPortgroupName] Object
[-AdminPassword] SecureString [-InfraVlan]
<Object> [-OvfItem] Object [-ApicVersion] Object [[-Library] String] [[-DatastoreName]
String] [[-Ip] String] [[-Netmask]String] [[-Gateway] String] [[-Nameserver] String]
[[-VmHostname] String] [CommonParameter]
```

例：

```
PowerCLI C:\> New-AveVM -HostName 198.51.100.15 -DomainName AVE-FI -MgmtPortgroupName
'VLAN418' -InfraVlan 5 -OvfItem "cisco-ave-2.0.0.466-r3" -Library 466 -Ip 10.197.143.195
-Netmask 255.255.255.0 -Gateway 198.51.100.160 -DatastoreName datastore-248 -ApicVersion
"4.0(1.0)" -Verbose

cmdlet New-AveVM at command pipeline position 1
Supply values for the following parameters:
AdminPassword: *****
Connecting to vCenter.....[ok]
Validating configuration.....[ok]
Deploying OVF (this might take several minutes).....[ok]
Applying Cluster configuration.....[ok]
Applying Cluster configuration.....[ok]
Applying VM configuration.....[ok]
Applying Host configuration.....[ok]
Powering On VM.....[ok]
PowerCLI C:\>
```

**ステップ 4 Get-AveVM** コマンドを使用して、展開済みの Cisco ACI Virtual Edge 仮想マシン (VM) のリストを取得します。

次のテキストはコマンドの構文です。

```
Get-AveVM [<CommonParameters>]
```

例：

```
PowerCLI C:\> Get-AveVM | Format-Table

VirtualMachine      HostName      DVS      ManagementIp
-----
cisco-ave_198.51.100.15_mininet  198.51.100.15  mininet  198.51.100.41
```

## Python を使用した Cisco ACI Virtual Edge のインストール

プレインストールの前提条件を満たしたら、Python を使用して Cisco ACI Virtual Edge をインストールすることができます。

まず Python ファイルを含む ZIP ファイルをダウンロードし、Python を実行する環境を設定し、Python コマンドを使用して vCenter でコンテンツ ライブラリを作成し、Cisco ACI Virtual Edge VM OVF ファイルを vCenter コンテンツ ライブラリにアップロードし、そしてコンテンツ ライブラリから新しい VM を展開します。

## Python 環境の設定

Python を使用して Cisco Application Centric Infrastructure (ACI) 仮想ポッド (vPod) または Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge をインストールできるように、Python 環境をセットアップします。



(注) Python の依存ファイルの問題を避けるため、仮想環境の使用を強く推奨します。

### 始める前に

次のことを既に実行済みである必要があります。

- Python 2.7.9 降のバージョンがあることを確認した。
- VMware vCenter 6.0 GA U3 以降があることを確認した。
- Git と PIP がインストールされていることを確認した。

### 手順

**ステップ 1** Cisco ACI vPod および Cisco ACI Virtual Edge を展開するための高次の Python 設定スクリプトが含まれている .zip ファイルをダウンロードします。

.zip ファイルには次のものが含まれています。

- `get-avevm.py` : 現在展開されている Cisco ACI Virtual Edge 仮想マシン (VM) のリストを取得します。
- `new-avevm.py` : 新しい Cisco ACI Virtual Edge VM を展開します。
- `remove-avevm.py` : Removes a Cisco ACI Virtual Edge VM.
- `content-library.py` : VMware vCenter コンテンツ ライブラリとやり取りします。
- `get-vpodvm.py` : 現在展開されている Cisco ACI vPod VM のリストを取得します。
- `new-vpodvm.py` : Cisco ACI vPod VM の新しいペア (1 つは仮想スパイン (vSpine) 、1 つは仮想リーフ (vLeaf) ) を展開します。
- `remove-vpodvm.py` : すべての Cisco ACI vPod VM を削除します。
- `requirements.txt` : PIP パッケージ管理システムで使用される Python の依存ファイルのリスト。

**ステップ 2** (オプションですが推奨) Python 仮想環境を設定します。

a) 次のコマンドを入力します。

例 :

```
$ pip install virtualenv
$ virtualenv venv
```

b) 次のいずれかのコマンドを入力します。

- Linux または Macintosh システムを使用している場合は、次のコマンドを入力します。

```
$ . venv/bin/activate
```

- Windows システムを使用している場合は、次のコマンドを入力します。

```
> ven\Scripts\activate
```

**ステップ 3** VMware vSphere 自動化ソフトウェア開発キット (SDK) をインストールします。

a) VMware vSphere 自動化 SDK を GitHub からダウンロードします。現在のところ Python パッケージ インデックス (PyPi) には最新バージョンはありません。

例 :

```
(venv) $ git clone https://github.com/vmware/vsphere-automation-sdk-python.git
(venv) $ cd vsphere-automation-sdk-python
```

Linux:

```
(venv) $ pip install --upgrade -r requirements.txt --extra-index-url file:///`pwd`/lib
```

Windows:

```
> pip install --upgrade --force-reinstall -r requirements.txt --extra-index-url
file:///absolute_dir_to_sdk/lib
```

**ステップ 4** その他のすべての依存ファイルをインストールします。

例 :

```
(venv) $ cd ../
(venv) $ pip install -r requirements.txt
```

requirements.txt ファイルには、スクリプトで必要なすべての依存ファイルが含まれています。このファイル内の依存ファイルのインストールは 1 回だけ行います。

---

## Python を使用した VMware vCenter コンテンツ ライブラリの管理

オープン仮想化フォーマット (OVF) ファイルを VMware vCenter コンテンツ ライブラリにアップロードします。これで、ファイル内のスクリプトで仮想マシン (VM) を展開できます。

既存のライブラリを使用するか、新規に作成できます。VMware vSphere Web クライアント UI で、またはこの項に記載している Python コマンドを使用して、新しいコンテンツ ライブラリを作成します。

手順

**ステップ 1** Create サブコマンドを使用して、新しいコンテンツ ライブラリを作成します。

次のテキストはコマンドの使用方法を示しています。

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Create --name NAME --datacenter DATACENTER
--datastore DATASTORE
```

例：

```
(venv) $ python content-library.py --vcenter 172.23.143.235 --vc-username admin
--vcpasssword
lab Create --name ave_repo --datacenter mininet --datastore 129-local
Connecting to vCenter.....[ok]
Creating content library 'ave_repo'.....[ok]
```

**ステップ 2** ave vmdk ファイルを VMware vCenter の任意のホストのデータストアにコピーします。

例：

```
scp cisco-ave-2.1.1.321-disk1.vmdk root@10.23.238.203:/vmfs/volumes/datastore2/
```

**ステップ 3 Upload** サブコマンドを使用して OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードします。

Python スクリプトを実行するローカル マシンで OVF ファイルを利用可能にする必要があります。コピーした vmdk ファイルの完全なデータストアパスを vmdk-ds-path に入力します。

次のテキストはコマンドの使用方法を示しています。

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Upload --library LIBRARY --item ITEM --path PATH
[--vmdk-ds-path VMDK_DS_PATH]
```

例：

```
(venv) $ python content-library.py --vcHost 10.23.219.150 --vcUser 'administrator' --vcPwd
`lab' Upload --library repo --item cisco-ave-2.1.1.321.ovf --path
/Users/User/dev/ovf/cisco-ave-2.1.1.321.ovf --vmdk-ds-path
ds:///vmfs/volumes/59348426-b1a50255-8787-cc167ee18b76/cisco-ave-2.1.1.321-disk1.vmdk
Connecting to vCenter.....[ok]
Extracting OVA.....[ok]
Validating.....[ok]
Uploading aci-vpod.14.0.0.84-disk1.vmdk.....[ok]
Uploading aci-vpod.14.0.0.84.ovf.....[ok]
Finishing up.....[ok]
```

**ステップ 4 Remove** サブコマンドを使用してコンテンツ ライブラリから項目を削除します。

次のテキストはコマンドの使用方法を示しています。

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Remove --library LIBRARY --item ITEM
```

例：

```
(venv) $ python content-library.py --vcenter 172.23.143.235 --vc-username admin
--vcpasssword
lab Remove --library repo --item vpod-14.0.0.84
Connecting to vCenter.....[ok]
Deleting content library item 'vpod-14.0.0.84'.....[ok]
```

## Python を使用して Cisco ACI Virtual Edge を展開する

Python スクリプトを使用して Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge を展開できます。Cisco Application Centric Infrastructure (ACI) 仮想ポッド (vPod) のコンポーネントとしてリモート サイトに Cisco ACI Virtual Edge を展開できます。または、Cisco ACI vPod の一部にせず展開することもできます。詳細については、Cisco ACI vPod を参照してください。



(注) 入力できる `-h` パラメータのいずれかのヘルプを取得する任意のスクリプトで。例：

```
# python new-avevm.py -h
```

### 始める前に

- Python 環境の設定を確認します。このガイドの手順 [Python 環境の設定 \(38 ページ\)](#) を参照してください。
- Python スクリプトを実行する前に `unset Python` 環境を設定するときを `access the Internet`(インターネットにアクセス、インターネットへのアクセス、インターネットアクセス、インターネット接続): プロキシを使用している場合

```
unset http_proxy
unset https_proxy
```

### 手順

**ステップ 1** Cisco ACI Virtual Edge の使用方法に応じて、次のいずれかのアクションを実行します。

オプション	説明
Cisco ACI Virtual Edge を導入する場合	結果
Cisco ACI vPod の一部として	ステップ 2 に進みます。
Cisco ACI vPod の一部としてではありません	ステップ 3 に進みます。

**ステップ 2** vPod サブコマンドを使用して Cisco ACI vPod の一部として Cisco ACI Virtual Edge を展開します。

次のテキストはコマンドの使用法を示しています。

```
usage: new-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --host-name
HOST_NAME --domain-name DOMAIN_NAME --mgmt-pg MGMT_PG
[--admin-password ADMIN_PASSWORD] --infra-vlan INFRA_VLAN
--ovf-item OVF_ITEM [--library LIBRARY]
[--datastore DATASTORE] [--ip IP] [--netmask NETMASK]
[--gateway GATEWAY] [--nameserver NAMESERVER]
[--vm-hostname VM_HOSTNAME] --apic-version APIC_VERSION
vPod --vpod-id VPOD_ID [--vtor1-ip VTOR1_IP]
[--vtor2-ip VTOR2_IP] [--vtep-ip VTEP_IP]
```

```
[--vtep-netmask VTEP_NETMASK]
[--vtep-gateway VTEP_GATEWAY]
```

例 :

```
python new-avevm.py --vcenter 172.23.143.235 --vc-username 'administrator@vSphere.local'
--vc-password 'vcpasssword' --host-name 172.23.143.129 --domain-name 'ave-dom1' --mgmt-pg
'VM Network' --infra-vlan 10 --ovf-item cisco-ave-2.0.0.476 --admin-password
'adminpassword' --apic-version '4.0(0.0)' vPod --vpod-id 2
```

```
Connecting to vCenter.....[ok]
Validating configuration.....[ok]
Deploying OVF (this might take several minutes).....[ok]
Applying Cluster configuration.....[ok]
Applying Cluster configuration.....[ok]
Applying VM configuration.....[ok]
Applying Host configuration.....[ok]
Powering On VM.....[ok]
```

(注) 管理ポートグループが VMware VDS 上にある場合は、VDS 名を --mgmt-pg 'vds-name / portgroup-name' の形式で指定する必要があります。

(注) 静的管理 IP アドレスを使用するには、vPod サブコマンドの前にある --ip パラメータを使用します。

```
[...] --ip 172.31.100.11 --netmask 255.255.255.0 --gateway 172.31.100.1
--nameserver 172.23.140.25 vPod [...]
```

**ステップ 3 Enterprise** サブコマンドを使用して Cisco ACI vPod の一部としてではなく Cisco ACI Virtual Edge を展開します。

次のテキストはコマンドの使用方法を示しています。

```
usage: new-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --host-name
HOST_NAME --domain-name DOMAIN_NAME --mgmt-pg MGMT_PG
[--admin-password ADMIN_PASSWORD] --infra-vlan INFRA_VLAN
--ovf-item OVF_ITEM [--library LIBRARY]
[--datastore DATASTORE] [--ip IP] [--netmask NETMASK]
[--gateway GATEWAY] [--nameserver NAMESERVER]
[--vm-hostname VM_HOSTNAME] --apic-version APIC_VERSION
{vPod,Enterprise} ...
```

例 :

```
(venv) $ python new-avevm.py --vcenter 172.23.143.235 --vc-username admin --vc-password
lab --host-name 172.23.143.129 --domain-name mininet --mgmt-pg 'VM Network' --infra-vlan
4
--ovf-item cisco-ave-build312 --apic-version '4.0(0.0)' --admin-password password
Enterprise
```

```
Connecting to vCenter.....[ok]
Validating configuration.....[ok]
Deploying OVF (this might take several minutes).....[ok]
Applying Cluster configuration.....[ok]
Applying Cluster configuration.....[ok]
Applying VM configuration.....[ok]
Applying Host configuration.....[ok]
Powering On VM.....[ok]
```

**ステップ 4 get-avevm.py** スクリプトを使用して、展開されている Cisco ACI Virtual Edge 仮想マシン (VM) のリストを取得します。

次のテキストはスクリプトの使用方法を示しています。

```
usage: get-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD]
```

例：

```
(venv) $ python get-avevm.py --vcenter 172.23.143.235 --vc-username admin --vc-password
lab
```

```
+-----+-----+-----+-----+
| Virtual Machine | Host | Domain | Management IP |
+-----+-----+-----+-----+
| cisco-ave_172.23.143.129_mininet | 172.23.143.129 | mininet | 172.31.143.146 |
| cisco-ave_172.23.143.228_mininet | 172.23.143.228 | mininet | None |
+-----+-----+-----+-----+
```

## Cisco ACI Virtual Edge 展開の確認

Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge を展開した後、展開を確認します。それには、Cisco ACI Virtual Edge (kni0) との通信に使用するインターフェイスに仮想トンネルエンドポイント (VTEP) の IP アドレスが用意されたことを確認します。また、OpFlex が起動していることを確認します。

始める前に

VMware vCenter で Cisco ACI Virtual Edge を展開している必要があります。

手順

**ステップ 1** `ipconfig` コマンドを入力し、出力を確認します。

例：

```
kni0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.3 netmask 255.255.252.0 broadcast 192.168.11.255
    inet6 fe80::250:56ff:fea7:fac prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:a7:0f:ac txqueuelen 1000 (Ethernet)
    RX packets 374443 bytes 52541802 (50.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 161054 bytes 20000611 (19.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

**ステップ 2** 適切な `vemcmd` コマンドを入力して、OpFlex が起動しているかどうかを確認します。

- Cisco ACI 仮想ポッド (vPod) の一部として Cisco ACI Virtual Edge を使用している場合は、次の例に示すようにコマンド `vemcmd show opflex cloud` を入力します。

```
AVE-36:~$ vemcmd show opflex cloud
Status: READY
Peer 1, host: 192.168.8.16, port: 8009, status: READY
Peer 2, host: 192.168.8.17, port: 8009, status: READY
Dvs name: comp/prov-VMware/ctrlr-[vpod]-vc/sw-dvs-1983
```

- Cisco ACI Virtual Edge を使用しており、Cisco ACI vPod の一部ではない場合は、次の例に示すように、コマンド **vemcmd show opflex** を入力します。

```
cisco-ave:~$ vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channell: 12 (Active)
Dvs name: comp/prov-VMware/ctrlr-[vpod]-vc/sw-dvs-1983
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 4093
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: VXLAN
NS GIPO: 228.1.1.1
```

### 次のタスク

本ガイドの [GUI を使用した Cisco ACI 仮想エッジ ライセンスの表示 \(44 ページ\)](#) および [インストール後の設定 \(47 ページ\)](#) セクションをお読みください。

## GUI を使用した Cisco ACI 仮想エッジ ライセンスの表示

Cisco APIC Release 3.2(1) 以降では、スマート ライセンス機能の一部として、Cisco ACI ファブリックの Cisco ACI Virtual Edge ライセンスを表示できます。

また、NX-OS スタイルの CLI コマンドを使用してライセンス情報を表示することもできます。詳細については、ナレッジベースの記事、『スマート ライセンス』を参照してください。[Cisco.com](#) で利用できます。

### 始める前に

スマート ライセンスを登録する必要があります。ナレッジベースの記事、『スマート ライセンス』を参照してください。[Cisco.com](#) で利用できます。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** **System > Smart Licensing** に移動します。

中央のペインの、**Smart License Usage** エリアにライセンス、その番号、およびステータスのリストが表示されます。Cisco ACI Virtual Edge のライセンスについては、**Count** カラムに、Cisco ACI の Cisco ACI Virtual Edge インスタンスの数が表示されます。カウントされるのは、オンにされ、OpFlex を通して接続されている Cisco ACI Virtual Edge インスタンスだけです。

**Count** カラムには、Cisco APIC によって管理されている VMware vCenter DVS に存在する Cisco ACI Virtual Edge インスタンスだけです。Cisco ACI Virtual Edge オンになっていないインスタンスも、ライセンスの対象としてカウントされます。

(注) アップデートやダウングレードの実行中には、Cisco ACI Virtual Edge のライセンス カウントが不正確になる場合があります。

## VMware vCenter でスタティック IP アドレスを設定する

Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge を展開後、VMware vCenter でスタティック IP アドレスを設定できます。Cisco ACI HTML5 vCenter プラグイン または Cisco ACI vCenter バージョンの Flash プラグインを使用して VMware vCenter にアクセスした後、次の手順を実行します。

- [VMware vSphere クライアントの HTML5 バージョンを使用したスタティック IP アドレスの設定 \(45 ページ\)](#)
- [VMware vSphere Web クライアントの Flash バージョンを使用したスタティック IP アドレスの設定 \(46 ページ\)](#)

## VMware vSphere クライアントの HTML5 バージョンを使用したスタティック IP アドレスの設定

Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge のスタティック IP アドレスを設定できます。Python または VMware PowerCLI を使用しない場合は、VMware vCenter でスタティック IP アドレスを設定できます。Cisco ACI HTML5 vCenter プラグインの HTML5 バージョンを使用する場合は、次の手順を実行します。

### 始める前に

VMware vCenter に Cisco ACI Virtual Edge がインストールされている必要があります。

### 手順

- ステップ 1 VMware vSphere Client にログインします。
- ステップ 2 [ホストおよびクラスタ (Hosts and Clusters)] > [データセンター (Datacenter)] > [ホスト (*host*)] に移動し、ホスト上の Cisco ACI Virtual Edge 仮想マシン (VM) を選択します。
- ステップ 3 メニューバーで、正方形の赤いアイコンをクリックして Cisco ACI Virtual Edge VM をシャットダウンし、[電源オフを確認 (Confirm Power Off)] ダイアログ ボックスで [はい (YES)] をクリックします。
- ステップ 4 左側のナビゲーション ペインで Cisco ACI Virtual Edge VM を選択した状態で、[設定 (Configure)] をクリックし、[vApp オプション (vApp Options)] をクリックします。
- ステップ 5 作業ウィンドウの右上にある [編集 (Edit)] をクリックします。

- ステップ 6** [vApp オプションの編集 (Edit vApp Options)] ダイアログ ボックスで、次のステップを実行します。
- [IP 割り当て (IP Allocation)] タブが選択されていることを確認します。
  - [認証中 (Authoring)] 領域で、DHCP および OVF 環境の [IP 割り当て (IP allocation)] チェック ボックスをオンのままにします。
  - [展開 (Deployment)] 領域で、[IP 割り当て (IP allocation)] ドロップダウン リストから [スタティック - 手動 (Static-Manual)] を選択します。
  - OK をクリックします。
- ステップ 7** 次の手順を実行して、認識されない OVF の IP アドレス、マスク、およびサブネット情報を入力します。
- [vApp オプション (vApp Options)] ペインで、[設定 (Configure)] タブをクリックします。
  - 作業ウィンドウの下部にある [プロパティ (Properties)] 領域で、[管理アドレス (Management Address)] のオプション ボタンをクリックし、[値を設定 (Set Value)] をクリックします。
  - [値を設定 (Set Value)] ダイアログ ボックスの [IP 値 (IP value)] フィールドに IP 管理アドレスを入力し、[OK] をクリックします。
  - [管理ネットマスク (Management Netmask)] および [管理ゲートウェイ (Management Gateway)] に対してステップ 7b および 7c を繰り返します。
- ステップ 8** 左側のナビゲーション ペインで Cisco ACI Virtual Edge VM を右クリックし、ドロップダウン リストから [電源 (Power)] を選択します。[電源オン (Power On)] を選択します。

## VMware vSphere Web クライアントの Flash バージョンを使用したスタティック IP アドレスの設定

Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge のスタティック IP アドレスを設定できます。Python または VMware PowerCLI を使用しない場合は、VMware vCenter でスタティック IP アドレスを設定できます。Cisco ACI HTML5 vCenter プラグインの Flash バージョンを使用する場合は、次の手順を実行します。

### 手順

- ステップ 1** VMware vCenter Web クライアントにログインします。
- ステップ 2** Cisco ACI Virtual Edge の電源を切ります。
- ステップ 3** ホストと仮想マシン (VM) に移動し、[設定 (Configure)] タブを選択します。
- ステップ 4** [VM] ペインで [編集 (Edit)] を選択し、[設定の編集 (Edit Settings)] ダイアログ ボックスで [vApp オプション (vApp Options)] を選択します。
- ステップ 5** [展開 (Deployment)] 領域で、[IP 割り当て (IP allocation)] ドロップダウン リストから [スタティック - マニュアル (Static-Manual)] を選択します。

ステップ6 [未認可 OVF (Unrecognized OVF)] セクション領域に、IP アドレス、マスク、およびゲートウェイ情報を入力します。

ステップ7 [OK] をクリックします。

## インストール後の設定

Cisco ACI Virtual Edge、をインストールしたら、次の主要な設定タスクを実行してください:

- アプリケーションプロファイルを展開します。これにはテナント、アプリケーションプロファイル、EPG、フィルタ、および契約の作成と、VM へのポート割り当てが含まれます。それからアプリケーションプロファイルを確認します。

手順については、『Cisco APIC 基本設定ガイド』を参照してください。

- 分散ファイアウォールを使用する場合は、インストール後に有効にします。『Cisco ACI Virtual Edge Configuration Guide』の「Distributed Firewall」の章を参照してください。
- Cisco ACI Virtual Edge が複数宛先のトラフィック、特にブレードスイッチを通るトラフィックを転送できるようにするには、インフラ BD サブネット下で IGMP クエリアを設定します。これにより、デバイスはそのレイヤ2マルチキャストツリーを構築できる余蘊ありません。

『Cisco ACI 仮想エッジ構成ガイド』の「IGMP クエリアとスヌーピングの設定」のセクションを参照してください、

『Cisco ACI 仮想エッジ構成ガイド』では、その他の設定タスクの手順も確認できます。これにはマイクロセグメンテーション、SPAN、EPG 内分離の適用、混合モードのカプセル化、および BPDU 機能が含まれます。





## 第 4 章

# Cisco AV から移行する Cisco ACI Virtual Edge

この章で説明する Cisco アクセス違反から移行 Cisco ACI Virtual Edge、さまざまな方法を含みます。

- [Cisco AVS から Cisco ACI Virtual Edge 移行する \(49 ページ\)](#)
- [Cisco AV から移行するための方法を Cisco ACI Virtual Edge \(49 ページ\)](#)
- [Cisco AVS から Cisco ACI Virtual Edge に移行するための前提条件 \(52 ページ\)](#)
- [Cisco ACI vCenter プラグインを使用して Cisco AVS から Cisco ACI Virtual Edge に移行する \(55 ページ\)](#)

## Cisco AVS から Cisco ACI Virtual Edge 移行する

Cisco AVS を使用している場合には、ホストとその VM をそのスイッチから Cisco ACI Virtual Edge に移行することができます。

いくつかの前提条件を満たした後に、vCenter プラグインを使用し、3つの方法のいずれかを使用して Cisco アプリケーション仮想スイッチ (AVS) から Cisco ACI Virtual Edge に移行してください。



(注) Cisco Application Policy Infrastructure Controller リリース 5.0 (1) 以降、Cisco AVS はサポートされなくなりました。Cisco AVS から Cisco ACI Virtual Edge へ移行する場合は、Cisco APIC 5.0(1) にアップグレードする前に移行してください。

## Cisco AV から移行するための方法を Cisco ACI Virtual Edge

3つの方法のいずれか vCenter プラグインに役立つ Cisco アクセス違反から移行 Cisco ACI Virtual Edge。各方式は、同じ vCenter GUI 画面の指示移行を自動化できます。選択した方法は、お客様のセットアップとネットワーク トポロジによって異なります。

- **DRS** : 移行するすべてのホストは同じ分散リソース スケジューラ (DRS) クラスタ。VCenter プラグインは、ホストをメンテナンス モードにすると DRS は、クラスタ内の別のホストにホストの Vm を自動的に移行します。

この方法では、ホストに存在するすべてのアクティブな Vm は最小限のトラフィックが失われる結果として、ホストから自動的に移動します。

- **ホストを予約** : 予約のホストを選択して、vCenter プラグインは、移行を進める前に、このホストにすべてのアクティブな Vm を移行します。

この方法では、ホストに存在するすべてのアクティブな Vm は最小限のトラフィックが失われる結果として、ホストから自動的に移動します。

- **インプレース移行** ]: ホストに移行 Cisco ACI Virtual Edge ホストで実行されているアクティブな Vm とします。場合は、この方法を使用する別のホストに Vm を移動してのみの導入を検討していない Cisco ACI Virtual Edge。




---

(注) この方法では、Vm のネットワークの接続性に大量の停止が発生します。

---

### DRS 移行ワークフロー

次の移行がクラスタ内のホストがないのでは Cisco ACI Virtual Edge オンライン OpFlex を実行しています。

1. ホストはメンテナンスモードに入ります。
2. Cisco ACI Virtual Edge DVS がホストに追加されます。  
確認します Cisco ACI Virtual Edge dvs には、内部が外部および内通ポート グループと Cisco AV 上には、同じポート グループ。
3. Pnic と vmknic はシスコの AV DVS からの移動、Cisco ACI Virtual Edge dvs にします。
4. ホストでの Vm の電源をオフのポート グループに Cisco アクセス違反から更新 Cisco ACI Virtual Edge。
5. Cisco AV dvs には、ホストから削除されます。
6. (選択した場合にアンインストールするよう)、Cisco AV モジュールは、ホストからアンインストールされます。
7. 「アフィニティ ルールは、DRS クラスタに配置されます。  
「アフィニティ ルールで実行されているすべての Vm の移動から DRS を防止する、Cisco ACI Virtual Edge までアップグレードされているホストを dvs に、Cisco ACI Virtual Edge VM が完全に展開します。
8. ホストはメンテナンス モードから取得されます。

9. Cisco ACI Virtual Edgeホストで VM を展開します。
10. OpFlex エージェントがオンラインになった。
11. DRS クラスタで「アフィニティ ルールが削除されます。

ホストに Cisco アクセス違反から移行を終了して今すぐ Cisco ACI Virtual Edge。

クラスタ内の任意のホストが稼働している場合は、DRS がチェックをクラスタ化、クラスタ内の別のホストを移行するときに Cisco ACI Virtual Edge。実行しているホストには、2 番目のホストからの Vm が移動するには、1 つが検出されると、Cisco ACI Virtual Edge クロス DVS VMotion を介して。新しいホストが十分なリソースを持っていない場合、元のホストで Vm が残されています。複数のホストが実行するとき Cisco ACI Virtual Edge、DRS クラスタ残高移行中の間でロードします。

#### ホストを予約 移行ワークフロー

予約のホストが Cisco AV を実行するかどうか、アクティブな Vm は、標準的な VMotion を使用して、予約のホストに移動されます。予約のホストが実行しているかどうか Cisco ACI Virtual Edge、アクティブな Vm は、クロス dvs に VMotion を使用して、予約のホストに移動します。



(注) 予約のホストの移行方式を使用して、予約のホストが実行しているかどうか Cisco ACI Virtual Edge、すべてのホストは、ESXi バージョン 6.0 を実行する必要があります。そうしないと、DVS 間の VMotion は機能しません。

1. ホストはメンテナンスモードに入ります。
2. Cisco ACI Virtual Edge DVS がホストに追加されます。
3. Pnic と vmknic はシスコの AV DVS から移動、Cisco ACI Virtual Edge dvs にします。
4. ホストでの Vm の電源をオフのポート グループに Cisco アクセス違反から更新 Cisco ACI Virtual Edge。
5. Cisco AV dvs には、ホストから削除されます。
6. Cisco AV モジュールは、ホストからアンインストールされます。
7. 「アフィニティ ルールは、DRS クラスタに配置されます。これにより、Vm で実行されている、Cisco ACI Virtual Edge DVS にアップグレードされているホストに移動します。
8. ホストはメンテナンス モードから取得されます。
9. Cisco ACI Virtual Edgeホストで VM を展開します。
10. OpFlex エージェントがオンラインになった。
11. ステップ 1 で予約のホストに VMotion によって自動的に移動された Vm が [VMotion で [だけに移行するホストに戻さ Cisco ACI Virtual Edge。

Vm は、標準的な VMotion を使用して、予約のホストに移動された場合に移動させるクロス DVS VMotion が使用されます。Vm は、クロス dvs に VMotion を使用して、予約のホストに移動された場合に移動して標準 VMotion が使用されます。

#### インプレース 移行ワークフロー

1. Cisco ACI Virtual Edge DVS がホストに追加されます。
2. Cisco ACI Virtual Edgeホストで VM を展開します。  
アップリンクが接続されていないと、OpFlex がダウンしています。
3. Pnic と vmknics はシスコの AV DVS から移動、Cisco ACI Virtual Edge dvs にします。  
Cisco AV で実行されている Vm には、この時点でネットワークの接続性が失われます。
4. OpFlex エージェントがオンラインになった。
5. VM ポート グループに Cisco アクセス違反から更新 Cisco ACI Virtual Edge。
6. Cisco AV dvs には、ホストから削除されます。



(注) Cisco ACI Virtual Edgeモジュールは、この方法を使用して、ホストにインストールされたまま; アンインストールするには、メンテナンス モードにホストを入れる必要があります。

## Cisco AVS から Cisco ACI Virtual Edge に移行するための前提条件

ホストと VM を Cisco アプリケーション仮想スイッチ (AVS) から Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge に移行する前に、次のタスクを実行してください。

- Cisco APIC 内に Cisco ACI Virtual Edge 用の VMM ドメインを作成します。  
すべてのポート グループを有する、関連付けられた DVS が vCenter 内ですでに作成されている必要があります。
- 移行を開始する前に、Cisco AVS VMM ドメインで ARP 学習を無効にします。  
Cisco AVS VMM ドメインで ARP 学習が有効になっている場合、Cisco ACI Virtual Edge VMMドメインの作成は失敗します。
- ホストが移行できるように OpFlex がオンラインであることを確認します。
- Cisco ACI Virtual Edge OVF ファイル を vCenter コンテンツ ライブラリにアップロードします。

手順については、このガイドのプロシージャ、[Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードする \(29 ページ\)](#) を参照してください

- アップグレードする予定のホスト上のすべての VM が、共有ストレージを使用していることを確認します。
- vmknic が使用するすべての EPG が、ネイティブ モードのスイッチを使用していることを確認します。



---

(注) EPG によるバックアップがない限り、vmknic を移行することはできません。

---

- Cisco ACI Virtual Edge 管理ツール (ACI vCenter プラグインを含む) を使用する場合には、vCenter 6.0 Update 3 移行を使用することを推奨します。
- すべてのホストが ESXi 6.0 以降を実行していることを確認します。移行中のすべてのホストと、予約ホスト移行を使用している場合には移行ホストが、ESXi の以前のバージョンを実行しているのではない限り、クロス DVS VMotion は失敗します。
- DRS クラスタの拡張 VMotion 互換性 (EVC) モードが Nehalem 以上に設定されていることを確認します。
- VMotion 移行が、Cisco ACI Virtual Edge のインストール済みホストの制限を超えることがないように計画します。制限は、ESXi ホストごとに 300 VM です。
- Cisco ACI Virtual Edge を混合モードまたは VLAN のモードで展開する場合には、2 つの VLAN プールを作成します。1 つはプライマリ カプセル化のため、もう 1 つはプライベート VLAN の実装のためです。

プライベート VLAN プールの役割は内部である必要があります。Cisco ACI Virtual Edge VXLAN モードで展開する場合には、プライベート VLAN プールだけが必要です。



---

(注) または、Cisco APIC GUI を使用して Cisco AVS から Cisco ACI Virtual Edge に移行する場合には、移行中にプライベート VLAN プールを作成することができます。

---

## GUI を使用して Cisco AVS VMM ドメインを Cisco ACI Virtual Edge に移行する

既存の Cisco AVS VMM ドメインを新しい Cisco ACI Virtual Edge ドメインに移行するには、Cisco APIC GUI を使用することができます。この方法は、手動でほとんどの Cisco AVS ドメインの設定を再現する必要がある新しい VMM ドメインの作成よりも、簡単です。

元のドメインのすべてのプロパティは保たれます。ただし、vCenter のクレデンシャルは再入力する必要があります。元の VMM ドメインは残ります。



(注) 移行できる Cisco AVS VMM ドメインは、一度に 1 つだけです。



(注) VMM ドメインに関連付けられているすべての EPG は、新しい Cisco ACI Virtual Edge VMM のドメインに、Cisco ACI Virtual Edge スイッチング モードも含めてコピーされます。

### 始める前に

Cisco AVS ドメインを作成します。このガイドの [GUI を使用した vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの作成 \(18 ページ\)](#) の手順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** に移動します。

**ステップ 3** **Inventory** ナビゲーション ウィンドウで、**VMM Domains** および **VMware** フォルダを展開し、移行する Cisco AVS ドメインを右クリックして、**Migrate to Cisco AVE** を選択します。

**ステップ 4** **Migrate To Cisco AVE** ダイアログボックスで、次の操作を実行します:

- a) **Virtual Switch Name** フィールドで、新しい Cisco ACI Virtual Edge VMM ドメインの名前を入力します。
- b) **VLAN Pool** ドロップダウンリストで、VLAN プールを選択するか、作成します。

Cisco ACI Virtual Edge を混合モードまたは VLAN のモードで展開する場合には、2 つの VLAN プールを作成します。1 つはプライマリ カプセル化のため、もう 1 つはプライベート VLAN の実装のためです。プライベート VLAN プールの役割は内部である必要があります。Cisco ACI Virtual Edge VXLAN モードで展開する場合には、プライベート VLAN プールだけが必要です。

- c) **vCenter Credentials** エリアで、**Re-enter required** をダブルクリックして、vCenter のパスワードを入力し、確認入力します。
- d) **Update** をクリックし、**OK** をクリックします。

### 次のタスク

本ガイドの [Cisco ACI vCenter プラグイン](#) を使用して Cisco AVS から Cisco ACI Virtual Edge に移行する (55 ページ) のセクションの手順に従います。

# Cisco ACI vCenter プラグイン を使用して Cisco AVS から Cisco ACI Virtual Edge に移行する

Cisco ACI vCenter プラグインを使用してホストとその VM を Cisco AVS から Cisco ACI Virtual Edge に移行するには、3つの移行方法のいずれかを選択します。方法ごとの手順はどれもほぼ同じです。

## 始める前に

このガイドのセクション [Cisco AVS から Cisco ACI Virtual Edge に移行するための前提条件 \(52 ページ\)](#) のタスクを完了している必要があります。また、VMM ドメインに移行している必要があります。このガイドのセクション [REST API を使用して Cisco AVS VMM ドメインを Cisco ACI Virtual Edge に移行する \(111 ページ\)](#) またはセクション [GUI を使用して Cisco AVS VMM ドメインを Cisco ACI Virtual Edge に移行する \(53 ページ\)](#) を参照してください。

## 手順

- ステップ 1 vSphere Web クライアントにログインします。
- ステップ 2 [Home]作業ウィンドウで、[Cisco ACI Fabric] アイコンをクリックします。
- ステップ 3 [Cisco ACI ファブリック (Cisco ACI Fabric)] ナビゲーション ウィンドウで、[インフラストラクチャ (Infrastructure)] をクリックします。
- ステップ 4 ページ上部の [AVS] タブをクリックします。
- ステップ 5 [ACI ドメインを更新 (Refresh ACI Domains)] ボタンをクリックします。
- ステップ 6 Cisco AVS 作業ウィンドウで、**Select an AVS Domain** ドロップダウンリストから、カーネル Cisco AVS ドメインを選択します。
- ステップ 7 Cisco AVS 作業ウィンドウの右側で、適切なチェックボックスをオンにして、移行するそれぞれのホストを選択します。
- ステップ 8 [ACI 仮想エッジに移行 (Migrate to ACI Virtual Edge)] をクリックします。AVS Migration ダイアログボックスが表示されます。
- ステップ 9 **Mode** ドロップダウンリストから、移行方法を選択します。  
**DRS**、**Reserve Host**、または **In-Place** を選択してください。詳細については、このガイドのセクション [Cisco AV から移行するための方法を Cisco ACI Virtual Edge \(49 ページ\)](#) を参照してください。  
保持のためのチェックボックスをチェックして、Cisco AVS カーネル モジュールを保持するように選択することができます。
- ステップ 10 前の手順で **Reserve Host** を選択した場合、表示される **Reserve Host** ドロップダウンリストからホストを選択します。
- ステップ 11 **Target VDS** エリアで、ホストの移行先にする Cisco ACI Virtual Edge ドメインを選択します。

複数の Cisco ACI Virtual Edge ドメインがある場合には、ドロップダウンリストからドメインを選択します。

**ステップ 12 ACI Virtual Edge** ドロップダウンリストから、Cisco ACI Virtual Edge のインストールの設定を選択します。

**ステップ 13 Management** ドロップダウンリストから、Cisco ACI Virtual Edge VM の管理インターフェイスのための管理ポート グループを選択します。

**ステップ 14 Datastore** ドロップダウンリストから、**Custom** を選択し、**Edit** をクリックします。

**ステップ 15 [カスタム AVE データストア選択 (Custom AVE Datastore selection)]** ダイアログ ボックスで、各 Cisco ACI Virtual Edge のローカルまたはリモート データ ストアを選択します。

(注) 高レベルの可用性を確保するには、存在する場合ローカル データ ストアを選択することをお勧めします。

(注) vCenter では、すべてのタイプのローカルストレージが表示されない場合があります。ただし、**[Use local datastore only]** チェックボックスをオフにすると、vCenter はすべてのローカル データ ストアを表示します。詳細については、VMware ウェブサイトのドキュメント『[When installing ESX/ESXi 4.x or 5.x to a physical server, the local SAS drive appears as a remote storage \(1027819\)](#)』を参照してください。

**ステップ 16 VM Password** フィールドに、Cisco ACI Virtual Edge VM の管理者パスワードを入力します。

**ステップ 17 Migration Validity** エリアで、「The configuration is valid」というメッセージが出ていることを確認してから、**OK** をクリックします。

設定が有効ではない場合、どの事前チェックが失敗したかということと、移行を進められない理由を示した、エラーメッセージが表示されます。確認された問題を修正してから、もう一度移行を実行してください。



## 第 5 章

# VMware VDS からの移行 Cisco ACI Virtual Edge

この章で説明する VMware VDS から移行 Cisco ACI Virtual Edge、さまざまな方法を含みます。

- [Cisco ACI Virtual Edge への VDS ドメインの移行について \(57 ページ\)](#)
- [VDS ドメインへの移行 Cisco ACI Virtual Edge GUI を使用して \(58 ページ\)](#)

## Cisco ACI Virtual Edge への VDS ドメインの移行について

VMware VDS ドメインが設定されている場合は、そのドメインを Cisco ACI Virtual Edge に移行できます。移行により、Cisco ACI Virtual Edge 機能を利用することができます。これには、VXLAN カプセル化と分散ファイアウォールを使用する機能が含まれます。

VDS ドメインを移行すると、Cisco APIC は vCenter の DVS に内部および外部およびポートグループを作成します。ドメインは Cisco ACI Virtual Edge ドメインとして表示されます。ただし、一部のエンドポイントを **native** VDS モードで動作させ、他のエンドポイントを **AVE** (Cisco ACI Virtual Edge) モードで動作させることもできます。つまり、エンドポイントは VDS または Cisco ACI Virtual Edge を介して切り替えられます。

Cisco APIC GUI、NX-OS スタイルの CLI、または REST API を使用して、VMware VDS ドメインを Cisco ACI Virtual Edge に移行することができます。



- (注) EPG の **native** から **AVE** (Cisco ACI Virtual Edge) への切り替えモードを変更するには、基盤となるスイッチングプラットフォームを通常の VMware DVS から Cisco ACI Virtual Edge に変更する必要があります。また、関連するすべてのポートを DVS から Cisco ACI Virtual Edge に移動する必要もあります。

この操作は、その EPG に関連するポートグループの再プログラミングを必要とします。そのためには、vCenter の操作が必要です。この操作が完了し、Cisco ACI Virtual Edge スイッチングプラットフォーム上でポートがフォワーディング状態が表示されるまで数秒かかります。時間の長さは、vCenter の負荷と、**native** モードから **AVE** モードに移行する EPG 上に存在するエンドポイントの数によって異なります。

# VDS ドメインへの移行 Cisco ACI Virtual Edge GUI を使用して

この手順は、新しいに既存の VMM ドメインを移行 Cisco ACI Virtual Edge VMM ドメイン。元の VMM ドメインのプロパティが保持されます。ただし、元の VMM ドメインのコピーはありません。

## 始める前に

- VMM ドメインを作成しておきます。プロシージャ「VMM ドメインプロファイルの作成」を参照してください、 [Cisco ACI 仮想化ガイド](#)。
- Cisco ACI Virtual Edge 混合モードまたは VLAN のモードで展開は、2 つの VLAN プールの作成: プライマリ カプセル化とプライベート VLAN の実装のいずれかのいずれか。  
プライベート VLAN プールの役割は内部である必要があります。Cisco ACI Virtual Edge プライベート VLAN プールが必要なだけ VXLAN モードで展開されます。



(注) VD から移行すると、プライベート VLAN のプールを作成する代わりに、Cisco ACI Virtual Edge。

- ファーストホップセキュリティを無効にしました。

以下の手順を実行します:

1. で、**テナント** タブ、テナントを選択し、最初のホップのセキュリティが有効になっているブリッジドメインに移動します。をクリックします **Advanced/トラブルシューティング** タブをクリックし、作業ウィンドウで、ポリシーを削除します。
2. [**テナント** タブ、信頼コントロール ポリシーを適用する EPG に移動し、をクリックします **一般的な** タブをクリックし、作業ウィンドウで FHS 信頼コントロール ポリシーを削除します。

## 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** 移動 仮想ネットワーク > インベントリ。

**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、展開、**VMM ドメイン** フォルダ、および **VMware** フォルダ、移行、およびを選択する VDS を右クリックしてドメイン **Cisco 平均への移行**。

**ステップ 4** **Migrate To Cisco AVE** ダイアログボックスで、次の操作を実行します:

- a) 平均ファブリック全体のマルチキャストアドレス フィールドで、マルチキャストアドレスを入力します。
- b) **Pool of Multicast Addresses (one per-EPG)** ドロップダウンリストで、プールを選択するか、作成します。
- c) **VLAN Pool** ドロップダウンリストで、**VLAN** プールを選択するか、作成します。

Cisco ACI Virtual Edge を混合モードまたは **VLAN** のモードで展開する場合には、2つの **VLAN** プールを作成します。1つはプライマリ カプセル化のため、もう1つはプライベート **VLAN** の実装のためです。プライベート **VLAN** プールの役割は内部である必要があります。Cisco ACI Virtual Edgeプライベート **VLAN** プールが必要なだけ **VXLAN** モードで展開されます。

- d) **[OK]** をクリックします。

ドメインに移行するには、元の名前を保持します。ただし、ナビゲーション ウィンドウで、ドメインをクリックすると表示できます値を **仮想スイッチ** から変更 **分散スイッチ** に **Cisco** 平均。

---

VDS ドメインへの移行 Cisco ACI Virtual Edge GUI を使用して



## 第 6 章

# Cisco ACI Virtual Edge のアップグレード

この章では、前提条件と手順を含む、Cisco ACI Virtual Edge のアップグレードについて説明します。

- [Cisco ACI 仮想エッジのアップグレードについて \(61 ページ\)](#)
- [Cisco APIC、ファブリック スイッチ、および Cisco ACI Virtual Edge での推奨アップグレード手順 \(63 ページ\)](#)
- [Cisco ACI Virtual Edge アップグレードのワークフロー \(64 ページ\)](#)
- [Cisco ACI Virtual Edge のアップグレードのための前提条件 \(64 ページ\)](#)
- [Cisco ACI Virtual Edge のアップグレード \(65 ページ\)](#)

## Cisco ACI 仮想エッジのアップグレードについて

Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge のアップグレードは、インストールに似ています。Cisco.com から Cisco ACI Virtual Edge OVF ファイルをダウンロードし、それを VMware vCenter のコンテンツ ライブラリにアップロードします。その後、ESXi ホストで Cisco ACI Virtual Edge を再展開してアップグレードします。

これらのアップグレードのタスクは、Cisco ACI vCenter プラグインをのみを使用して行います。VMware PowerCLI または Python スクリプトを使用することはできません。

Cisco ACI vCenter プラグインは、もともとは Adobe Flash で動作するように設計されていました。ただし、Adobe は VMware vSphere バージョン 6.7 で Flash を非推奨にしたため、2020 年の終わりに Flash の更新を停止します。VMware vSphere 6.7 リリース以降、HTML5 で動作するように設計された新しいバージョン (Cisco ACI HTML5 vCenter プラグイン) が使用可能になりました。この項では、両方のプラグインのアップグレード手順について説明します。



- (注)
- VMware vSphere クライアントの名前は、Flash バージョンと HTML5 バージョンのどちらを使用するかによって異なります。Flash バージョンは、VMware vSphere Web クライアントと呼ばれます。HTML5 バージョンは、VMware vSphere Client と呼ばれます。
  - vSphere (シック) クライアントを Cisco ACI Virtual Edge のアップグレードまたはその vApp プロパティの変更には使用しないでください。Cisco ACI vCenter プラグインのみを使用します。Cisco ACI Virtual Edge の vApp プロパティを変更するには、vSphere Web クライアントのみを使用してください。
  - Cisco ACI Virtual Edge アップグレードは、VMware vCenter 7.0U1 の Cisco ACI ファブリック プラグインを介してホストで停止します。また、新しい Cisco ACI Virtual Edge 仮想マシン (VM) をインストールするためにホストをメンテナンスモードにできません。これは、vSphere Cluster Services (vCLS) 対応の VM がデフォルトでクラスタに展開されている VMware vCenter 7.0U1 で Cisco ACI Virtual Edge をアップグレードしようとするると発生します。これは、分散リソース スケジューラ (DRS) およびハイ アベイラビリティに必要です。  
  
この問題を解決するには、Cisco ACI Virtual Edge VM のアップグレードがスケジュールされているクラスタ内のホストから、クラスタ内の他のホストに vCLS VM を手動で移行します。
  - Cisco Application Policy Infrastructure Controller 5.0(x) 以降のリリースにアップグレードする前に、Cisco Application Virtual Switch (AVS) から Cisco ACI Virtual Edge (APIC) に移行します。シスコの AVS VMM ドメインは、Cisco APIC リリース 5.0(x) 以降ではサポートされていません。

以下のセクションでは、前提条件とインストールについて説明します。

Cisco Cisco ACI Virtual Edge のタスクの詳細については、このガイドの以下のセクションを参照してください。

- Cisco ACI Virtual Edge のインストール : [Cisco ACI Virtual Edgeのインストール \(9 ページ\)](#) 章を参照してください。
- Cisco AVS から Cisco ACI Virtual Edge に移行する : [Cisco AV から移行するCisco ACI Virtual Edge \(49 ページ\)](#) の章を参照してください。
- VMware VDS から Cisco ACI Virtual Edge に移行する : [VMware VDS からの移行Cisco ACI Virtual Edge \(57 ページ\)](#) の章を参照してください。

# Cisco APIC、ファブリック スイッチ、および Cisco ACI Virtual Edge での推奨アップグレード手順

ファブリック スイッチ上の Cisco APIC、NX-OS ソフトウェア、または Cisco ACI Virtual Edge をアップグレードする際には、互換性を保つために、それらのすべてアップグレードしてください。

ネットワークトラフィックの中断を避けるには、次の順序でそれぞれのアップグレードを実行することをお勧めします:



**重要** Cisco APIC、ファブリック スイッチ、および Cisco ACI Virtual Edge をアップグレードする前に、ソフトウェアの互換性情報を『*Cisco Application Policy Infrastructure Controller Release Notes*』および *Cisco ACI Virtual Edge* 『*Release Notes*』でチェックしてください。すべてのマニュアルは [Cisco.com](https://www.cisco.com) で入手できます。

1. Cisco APIC ソフトウェア イメージ — 『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』の手順に従います。

Cisco APIC クラスタを使用している場合は、クラスタが 1 つずつ自動的にアップグレードされます。

2. ファブリック スイッチ上のスイッチ ソフトウェア — 『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』の手順に従います。

アップグレード中のトラフィックの中断を避けるには、TOR とスパインを別々のファームウェア/メンテナンス グループに配置してから、それぞれのファームウェア/メンテナンス グループを個別にアップグレードすることによって、Cisco ACI Virtual Edge トラフィック用のパスを確保してください。

3. Cisco ACI Virtual Edge — 次のタスクを実行します:

1. この章の手順に従います。
2. 次のいずれかの手順を実行します:
  - 現行リリースで VIB を保持することに決定した場合には、VIB で `vem restart` コマンドを実行します。
  - VIB をアップグレードする場合ことに決定した場合は、VIB を新しいリリースにアップグレードします。

# Cisco ACI Virtual Edge アップグレードのワークフロー

このセクションでは、Cisco ACI Virtual Edge をアップグレードするために必要なタスクの概要について説明します。

1. すべての前提条件を満たします。手順については、このガイドの[Cisco ACI Virtual Edge のアップグレードのための前提条件](#) (64 ページ) のセクションを参照してください。
2. Cisco ACI Virtual Edge オープン仮想化フォーマット (OVF) ファイルを Cisco.com からダウンロードしてから、vCenter コンテンツ ライブラリにアップロードします。手順については、このガイドの[Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードする](#) (65 ページ) のセクションを参照してください。
3. Cisco ACI Virtual Edge を ESXi ホストに導入します。手順については、このガイドの「[Cisco ACI vCenter プラグインを使用した ESXi ホストでの Cisco ACI Virtual Edge のデプロイ](#) (66 ページ)」のセクションを参照してください。

## Cisco ACI Virtual Edge のアップグレードのための前提条件

Cisco ACI Virtual Edge をアップグレードする前に、次のタスクを実行してください:

- アップグレードを計画している Cisco ACI Virtual Edge が正しく設定されおり、問題なく動作することを確認します。
- 必要なバージョンにアップグレードするための情報について、Cisco.com の [Cisco ACI Virtual Edge リリース ノート](#) をチェックします。
- OpFlex がオンラインであることを確認します。
- Cisco ACI vCenter プラグインを使用する場合には、vCenter 6.0 更新 3 以降を使用することを推奨します。
- Cisco ACI vCenter プラグインを使用して Cisco ACI Virtual Edge をアップグレードする場合は、最初にプラグインを Cisco APICバージョン (4.x) に付属のバージョンにアップグレードする必要があります。
- 静的または DHCP IP プールを使用する場合には、十分な IP アドレスがあることを確認します。

静的または DHCP IP プールには、VMware vCenter のデータセンターの Cisco ACI 仮想エッジサービスで使用するよりも多くの IP アドレスが必要です。そうでないと、新しい Cisco ACI 仮想エッジへのアップグレードは失敗します。

- ホストが DRS クラスタの一部ではない場合には、アップグレードの前に非 Cisco ACI Virtual Edge の VM を手動でホストから出すか、シャットダウンします。ホストが DRS クラスタ以外の一部である場合には、非 Cisco ACI Virtual Edge の VM はホストから自動的に移動されます。

# Cisco ACI Virtual Edge のアップグレード

プレインストールの前提条件を満たした後に、VMware vCenter を使用して Cisco ACI Virtual Edge をインストールすることができます。プロセスを自動化する Cisco ACI vCenter プラグインを使用します。

最初に、Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter コンテンツ ライブラリにアップロードします。ESXi ホスト上に Cisco ACI Virtual Edge を展開することができます。



- (注) コンテンツ ライブラリとしてローカル データ ストアを使用する場合には、ホストを削除してからコンテンツ ライブラリを再度作成し、vCenter に再アタッチします。ホストを再アタッチするとデータ ストアの ID が変更されるため、コンテンツ ライブラリとデータ ストアの間の関連づけが解除されるからです。



- (注) Cisco ACI Virtual Edge を展開した後に、vCenter インベントリから削除し、追加し直してはなりません。これを行うと、導入時に加えたすべての設定が削除されます。既存のものをインベントリに戻すのではなく、Cisco ACI Virtual Edge を新しく追加してください。

## Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードする

Cisco ACI Virtual Edge VM OVF ファイルを、Cisco ACI Virtual Edge ESXi ホストに展開する前に、VMware vCenter にアップロードします。

### 始める前に

次のことは既に実行済みであるとします：

- 自分のコンピュータに OVF ファイルの入ったフォルダをダウンロードします。
- Cisco.com にある Cisco ACI Virtual Edge のリリースをチェックして、OVF ファイルが Cisco APIC のバージョンと互換性があることを確認します。
- Cisco ACI vCenter プラグイン内で Cisco ACI ファブリックを登録します。

### 手順

**ステップ 1** vSphere Web クライアントにログインします。

**ステップ 2** [Content Libraries] を選択します。

Cisco ACI Virtual Edge VM OVF をアップロードしたものを受け取るため、既存のコンテンツ ライブラリを使用するか、作成します。手順については、VMware のドキュメンテーションを参照してください。

**ステップ 3** ライブラリを選択し、[Import item] をクリックします。

**ステップ 4** [Import library item] ダイアログボックスで、[Browse] ボタンをクリックします。

**ステップ 5** ポップアップ ダイアログボックスで、OVF ファイルを選択し、[Open] をクリックします。

OVF ファイルがコンテンツ ライブラリにアップロードされると、作業ウィンドウの **Templates** タブに表示されます。

## Cisco ACI vCenter プラグインを使用した ESXi ホストでの Cisco ACI Virtual Edge のデプロイ

Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードしたら、ESXi ホストに Cisco ACI Virtual Edge を展開します。

### 始める前に

Cisco ACI Virtual Edge VM OVF ファイルを VMware vCenter にアップロードしている必要があります。



- (注) VMware vCenter 6.0 Web Client を使用している場合は、OVF ファイルを参照するポップアップ ウィンドウが表示されないことがあります。この場合、OVF と仮想マシンディスクファイル (VMDK) を HTTP サーバーにアップロードします。その後、サーバーから OVF ファイル URL を使用して、OVF ファイルをコンテンツ ライブラリにダウンロードします。

### 手順

**ステップ 1** vSphere Web クライアントにログインします。

**ステップ 2** [Home] 作業ウィンドウで、[Cisco ACI Fabric] アイコンをクリックします。

**ステップ 3** Cisco ACI Fabric ナビゲーション ウィンドウで、**ACI Virtual Edge** をクリックします。

**ステップ 4** 複数の仮想ドメインがある場合、**ACI Virtual Edge** 作業ウィンドウで、**Select an ACI Virtual Edge Domain** ドロップダウンリストからドメインを選択します。

仮想ドメインが 1 つだけの場合、スキップして次の手順に進みます。

**ステップ 5** Cisco ACI Virtual Edge を展開するホストを選択します。

**ステップ 6** [**ACI Virtual Edge version**] ドロップダウン リストから、デプロイするバージョンを選択します。

- ステップ 7** [Management PortGroup] ドロップダウンリストから、管理ポートグループを選択します。
- ステップ 8** [Datastore] ドロップダウンリストから [Custom] を選択し、[Edit] をクリックします。
- ステップ 9** [カスタム AVE データストアの選択 (Custom AVE Datastore selection) ] ダイアログボックスで、それぞれの Cisco ACI Virtual Edge にローカルまたはリモートのデータストアを選択します。
- (注) より高いレベルの可用性を確保するために、ローカルデータストアがある場合はそれを選択することを推奨します。
  - (注) vCenter では、すべてのタイプのローカルストレージが表示されない場合があります。ただし、**Use local datastore only** チェックボックスをオフにすると、vCenter はすべてのローカルデータストアを表示します。詳細については、VMware web サイトのドキュメンテーションを参照してください。
- ステップ 10** **VM Admin Password** フィールドに、Cisco ACI Virtual Edge VM の新しいパスワードを入力します。
- ステップ 11** **Install/Upgrade ACI Virtual Edge** をクリックします。
- ステップ 12** ダイアログボックスで、**Yes** をクリックします。
- インストールされたホストは作業ウィンドウに OpFlex のステータス、Cisco ACI Virtual Edge VM、および管理 IP のステータスを表示します。OpFlex がアップ状態になるまで少しかかる場合があります。
-





## 第 7 章

# Cisco ACI Virtual Edge のアンインストール

この章で説明のアンインストール Cisco ACI Virtual Edge の前提条件とアンインストール方法を含めて、します。

- [Cisco ACI Virtual Edge のアンインストールについて \(69 ページ\)](#)
- [Cisco ACI Virtual Edge のアンインストールのワークフロー \(69 ページ\)](#)
- [Cisco ACI vCenter プラグインを使用して、Cisco ACI Virtual Edge をアンインストールする \(70 ページ\)](#)
- [VMware PowerCLI を使用した Cisco ACI Virtual Edge のアンインストール \(72 ページ\)](#)
- [Python を使用した Cisco ACI Virtual Edge のアンインストール \(73 ページ\)](#)

## Cisco ACI Virtual Edge のアンインストールについて

テストのために Cisco ACI Virtual Edge を削除しなければならない場合があります。または、Cisco ACI ファブリックからすべての設定を削除する必要がある場合は、ファブリックを初期状態にリセットします。

Cisco ACI Virtual Edge は、Cisco ACI vCenter プラグイン、VMware PowerCLI、または Python スクリプトを使用してアンインストールできます。



- (注) Cisco ACI Virtual Edge を使用するには、管理ツール (ACI vCenter プラグイン、VMware PowerCLI と Python スクリプト)、vCenter 6.0 Update 3 以降を使用することを推奨します。

## Cisco ACI Virtual Edge のアンインストールのワークフロー

Cisco ACI Virtual Edge のアンインストールを実行するタスクの順序は、アンインストール後も VMM ドメインを使用できるように保持するかどうかによって異なります。

- Cisco ACI Virtual Edge を削除し、VMM ドメインを使用できるように保持する (ネイティブモード)。

1. Cisco ACI Virtual Edge ポート グループからすべての VM を削除する。  
または、Cisco ACI Virtual Edge EPG のスイッチングモードを AVE からネイティブに変更する。
  2. Cisco ACI vCenter プラグイン、VMware PowerCLI または Python スクリプトを使用して、Cisco ACI Virtual Edge VM をアンインストールする。このガイドの指示に従ってください。
- Cisco ACI Virtual Edge を削除して VMM ドメインを削除するには、次の手順に従います:
    1. EPG ポート グループからすべての VM を削除します。
    2. Cisco ACI vCenter プラグイン、VMware PowerCLI または Python スクリプトを使用して、Cisco ACI Virtual Edge VM をアンインストールする。このガイドの指示に従ってください。
    3. Cisco ACI Virtual Edge VDS からすべてのホストを削除します。
    4. ポート グループを削除するには、EPG へのすべての VMM ドメイン関連付けを削除します。
    5. Cisco ACI Virtual Edge VMM ドメインを削除します。

## Cisco ACI vCenter プラグインを使用して、Cisco ACI Virtual Edge をアンインストールする



(注) 他のホストが Cisco ACI Virtual Edge を使用する VM を持つ DRS クラスタを使用している場合は、Cisco ACI Virtual Edge をアンインストールする前にホストをメンテナンス モードにすることをお勧めします。メンテナンス モードに入ると、Cisco ACI Virtual Edge がアンインストールされた後に他の VM がホストに移行するのを防ぐことができます。クラスタ内に、VM が Cisco ACI Virtual Edge を使用している他のホストが存在しない場合は、ホストをメンテナンス モードにせずに、Cisco ACI Virtual Edge をアンインストールすることができます。

### 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 [Cisco ACI Fabric] > [ACI Virtual Edge] を選択します。
- ステップ 3 作業ウィンドウの中央にある、[Select an ACI Virtual Edge Domain] ドロップダウンリストから、ドメインを選択します。

ドメインを選択すると、VMM ドメインに関連する vCenter 内の1つまたは複数のホストが作業ウィンドウに表示されます。

**ステップ 4** 適切なチェックボックスまたは複数のチェックボックスをクリックして、1つまたは複数のホストを選択します。

**ステップ 5** 手順 4 で複数のホストを選択する場合は、**[Uninstall ACI Virtual Edge]** ボタンの下に、**[+]** と **[-]** ボタンを使用して同時に Cisco ACI Virtual Edge をアンインストールするホストの数を選択します。

**ステップ 6** **[Uninstall ACI Virtual Edge]** をクリックします。

**ステップ 7** **[Uninstall AVE]** ダイアログボックスで、**[Yes]** をクリックして Cisco ACI Virtual Edge のアンインストールを続行することを確認します。

警告ポップアップが表示され、選択したホストのいずれかが DRS クラスタの一部である場合に、アンインストールの一部としてホストをメンテナンスモードにすることに同意するかどうかを尋ねます。

**ステップ 8** 次のいずれかの操作セットを完了します。

次の場合は...	次の操作...
メンテナンス モードに入っているホストでアンインストールを進める	<b>[Yes]</b> をクリックします。
アンインストールを続行しますが、ホストをメンテナンス モードにしない	<p><b>[No]</b> をクリックします。</p> <p>次の確認メッセージが表示されます。</p> <ul style="list-style-type: none"> <li>ホストをメンテナンス モードにしないでアンインストールを続行するには、<b>[Yes]</b> をクリックします。</li> <li>アンインストールをキャンセルするには <b>[No]</b> をクリックします。</li> </ul>
アンインストールを続行しますか?	アンインストールをキャンセルするには <b>[No]</b> をクリックします。

中央の作業ウィンドウでは、ホストの **[Status]** カラムにアンインストールの進行状況が表示されます。**[Recent Tasks]** エリアでは、個々のアンインストールタスクの進行状況を表示することもできます。アンインストールが完了すると、**[Not installed]** がホストの **[Status]** カラムに表示されます。

### 次のタスク

ホストが DRS クラスタの一部である場合、ホストが Cisco ACI Virtual Edge DVS から削除されていない限り、メンテナンス モードから移動しないでください。

# VMware PowerCLI を使用した Cisco ACI Virtual Edge のアンインストール

Windows プラットフォームを使用している場合は、VMware PowerCLI を使用して Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge をアンインストールできます。

## 始める前に

スクリプトは、Cisco ACI Virtual Edge VM に依存している既存のデータ仮想マシン (VM) をチェックします。Cisco ACI Virtual Edge VM を削除する前に、Cisco ACI Virtual Edge DVS からすべてのデータ VM を削除します。

## 手順

**Remove-AveVM** コマンドを使用して Cisco ACI Virtual Edge をアンインストールします。

次のテキストはコマンドの構文です。

```
Remove-AveVM [[-HostName] Object] [[-DomainName] Object] [CommonParameters]
```

### 例 :

```
PowerCLI C:\> Remove-AveVM -HostName 172.23.143.129 -DomainName mininet
```

メンテナンス モードでの出力 :

```
Connecting to vCenter.....[ok]
Fetching existing AVE VM.....[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: yes
Validating DRS cluster cluster.....[ok]
Adding affinity rule on DRS cluster cluster.....[ok]
Waiting for all VMs to move out of host 172.23.143.129.....[ok]
Powering off the AVE VM.....[ok]
Deleting VM.....[ok]
Entering maintenance mode.....[ok]
Removing affinity rule on DRS cluster.....[ok]
Cleaning up.....[ok]
```

メンテナンス モードなしの出力 :

```
Connecting to vCenter.....[ok]
Fetching existing AVE VM.....[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: no
Do you wish to cancel the uninstall, or continue the uninstall without placing the ho
st in maintenance mode (not recommended) [cancel/continue]: continue
```

```
Deleting VM.....[ok]
Cleaning up.....[ok]
```

## Python を使用した Cisco ACI Virtual Edge のアンインストール

アンインストールは Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge Python スクリプトを使用して行えます。

### 始める前に

スクリプトは、Cisco ACI Virtual Edge VM に依存している既存のデータ仮想マシン (VM) をチェックします。Cisco ACI Virtual Edge VM を削除する前に、Cisco ACI Virtual Edge VM からすべてのデータ VM を削除します。

### 手順

remove-avevm.py スクリプトを使用して、特定のドメインの特定のホストから Cisco ACI Virtual Edge をアンインストールします。

次のテキストはスクリプトの使用方法を示しています。

```
usage: remove-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --host-name
HOST_NAME --domain-name DOMAIN_NAME
[--ignore-active-vm]
```

### 例 :

```
(venv) $ python remove-avevm.py --vcenter 172.23.143.235 --vc-username admin
--vc-password lab --host-name 172.23.143.129 --domain-name mininet
```

### メンテナンス モードでの出力 :

```
Connecting to vCenter.....[ok]
Fetching existing AVE VM.....[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: yes
Validating DRS cluster cluster.....[ok]
Adding affinity rule on DRS cluster cluster.....[ok]
Waiting for all VMs to move out of host 172.23.143.129.....[ok]
Powering off the AVE VM.....[ok]
Deleting VM.....[ok]
Entering maintenance mode.....[ok]
Removing affinity rule on DRS cluster.....[ok]
Cleaning up.....[ok]
```

### メンテナンス モードなしの出力 :

```
Connecting to vCenter.....[ok]
Fetching existing AVE VM.....[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: no
Do you wish to cancel the uninstall, or continue the uninstall without placing the ho
st in maintenance mode (not recommended) [cancel/continue]: continue
Deleting VM.....[ok]
Cleaning up.....[ok]
```

---



## 付録 **A**

# サポートされるトポロジ

この付録では、Cisco ACI Virtual Edge でサポートされるトポロジについて説明します。



### 重要

この付録に含まれていないトポロジはまだテストされておらず、サポートされていません。



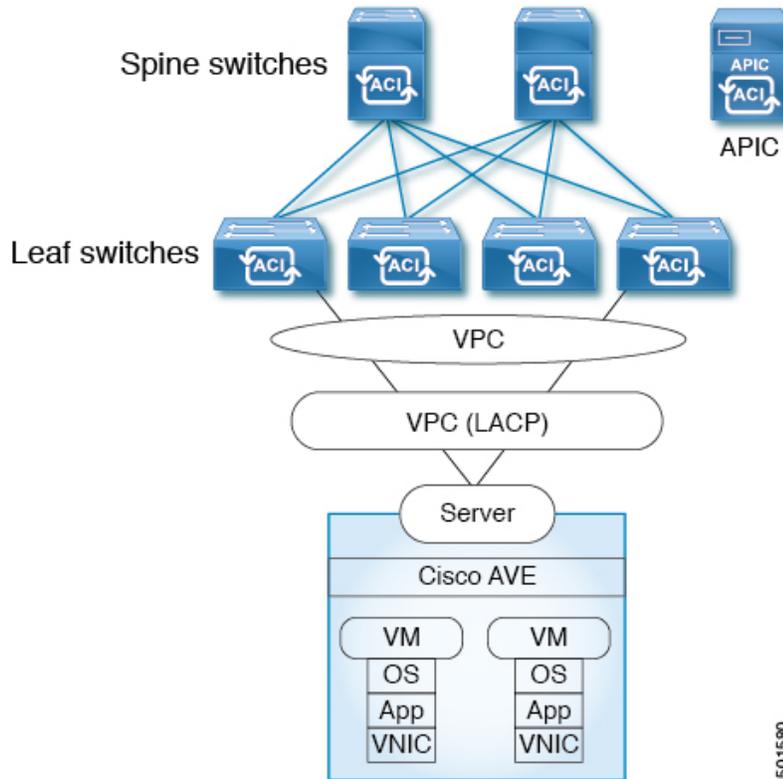
(注) どのトポロジでも、可能であり、ハードウェアでサポートされている場合には、LACPを使用することを推奨します。LACPが可能でない場合に限り、MACピニングを使用してください。

- [直接接続 \(75 ページ\)](#)
- [シスコ ファブリック エクステンダ \(77 ページ\)](#)
- [Cisco UCS ファブリック インターコネクトでの VPC \(77 ページ\)](#)
- [Cisco Nexus 5000 および MAC ピン接続によるデュアルサイド VPC \(78 ページ\)](#)
- [Cisco Nexus 5000 および VPC によるデュアルサイド VPC \(79 ページ\)](#)
- [Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトを使用したシングルサイド VPC \(80 ページ\)](#)
- [Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトによるデュアルサイド VPC \(81 ページ\)](#)

## 直接接続

このトポロジでは、ESXi ハイパーバイザを Cisco Application Policy Infrastructure Controller (APIC) に直接接続します。

図 4: 直接接続



このトポロジを使用するには、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] の下と Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge 仮想マシンマネージャ (VMM) ドメインの作成時にポートチャネルポリシーを設定する必要があります。次の手順を参照してください。

- 本ガイドの「Cisco ACI 仮想エッジ設定ガイド」の「GUIを使用したポートチャネルまたは仮想ポートチャネルの設定」
- (本ガイドの Cisco ACI Virtual Edge の VMM ドメイン プロファイルの作成 (92 ページ) )

または、ファブリック ウィザードの設定ウィザードを使用して VMM ドメイン プロファイルを設定できます。その場合、「Cisco ACI 仮想エッジ設定ガイド」の手順を使用してポートチャネルを設定する必要はありません。



- (注) VPC リーフ ペアへの直接接続で MAC ピニングを使用しないでください。代わりに、Link Aggregation Control Protocol (LACP) または拡張 LACP を使用して、冗長性と信頼性を提供します。直接接続で MAC ピニングを使用すると、ピア リーフ スイッチの再起動時にトラフィックが失われます。MAC ピニングは、サウスバウンドインターフェイスを使用する Cisco UCS ファブリック インターコネクトなど、仮想ポートチャネル (VPC) をサポートできない場合のみ使用してください。

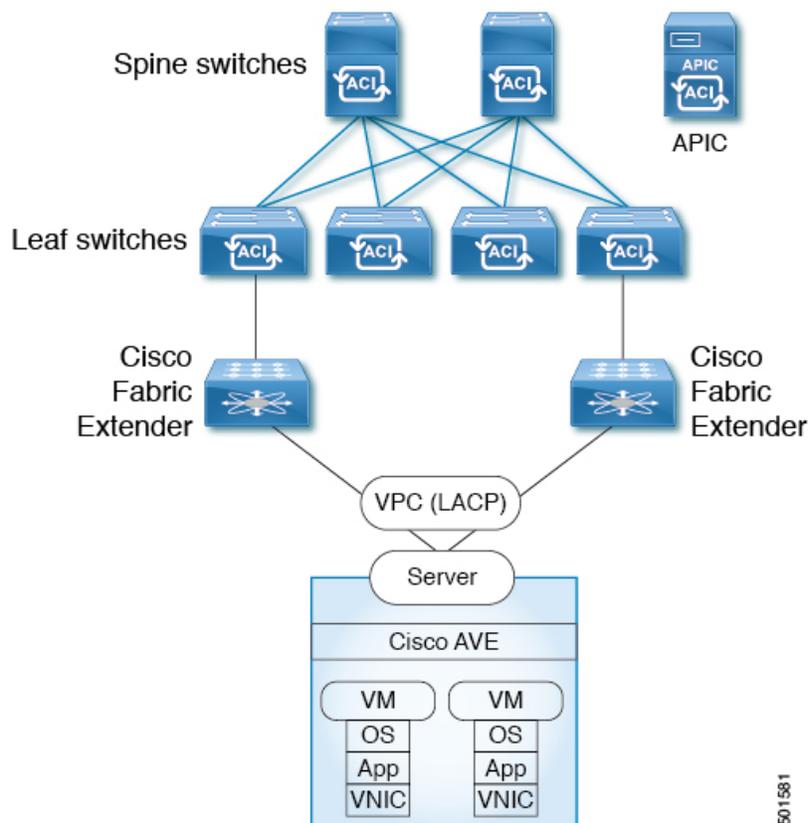
## シスコ ファブリック エクステンダ

このトポロジでは、ファブリック エクステンダ (FEX) 経由で ESXi ハイパーバイザを Cisco APIC に接続します。ESXi は次のものに接続できます。

- 仮想ポート チャンネル (VPC) を使用した複数のリーフ スイッチ
- ポート チャンネル (MAC ピン接続または LACP バンドル) を使用した単一のリーフ スイッチ

次の図では、VPC が例として使用されています。その代わりに、ポート チャンネルを使用することもできます。

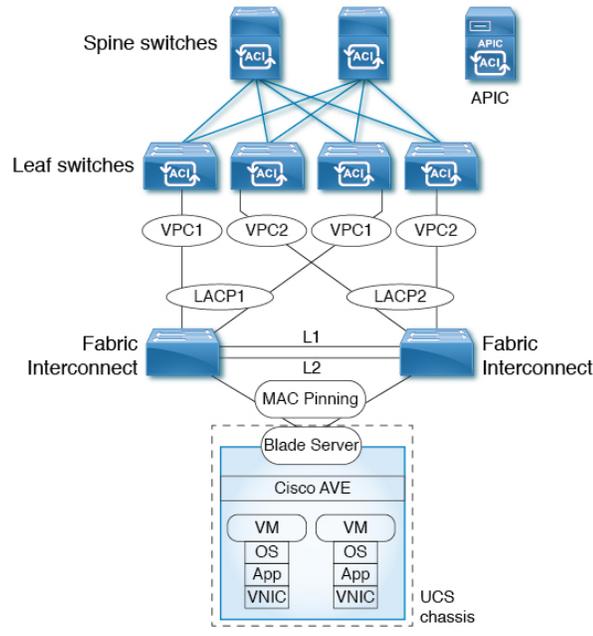
図 5: シスコ ファブリック エクステンダのトポロジ



## Cisco UCS ファブリック インターコネクトでの VPC

このトポロジでは、Cisco UCS ファブリック インターコネクト、VPC、LACP、および MAC ピニングを使用して、ESXi ハイパーバイザを Cisco APIC に接続します。

図 6: Cisco UCS ファブリック インターコネクト トポロジでの VPC



このトポロジでは、Cisco ACI Virtual Edge は MAC ピニングでのみ設定できます。これは、Cisco UCS ファブリック インターコネクトが、ブレードサーバへのサウスバウンドポートでの LACP または vLACP をサポートしていないためです。したがって、図は Cisco ACI Virtual Edge 側の MAC ピニングのみを示しています。

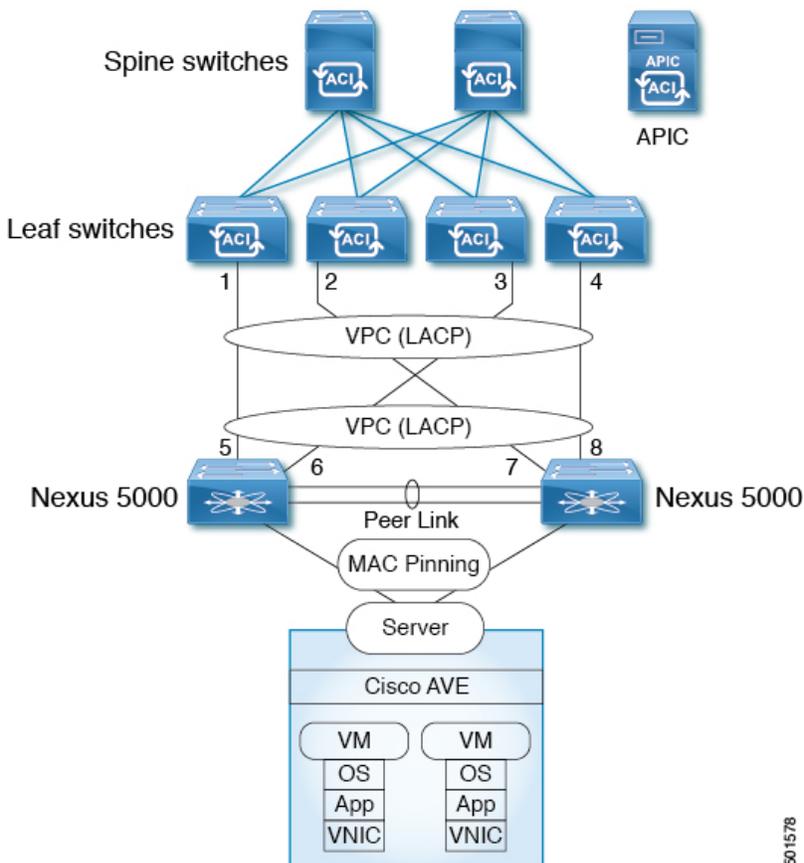


(注) このトポロジは、同じ Top-of-Rack (TOR) スイッチ ペアに接続された 2 つのファブリック インターコネクトもサポートします。

## Cisco Nexus 5000 および MAC ピン接続によるデュアルサイド VPC

このトポロジでは、Cisco Nexus 5000 スイッチ、仮想ポート チャネル、および MAC ピン接続を介して ESXi ハイパーバイザを Cisco Application Policy Infrastructure Controller (APIC) に接続します。

図 7: Cisco Nexus 5000 および MAC ピン接続によるデュアルサイド VPC のトポロジ



501578

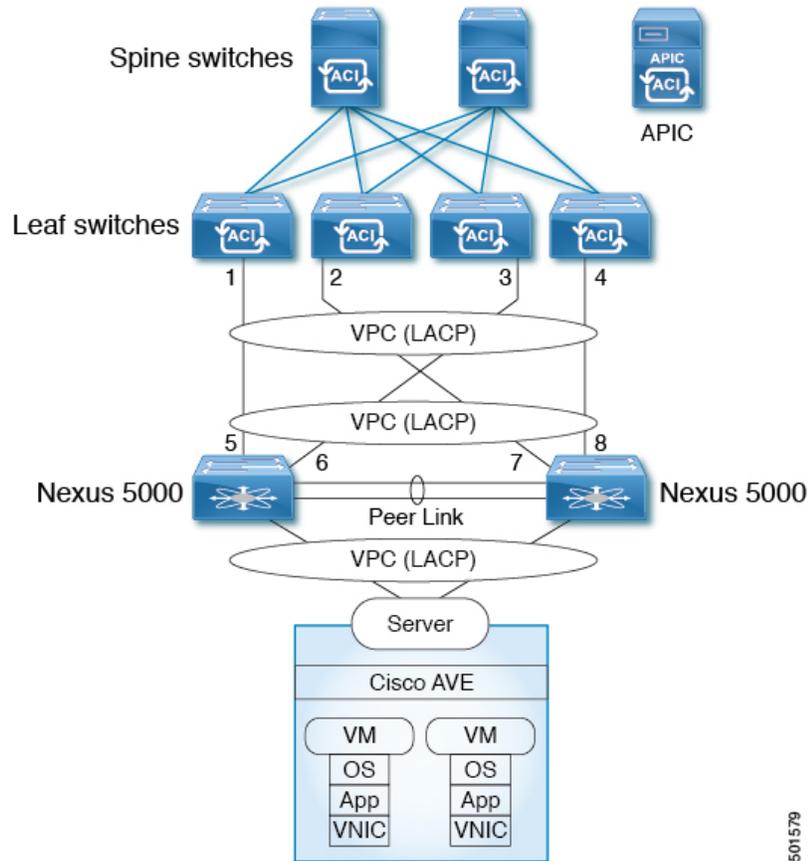


(注) リーフスイッチと Cisco Nexus 5000 スイッチをシングルサイド VPC トポロジで接続することもできます。

## Cisco Nexus 5000 および VPC によるデュアルサイド VPC

このトポロジでは、Cisco Nexus 5000 スイッチおよび仮想ポートチャネルを介して ESXi ハイパーバイザを Cisco Application Policy Infrastructure Controller に接続します。

図 8: Cisco Nexus 5000 および VPC によるデュアルサイド VPC のトポロジ



501579

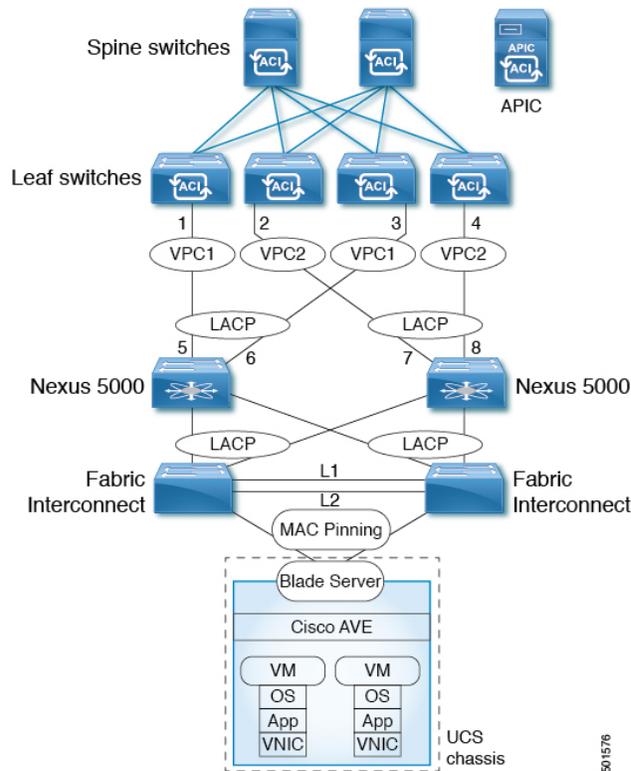


(注) リーフ スイッチおよびシングル側 VPC トポロジで接続されている Cisco Nexus 5000 スイッチを設定することができます。

## Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトを使用したシングルサイド VPC

このトポロジでは、ESXi ハイパーバイザがリーフ スイッチに MAC ピン接続を使用して、直接的に、または Cisco Nexus 5000 スイッチおよび Cisco UCS シリーズ ファブリック インターコネクト経由で接続されます。

図 9: Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトトポロジを使用したシングルサイド VPCトポロジ

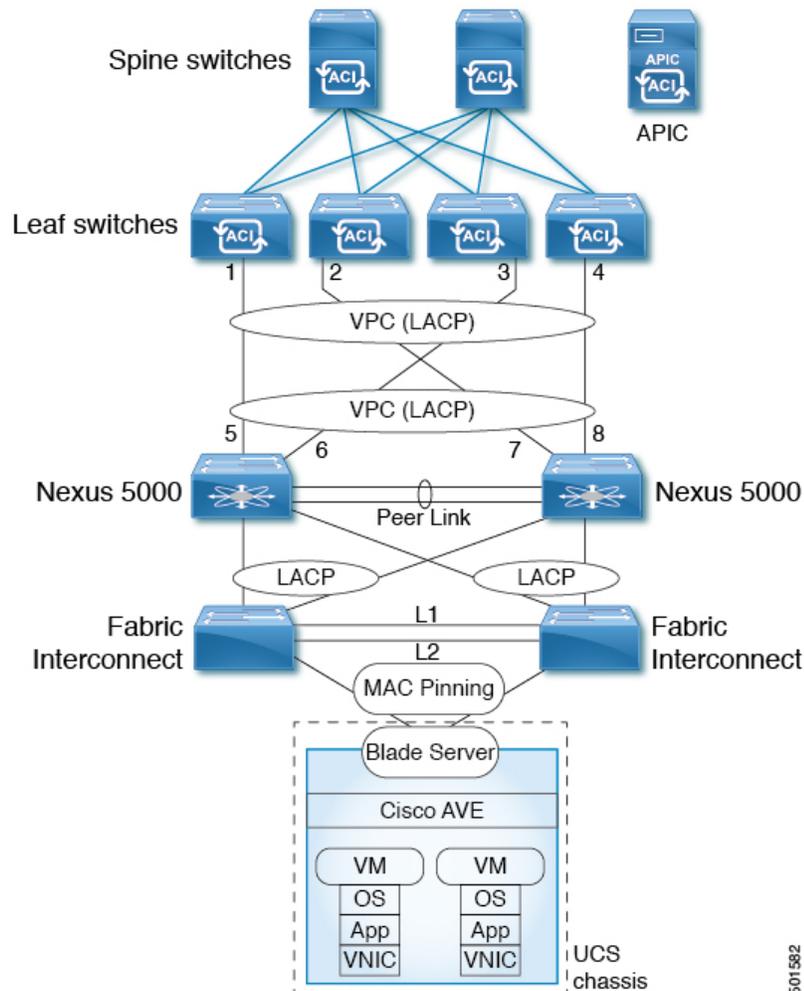


このトポロジでは、Cisco ACI Virtual Edge は MAC ピンでのみ設定できます。これは、Cisco UCS ファブリック インターコネクトが、ブレードサーバ側のサウスバンドポートで LACP をサポートしていないためです。したがって、この図では、Cisco ACI Virtual Edge 側でのみ MAC ピンニングが示されています。

## Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトによるデュアルサイド VPC

このトポロジでは、MAC ピンニングを使用し、ESX ハイパーバイザをリーフ スイッチに直接、または Cisco Nexus 5000 スイッチおよび Cisco UCS ファブリック インターコネクトを経由して接続します。

図 10 : Cisco Nexus 5000 および Cisco UCS ファブリック インターコネクトによるデュアルサイド VPC トポロジ



このトポロジでは、Cisco ACI Virtual Edge は MAC ピニングでのみ設定できます。これは、Cisco UCS ファブリック インターコネクトが、ブレードサーバ側のサウスバンドポートで LACP をサポートしていないためです。したがって、この図では、Cisco ACI Virtual Edge 側でのみ MAC ピンニングが示されています。

501582



## 付録 **B**

# 作成 vCenter ドメイン、インターフェイス、およびスイッチのプロファイルの代替手順

インストールする前に設定タスクを実行するための unified 設定ウィザードの使用をお勧め Cisco ACI Virtual Edge。ただし、別の詳細なポリシーを設定する必要がある場合があります。

この付録には、vCenter ドメイン プロファイルとインターフェイスおよびスイッチのプロファイルのさまざまな種類の作成の個々の手順が含まれています。

- [ポート チャネル スイッチおよびインターフェイスのプロファイルの作成 \(83 ページ\)](#)
- [GUI を使用した VPC インターフェイスとスイッチ プロファイルの作成 \(85 ページ\)](#)
- [GUI を使用して FEX ノードのインターフェイスとスイッチ プロファイルを作成する \(88 ページ\)](#)
- [インターフェイス ポリシー グループを変更して vSwitch 側のポリシーをオーバーライドする \(90 ページ\)](#)
- [Cisco ACI Virtual Edge の VMM ドメイン プロファイルの作成 \(92 ページ\)](#)

## ポートチャネルスイッチおよびインターフェイスのプロファイルの作成

インストールする前に Cisco ACI Virtual Edge スイッチを作成し、インターフェイスのプロファイル。

### 始める前に

この手順の d は、手順 4 では、ドロップダウンリストから、リーフ スイッチ ノード ID を選択します。これは、ESXi またはレイヤ 2 クラウド ホストに接続されているリーフ スイッチの ノード ID と一致する必要があります。リーフ スイッチ ノード ID を確認します **Fabric Membership** ウィンドウに移動し、 **ファブリック > インベントリ > Fabric Membership** 。

## 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 ポリシー ナビゲーション ウィンドウでは、展開、**スイッチ** フォルダ、および **リーフ** スイッチ フォルダ。
- ステップ 4 **Profiles** フォルダを右クリックし、**Create Leaf Profile** を選択します。
- ステップ 5 **Create Leaf Profile (STEP 1 > Profile)** ダイアログボックスで、次の手順を実行します:
- [Name] フィールドに、名前を入力します
  - Leaf Selectors** フィールドで、+ アイコンをクリックして、新しいスイッチセクタを作成します。
  - [Name] フィールドに、名前を入力します
  - [Blocks] フィールドで、ドロップダウンリストからリーフ スイッチ ノード ID を選択します。
  - Update** をクリックします。
  - [Next] をクリックします。
- ステップ 6 **Create Leaf Profile (STEP 2 > Associations)** ダイアログボックスの **Interface Selectors Profiles** エリアで、+ アイコンをクリックして、新しいインターフェイスセクタ プロファイルを作成します。
- ステップ 7 **[Create Interface Profile]** ダイアログボックスで、次の手順を実行します。
- [Name] フィールドに、vLeaf 名を入力します。
  - [Interface Selectors] 領域で、[+] アイコンをクリックして新しいインターフェイスセクタを作成します。
- ステップ 8 **[Create Access Port Selector]** ダイアログボックスで、次の手順を実行します。
- [Name] フィールドでセクタの名前を入力します。
  - [Interface IDs] フィールドで、ESXi ホストに接続された物理インターフェイスのアクセスポートインターフェイス ID を入力します。
  - [Interface Policy Group] ドロップダウンリストで、[Create PC Interface Policy Group] を選択します。
- ステップ 9 [Create PC Interface Policy Group] ダイアログボックスで、[Name] フィールドにポリシーグループ名を入力します。
- ステップ 10 [Port Channel Policy] フィールドで、ドロップダウンリストから [Create Port Channel Policy] を選択します。
- ステップ 11 [Create Port Channel Policy] ダイアログボックスで、次の手順を実行します:
- [Name] フィールドにポリシー名を入力します。
  - [Mode] フィールドで、次の値の 1 つを選択します。
    - **Static Channel - Mode On**
    - **LACP Active**

- LACP Passive
- MAC Pinning
- MAC Pinning-Physical-NIC-load

(注) VPC リーフ ペアへの直接接続で MAC ピニングを使用しないでください。代わりに、Link Aggregation Control Protocol (LACP) または拡張 LACP を使用して、冗長性と信頼性を提供します。直接接続で MAC ピニングを使用すると、ピア リーフ スイッチの再起動時にトラフィックが失われます。MAC ピニングは、サウスバウンドインターフェイスを使用する Cisco UCS ファブリック インターコネクトなど、仮想ポートチャネル(VPC)をサポートできない場合にのみ使用してください。

c) [Submit] をクリックします。`

**ステップ 12** [Create PC Interface Policy Group] ダイアログボックスで、次の手順を実行します。

- エンティティ プロファイルの接続されている フィールドで、以前に作成したプロファイルを選択またはドロップダウンリストから 1 つを作成します。
- [Submit] をクリックします。`

**ステップ 13** [Create Access Port Selector] ダイアログボックスで、[OK] をクリックします。

**ステップ 14** [Create Leaf Interface Profile] ダイアログボックスで、[Submit] をクリックします。

**ステップ 15** **Create Leaf Profile** ダイアログボックスで、新しいインターフェイス プロファイルを選択し、**Finish** をクリックします。

## GUI を使用した VPC インターフェイスとスイッチ プロファイルの作成

### 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** および **Switch** フォルダを展開します。

**ステップ 4** **VPC Domain** フォルダを右クリックして、**Create VPC Domain Policy** を選択します。

**ステップ 5** [Create VPC Domain Policy] ダイアログボックスで、次の手順を実行します。

- [Name] フィールドにポリシーの名前を入力します。
- [Peer Dead Interval] フィールドに、値を入力します。  
範囲は 3 ~ 300 秒です。

c) **Submit** をクリックしてポリシーを保存します。

- ステップ 6** **Policies** ナビゲーション ウィンドウで、**Switches** と **Leaf Switches** フォルダを展開し、**Profiles** フォルダを右クリックし、**Create Leaf Profile** を選択します。
- ステップ 7** **Create Leaf Profile** ダイアログボックスで、次の手順を実行します:
- Name** フィールドに、プロファイルの名前を入力します。
  - Leaf Selectors** エリアで、+ アイコンをクリックします。
  - Name** フィールドに、セレクトタの名前を入力します。
  - Blocks** ドロップダウンリストから、ポリシー グループに関連付けるリーフを選択します。
  - Update** をクリックします。
  - [Next] をクリックします。
- ステップ 8** **Create Leaf Profile** ダイアログボックスの **Interface Selector Profiles** エリアで、+ アイコンをクリックします。
- ステップ 9** **Create Leaf Interface Profile** ダイアログボックスで、次の手順を実行します:
- [Name] フィールドに、プロファイルの名前を入力します。
  - [Interface Selectors] 領域で、[+] アイコンをクリックします。
- ステップ 10** [Create Access Port Selector] ダイアログボックスで、次のアクションを実行します。
- Name** フィールドに、セレクトタの名前を入力します。
  - Interface IDs** フィールドに、範囲の値を入力します。
  - Interface Policy Group** ドロップダウンメニューで、ドロップダウンリストから **Create VPC Interface Policy Group** を選択します。
- ステップ 11** **Create VPC Interface Policy Group** ダイアログボックスで、次の手順を実行します:
- Name** フィールドにポリシー グループの名前を入力します。
  - Port Channel Policy** ドロップダウンメニューで、ドロップダウン リストから **Create Port Channel Policy** を選択します。
- ステップ 12** [Create Port Channel Policy] ダイアログボックスで、次のアクションを完了します。
- [Name] フィールドにポリシーの名前を入力します。
  - [Mode] フィールドで、次のオプションのうちセットアップに適したものを 1 つ選択します。
    - **Static Channel - Mode On**
    - **LACP Active**
    - **LACP Passive**
    - **MAC Pinning**
    - **MAC Pinning-Physical-load**

(注) VPC リーフ ペアへの直接接続で MAC ピニングを使用しないでください。代わりに、Link Aggregation Control Protocol (LACP) または拡張 LACP を使用して、冗長性と信頼性を提供します。直接接続で MAC ピニングを使用すると、ピア リーフスイッチの再起動時にトラフィックが失われます。MAC ピニングは、サウスバウンドインターフェイスを使用する Cisco UCS ファブリック インターコネクトなど、仮想ポートチャネル (VPC) をサポートできない場合にのみ使用してください。

c) **Submit** をクリックします。

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

a) [Attached Entity Profile] フィールドで、ドロップダウンリストから [default] を選択します。

接続可能エンティティプロファイルを新規作成して、ノードポリシーの作成後にポリシーをオーバーライドできます。これを行う必要がある状況としては、Cisco ACI Virtual Edge を実行している ESXi ホストとリーフの間に中間レイヤー 2 デバイスがある場合や、ファブリック側で LACP およびトップオブブラック (ToR) スイッチ/リーフを使用する一方で、Cisco ACI Virtual Edge 側で MAC ピン接続などの別のポリシーを使用する場合などがあります。

b) [**Submit**] をクリックします。

**ステップ 14** [Create Access Port Selector] ダイアログボックスで、[**OK**] をクリックします。

**ステップ 15** **Create Leaf Interface Profile** ダイアログボックスで、**Submit** をクリックします。

**ステップ 16** **Create Leaf Profile** ダイアログボックスで、次の手順を実行します:

a) [Interface Selector Profiles] 領域で、ステップ 9 a で作成したインターフェイス セクタ プロファイルのチェックボックスをオンにします。

b) [**Finish**] をクリックします。

**ステップ 17** VPC に 2 番目のリーフを追加するには、次の手順を実行します。

a) ステップ 1 ~ 10 b を繰り返します。ただし、ステップ 7 b では、他のリーフのノード ID を入力します。

b) **Create Access Port Selector** ダイアログボックスで、手順 11 a で作成したポリシー グループの名前を選択します。

c) [**OK**] をクリックします。

d) ステップ 15 および 16 を繰り返します。

**ステップ 18** **Policies** ナビゲーション ウィンドウで、**Policies** および **Switch** フォルダを展開します。

**ステップ 19** **Virtual Port Channel default** を右クリックして、**Create VPC Explicit Protection Group** を選択します。

**ステップ 20** [Create VPC Explicit Protection Group] ダイアログボックスで、保護グループの名前、ID、スイッチの値を入力します。**Submit** をクリックして、保護グループを保存します。

(注) リーフスイッチの各ペアには、固有 ID を有する VPC 明示保護グループが 1 つあります。

- (注) 同一の仮想ポート チャンネル ポリシーには、複数の VPC 明示保護グループを含めることができます。

## GUI を使用して FEX ノードのインターフェイスとスイッチ プロファイルを作成する



- (注) リーフに直接接続している FEX がある場合には、本ガイドのトポロジの付録の「シスコ ファブリック エクステンダ」のセクションで、制限について参照してください。

### 始める前に

この手続きの手順4では、FEXに接続されるリーフスイッチのノードIDをドロップダウンリストから選択します。これは、ESXiまたはレイヤ2クラウドホストに接続されているリーフスイッチのノードIDと一致する必要があります。[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ファブリック メンバーシップ (Fabric Membership)] に移動して、[ファブリック メンバーシップ (Fabric Membership)] ウィンドウでリーフスイッチノードIDをチェックします。

### 手順

- ステップ 1** Cisco Application Policy Infrastructure Controller (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、**Switches** と **Leaf Switches** フォルダを展開します。
- ステップ 4** **Profiles** フォルダを右クリックして、**Create Leaf Profile** を選択します。
- ステップ 5** **Create Leaf Profile STEP 1 > Profile** ダイアログボックスで、次の手順を実行します。:
- [Name] フィールドに、プロファイルの名前を入力します。
  - Leaf Selectors** フィールドで、+ アイコンをクリックします。
  - [Name] フィールドに、名前を入力します
  - [Blocks] フィールドで、ドロップダウンリストから FEX に接続されるリーフスイッチノード ID を選択します。
  - [Blocks] ドロップダウン矢印または [Create Switch Profile] ダイアログボックスのどこかをクリックすると、[Update] ボタンを表示できます。
  - Update** をクリックします。
  - [Next] をクリックします。

- ステップ 6** **Create Leaf Profile STEP 2 > Associations** ダイアログボックスの **Interface Selectors Profiles** エリアで、+ アイコンをクリックして、新しいインターフェイス セレクタ プロファイルを作成します。
- ステップ 7** **Create Leaf Interface Profile** ダイアログボックスで、次の手順を実行します。
- [Name] フィールドに、vLeaf 名を入力します。
  - [Interface Selectors] 領域で、[+] アイコンをクリックして新しいインターフェイス セレクタを作成します。
- ステップ 8** **[Create Access Port Selector]** ダイアログボックスで、次の手順を実行します。
- Name** フィールドでセレクタの名前を入力します。
  - [Interface IDs] フィールドで、FEX に接続されているリーフ上のアクセス ポート インターフェイス ID を入力します。
  - [Connected To Fex] チェックボックスをオンにします。
  - [FEX Profile] ドロップダウン リストから、[Create FEX profile] を選択します。
- ステップ 9** **Create FEX Profile** ダイアログボックスで、次の手順を実行します。
- [Name] フィールドに、FEX プロファイルの名前を入力します。
  - [FEX Access Interface Selectors] 領域で、[+] アイコンをクリックして FEX アクセス ポートを指定します。
- ステップ 10** **[Create Access Port Selector]** ダイアログボックスで、次の手順を実行します。
- [Name] フィールドに、セレクタの名前を入力します。
  - [Interface IDs] 領域で、Cisco ACI Virtual Edge をホストしている ESXi サーバに接続されている FEX 上のアクセス ポートを指定します。
  - Interface Policy Group** エリアで、ドロップダウン リストからインターフェイス オプションを選択します。
- Create PC Interface Policy Group、Create VPC Interface Policy Group、または Create Leaf Access Port Policy Group** のいずれかを選択できます。
- ステップ 11** ステップ 10 c で選択したオプション ダイアログボックスで、次の手順を実行します:
- [Name] フィールドに、アクセス ポリシーのグループ名を入力します。
  - [Attached Entity Profile] 領域で、適切な接続されたエンティティ プロファイルを選択します。
  - Submit** をクリックします。
- ステップ 12** **Create Access Port Selector** ダイアログボックスで、新たに作成されたアクセス ポート ポリシーグループが **Interface Policy Group** エリアに表示されていることを確認し、**OK** をクリックします。
- ステップ 13** **Create FEX Profile** ダイアログボックスで、新たに作成された FEX アクセス インターフェイスセレクタ プロファイルが **FEX Access Interface Selectors** エリアに表示されていることを確認し、**Submit** をクリックします。
- ステップ 14** **[Create Access Port Selector]** ダイアログボックスで、次の手順を実行します。
- 新しく作成された FEX プロファイルが **FEX Profile** エリアにに表示されていることを確認します。

- b) **FEX ID** フィールドに ID を入力します。
- c) [OK] をクリックします。

**ステップ 15 Create Leaf Interface Profile** ダイアログボックスで、リーフ側インターフェイス ポートセクタ プロファイルがあることを確認して、**Submit** をクリックします。

**ステップ 16 Create Leaf Profile STEP 2 > Associations** ダイアログボックスの **Interface Selector Profiles** エリアで、FEX 用に作成したインターフェイスセクタ プロファイルのチェック ボックスをオンにして、**Finish** をクリックします。

### 次のタスク

FEX ノード ポリシーの設定が成功したことを確認する必要があります。ただし、Cisco APIC が設定を完了するまで 10 分程度待つ必要があります。

FEX ノード ポリシーの設定を確認するには、Cisco APIC GUI で以下の手順を実行します。

1. **Fabric > Inventory** を選択します。
2. **Inventory** ナビゲーション ウィンドウで、FEX ノード プロファイルが作成されたリーフ ノードを含むポッドのフォルダを展開します。
3. リーフ ノードのフォルダのアイコンをクリックします。
4. **Fabric Extenders** フォルダを選択します。
5. **Fabric Extenders** 作業ウィンドウで、FEX が存在することを確認します。

## インターフェイス ポリシー グループを変更して vSwitch 側のポリシーをオーバーライドする

ノード ポリシーを作成後、独自のアタッチ可能なエンティティ プロファイルを作成することが必要となる場合があります。このことは、リーフと Cisco ACI Virtual Edge を実行している ESXi ホストの間に、中間レイヤ 2 デバイスが存在している場合に必要となります。このようなデバイスとしては、Cisco Nexus 5000/7000 シリーズ スイッチやブレード サーバ (Unified Computing System [UCS]) があります。

オーバーライドにより、中間デバイスのため、および Cisco ACI Virtual Edge ホスト アップリンクのために独立したリンク ポリシーを設定することが可能になります。たとえば、UCS ファブリック インターコネクタが ACI に接続されていて、Cisco ACI Virtual Edge ホストが UCS ブレード上で動作している場合には、ポート チャネル ポリシーを使用している FI チャネルごとに UCS ファブリック インターコネクタ アップリンクを設定しながら、UCS ブレードのホスト vNIC は MAC ピニングを使用して別個に設定できるようにすることが必要なことがあるかもしれません。



- (注) 次の両方に該当するときには vSwitch ポリシーを選択する必要がある場合があります;
- vSwitch をホストする ESXi サーバが、レイヤ 2 スイッチまたはブレードサーバを介してリーフに接続されている。
  - レイヤ 2 デバイスと ESXi サーバによってホストされる vSwitch 間のインターフェイスグループポリシーが、レイヤ 2 スイッチとリーフ間のインターフェイスグループポリシーと異なっている必要があるネットワークである。ポリシーには、ポートチャネル、Cisco Discovery Protocol (CDP)、Link Layer Discovery Protocol (LLDP)、スパニングツリープロトコル (STP) およびファイアウォールが含まれます。

### 始める前に

- カスタムのアタッチ可能なエンティティプロファイルを作成する前に、VMware vCenter ドメインを作成する必要があります。詳細については、このガイドの [Cisco ACI Virtual Edge の VMM ドメインプロファイルの作成 \(92 ページ\)](#) のセクションを参照してください。



- (注) vCenter ドメインを作成するには、アタッチ可能なエンティティプロファイルを選択する必要があります。ただし、まだ存在しない場合には、**Attachable Entity Profile** フィールドを空白のままにするか、デフォルトを選択します。カスタムプロファイルを作成した後で、それを vCenter ドメインに関連付けることができます。

- [ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] > [インターフェイス (Interfaces)] > [リーフインターフェイス (Leaf Interfaces)] > [プロファイル (Profiles)] で、ポートセレクトラを持つ適切なインターフェイスプロファイルが作成されていることを確認します。後ほどポートをオーバーライドポリシーに関連付けます。
- vCenter ドメイン用に vSwitch 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 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** および **Global** フォルダを展開し、**Attachable Access Entity Profiles** フォルダを右クリックして、**Create Attachable Access Entity Profile** を選択します。
- ステップ 4 **Create Attachable Access Entity Profile, Step 1 > Profiles** 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、プロファイルの名前を入力します。

- b) [Enable Infrastructure VLAN] チェックボックスをオンにします。
- c) [+] アイコンをクリックして [Domains] を展開し、アタッチ可能なエンティティ プロファイルに関連付ける VMM ドメインを追加します。
- d) **Update** をクリックします。
- e) [Next] をクリックします。

**ステップ 5** **Create Attachable Access Entity Profile, Step 2> Association to Interfaces** ダイアログボックスで、アタッチ可能なエンティティプロファイルと関連付ける必要のあるインターフェイスポリシーグループを選択します。

(注) 各インターフェイス ポリシー グループに対して、[All] または [Specific] オプション ボタンを選択できます。All ラジオ ボタンは、インターフェイス ポリシー グループからのすべてのインターフェイスを、アタッチ可能なエンティティプロファイルに関連付けます。Specific ラジオ ボタンは、特定のノードからの特定のインターフェイスを関連付けます。インターフェイス ポリシー グループに対し Specific オプション ボタンを選択すると、スイッチ ID とインターフェイスを指定し、その後、Update ボタンをクリックするように求められます。

**ステップ 6** [Finish] をクリックします。

**ステップ 7** **Virtual Networking > Inventory** に移動します。

**ステップ 8** 左側のナビゲーション ウィンドウで、**VMM Domains** および **VMware** フォルダを展開し、関連する VMM ドメインを選択します。

**ステップ 9** 作業ウィンドウで、**VSwitch Policy** タブをクリックします。

**ステップ 10** [vSwitch policy] ドロップダウン リストから、オーバーライド ポリシーとして適用するネットワーク ポリシーを選択します。

**ステップ 11** [送信 (Submit) ] をクリックします。

## Cisco ACI Virtual Edge の VMM ドメイン プロファイルの作成

Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge をインストールする前に、そのための VMM ドメインを Cisco Application Policy Infrastructure Controller (APIC) で作成する必要があります。



- (注) Cisco ACI Virtual Edge エンドポイント グループのアップリンクを設定するには、次の手順を使用します。[ファブリック (Fabric) ] タブの設定ウィザードを使用して Cisco ACI Virtual Edge VMM ドメインを作成する場合は、アップリンクを設定できません。ただし、Cisco ACI Virtual Edge をすでに作成している場合は、アップリンクを追加できます。「[Cisco ACI 仮想化ガイド、リリース 4.2 \(x\)](#)」の手順「VMM ドメインの編集とアップリンクの変更」を参照してください。

## 始める前に

- マルチキャスト IP アドレス プールに、VMware vCenter ドメインにパブリッシュされる EPG 数に対応するのに十分なマルチキャスト IP アドレスがあることを確認します。VMware vCenter ドメインにすでに関連付けられているマルチキャスト アドレス プールに IP アドレスをいつでも追加できます。
- 十分な VLAN ID があることを確認します。これを行わないと、ポートの EPG がカプセル化を使用できないと報告することがあります。
- VMware vCenter がインストールおよび設定されており、インバンド/アウトオブバンド管理ネットワークを介して到達可能である必要があります。
- VMware vCenter に対する管理者/ルートのクレデンシャルがあることを確認します。
- インターフェイスおよびスイッチのプロファイルを作成します。手順については、このガイドの「ポート チャネル スイッチおよびインターフェイス プロファイルの作成」を参照してください。
- (オプション) アタッチ可能なエンティティ プロファイル (AEP) を作成します。

vCenter ドメイン プロファイルの作成中には、AEP を選択するかまたは作成するように求められます。事前に 1 つ作成する場合には、[『Cisco ACI Virtual Edge Configuration Guide』](#)の「Configuring an Attachable Entity Profile Using the GUI」に記されている手順に従ってください。



(注) Cisco ACI Virtual Edge VMM ドメインに割り当てられた AEP 内のインフラストラクチャ VLAN を有効にします。これは、VMware vCenter ドメイン プロファイルの作成前または作成中に AEP を作成するかどうかに関係なく実行します。 **Create Attachable Access Entity Profile** ダイアログボックスで、**Enable Infrastructure VLAN** チェック ボックスをオンにします。

## 手順

- ステップ 1 Cisco APIC にログインします。
- ステップ 2 [仮想ネットワークング (Virtual Networking)] > [インベントリ (Inventory)] に移動します。
- ステップ 3 [Inventory] ナビゲーション ウィンドウで、**VMM Domains** 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 4 **Create vCenter Domain** ダイアログボックスで、次の手順を実行します:
  - a) **Virtual Switch Name** フィールドに名前を入力します。
  - b) **Virtual Switch Area** で、**Cisco AVE** を選択します。

**Cisco AVE** を選択すると、Cisco ACI Virtual Edge のための VMM ドメインが作成されます。

(注) VMware vSphere Proactive HA を使用する場合は、次の 2 つのサブステップを実行します。Cisco APIC は VMware vCenter に、動作していない Cisco ACI Virtual Edge を持つホストを隔離し、動作している Cisco ACI Virtual Edge を持つホストに VM を移動するように指示します。この機能は、Cisco ACI vPod の一部として Cisco ACI Virtual Edge を使用することはできません。

また、VMware vCenter で Proactive HA を有効にする必要があります。このガイドの付録「[VMware vSphere Proactive HA を使用して Cisco ACI 仮想エッジ可用性を改善する \(97 ページ\)](#)」を参照してください。

- c) [AVEタイムアウト時間 (秒) (AVE Time Out Time (seconds))] セレクタを使用して、VMware vCenter をトリガーして、非稼働状態の Cisco ACI Virtual Edge を持つホストを隔離し、ホストから VM を移動する期間を選択します。

10 – 300 秒の範囲で任意の値を選択できます。デフォルトは 30 秒です。

- d) [ホスト可用性保証 (Host Availability Assurance)] チェックボックスをオンにします。このチェックボックスをオンにすると、VMware vCenter に VMware Proactive HA オブジェクトが作成されます。このオブジェクトを使用すると、VMware vCenter が非稼働の Cisco ACI Virtual Edge を持つホストを検疫し、ホストから VM を移動できます。

(注) 稼働していない Cisco ACI Virtual Edge を持つホストを検疫するには、vCenter で VMware Proactive HA をアクティブ化する必要があります。

- e) [Switching Preference] 領域で、[No Local Switching] または [Local Switching] を選択します。

スイッチングの設定については、[Cisco ACI Virtual Edge とは \(3 ページ\)](#) のセクションを参照してください。本ガイドの「概要」の章にあります。

(注) **No Local Switching** を選択した場合に使用できるのは、VXLAN カプセル化だけです。

- f) ステップ 4f で [ローカル切り替え (Local Switching)] を選択した場合には、[デフォルトの Encap モード (Default Encap Mode)] エリアでモードを選択します。

**VLAN mode** または **VXLAN mode** を選択できます。同じ VMM ドメイン内で両方のカプセル化方式を使用することもできます。『[Cisco ACI Virtual Edge Configuration Guide](#)』の「Mixed-Mode Encapsulation Configuration」のセクションを参照してください。

- g) **Associated Attachable Entity Profile** ドロップダウンリストで、プロファイルを作成するか、以前に作成したものを選択します。

手順については、『[Cisco ACI Virtual Edge Configuration Guide](#)』の「Configuring an Attachable Entity Profile Using the GUI」を参照してください。

- h) [VLAN Pool] ドロップダウン リストで、VLAN プールを選択するか作成します。

Cisco ACI Virtual Edge を混合モードまたは VLAN のモードで展開する場合には、2 つの VLAN プールを作成します。1 つはプライマリカプセル化のため、もう 1 つはプライベート VLAN の実装のためです。プライベート VLAN プールの役割は内部である必要があります。

ます。Cisco ACI Virtual Edgeプライベート VLAN プールが必要なだけ VXLAN モードで展開されます。

- i) **[AVE ファブリックワイド マルチキャスト アドレス (AVE Fabric-Wide Multicast Address)]** フィールドで、アドレスを入力します。
- j) **Pool of Multicast Addresses (one per-EPG)** ドロップダウンリストで、プールを選択するか作成します。
- k) **[vCenter クレデンシヤル (vCenter Credentials)]** エリアで **[+]** (プラス) アイコンをクリックし、**[vCenter クレデンシヤルの作成 (Create vCenter credential)]** ダイアログ ボックスで次の手順に従います。**[名前 (Name)]** フィールドに VMware vCenter アカウント プロファイル名を入力し、**[ユーザー名 (Username)]** フィールドに VMware vCenter ユーザ名を入力し、VMware vCenter のパスワードをの入力と確認入力を行ってから、**[OK]** をクリックします。
- l) **[vCenter]** エリアで **[+]** (プラス) アイコンをクリックし、**[vCenter コントローラの作成 (Create vCenter Controller)]** ダイアログ ボックスで次の手順に従います。VMware vCenter コントローラ名、VMware vCenter のホスト名か IP アドレス、DVS のバージョン、データセンター名 (VMware vCenter で設定されたデータセンター名と一致している必要があります) を入力し、前の手順で作成したクレデンシヤルを選択して、**[OK]** をクリックします。

DVS バージョン 5.5 以降を選択できます。

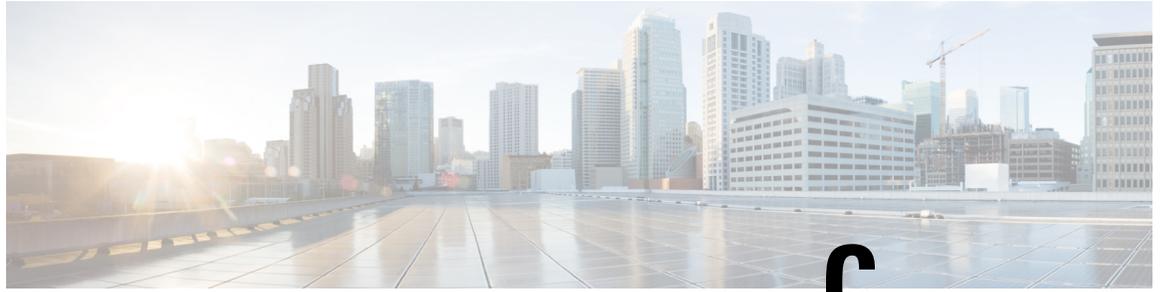
(注) 同じドメインに複数の vCenter コントローラを作成できます。さらに vCenter コントローラを作成する場合は、新しい vCenter コントローラごとにこのサブステップを繰り返します。

- m) **Create vCenter Domain** ダイアログボックスで **Submit** をクリックします。  
VMware 作業ウィンドウには、新しく作成された VMM ドメインが表示されます。これは VMware vCenter にプッシュされます。
- n) **[アップリンクの数 (Number of Uplinks)]** ドロップダウン リストから、仮想スイッチ アップリンク ポート グループへのアップリンクの数を選択します。  
最大 32 個のアップリンクを仮想スイッチアップリンク ポート グループに関連付けることができます。この手順は任意です。値を選択しない場合、デフォルトで 8 つのアップリンクがポートグループに関連付けられます。VMM ドメインの作成が完了したら、アップリンクに名前を付けることができます。EPG の VMM ドメインの関連付けを作成または編集するときに、アップリンクのフェールオーバーを設定することもできます。
- o) **ポート チャネル モード、vSwitch ポリシー、およびその他の機能を設定に応じて設定** します。

vSwitch ポリシー内のポート チャネル ポリシーは、サポートされるトポロジ要件に一致するように正しく設定する必要があります。

### 次のタスク

- VMware vCenter の vSphere Web クライアントを使用して、新たに作成された Cisco ACI Virtual Edge DVS に、1 つ以上の ESXi ホストとその PNIC を追加します。
- VMware vCenter で vSphere Proactive HA をまだ有効にしていない場合は、有効にします。
- アップリンクの名前を変更するか、それらのフェールオーバーを設定します。



## 付録 C

# VMware vSphere Proactive HA を使用して Cisco ACI 仮想エッジ可用性を改善する

- [Cisco ACI 仮想エッジ可用性の改善 \(97 ページ\)](#)
- [vSphere Proactive HA を使用する利点 \(99 ページ\)](#)
- [vSphere Proactive HA の仕組み \(100 ページ\)](#)
- [VMware vSphere Proactive HA を設定するための前提条件 \(102 ページ\)](#)
- [vSphere Proactive HA in Cisco APIC で vSphere Proactive HA を有効にする \(102 ページ\)](#)
- [VMware vCenter で vSphere Proactive HA を有効にする \(103 ページ\)](#)
- [ESXi ホストのヘルス レベルの手動設定 \(104 ページ\)](#)
- [VM グループ検疫保護 \(105 ページ\)](#)

## Cisco ACI 仮想エッジ可用性の改善

Cisco ACI Virtual Edge の可用性を向上させるために、vCenter 6.5 以降で VMware vSphere Proactive HA を使用できます。

Cisco Application Policy Infrastructure Controller (APIC) と VMware は連携して動作しない Cisco ACI Virtual Edge を検出し、そのホストを分離し、その仮想マシン (VM) を動作中のホストに移動します。そうしないと、Cisco ACI Virtual Edge がクラッシュすると、すべての VM がネットワーク接続を失う可能性があります。

VMware vCenter で vSphere Proactive HA を有効にして設定します。Cisco APIC でこの機能は **ホスト可用性保証** と呼ばれます。ホストが検疫され、VM が移動されるまでに Cisco ACI Virtual Edge が動作しない時間を指定できます。



- (注)
- VMware vCenter への登録に使用する Cisco APIC アカウントの権限には、管理者権限または Cisco Application Centric Infrastructure (ACI) vCenter プラグインにアクセスする権限が必要です。
  - vSphere Proactive HA は、Cisco ACI 仮想ポッドに含まれている場合 Cisco ACI Virtual Edge は使用できません。
  - ホスト可用性保証を機能させるには、Cisco APIC vCenter ドメインの作成に使用する VMware vCenter アカウントに、VMware vCenter に対する「ヘルス プロバイダー」書き込み権限が必要です。

### vSphere Proactive HA による可用性の向上の仕組み

ホスト可用性保証を有効にすると、Cisco APIC では VMware vCenter で vSphere Proactive HA プロバイダー オブジェクトが作成されます。オブジェクトを使用すると、VMware vCenter が非稼働の Cisco ACI Virtual Edge を搭載したホストを検疫し、そのホストから VM を移動できます。Cisco APIC で、検疫をトリガーする積極性も指定します。これらのタスクは、Cisco ACI Virtual Edge の vCenter ドメインを作成するときに実行します。

ホスト可用性保証が設定され、有効になっている場合、Cisco APIC は VMware vCenter で Cisco ACI Virtual Edge をモニタします。VMware vCenter インベントリと OpFlex ステータスを使用して、Cisco ACI Virtual Edge が良好な状態か不良な状態かを判断します。Cisco APIC により Cisco ACI Virtual Edge が不良状態であることが検出されると、影響を受けるホストを検疫するよう VMware vCenter に指示します。

VMware vCenter は、クラスタに設定する 3 つの修復モードのいずれかに従って、ホストを検疫モードにします。

- **[検疫 (Quarantine)]** : ホストの状態が黄色と赤のレベルの場合、検疫モードになります。



- (注) Cisco ACI Virtual Edge リリース 2.1(1) では、ホストが動作を停止したときに VM グループが Cisco ACI Virtual Edge ホストから移動するようになります。この設定は、特定のホストで VM を保持するアフィニティグループを上書きします。詳細については、このガイドの「VM グループ検疫保護」の項を参照してください。

- **[混合 (Mixed)]** : 黄色レベルのホストの状態は検疫モードになります。赤レベルのホストの状態はメンテナンス モードになります。



- (注) VMware vCenter では混合修復モードを選択できますが、結果の動作は隔検疫修復モードと同じです。

- **メンテナンス**：黄色と赤のレベルのヘルスを持つホストは、メンテナンスモードになります。



**重要** vSphere Proactive HA を使用する場合は、メンテナンスモード修復を選択しないでください。メンテナンスモードでは Cisco ACI Virtual Edge を電源をオフにする必要があるため、ホストが正常な状態に戻ることはありません。検疫モードまたは混合モードのみを使用します。

VMware vCenter は、そのホスト上の VM を動作している Cisco ACI Virtual Edge とともに移動します。ただし、正常なホストが使用できない場合、検疫中のホストはデータ VM を実行する可能性があり、分散リソーススケジューラ (DRS) ルールによって検疫されたホストにピン接続された VM はホスト上にとどまります。また、VMware vCenter は、検疫されたホストへの VM の移動を回避します。ただし、隔離内のホストに新しい VM を展開できます。

## vSphere Proactive HA を使用する利点

vSphere Proactive HA 機能を使用すると、Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge 障害を検出して対処できます。がダウンすると、AVE スイッチングモードで VMware vCenter ポートグループに接続されているすべての仮想マシン (VM) がネットワーク接続を失います。Cisco ACI Virtual Edge

vSphere Proactive HA は、次の状況でも接続の切断を防ぐことができます。

- **vSphere DRS**：ロードバランシング vSphere 分散リソーススケジューラ (DRS) 機能は、vSphere vMotion を使用して VM を自動的に移動し、アフィニティルールで定義した動作を適用します。

ただし、DRS は Cisco ACI Virtual Edge を考慮しません。したがって、CPU とメモリの使用率を最適化する際に、Cisco ACI Virtual Edge が動作しているホストから Cisco ACI Virtual Edge が動作していないホストに VM を移行できます。

- **メンテナンスモードへの移行**：ホストをメンテナンスモードにすると、DRS はホストのすべての VM を別のホストに自動的に移行します。すべての VM が移動されると、ホストはメンテナンスモードになります。

ただし、Cisco ACI Virtual Edge はホストに固定されているため、DRS は Cisco ACI Virtual Edge を移動しないため、ホストはメンテナンスモードになりません。したがって、vSphere Proactive HA がない場合は、Cisco ACI Virtual Edge ホストの電源をオフにしてメンテナンスモードを開始する必要があります。

- **メンテナンスモードの終了**：ホストのメンテナンスモードを終了すると、すべての CPU とメモリが再び使用可能になるため、DRS は VM をそのホストに移行できます。ただし、Cisco ACI Virtual Edge は手動で電源をオンにする必要があります。これは、DRS が VM の

ホストへの移動を開始する前に Cisco ACI Virtual Edge が準備できていない可能性があることを意味します。

ただし、vSphere Proactive HA は Cisco ACI Virtual Edge を単独で起動し、準備が整うまで VM のホストへの移動を遅らせることができます。



**重要** ホストは、Cisco ACI Virtual Edge 2.1(1a)以降のリリースでのみ、自動的にメンテナンスモードを開始および終了します。以前のリリースでは、vSphere Proactive HA を使用する場合は、ホストを手動でメンテナンスモードに切り替えたり、メンテナンスモードを解除したりする必要があります。

## vSphere Proactive HA の仕組み

VMware vCenter および Cisco Application Policy Infrastructure Controller (APIC) で vSphere Proactive HA を有効にして設定します。この機能は、**ホスト可用性保証**と呼ばれます。

vSphere Proactive HA 機能を有効にして設定すると、VMware vCenter に vSphere Proactive HA プロバイダーオブジェクトが作成されます。オブジェクトを使用すると、VMware vCenter が非稼働の Cisco ACI Virtual Edge を搭載したホストを検査し、そのホストから VM を移動できます。

この機能は、Cisco ACI Virtual Edge Virtual Machine Manager (VMM) ドメイン内のすべての ESXi ホストに、ヘルスステータス（緑、黄色、または赤）も割り当てます。Cisco ACI Virtual Edge 分散仮想スイッチ (DVS) がホストに追加されていない場合、または DVS が追加され、OpFlex がオンラインの場合、ステータスは緑色です。DVS が追加され、OpFlex がオフラインの場合、ステータスは黄色です。

また、ホストに対して検査をトリガーする頻度を指定することもできます。

vSphere Proactive HA を有効にして設定すると、Cisco APIC および VMware vCenter が連携して非動作 Cisco ACI Virtual Edge を検出し、分離します。

1. Cisco APIC は VMware vCenter で Cisco ACI Virtual Edge をモニタします。

VMware vCenter インベントリと OpFlex ステータスを使用して、Cisco ACI Virtual Edge が良好な状態か不良な状態かを判断します。Cisco APIC により Cisco ACI Virtual Edge が不良状態であることが検出されると、黄色レベルを使用して、影響を受けるホストを検査するよう VMware vCenter に指示します。

2. VMware vCenter は、VMware vCenter でクラスタに設定する修復モードに従って、ホストを検査モードにします。



(注) VMware vCenter には赤色のステータスが存在します。Cisco APIC に存在しません。

- **[検疫 (Quarantine)]** : ホストの状態が黄色と赤のレベルの場合、検疫モードになります。



(注) Proactive HA クラスタでは、アップリンクまたは物理ネットワーク インターフェイスカード (PNIC) がホストから取り外されたときに OpFlex がダウンしても、VMware vCenter は Cisco ACI Virtual Edge ホストを隔離に移動しません。

- **[混合 (Mixed)]** : 黄色レベルのホストの状態は検疫モードになります。赤レベルのホストの状態はメンテナンス モードになります。



(注) VMware vCenter では混合修復モードを選択できますが、結果の動作は隔検疫修復モードと同じです。



(注) vSphere Proactive HA を使用する場合は、メンテナンス モード修復を選択しないでください。メンテナンスモードでは、Cisco ACI Virtual Edge の電源をオフにして、ホストが正常な状態に戻らないようにする必要があります。検疫または混合修復モードのみを使用します。

3. VMware 分散リソース スケジューラ (DRS) は、動作していないホストの VM を Cisco ACI Virtual Edge が動作しているホストに移動します。



(注) 正常なホストが使用できず、検疫されたホストに対して DRS ルールによってピン接続された VM がホスト上にとどまっている場合、検疫中のホストは引き続きデータ VM を実行する可能性があります。また、VMware vCenter は、検疫されたホストへの VM の移動を回避します。ただし、隔離内のホストに新しい VM を展開できます。



(注) Cisco ACI Virtual Edge リリース 2.1 (1) 以降では、ホストの動作が停止したときに VM グループが Cisco ACI Virtual Edge ホストから移動するようにできます。この設定は、特定のホストで VM を保持するアフィニティグループを上書きします。詳細については、このガイドの [VM グループ検疫保護 \(105 ページ\)](#) を参照してください。

4. Cisco APIC は、メンテナンスモードになっているホストまたはリポートしているホストの VMware vCenter イベントを監視し、電源がオンになっている VM がホストに残っている場合のみ Cisco ACI Virtual Edge の電源をオフにします。

5. ホストがリブートまたはメンテナンスモードから取得されたとき、Cisco APICにより Cisco ACI Virtual Edge の電源がオンになります。

## VMware vSphere Proactive HA を設定するための前提条件

VMware vSphere Proactive HA を設定する前に、次のタスクを実行します。

Cisco APICvCenter ドメインの作成に使用する VMware vCenter アカウントに、VMware vCenter に対する「ヘルス プロバイダー」書き込み権限があることを確認します。

## vSphere Proactive HA in Cisco APIC で vSphere Proactive HA を有効にする

Cisco Application Policy Infrastructure Controller (APIC) で Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge を改善するには、次のタスクを行います。

- Cisco Application Centric Infrastructure (ACI) 仮想エッジ VMM ドメインでのホスト可用性保証の有効化
- Cisco ACI Virtual Edge 上のホストが動作を停止するまでの VMware vCenter の隔離期間を指定する

これらのタスクは、Cisco ACI Virtual Edge 向け vCenter ドメインを作成するときに Cisco APIC GUI で実行できます。手順については、このガイドの「[Cisco ACI Virtual Edge の VMM ドメイン プロファイルの作成 \(92 ページ\)](#)」の項を参照してください。

これらのタスクは、Cisco APIC GUI の代わりに NX-OS style CLI および REST API を使用して実行できます。このガイドの [NX-OS Style CLI を使用して vSphere Proactive HA を有効にする \(108 ページ\)](#) と [REST API を使用して vSphere Proactive HA を有効にする \(113 ページ\)](#) を参照してください。



- (注) Proactive HA がすでに設定されている状態でクラスタにホストを追加し、Cisco ACI Virtual Edge VMM ドメインにホストを追加またはホストをアタッチするとき、それらのホストはある状況かでは適切に動作しない可能性があります。Cisco ACI Virtual Edge または OpFlex がダウンしたとき、Proactive HA でホストが適切に動作しない可能性があります。ホストのヘルスステータスが Cisco Application Policy Infrastructure Controller (APIC) で黄色に適切に設定されているにもかかわらず、ホストが検疫モードにならない可能性もあります。

この問題を修正するには、クラスタの Proactive HA を無効にして、再度有効にします。

# VMware vCenter で vSphere Proactive HA を有効にする

始める前に

vSphere Proactive High Availability (HA) を使用するには、VMware vCenter 6.5 以降が必要です。



- (注) Proactive HA がすでに設定されている状態でクラスタにホストを追加し、Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge VMM ドメインにホストを追加またはホストをアタッチするとき、それらのホストはある状況かでは適切に動作しない可能性があります。Cisco ACI Virtual Edge または OpFlex がダウンしたとき、Proactive HA でホストが適切に動作しない可能性があります。ホストのヘルス ステータスが Cisco Cisco Application Policy Infrastructure Controller (APIC) で黄色に適切に設定されているにもかかわらず、ホストが検疫モードにならない可能性があります。

この問題を修正するには、クラスタの Proactive HA を無効にして、再度有効にします。

手順

- ステップ 1 VMware vCenter Web クライアントにログインします。
- ステップ 2 [ホーム (Home)] > [ホストおよびクラスタ (Host and Cluster)] > [クラスタ (cluster)] > [設定 (Configure)] > [編集 (Edit)] を選択します。
- ステップ 3 [クラスタ設定の編集 (Edit Cluster Settings)] ダイアログボックスで、左側のナビゲーションペインで [vSphere Availability] を選択し、作業ペインで [Proactive HA をオンにする (Turn on Proactive HA)] チェックボックスをオンにします。
- ステップ 4 左側のナビゲーションペインで、[Proactive HA の障害と応答 (Proactive HA Failures and Responses)] を選択し、次の手順を実行します。
  - a) [修復 (Remediation)] ドロップダウン リストから、修復レベルを選択します。

[検疫 (Quarantine)] (黄色と赤のレベルのホストを検疫モードにする) または [混合 (Mixed)] (黄色のホストを隔離モードにし、赤色のホストをメンテナンスモードにする) を選択します。

(注) [メンテナンス (Maintenance)] を選択しないでください。選択すると、黄色と赤色のホストがメンテナンスモードになります。メンテナンスモードでは、Cisco ACI 仮想エッジの電源をオフにする必要があります。これにより、ホストが正常な状態に戻ることはありません。
  - b) vSphere Proactive HA プロバイダーの横にあるチェックボックスをオンにして有効にします。

Cisco Application Policy Infrastructure Controller (APIC) で作成されたプロバイダーの名前は「vmm-domain-name\_APIC」になります。

## ESXi ホストのヘルス レベルの手動設定

デフォルトでは、VMware ホストの状態は、そのホストにある Cisco Application Centric Infrastructure (ACI) 仮想エッジの状態によって決まります。

Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge でメンテナンスを実行する必要がある場合は、デフォルトを上書きできます。Cisco ACI Virtual Edge が正常に動作しているときにホストの状態を黄色または赤色に設定すると、対応するホストが検疫モードになります。

または、Cisco ACI Virtual Edge がダウンした場合でも、そのホストが隔離されたくない場合があります。状態を緑に設定すると、ホストがアクティブになり、ホストの vSphere Proactive HA が無効になります。

ヘルス状態を手動で緑色に設定すると、Cisco Application Policy Infrastructure Controller (APIC) によりホストステータスを黄色または赤色に変更されることを防ぎます。Cisco APIC GUI、NX-OS スタイル CLI、または REST API を使用して、ヘルス状態を表示および設定できます。セクション「[Cisco APIC GUI を使用して Cisco ACI 仮想エッジホストの状態を表示して設定する \(104 ページ\)](#)」を参照してください。また、VMware vCenter でホストのヘルス状態とイベントを表示することもできます。「[VMware vCenter のホスト向けヘルスアップデートのトラッキング \(105 ページ\)](#)」を参照してください。

## Cisco APIC GUI を使用して Cisco ACI 仮想エッジホストの状態を表示して設定する

### 始める前に

- Cisco ACI Virtual Edge を含むホストが必要です。
- ホスト可用性保証は、Cisco Application Policy Infrastructure Controller (APIC) 上の VMM ドメインに対して有効に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 [仮想ネットワーク (Virtual Networking)] > [インベントリ (Inventory)] > [VMM ドメイン (VMM Domains)] > [VMware] > [VMM ドメイン (VMM domain)] > [コントローラ (Controllers)] に進み、コントローラをクリックします。

- ステップ3 [コントローラインスタンス (Controller Instance)] 作業ウィンドウの [ヘルス ポリシー (Health Policy)] 領域で、[+] (プラス アイコン) をクリックします。
- ステップ4 ホスト IP アドレスを入力し、ドロップダウンリストから状態を選択して、[更新 (Update)] をクリックします。
- ステップ5 [送信 (Submit)] をクリックします。

## VMware vCenter のホスト向けヘルス アップデートのトラッキング

Proactive HA を有効にすると、VMware vCenter でイベントを表示して、ホストのヘルス アップデートを追跡できます。

### 手順

- ステップ1 VMware vCenter Web クライアントにログインします。
- ステップ2 ホストに移動します。
- ステップ3 中央の作業ウィンドウで、[モニタ (Monitor)] タブ、[タスクとイベント (Tasks & Events)]、[イベント (Events)] の順にクリックします。

[説明 (Description)] ペインには、ホストのイベントが表示されます。[タイプ (Type)] カラムで、VMware vCenter は、劣化ステータスやホストの隔離モードへの連続した移行など、ホストの状態の変化に関する警告を表示します。正常性の問題の報告からホストが別のモードに移行するまでに 30 秒の遅延が生じることがあります。

## VM グループ検疫保護

ホスト保証可用性を有効にすると、Cisco Application Centric Infrastructure (ACI) 仮想エッジで障害が発生した場合でも、仮想マシン (VM) が使用可能になります。ホスト保証可用性は、Cisco ACI Virtual Edge が非稼働状態の ESXi ホストのヘルス ステータスを黄色または赤色に設定することで、Cisco APIC により VM の vMotion をトリガーします。

ただし、分散リソース スケジューラ (DRS) のアフィニティ ルールとロード バランシングの設定により、VM が動作しないホストにとどまるか、配置されないことがあります。保護された VM グループを設定すると、Cisco APIC により VMware vCenter で非アフィニティ ルールを自動作成できます。これは、グループの VM 部分を強制的に非稼働ホストから移動します。

VM グループを保護するには、VMware vCenter で VM グループを作成し、Cisco APIC で VM グループの保護を有効にする必要があります。各 VM グループには、Cisco ACI Virtual Edge を使用するすべての VM が必要です。

特定のコントローラの Cisco Application Policy Infrastructure Controller (APIC) で VM グループ保護を設定します。Cisco APIC GUI、NX-OS スタイル CLI、または REST API を使用できます。



- (注) VM グループ隔離の保護を機能させるには、Cisco APIC vCenter ドメインの作成に使用する VMware vCenter アカウントに、VMware vCenter の「クラスタ」オブジェクトに対する書き込み権限が必要です。

## Cisco APIC GUI を使用した VM グループ保護の設定

Cisco APIC GUI を使用して VM グループ保護を設定できます。

### 始める前に

VMware vCenter で VM グループを設定し、Cisco Application Policy Infrastructure Controller (APIC) で vSphere Proactive HA を有効に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 [仮想ネットワーク (Virtual Networking)] > [インベントリ (Inventory)] > [VMM ドメイン (VMM Domains)] > [VMware] > [VMM ドメイン (VMM domain)] > [コントローラ (Controllers)] > [コントローラ (controller)] に進みます。
- ステップ 3 [コントローラ (Controller)] 作業ウィンドウで、[ポリシー (Policy)] および [全般 (General)] タブを選択します。
- ステップ 4 [保護済み VM グループ (Protected VM Groups)] 領域で、1 つ以上の VM グループのチェックボックスをオンにします。
- ステップ 5 [送信 (Submit)] をクリックします。



## 付録 **D**

# NX-OS Style CLI を使用してタスクを実行する

---

- [Cisco ACI 仮想エッジへの移行 \(107 ページ\)](#)
- [VMware vSphere Proactive HA を使用して Cisco ACI 仮想エッジの可用性の向上 \(108 ページ\)](#)

## Cisco ACI 仮想エッジへの移行

### NX-OS スタイルの CLI を使用して VDS ドメインを Cisco ACI Virtual Edge へ移行する

移行時に、ドメインで Cisco ACI Virtual Edge を使用できるようにします。

始める前に

VMM ドメインを作成しておきます。[Cisco ACI Virtualization Guide](#) の「Creating a VMM Domain Profile」の手順を参照してください。

手順

---

VDS VMM ドメインを移行します。

例：

```
apicl(config)# vmware-domain mininet
apicl(config-vmware)# configure-ave
apicl(config-vmware-ave)# vxlan multicast-pool 225.2.1.1-225.2.1.100
apicl(config-vmware-ave)# exit
apicl(config-vmware)# exit
apicl(config)# exit
apicl#
```

---

# VMware vSphere Proactive HA を使用して Cisco ACI 仮想エッジの可用性の向上

## NX-OS Style CLI を使用して vSphere Proactive HA を有効にする

NX-OS スタイル CLI を使用して、Cisco Application Policy Infrastructure Controller (APIC) のいくつかのタスクを実行できます。

- ホスト可用性保証を有効にします。これにより、VMware vCenter に存在する vSphere Proactive HA プロバイダー オブジェクトが作成されます。このオブジェクトを使用すると、VMware vCenter は動作していない Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge を持つホストを隔離し、その VM を移動できます。
- VMware vCenter が稼働していない Cisco ACI Virtual Edge を持つホストを検疫し、VM をホストから移動するまでの期間を設定します。



(注) Proactive HA がすでに設定されている状態でクラスタにホストを追加し、Cisco ACI Virtual Edge VMM ドメインにホストを追加またはホストをアタッチするとき、それらのホストはある状況かでは適切に動作しない可能性があります。Cisco ACI Virtual Edge または OpFlex がダウンしたとき、Proactive HA でホストが適切に動作しない可能性があります。ホストのヘルスステータスが Cisco Application Policy Infrastructure Controller (APIC) で黄色に適切に設定されているにもかかわらず、ホストが検疫モードにならない可能性もあります。

この問題を修正するには、クラスタの Proactive HA を無効にして、再度有効にします。

### 手順

**ステップ 1** ホスト可用性保証を有効にします。

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# avail-monitor enable
apic1(config-vmware)# show run
# Command: show running-config vmware-domain mininet
# Time: Mon Aug  6 22:05:58 2018
vmware-domain mininet
  vlan-domain member mininet type vmware
  vcenter 172.23.143.235 datacenter mininet dvs-version 6.0
  # username admin
  esx-avail-override 172.23.143.228 yellow
  exit
configure-ave
  switching mode vxlan
  multicast-address 225.1.1.1
  vxlan multicast-pool 225.2.1.1-225.2.1.100
```

```
exit
avail-monitor enable
exit
apicl(config-vmware)#
```

**ステップ 2** Cisco ACI Virtual Edge タイムアウトを設定します。

```
apicl# config
apicl(config)# vmware-domain mininet
apicl(config-vmware)# configure-ave
apicl(config-vmware-ave)# ave-timeout 10
```

10 ～ 100 秒の任意の値を選択できます。デフォルトは 30 秒です。

---

### 次のタスク

VMware vCenter で VMware vSphere Proactive HA 機能をまだ有効にしていない場合は、有効にします。このガイドの [VMware vCenter で vSphere Proactive HA を有効にする \(103 ページ\)](#) セクションを参照してください。

特定のホストの状態を設定して、Cisco ACI Virtual Edge の状態に基づいてデフォルトの状態を上書きできます。 [ESXi ホストのヘルス レベルの手動設定 \(104 ページ\)](#) の項を参照してください。

## NX-OS Style CLI を使用して Cisco ACI 仮想エッジホストで状態を設定する

### 始める前に

Cisco ACI Virtual Edge を含むホストが必要です。

### 手順

---

ホストの状態を設定します。

```
apicl# config
apicl(config)# vmware-domain mininet
apicl(config-vmware)# vcenter 192.168.0.235 datacenter apicl(config-vmware)# vcenter
172.23.143.235 datacenter mininet
apicl(config-vmware-vc)# esx-avail-override 192.168.0.1 yellow
apicl(config-vmware-vc)# show run
# Command: show running-config vmware-domain mininet vcenter 192.168.0.235 datacenter
mininet
# Time: Mon Aug 6 23:47:17 2018
vmware-domain mininet
vcenter 192.168.0.235 datacenter mininet dvs-version 6.0
# username admin
esx-avail-override 192.168.0.1 yellow
exit
```

```
exit
apicl(config-vmware-vc)#
```

---

## NX-OS Style CLI を使用して VM グループ保護を設定する

NX-OS style CLI を使用して、Cisco Application Centric Infrastructure (ACI) 仮想エッジ ホストが動作を停止した場合に、特定の VM グループを動作中のホストに移動することができます。

### 始める前に

VMware vCenter で VM グループを設定し、Cisco Application Policy Infrastructure Controller (APIC) で vSphere Proactive HA を有効にする必要があります。

### 手順

---

VM グループ保護を設定します。

例：

```
apicl# config
apicl(config)# vmware-domain mininet
apicl(config-vmware)# vcenter 192.168.0.1 datacenter mininet
apicl(config-vmware-vc)# protect-vm-group "AVE_Cluster_Name/VM_Group_Name"
```

*AVE\_Cluster\_Name* は、VM グループが定義され、アフィニティ ルールがプログラムされている VMware vCenter 上の ESXi クラスタの名前です。VM グループはクラスタ固有です。  
*VM\_Group\_Name* は、指定したクラスタに存在する VM グループの名前です。

---



## 付録 E

# REST API を使用してタスクを実行する

- [Cisco ACI 仮想エッジへの移行 \(111 ページ\)](#)
- [VMware vSphere Proactive HA による Cisco ACI 仮想エッジの可用性の向上 \(113 ページ\)](#)

## Cisco ACI 仮想エッジへの移行

### REST API を使用して Cisco AVS VMM ドメインを Cisco ACI Virtual Edge に移行する

Cisco AVS から Cisco ACI Virtual Edge に移行する前に、ホストと VM で VMM ドメインの準備ができていない必要があります。VMM ドメインは、REST API を使用して移行することができます。この方法は、手動でほとんどの Cisco AVS ドメインの設定を再現する必要がある新しい VMM ドメインの作成よりも、簡単です。



(注) 移行できる Cisco AVS VMM ドメインは、一度に 1 つだけです。

#### 手順

名前、作成する Cisco ACI Virtual Edge ドメインの名前、およびユーザアカウント情報を入力して、Cisco AVS VMM ドメインを移行します。

以前の Cisco AVS のユーザアカウント情報として、ユーザ名とパスワードを入力する必要があります。オプションとして、新しい VLAN プールを指定します。

#### 例 :

次の例では、prod-avs という名前の Cisco AVS ドメインを ave という名前のドメインに移行します。また、Cisco ACI Virtual Edge ドメインの VLAN プールも作成します。

```
{{ifc}}/mqapi2/migrateVMwareDomain.xml?name=prod-avs
<vmmDomP dn="uni/vmmp-VMware/dom-ave" name="ave" enableAVE="true" >
  <vmmUsrAccP name="adminAcc" usr="administrator@vsphere.local" pwd="In$1eme1" />
```

```
<infraRsVlanNs tDn="uni/infra/vlanns-[inst_pvlan]-dynamic"/>
</vmmDomP>
```

デフォルトでは、Cisco AVS ドメインからのすべての EPG が、新しいドメインに自動的に関連付けられます。EPG の関連付けを行わない場合には、`migrateEPGs = false` パラメータを追加します。

Cisco AVS ドメインの EPG を新しい Cisco ACI Virtual Edge ドメインに関連付けても、元の関連付けは削除されません。

### 次のタスク

本ガイドの [Cisco ACI vCenter プラグイン](#) を使用して Cisco AVS から Cisco ACI Virtual Edge に移行する (55 ページ) のセクションの手順に従います。

## REST API を使用して VDS ドメインを Cisco ACI Virtual Edge へ移行する

### 始める前に

VMM ドメインを作成しておきます。[Cisco ACI Virtualization Guide](#) の「VMM ドメインプロファイルの作成」の手順を参照してください。

### 手順

**ステップ 1** マルチキャスト アドレス プールを作成していない場合は作成します。

例 :

```
<polUni>
<infraInfra>
  <fvnsMcastAddrInstP name="mcast1">
    <fvnsMcastAddrBlk name="mcastrange" from="225.2.1.1" to="225.2.1.100"/>
  </fvnsMcastAddrInstP>
</infraInfra>
</polUni>
```

**ステップ 2** VMM ドメインで `enableAVE=true` 設定し、マルチキャスト アドレス プールを VMM ドメインに関連付けます。

例 :

```
<polUni>
<vmmProvP vendor="VMware">
  <vmmDomP name="mininet" enableAVE="true">
    <vmmRsDomMcastAddrNs tDn="uni/infra/maddrns-mcast1"/>
  </vmmDomP>
</vmmProvP>
</polUni>
```

# VMware vSphere Proactive HA による Cisco ACI 仮想エッジの可用性の向上

## REST API を使用して vSphere Proactive HA を有効にする

REST API を使用して、Cisco Application Policy Infrastructure Controller (APIC) のいくつかのタスクを実行できます。

- ホスト可用性保証を有効にします。これにより、VMware vCenter に存在する vSphere Proactive HA プロバイダー オブジェクトが作成されます。このオブジェクトを使用すると、VMware vCenter は動作していない Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge を持つホストを隔離し、その VM を移動できます。
- VMware vCenter が稼働していない Cisco ACI Virtual Edge を持つホストを検査し、VM をホストから移動するまでの期間を設定します。



(注) Proactive HA がすでに設定されている状態で Cisco ACI Virtual Edge クラスタにホストを追加し、Cisco ACI Virtual Edge VMM ドメインにホストを追加またはホストをアタッチするとき、それらのホストはある状況かでは適切に動作しない可能性があります。Cisco ACI Virtual Edge または OpFlex がダウンしたとき、Proactive HA でホストが適切に動作しない可能性があります。ホストのヘルス ステータスが Cisco Application Policy Infrastructure Controller (APIC) で黄色に適切に設定されているにもかかわらず、ホストが検査モードにならない可能性もあります。

この問題を修正するには、クラスタの Proactive HA を無効にして、再度有効にします。

### 手順

**ステップ 1** ホスト可用性保証を有効にします。

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware" >
    <vmmDomP name="mininet" hvAvailMonitor="yes">
  </vmmDomP>
</vmmProvP>
</polUni>
```

**ステップ 2** Cisco ACI Virtual Edge タイムアウトを設定します。

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware">
    <vmmDomP name="mininet" aveTimeOut="10">
  </vmmDomP>
```

```
</vmmProvP>
</polUni>
```

10 ～ 100 秒の任意の値を選択できます。デフォルトは 30 秒です。

### 次のタスク

VMware vCenter で VMware vSphere Proactive HA 機能をまだ有効にしていない場合は、有効にします。このガイドの [VMware vCenter で vSphere Proactive HA を有効にする \(103 ページ\)](#) セクションを参照してください。

特定のホストの状態を設定して、Cisco ACI Virtual Edge の状態に基づいてデフォルトの状態を上書きできます。 [ESXi ホストのヘルス レベルの手動設定 \(104 ページ\)](#) の項を参照してください。

## REST API を使用して REST API 仮想エッジで状態を設定する

### 始める前に

Cisco ACI Virtual Edge を含むホストが必要です。

### 手順

ホストの状態を設定します。

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware">
    <vmmDomP name="mininet">
      <vmmCtrlrP name="vc65.xyz.com">
        <vmmHvAvailPol>
          <vmmHvDesiredSt host="172.23.143.228" state="yellow"/>
        </vmmHvAvailPol>
      </vmmCtrlrP>
    </vmmDomP>
  </vmmProvP>
</polUni>
```

## REST API を使用して VM グループ保護を設定する

REST API を使用して、Cisco Application Centric Infrastructure (ACI) 仮想エッジホストが動作を停止した場合に、特定の VM グループを動作中のホストに移動することができます。

### 始める前に

VMware vCenter で VM グループを設定し、Cisco Application Policy Infrastructure Controller (APIC) で vSphere Proactive HA を有効にする必要があります。

## 手順

---

VM グループ保護を設定します。

例：

```
<polUni>
<vmmProvP vendor="VMware">
  <vmmDomP name="mininet" hvAvailMonitor="true">
    <vmmCtrlrP name="vc65.xyz.com">
      <vmmHvAvailPol>
        <vmmProtectedVmGroup
tDn="comp/prov-VMware/ctrlr-[mininet]-vc65.xyz.com/hvcluster-domain-c94/vmgroup-vm01"></vmmProtectedVmGroup>

        </vmmHvAvailPol>
      </vmmCtrlrP>
    </vmmDomP>
  </vmmProvP>
</polUni>
```

上記の例では、次の点に注意してください。

- `vmmProtectedVmGroup` の `tDN` プロパティは、`compVmGroup` (vCenter インベントリから取得される VM グループ) の `dn` プロパティです。
  - GET:`https://{apic}/api/node/class/compVmGroup.xml` を介して `compVmGroup` のリストはクエリできます。
-

