Cisco UCS Director リリース 6.5 アプリケーション コンテナ ガイド

初版：2017 年 07 月 11 日

最終更新：2017 年 09 月 27 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/**）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。

目 次

はじめに

対象読者

このマニュアルは、Cisco UCS Director を使用し、以下の少なくとも 1 つの分野において責任と専門知識を持つデータセンター管理者を主に対象としています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ
- 仮想化および仮想マシン

表記法

テキストのタイプ	表示
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メインタイトル] のように示しています。

テキストのタイプ	表示
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*Italic*）で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、`courier` フォントで示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体 **this font** で示しています。 CLI コマンド内の変数は、イタリック体 *this font* で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注）「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

ヒント　「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

ワンポイント アドバイス　「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　安全上の重要事項

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

これらの注意事項を保管しておいてください。

関連資料

『Cisco UCS DirectorDocumentation Roadmap』

Cisco UCS Director の資料の詳細なリストについては、次の URL にある『*Cisco UCS Director Documentation Roadmap*』を参照してください。http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html

『Cisco UCS Documentation Roadmaps』

すべての B シリーズ マニュアルの完全なリストについては、『*Cisco UCS B-Series Servers Documentation Roadmap*』（URL：http://www.cisco.com/go/unifiedcomputing/b-series-doc）を参照してください。

すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

（注）　『*Cisco UCS B-Series Servers Documentation Roadmap*』には Cisco UCS Manager および Cisco UCS Central のドキュメントのリンクが含まれています。『*Cisco UCS C-Series Servers Documentation Roadmap*』には Cisco Integrated Management Controller のドキュメントのリンクが含まれています。

マニュアルに関するフィードバック

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

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス リクエストの送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

第 1 章

新機能および変更情報

この章は、次の項で構成されています。

このリリースの新規情報および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

表 *1*：*Cisco UCS Director*、リリース *6.5* の新しい動作と動作変更

機能	説明	参照先
VM でリンク クローンを使用	仮想ディスク ストレージを共有する 2 つ以上の関連する VM であるリンクされた VM を展開するためのサポートを提供します。	フェンスド仮想コンテナ用のアプリケーション コンテナ テンプレートの作成, （36 ページ）

機能	説明	参照先
コンテンツライブラリテンプレートを使用して、VMをプロビジョニングします。	VMプロビジョニング用のコンテンツ ライブラリ VM テンプレートからVMテンプレートを選択するためのサポートを提供します。	• 階層化アプリケーション ゲートウェイ ポリシーの作成, （16 ページ） • アプリケーション コンテナ テンプレートの作成, （19 ページ） • フェンスド仮想コンテナ用のアプリケーション コンテナ テンプレートの作成, （36 ページ） • 仮想インフラストラクチャ ポリシーの作成, （55 ページ） • VSG 用アプリケーション テンプレートの作成, （57 ページ） • ファブリック アプリケーション コンテナ テンプレートの作成, （70 ページ） • アプリケーション プロファイルの追加, （104 ページ） • アプリケーション プロファイルの複製, （118 ページ） • アプリケーション プロファイルの編集, （131 ページ） • VM の追加, （170 ページ）

第 2 章

アプリケーション コンテナの概要

この章は、次の項で構成されています。

アプリケーション コンテナ

アプリケーション コンテナは、エンドユーザに対するアプリケーションのプロビジョニングにテンプレートを利用するアプローチです。各アプリケーション コンテナは、VMware および HyperV 仮想マシン（VM）やベア メタル サーバ（BM）の集合です。アプリケーション コンテナには、管理者によって指定されたルールに基づく内部プライベート ネットワークがあります。アプリケーション コンテナには 1 つ以上の VM または BM を含めることができ、外部クラウドまたはパブリック クラウドにはフェンシング ゲートウェイ（たとえば、仮想セキュア ゲートウェイ）で保護することができます。

Cisco UCS Director は、アプリケーション コンテナをサポートします。また、1 つ以上のネットワークや VM または BM でコンテナ テンプレートを定義できます。アプリケーション コンテナをテンプレートから作成する場合、Cisco UCS Director は自動で VM または BM を導入し、ネットワークとアプリケーション サービスを設定します。Cisco UCS Director はレイヤ 2 変更の仮想スイッチと物理スイッチも自動で設定します。

アプリケーションをプロビジョニングするために Cisco UCS Director を設定する場合は、適切なポリシー、ワークフロー、テンプレートを設定した 1 つ以上のアプリケーション コンテナ テンプレートを作成します。アプリケーション コンテナテンプレートによって、エンドユーザ対してアプリケーションをどのようにプロビジョニングするかが決定します。次のいずれか、またはすべてを定義できます。

- 物理サーバまたは仮想マシン

- 予約ストレージの量
- 使用可能な最大 CPU
- 使用可能な最大メモリ
- オペレーティング システムのバージョン
- VLAN の範囲
- ゲートウェイまたはファイアウォール（必要に応じて）
- ロード バランサ（必要に応じて）
- 必要な承認（必要に応じて）
- アクセス制御リスト（ACL）ルールまたは他の L3 サービス（必要な場合）
- アプリケーション コンテナに関するコスト（必要に応じて）

Cisco UCS Director は複数のタイプのアプリケーション コンテナをサポートします。実装する必要があるアプリケーション コンテナのタイプは、展開の設定によって異なります。アプリケーション コンテナの設定に必要な手順は、実装するタイプによって異なります。

アプリケーション コンテナのタイプ

さまざまな展開シナリオで使用されるアプリケーション コンテナ タイプは次のとおりです。

- フェンスド仮想：フェンスド仮想コンテナは、内部プライベート ネットワークを使用する VM の集合で、管理者によって指定されたルールに基づいています。フェンスド コンテナは、パブリックまたは外部クラウドのフェンシング ゲートウェイによって保護されている 1 つまたは複数の仮想マシンを持つことができます。これは VM での使用に最も一般的なアプリケーション コンテナのタイプです。詳細については、このガイドの「フェンスド仮想コンテナの設定」の章を参照してください。
- Virtual Secure Gateway（VSG）：Cisco Virtual Secure Gateway（VSG）コンテナ タイプは、強化されたセキュリティを仮想環境で提供するために使用します。Cisco UCS Director を使用して、Prime Network Services Controller（PNSC）とともに、その内部ファイアウォール（Cisco Virtual Security Gateway）を設定できます。このファイアウォールは、設定後、アプリケーション コンテナに統合されます。詳細については、このガイドの「仮想セキュア ゲートウェイ アプリケーション コンテナの設定」の章を参照してください。
- Application Centric Infrastructure Controller（APIC）コンテナ：APIC コンテナは Cisco APIC 展開で使用します。APIC は、シスコ アプリケーション セントリック インフラストラクチャ（ACI）に自動化、管理、モニタリング、およびプログラマビリティを提供する統合ポイントです。APIC は、インフラストラクチャの物理コンポーネントと仮想コンポーネントに対して統一された運用モデルを提供し、あらゆるアプリケーションをどこからでも展開、管理、モニタリングできるようにします。また、さらに大規模なクラウド ネットワークの中央制御エンジンとなります。APIC は、ユーザ定義のアプリケーション要件とポリシーに基づき、ネットワークのプロビジョニングと制御をプログラムによって自動化します。Cisco UCS

Director により、Cisco APIC をサポートするアプリケーション コンテナを作成します。APIC コンテナの詳細については、このガイドの「Cisco Application Policy Infrastructure Controller Container の設定」の章、およびこのリリースの『Cisco UCS Director APIC Management Guide』を参照してください。

- ファブリック：ファブリック アプリケーション コンテナは Dynamic Fabric Automation（DFA）ネットワークの配備に使用します。Cisco Unified Fabric Automation は、接続されたすべてのデバイスが同じホップ数で到達可能な、マルチステージのスイッチング ネットワークです。Cisco Unified Fabric Automation 組織ファブリックにより、スケールアウト モデルを使用した最適な拡張が可能になります。DFA ネットワーク内のアプリケーション コンテナの詳細については、このガイドの「ファブリック コンテナの設定」の章、および『Cisco UCS Director Unified Fabric Automation Management Guide』を参照してください。

アプリケーション コンテナの表示

Cisco UCS Director でアプリケーション コンテナを表示するには、[ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

[ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。
アプリケーション コンテナは、カラー スキームを使用してコンテナのステータスを識別します。

- 緑：すべての VM およびベア メタル サーバ（BM）の電源がオンの状態です。コンテナ設定に GW が含まれている場合は、ゲートウェイ（GW）もオンになっています。
- 黄色：要求されたいずれかの BM がまだ進行中/エラー状態であるか、またはいずれかのアプリケーション VM がダウンしています。
- 青：コンテナのプロビジョニングが進行中です。
- グレー：VM と BM がコンテナにありません。
- 赤：GW を含めて、すべての VM および BM の電源がオフになっています。

サポートされているレイヤ 4 からレイヤ 7 のサービス

アプリケーション コンテナは単一層または多層アプリケーションのいずれかをプロビジョニングするように設定できます。さらに、アプリケーションでプロビジョニングされる、ロード バランサまたはファイアウォールなどのアプリケーション サービスを追加することを選択できます。アプリケーション コンテナを作成する前に、これらのオプションのどちらを実装するかを決定する必要があります。

ファイアウォール（Firewall）

ファイアウォールは、アプリケーションに内部または外部ゲートウェイとして追加できます。ゲートウェイはファイアウォールを経由してアプリケーションに至るトンネルをリダイレクトして作成します。ファイアウォールを使用する場合、ユーザはいずれかのアプリケーション VM の IP アドレスを知っている必要はありません。代わりに、ユーザはゲートウェイの IP アドレスを使ってログインし、アプリケーションまたはデータベース VM にリダイレクトされます。ゲートウェイを介して許可されるトラフィックの種類を定義するルールを作成することもできます。

階層型アプリケーションゲートウェイポリシーで使用するファイアウォールを定義します。その後このポリシーは、アプリケーションコンテナテンプレートに組み込まれます。次のいずれかのタイプのファイアウォールを追加できます。

- Linux VM：デフォルトのオプションでは、適切なファイアウォールと NAT ルールが VM 上にプロビジョニングされます。
- Cisco ASA：この物理ゲートウェイでは、内部システムおよびアプリケーションそれぞれに対して明示的に設定を行わなくても、単方向（内部から外部へ）の接続が可能です。
- Cisco ASAv：この仮想ゲートウェイは通常、アプリケーションのプロビジョニング中に、ASAv 展開ポリシーを使用して VM テンプレートから展開します。ASAv では、内部システムおよびアプリケーションごとに明示的に設定することなく、一方向（内部から外部）の接続が可能です。

ロード バランサ

多層アプリケーション用にロードバランサを含めることができます。ロードバランサは、サーバ間で通信とワークロードを管理します。たとえば、ロード バランサは、ユーザを識別し、いくつかのアプリケーション サーバの 1 つにユーザをリダイレクトして、どのアプリケーション サーバも過負荷にならないようにします。

サポートされているロードバランサの詳細については、『Cisco UCS Director Compatibility Matrix』を参照してください。

第 3 章

ゲートウェイの実装

この章は、次の項で構成されています。

Linux ゲートウェイ

これはデフォルト ゲートウェイであり、適切なファイアウォールと NAT ルールを VM 上でプロビジョニングします。

Cisco適応型セキュリティアプライアンス（ASA）ゲートウェイ

Cisco UCS Director は、物理適応型セキュリティ アプライアンス（ASA）ゲートウェイを利用するアプリケーション コンテナを作成する機能を提供します。

物理ゲートウェイでは、内部システムおよびアプリケーションそれぞれに対して明示的に設定を行わなくても、単方向（内部から外部へ）の接続が可能です。

Cisco適応型セキュリティ仮想アプライアンスゲートウェイ

Cisco UCS Director は、適応型セキュリティ仮想アプライアンス（ASAv）ゲートウェイを利用するアプリケーション コンテナを作成する機能を提供します。Cisco ASAv は、シスコ アプリケーション セントリック インフラストラクチャ（ACI）環境の従来の階層型データセンター展開も、

ファブリックベースの展開もサポートします。ASAv は、物理、仮想、アプリケーション セントリック、SDN、クラウドの各環境全体にわたって一貫性のある透過的なセキュリティを提供します。

ASAv は、ファイアウォール機能を仮想化環境にもたらし、マルチテナント アーキテクチャ内のデータセンター トラフィックを保護します。ASAv はデータセンター環境用に最適化されているため、vSwitch をサポートします。したがって、ASAv はシスコのデータセンターだけでなく、ハイブリッドやシスコ以外のデータセンターでも展開でき、大幅な管理費の削減や柔軟性および運用効率の改善を実現します。

ACI の展開では、Cisco Application Policy Infrastructure Controller（APIC）でネットワーク管理とセキュリティ管理の両方を一元管理できます。APIC は、ASAv セキュリティをサービスとして提供し、ポリシーを管理し、環境全体をモニタして、分散インフラストラクチャ全体の統合ビューを提供します。ASAv ゲートウェイの作成や削除など、多くの APIC 機能が Cisco UCS Director を通じて制御できます。

第 4 章

ロード バランシングの実装

この章は、次の項で構成されています。

F5 ロード バランシング

Cisco UCS Director では、F5ロード バランサの作成とモニタリングをサポートします。

ルーティング環境ではロード バランシングが広く利用される可能性がありますが、仮想ネットワーキングや VM 環境における重要性も高まっています。サーバのロード バランシングは、複数の仮想サーバへトラフィックを分散するメカニズムであり、アプリケーションおよびサーバのリソース使用率を向上させます。

サーバ ロードバランシング（SLB）は、サービスを提供するためにロードバランシングデバイスがクライアント リクエストを送信すべきサーバを決定するプロセスです。たとえば、クライアント リクエストは、Web ページの HTTP GET やファイルをダウンロードするための FTP GET で構成できます。ロードバランサのジョブは、クライアントリクエストを正常に実行でき、かつ、全体として、サーバにもサーバ ファームにも負荷をかけすぎることなく、最短時間でそれを実行するためのサーバを選択することです。

設定するロード バランシング アルゴリズム、つまりプレディクタに応じて、F5 BIG-IP では一連のチェックおよび計算を実行し、各クライアント要求に最良に対応できるサーバを決定します。F5 BIG-IP は、負荷に対して接続数が最小のサーバ、送信元または宛先アドレス、cookie、URL、HTTP ヘッダーなど、いくつかの要因に基づいてサーバを選択します。

ロード バランシングのプロセス フロー概要は次のとおりです。

1 クライアントがロード バランサのサービスに接続しようとします。

2 ロード バランサが接続を許可します。

3 ロードバランサが、接続を受信するホストを決定し、選択したホストのサービスと一致させるために宛先 IP アドレス（またはポート）を変更します。

4 ホストがロード バランサの接続を受け入れ、元の送信元、クライアント（デフォルト ルート経由）、およびロード バランサに応答を返します。

5 ロード バランサは、ホストから返却パケットを取得し、この時点で送信元 IP アドレス（またはポート）を変更して、仮想サーバ IP アドレスおよびポートに応答し、パケットをクライアントに戻します。

6 クライアントは、それが仮想サーバからのものであると想定して返却パケットを受け取り、残りのプロセスを続行します。

Cisco UCS Director が、F5 ロード バランサの管理、オーケストレーション、およびモニタリングを有効にします。次に、重要なプロセスの概要を示します。

1 F5 ロードバランサを追加します。F5 ロードバランサを追加するには、[管理（Administration）] > [物理アカウント（Physical Accounts）] を選択します。[物理アカウント（Physical Accounts）] ページで、[ネットワーク要素の管理（Managed Network Elements）] をクリックし、次に [ネットワーク要素を追加（Add Network Element）] をクリックします。

2 F5 ロード バランサを管理対象要素として追加するときに、Cisco UCS Director は Cisco UCS Director タスク インベントリ収集をトリガーします。[システムのタスク（System Tasks）] で設定されるポーリング間隔でインベントリ収集の頻度を指定します。

3 F5 ロード バランサがポッドに追加されると、ポッド環境のその他すべてのコンポーネントと一緒にアカウント レベルでリストされます。F5 コンポーネント情報を表示するには、[物理（Physical）] > [ネットワーク（Network）] を選択します。[ネットワーク（Network）] ページで、ポッドを選択し、[管理対象ネットワーク要素（Managed Network Elements）] をクリックします。

Cisco UCS Director を使用して、F5 デバイス上でロード バランシングを実装する方法は 2 つあります。

1 iApps（BIG-IP）アプリケーション サービスを使用する。

   iApps アプリケーション テンプレートは、サーバを一貫して導入、管理、モニタリングするインターフェイスとして機能することにより、BIG-IP システムを HTTP アプリケーション向けに構成することを可能にします。デフォルトの iApps テンプレートを使用するか、F5 デバイスでロード バランシングを実装するテンプレートを作成し、カスタマイズできます。

2 Cisco UCS Director を使用して、以下を実行します。

   - 管理対象要素のセットアップ
   - プールの作成
   - プール メンバの追加
   - 仮想サーバの作成

F5アプリケーションコンテナのセットアップのワークフロー タスクについて

Cisco UCS Director には、ワークフロー デザイナを使用したロード バランサへの接続に役立つ F5 BIG-IP ワークフローが含まれています。重要なワークフロー タスクを以下に示します。

- コンテナ VM リソースの割り当て
- コンテナのプロビジョニング：ネットワーク
- コンテナのプロビジョニング：VM
- コンテナの再同期：VM
- コンテナ ゲートウェイのセットアップ
- コンテナ F5 ロード バランサのセットアップ
- コンテナ電子メールの送信

F5 ロード バランシング アプリケーション コンテナの前提条件

Cisco UCS Director 内で F5 ロード バランシング アプリケーション コンテナを作成する前に、次のタスクを実行する必要があります。

- フェンスド コンテナのセットアップ
- フェンスド コンテナのセットアップ：ASA ゲートウェイ

ヒント　コンテナ ロード バランサのセットアップ タスクは、アプリケーション サービスを手動で作成するために提供されています。このタスクは、「フェンスド コンテナ セットアップ：ASA ゲートウェイ」タスクと統合され、F5 ロードバランシング アプリケーション コンテナを作成します。

F5ロードバランシングアプリケーションコンテナのセットアップに関する要件

Cisco UCS Director は、F5 ロード バランシング プロパティを包含 VM に提供するアプリケーション コンテナを作成できます。Cisco UCS Director プロセス ワークフローの概要を次に示します。

1. ロード バランシング ポリシーの作成
2. ネットワーク要素の追加
3. 仮想インフラストラクチャ ポリシーの作成
4. 階層化アプリケーション ゲートウェイ ポリシーの作成（オプション）
5. コンテナ テンプレートの作成
6. コンテナの作成

F5 Big IP ネットワーク設定の制限

ゲートウェイおよびF5 BIG-IPデバイスで必要なネットワーク設定を手動で行う必要があります。

（注） ゲートウェイでの VLAN 設定と NAT 設定とともに、F5 デバイスでの関連ネットワーク設定は、Cisco UCS Director を使用した F5 アプリケーション コンテナのサポートの一環として行うことはできません。この特定の自動化プロセスについては、近日中にリリースされる Cisco UCS Director で対応します。

ネットワーク機器の追加

ロードバランシングをサポートする仮想サーバを作成するには、最初にネットワーク機器をCisco UCS Director に追加しておく必要があります。ロード バランサを Cisco UCS Director のネットワーク機器として追加した後、[管理するネットワーク機器（Managed Network Element）] 画面にその機器が表示されます。

はじめる前に

このタスクを完了するには、アプライアンスにログインする必要があります。

ステップ 1 [管理（Administration）] > [物理アカウント（Physical Accounts）] を選択します。

ステップ 2 [物理アカウント（Physical Accounts）] ページで [管理するネットワーク機器（Managed Network Elements）] をクリックします。

ステップ 3 [ネットワーク機器の追加（Add Network Element）] をクリックします。

ステップ 4 [ネットワーク機器の追加（Add Network Element）] 画面で、次のフィールドに値を入力します。

名前	説明
[ポッド（POD）] ドロップダウン リスト	ネットワーク要素が属するポッドを選択します。

名前	説明
[デバイス カテゴリ（Device Category）] ドロップダウン リスト	このネットワーク要素のデバイス カテゴリを選択します。たとえば [F5 ロード バランサ（F5 Load Balancer）] を選択します。
[デバイスIP（Device IP）] フィールド	このデバイスの IP アドレス。
[プロトコル（Protocol）] ドロップダウン リスト	使用されるプロトコルを選択します。リストには次の内容が含まれます。 • Telnet • SSH • HTTP • HTTPS （注） F5 ロード バランサ デバイスを使用する場合、HTTP および HTTPS のみを選択できます。
[ポート（Port）] フィールド	使用するポート番号。
[ログイン（Login）] フィールド	ログイン名。
[パスワード（Password）] フィールド	ログイン名に関連付けられるパスワード。

ステップ 5 [送信（Submit）] をクリックします。

F5 ロード バランサの追加が、システム タスクのインベントリ収集のトリガーとなります。[システムのタスク（System Tasks）] 画面で設定されるポーリング間隔でインベントリ収集の頻度を指定します。

次の作業

仮想サーバを変更または編集するには、サーバを選択して [変更（Modify）] をクリックします。仮想サーバを削除するには、サーバを選択して [削除（Delete）] をクリックします。

F5 ロード バランシング ポリシーの追加

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [F5 ロード バランサ ポリシー（F5 Load Balancer Policies）] をクリックします。

ステップ 3 [（+）ポリシーの追加（(+) Add Policy）] をクリックします。

ステップ 4 [F5 ロード バランサ ポリシーの追加（Add F5 Load Balancer Policy）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	F5 ロード バランサ アプリケーション ポリシーに割り当てる名前。
[ポリシーの説明（Policy Description）] フィールド	このポリシーの説明。
[ロード バランサ アカウント タイプ（Load Balancer Account Type）] ドロップダウン リスト	[物理（Physical）] を選択します。
[F5 アカウントの選択（Select F5 Account）] フィールド	[F5 アカウントの選択（Select F5 Account）] を展開して、使用可能なリストから [F5 ロード バランサ（F5 load balancer）] アカウントを選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

次の作業

仮想インフラストラクチャ ポリシーを作成します。

F5 ロード バランシング仮想インフラストラクチャ ポリシーの追加

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [仮想インフラストラクチャ ポリシー（Virtual Infrastructure Policies）] をクリックします。

ステップ 3 [ポリシーを追加（+）（Add Policy (+)）] をクリックします。

ステップ 4 [仮想インフラストラクチャ ポリシー仕様（Virtual Infrastructure Policy Specification）] 画面で、次のフィールドに入力します。

名前	説明
[テンプレート名（Template Name）] フィールド	ポリシーの一意の名前。
[テンプレートの説明（Template Description）] フィールド	このポリシーの説明。
[コンテナ タイプ（Container Type）] ドロップダウン リスト	[フェンスド仮想（Fenced Virtual）] をコンテナ タイプとして選択します。
[仮想アカウントの選択（Select Virtual Account）] ドロップダウン リスト	仮想インフラストラクチャ ポリシーを適用する仮想アカウントを選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [仮想インフラストラクチャ ポリシー：フェンシング ゲートウェイ（Virtual Infrastructure Policy - Fencing Gateway）] 画面で、次のフィールドに入力します。

名前	説明
[ゲートウェイが必要（Gateway Required）] チェック ボックス	ゲートウェイ ポリシーを選択する場合は、このチェック ボックスをオンにします。選択しない場合は、[次へ（Next）] をクリックします。
[ゲートウェイ ポリシーの選択（Select Gateway Policy）] ドロップダウン リスト	[ゲートウェイが必要（Gateway Required）] チェック ボックスをオンにすると、このフィールドで、仮想インフラストラクチャ ポリシーに対してゲートウェイ ポリシーを選択できます。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [仮想インフラストラクチャ ポリシー：フェンシング ロード バランシング（Virtual Infrastructure Policy - Fencing Load Balancing）] 画面で、次のフィールドに入力します。

名前	説明
[F5 ロード バランサが必要（F5 Load Balancer Required）] チェックボックス	仮想インフラストラクチャ ポリシーに対して F5 ロード バランシングを選択するには、このチェック ボックスをオンにします。
[F5 ロードバランサ ポリシーの選択（Select F5 Load Balancer Policy）] ドロップダウン リスト	[F5 ロード バランサが必要（F5 Load Balancer Required）] チェック ボックスをオンにすると、このフィールドで F5 ロードバランシング ポリシーを選択できます。

ステップ 9 [次へ（Next）] をクリックして、設定の概要を表示します。

ステップ 10 [送信（Submit）] をクリックします。

次の作業

階層化アプリケーション ゲートウェイ ポリシーを設定します。

階層化アプリケーション ゲートウェイ ポリシーの作成

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [階層型アプリケーションのゲートウェイ ポリシー（Tiered Application Gateway Policies）] をクリックします。

ステップ 3 [（+）ポリシーの追加（(+) Add Policy）] をクリックします。

ステップ 4 [ポリシー仕様（Policy Specification）] 画面で、次のフィールドに値を入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	F5 ロード バランサ階層化アプリケーション ゲートウェイ ポリシーに割り当てる名前。
[ポリシーの説明（Policy Description）] フィールド	このポリシーの説明。
[ゲートウェイ タイプ（Gateway Type）] ドロップダウン リスト	ゲートウェイ タイプを選択します。
[仮想アカウントの選択（Select Virtual Account）] ドロップダウン リスト	コンテナを展開するクラウド アカウントを選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ゲートウェイ - Linux（Gateway - Linux）] 画面で、Linux ゲートウェイ タイプの次のフィールドに入力します（該当する場合）。

名前	説明
[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision gateway VM using Content Library template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VMイメージテンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ テンプレートを使用したゲートウェイ VM のプロビジョニング（Provision gateway VM using Content Library template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。
[ゲートウェイの VM イメージ（VM Image for the Gateway）] ドロップダウン リスト	このフィールドは、[コンテキスト ライブラリ テンプレートを使用したゲートウェイ VM のプロビジョニング（Provision gateway VM using Content Library template）] チェック ボックスがオフの場合にのみ表示されます。リストからゲートウェイの VM イメージを選択します。
[仮想 CPU の数（Number of Virtul CPUs）] フィールド	ポリシーに従って許可される仮想 CPU の数。
[メモリ（Memory）] ドロップダウン リスト	メモリのサイズを選択します。
[CPU 予約（MHz）（CPU Reservation in MHz）] フィールド	ポリシーに従って予約される CPU の数。
[メモリ予約（MB）（Memory Reservation in MB）] フィールド	ポリシーに対して予約されるメモリの最大量（MB 単位）。
[テンプレート用の root ログイン（Root Login for the Template）] フィールド	テンプレートにアクセスするための root ログイン名。
[テンプレート用の root パスワード（Root password for the Template）] フィールド	テンプレートにアクセスするための root パスワード。
[ゲートウェイ パスワード共有のオプション（Gateway Password Sharing Option）] ドロップダウン リスト	ゲートウェイ VM の root パスワードをエンドユーザと共有する場合とその方法。

ステップ 7 [ポリシー仕様（Policy Specification）] 画面で、Cisco ASA ゲートウェイ タイプの次のフィールドに入力します。

名前	説明
[ユニファイド ファブリックの使用（Use Unified Fabric）] チェック ボックス	ユニファイド ファブリックを使用するには、このボックスをオンにします。
[デバイスの選択（Select Device）] ドロップダウン リスト	Cisco ASA デバイスを選択します。
[外部インターフェイス（Outside Interface）] ドロップダウン リスト	Cisco ASA デバイスの外部インターフェイスを選択します。
[外部インターフェイスの IP アドレス（Outside Interface IP Address）] フィールド	このフィールドは、[ユニファイド ファブリックの使用（Use Unified Fabric）] チェック ボックスがオフになっている場合にのみ表示されます。外部インターフェイスの IP アドレス。
[外部インターフェイスの VLAN ID（Outside Interface VLAN ID）] フィールド	このフィールドは、[ユニファイド ファブリックの使用（Use Unified Fabric）] チェック ボックスがオフになっている場合にのみ表示されます。外部インターフェイスに関連付けられている VLAN ID。
[内部インターフェイス（Inside Interfaces）] フィールド	リストから内部インターフェイスを選択します。

ステップ 8 [ポリシー仕様（Policy Specification）] 画面で、Cisco ASAv ゲートウェイ タイプの次のフィールドに入力します。

名前	説明
[ユニファイド ファブリックの使用（Use Unified Fabric）] チェック ボックス	ユニファイド ファブリックを使用するには、このボックスをオンにします。
[ASAv OVF] フィールド	テーブルから Cisco ASAv デバイスの OVF ファイルを選択するには、このチェック ボックスをオンにします。

名前	説明
[ASAv ポリシー（ASAv Policy）] フィールド	テーブルから ASAv 展開ポリシーを選択するには、このチェック ボックスをオンにします。この展開ポリシーは、事前に [ポリシー（Policies）] > [仮想/ハイパーバイザ ポリシー（Virtual/Hypervisor Policies）] > [サービスの提供（Service Delivery）] > [ASAv 展開ポリシー（ASAv Deployment Policy）] を選択して作成します。
[外部インターフェイス（Outside Interface）] フィールド	テーブルから外部インターフェイスを選択するには、このチェック ボックスをオンにします。
[内部インターフェイス（Inside Interfaces）] フィールド	テーブルから内部インターフェイスを選択するには、このチェック ボックスをオンにします。[ユニファイド ファブリックの使用（Use Unified Fabric）] チェック ボックスをオンにすると、ドロップダウン リストから内部インターフェイスを選択できます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 設定の概要を表示したら、[送信（Submit）] をクリックします。

アプリケーション コンテナ テンプレートの作成

（注） この手順は、テンプレートを更新する手順をキャプチャしません。テンプレートを変更した場合は、そのテンプレートから新たに作成されたコンテナにのみテンプレートが適用されます。このテンプレートでは、さまざまなネットワーク（DFA ネットワークを含む）で使用するアプリケーション コンテナを作成できます。

はじめる前に

仮想インフラストラクチャ ポリシーを作成します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 [テンプレートの追加（Add Template）] をクリックします。[アプリケーション コンテナ テンプレートの追加（Add Application Container Template）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[テンプレート名（Template Name）] フィールド	新しいテンプレートの名前。
[テンプレートの説明（Template Description）] フィールド	テンプレートの説明。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [アプリケーション コンテナ テンプレート：仮想インフラストラクチャ ポリシーの選択（Application Container Template - Select a Virtual infrastructure policy）] 画面が表示されます。次の選択を実行します。

名前	説明
[仮想インフラストラクチャ ポリシーの選択（Select Virtual Infrastructure Policy）] ドロップダウン リスト	コンテナを展開するためのポリシーを選択します。 （注） ロードバランシング ポリシーを選択します（以降のウィザード画面には、該当するロード バランシング情報が入力されます）。

ステップ 6 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：内部ネットワーク（Application Container Template - Internal Networks）] 画面が表示されます。
コンテナに複数のネットワークを追加して設定できます。これらのネットワークは、このテンプレートを使用してプロビジョニングされる VM に適用されます。

ステップ 7 [ネットワーク（Newtorks）] を展開し、[追加（+）（Add (+)）] アイコンをクリックしてネットワークを追加します。[ネットワークへのエントリの追加（Add Entry to Networks）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[ダイナミック ファブリック ネットワーク（Dynamic Fabric Network）] チェックボックス	オンにした場合は、デジタル ファブリック自動化（DFA）ネットワークで使用するアプリケーション コンテナが有効になります。

名前	説明
[ネットワーク名（Network Name）] フィールド	ネットワーク名。この名前はコンテナで一意である必要があります。
[ファブリック アカウント（Fabric Account）] ドロップダウン リスト	ファブリック アカウントを選択します。
[ネットワーク IP アドレス（Network IP Address）] フィールド	コンテナのネットワーク IP アドレス。
[ネットワークマスク（Network Mask）] フィールド	コンテナのネットワーク マスク アドレス。
[ゲートウェイ IP アドレス（Gateway IP Address）] フィールド	ネットワークのデフォルトゲートウェイの IP アドレス。この IP アドレスの NIC が GW VM に作成されます。

ステップ 8 [送信（Submit）] をクリックします。
この後、アプリケーション コンテナでプロビジョニングされる VM を追加して設定できます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [追加（+）（Add (+)）] アイコンをクリックして VM を追加します。[仮想マシンへのエントリの追加（Add Entry to Virtual Machines）] ダイアログ ボックスが表示されます。次のフィールドに入力します。

名前	説明
[VM名（VM Name）] フィールド	VM の名前。
[説明（Description）] フィールド	VM の説明。
[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VM イメージ テンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。

名前	説明
[VM イメージ（VM Image）] ドロップダウン リスト	このフィールドは、[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックスがオフになっている場合にのみ表示されます。展開する VM イメージを選択します。
[仮想 CPU の数（Number of Virtual CPUs）] ドロップダウン リスト	コンテナ内に許可できる仮想 CPU の数を選択します。
[メモリ（Memory）] ドロップダウン リスト	メモリのサイズを選択します。
[CPU予約(MHz)（CPU Reservation (MHz)）] フィールド	VM 用に予約する CPU。
[メモリ予約(MB)（Memory Reservation (MB)）] フィールド	VM のメモリ予約。
[ディスク サイズ（GB）（Disk Size (GB)）] フィールド	VM のカスタム ディスク サイズ。テンプレートのディスク サイズを使用するには、値に 0 を指定します。指定したディスク サイズで選択したイメージのディスク サイズが上書きされます。
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	VMのユーザ名とパスワードをエンドユーザと共有するためのオプションを選択します。[パスワードのリセット後に共有（Share after password reset）] または [共有テンプレート クレデンシャル（Share template credentials）] を選択した場合、エンドユーザは選択したテンプレートのユーザ名とパスワードを指定する必要があります。

名前	説明
[VM ネットワーク インターフェイス（VM Network Interfaces）] フィールド	[VM ネットワーク インターフェイス（VM Network Interfaces）] を展開して、[追加（+）（Add (+)）] をクリックして VM ネットワーク インターフェイスを追加します。別のネットワーク インターフェイスを追加する場合は、[追加（+）（Add (+)）] をクリックします。 新しいVMネットワークインターフェイスを追加するには、次のフィールドに入力します。 • [VM ネットワーク インター フェース名（VM Network Interface Name）] フィールド：VM ネットワーク インターフェイスの名前。 • [ネットワークの選択（Select the Network）] ドロップダウン リスト：ネットワークを選択します。 • [アダプタ タイプ（Adapter Type）] ドロップダウン リスト：アダプタのタイプを選択します。 • [IP アドレス（IP Address）] フィールド：ネットワークの IP アドレス。
[最大数量（Maximum Quantity）] フィールド	作成後にこのコンテナで追加可能なインスタンスの最大数を示します。
[初期数量（Initial Quantity）] フィールド	コンテナを作成する際にプロビジョニングする VM インスタンスの数を示します。

ステップ 11 [送信（Submit）] をクリックします。

ステップ 12 [アプリケーション コンテナ テンプレート：F5 アプリケーション サービス（Application Container Template - F5 Application Service）] 画面で、次のフィールドに入力します。

名前	説明
[アプリケーション サービス名（Application Service Name）] フィールド	アプリケーション サービスの名前。
[テンプレート（Template）] フィールド	テンプレートを選択します。
[Ipアドレス（IP Address）] フィールド	ネットワークの IP アドレス。

名前	説明
[仮想 サーバ IP（Virtual Server IP）] フィールド	仮想サーバの IP アドレス。
[仮想 サーバ ポート（Virtual Server Port）] フィールド	仮想サーバで使用されるポート。
[仮想サーバの FQDN 名（FQDN names of Virtual Server）] フィールド	FQDN 仮想サーバの名前。 （注） 各 FQDN 名をカンマで区切ります。
[ノード リスト（Nodes List）] ドロップダウン リスト	ノードのリストからノードを選択して、[送信（Submit）] をクリックします。ノードのリストに、仮想サーバに関連付けるノードが表示されていない場合は、以下のようにします。 • [追加（+）（Add (+)）] アイコンをクリックしてノードを追加します。[ノード リストへのエントリの追加（Add Entry to Nodes list）] ダイアログボックスが表示されます。 • ノード IP アドレス、ポート、および接続制限を指定した後、[送信（Submit）] をクリックします。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 [アプリケーション コンテナ テンプレート：展開ポリシー（Application Container Template - Deployment Policies）] 画面が表示されます。
VM のプロビジョニングに必要なコンピューティング、ストレージ、ネットワーク、システムポリシー、コスト モデルを選択する必要があります。ポリシーとは、アプリケーション コンテナ内で新しい VM を（システム リソースの可用性に基づいて）どこにどのようにプロビジョニングするかを決定するルールの集まりです。

- ネットワーク ポリシーは、仮想ファイアウォール（コンテナ ゲートウェイ）の外部インターフェイスの展開にのみ使用されます。
- 選択したネットワーク ポリシー内のポートグループは、ゲートウェイ VM がプロビジョニングされるホスト上に存在する必要があります。
- ネットワーク ポリシーは、スタティック *IP* プールまたは *DHCP* のいずれかを使用できます。ただし、コンテナ タイプ が VSG の場合は、ネットワーク ポリシーはスタティック IP プールのみを使用する必要があります。VSG VM には IP アドレスが入力として必要です。現在、VSG VM の展開に DHCP を指定するプロビジョニングはありません。
- プロビジョニング済みの VM（コンテナ ゲートウェイ）のネットワーク アダプタ設定は、テンプレートの設定と同様である必要があります。このアプリケーション コンテナに使用されるネットワーク

ポリシーで、[テンプレートからアダプタをコピーする（Copy Adapter from Template）] チェックボックスをオンにする場合としない場合があります。

次のフィールドに入力します。

名前	説明
[コンピューティング ポリシー（Compute Policy）] ドロップダウン リスト	コンピューティング ポリシーを選択します。
[ストレージ ポリシー（Storage Policy）] ドロップダウン リスト	ストレージ ポリシーを選択します。
[ネットワークポリシー（Network Policy）] ドロップダウン リスト	ネットワーク ポリシーを選択します。
[システム ポリシー（Systems Policy）] ドロップダウン リスト	システム ポリシーを選択します。
[コスト モデル（Cost Model）] ドロップダウン リスト	コスト モデルを選択します。

ステップ 15 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：オプション（Application Container Template - Options）] 画面が表示されます。
セルフサービス エンド ユーザの特定の権限を有効または無効にするオプションを選択できます。

次のフィールドに入力します。

名前	説明
[VM のセルフサービス電源管理の有効化（Enable Self-Service Power Management of VMs）] チェックボックス	オンにした場合は、VM のセルフサービス電源管理が有効になります。
[VM のセルフサービス サイズ変更の有効化（Enable Self-Service Resizing of VMs）] チェック ボックス	オンにした場合は、VM のセルフサービスのサイズ変更が有効になります。
[セルフサービス VM スナップショット管理の有効化（Enable Self-Service VM Snapshot Management）] チェックボックス	オンにした場合は、セルフサービス VM スナップショット管理が有効になります。

名前	説明
[VNC ベースのコンソール アクセスの有効化（Enable VNC Based Console Access）] チェック ボックス	オンにした場合は、VNC ベースのコンソール アクセスが有効になります。
[コンテナのセルフサービス削除の有効化（Enable Self-Service Deletion of Containers）] チェック ボックス	オンにした場合は、コンテナのセルフサービス削除が有効になります。
[テクニカル サポート用の電子メール（Technical Support Email Addresses）] フィールド	テクニカルサポートの電子メールアドレス。コンテナの展開後に、このフィールドに入力した 1 つ以上の電子メールアドレスに詳細なテクニカル電子メールが送信されます。

ステップ 16 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：セットアップ ワークフロー（Application Container Template - Setup Workflows）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[コンテナ セットアップ ワークフロー（Container Setup Workflow）] ドロップダウン リスト	[コンテナ セットアップ ワークフロー（Container Setup Workflow）] を展開して、アプリケーション コンテナを確立するワークフローをオンにします。

ステップ 17 [次へ（Next）] をクリックし、アプリケーション コンテナ テンプレートの作成を実行して、[概要（Summary）] 画面を表示します。

（注） ロード バランシング基準の概要のエントリが含まれていることを確認します。

ステップ 18 [送信（Submit）] をクリックします。

テンプレートを使用したアプリケーション コンテナの作成

アプリケーションコンテナテンプレートを作成した後は、テンプレート管理機能を使用して他のアプリケーション コンテナを作成できます。VSG 環境で使用するテンプレートを作成する場合は、VSG 用アプリケーション テンプレートの作成, （57 ページ）を参照してください。

（注） アプリケーション コンテナは、そのネットワークに固有の VLAN を使用する必要があります。VLAN を使用する（VMware）vCenter に他にポート グループがない場合もあります。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 テンプレートを選択します。

ステップ 4 [コンテナの作成（Create Container）] をクリックします。

ステップ 5 [テンプレートからのコンテナの作成（Create Container from Template）] 画面で、次のフィールドに入力します。

（注） プライベート ネットワーク名、サービス名、およびコンテナ名を組み合わせた長さは最大 32 文字にする必要があります。

名前	説明
[コンテナ名（Container Name）] フィールド	コンテナの名前。この名前は一意である必要があります。
[コンテナ ラベル（Container Label）] フィールド	コンテナのラベル。
[テナント（Tenant）] フィールド	[テナント（Tenant）] を展開し、使用するテナントを選択して [検証（Validate）] をクリックします。
[プライベート ネットワーク名（Private Network Name）] フィールド	このフィールドは、プライベート ネットワークがあるテナントが選択されている場合にのみ表示されます。[選択（Select）] をクリックして、選択したテナントに関連付けられたプライベート ネットワークの名前を選択します。
[ネットワーク スループット（Network Throughput）] ドロップダウン リスト	プライベート ネットワークのスループットを選択します。 （注） このフィールドは、プライベート ネットワークがあるテナントではサポートされていません。
以下のフィールドは、[テナント（Tenant）] フィールドでプライベート ネットワークを持つテナントが選択されている場合にのみ表示されます。つまり、これらのフィールドは、内部階層ごとにさまざまな VM インスタンスをサポートする能力を持つテナントに対してのみ表示されます。	

名前	説明
[VM ラベル プレフィックスのカスタマイズ（VM Labels Prefix Customization）] フィールド	各階層の VM のカスタマイズされたプレフィックス名。 （注） プレフィクス名は、管理者が各階層のプレフィクスを定義する、アプリケーション プロファイルの VM ラベル プレフィクスから取得されます。アプリケーション コンテナの展開時に、アプリケーション プロファイルで定義されている内容からプレフィックスを更新できます。
WEB/APP/DB 階層などの内部階層の最大数は、次のフィールドでは例としてのみ示します。アプリケーション プロファイル内の定義に従い、4 つ以上の階層がある場合があります。フィールドの数は、アプリケーション プロファイルの一部として定義されている内部階層番号に基づいて表示されます。	
[<WEB> 階層の最大数（Maximum Quantity for <WEB> tier）] フィールド	<Web> 階層内の VM インスタンスの最大数。
[<APP>階層の最大数（Maximum Quantity for <APP> tier）] フィールド	<アプリケーション> 階層内の VM インスタンスの最大数。
[<DB> 階層の最大数（Maximum Quantity for <DB> tier）] フィールド	<データベース> 階層内の VM インスタンスの最大数。
（注） アプリケーション プロファイルに指定された内部階層名は動的にフェッチされ、コンテナ作成アクション中にフィールドに表示されます。コンテナ作成アクション中にいずれかの内部階層の最大数量が変更された場合、この値は、階層ごとのサブネットを割り当てるためのホストサイズの最大数と見なされます。	
以下のフィールドは、[テナント（Tenant）] フィールドでプライベート ネットワークを持つテナントが選択されている場合には表示されません。	
[ディザスタ リカバリの有効化（Enable Disaster Recovery）] チェックボックス	コンテナにディザスタリカバリ サービスを有効にするには、このチェックボックスをオンにします。
[リソースの制限の有効化（Enable Resource Limits）] チェック ボックス	vCPU の数、メモリ、最大ストレージ、およびコンテナのサーバの最大数を指定するには、このチェック ボックスをオンにします。
[ネットワーク管理の有効化（Enable Network Management）] チェックボックス	コンテナにネットワーク管理サービスを有効にするには、このチェックボックスをオンにします。 （注） このフィールドは、APIC デバイス パッケージによって管理されているレイヤ 4 およびレイヤ 7 デバイスのみに適用されます。

名前	説明
[階層ラベルのカスタマイズ（Tier Label Customization）] 領域	このフィールドは、APIC コンテナにのみ表示されます。階層ラベルのカスタマイズされた名前。

ステップ 6 [送信（Submit）] をクリックします。[送信結果（Submit Result）] ダイアログボックスが表示されます。

（注） [送信結果（Submit Result）] ダイアログ ボックスに表示されたサービス リクエストを書き留めてください。

ステップ 7 [OK] をクリックします。

（注） サービス リクエストの詳細情報を表示することで、コンテナ作成の経過を表示できます。

ステップ 8 [アプリケーション コンテナ（Application Containers）] タブをクリックします。
[アプリケーション コンテナ（Application Containers）] ペインに新しいコンテナが表示されます。

サービス リクエストの開始

（注） F5 ロード バランシングは、フェンスド仮想コンテナのみでサポートされています。

ステップ 1 [組織（Organizations）] > [サービス リクエスト（Service Requests）] を選択します。

ステップ 2 [高度なフィルタ（Advanced Filter）] ボタン（インターフェイスの右隅）をクリックします。

ステップ 3 [列で検索（Search in Column）] ドロップダウン リストから、[リクエスト タイプ（Request Type）] を選択します。

ステップ 4 [テキスト（Text）] フィールドに **Advanced** を入力します。

ステップ 5 [フィルタ（Filter）] をクリックします。

ステップ 6 [フェンスド コンテナ セットアップ（Fenced Container Setup）] ワークフローをダブルクリックします。

第 5 章

フェンスド仮想コンテナの設定

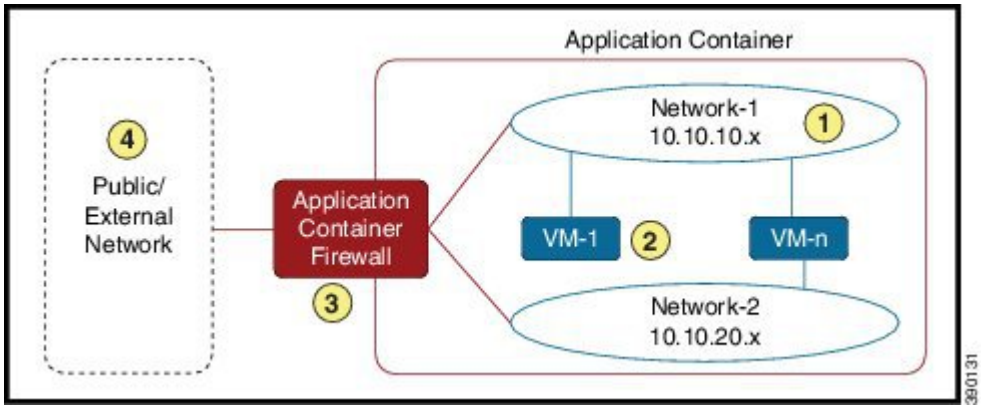
この章は、次の項で構成されています。

フェンスド仮想コンテナ

フェンスド仮想コンテナは、内部プライベート ネットワークを使用する仮想マシン（VM）の集合で、管理者によって指定されたルールに基づいて作成されます。フェンスド コンテナは、パブリックまたは外部クラウドのフェンシング ゲートウェイによって保護されている 1 つまたは複数の仮想マシンを持つことができます。Cisco UCS Director はフェンスド コンテナをサポートし、1 つ以上のフェンスド ネットワークと VM を使用するコンテナ テンプレートを定義できます。フェンスド コンテナをテンプレートから作成する場合は、Cisco UCS Director は自動で VM を導入し、

ネットワークとファイアウォールを設定します。Cisco UCS Director はレイヤ 2 変更の仮想スイッチと物理スイッチも自動で設定します。

図 *1*：フェンスド仮想コンテナ：サンプル



フェンスド コンテナを作成および管理するには、次の手順を実行します。

1 ゲートウェイ ポリシーの定義：ゲートウェイ ポリシーに、コンテナのゲートウェイ タイプと、ゲートウェイが展開されるクラウド アカウント（vCenter）のゲートウェイ タイプを定義する必要があります。

2 フェンスド コンテナ テンプレートの定義：テンプレートで次のタスクを実行する必要があります。

   - コンテナを作成するクラウド アカウントを定義します。
   - ネットワークの設定
   - コンテナの VM の追加
   - ポート マッピングと発信のアクセス制御リスト（ACL）の定義
   - ゲートウェイ ポリシー（以前に作成）の選択
   - VM プロビジョニングを定義する展開ポリシーの選択
   - コンテナのセルフサービス オプションの選択
   - ワークフローの選択（任意）

3 定義されたコンテナ テンプレートからのフェンスド コンテナの作成：フェンスド コンテナはステップ 2 で定義したテンプレートから作成されます。コンテナを作成するグループを選択する必要があります。

4 フェンスド コンテナ：フェンスド コンテナを作成すると、コンテナの電源管理、コンテナへの VM の追加、コンテナのクローニングまたは削除、VM 用コンテナのオープンとレポートの表示など、さまざまな管理アクションを実行できます。

フェンスド仮想コンテナの前提条件

以下に示すのは、フェンスド仮想コンテナ構成の前提条件です。

- 分散仮想ポートグループまたは分散仮想ポートグループ N1K をコンテナ VM リソース割り当てタスクで仮想ネットワーク タイプとして使用する場合は、コンテナ VM リソース割り当てタスクでプライマリ DVSwitch 名と代替 DVSwitch 名を必ず指定します。デフォルトでは、仮想ネットワーク ポートグループは、仮想ネットワーク タイプとして設定されます。

フェンスド仮想コンテナの制限

次に示すのは、フェンスド仮想コンテナの制限です。

- F5 ロード バランシングは、フェンスド仮想コンテナでサポートされます。

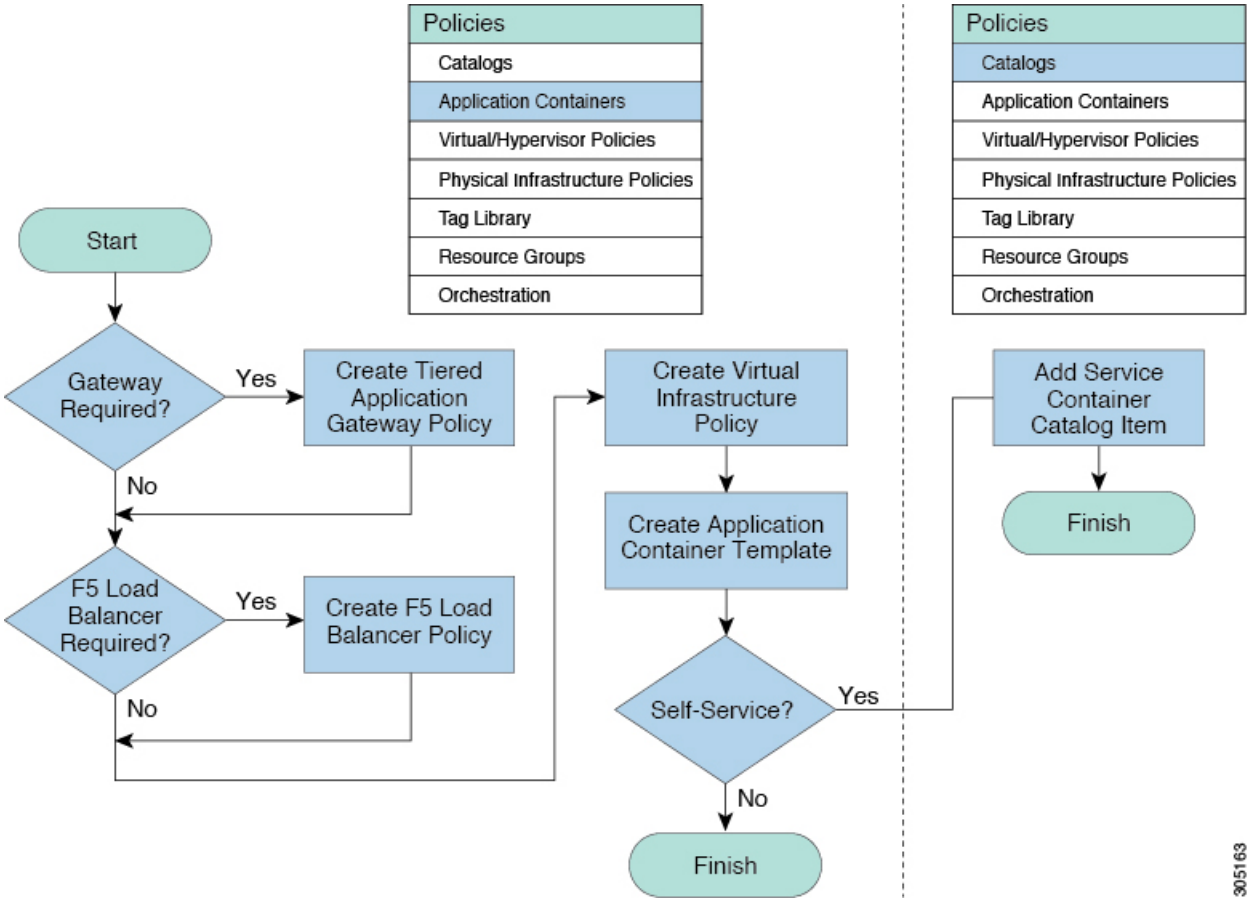
フェンスド仮想アプリケーションコンテナ作成のプロセス

次のプロセスは、Cisco UCS Director 内のフェンスド仮想アプリケーション コンテナの作成について説明しています。

1. ゲートウェイが必要な場合は、階層化アプリケーション ゲートウェイ ポリシーを作成します。
2. ロード バランサが必要な場合は、ロード バランサ ポリシーを作成します。
3. クラウド アカウント、コンテナのタイプ、および、該当する場合は仮想化アプリケーション ゲートウェイとロード バランサのポリシーを定義する仮想インフラストラクチャ ポリシーを作成します。
4. アプリケーション コンテナ テンプレートを作成します。
   a. ネットワークを追加します（アプリケーション階層ごとに 1 つのネットワーク）。
   b. 仮想マシンとベアメタル サーバを追加します。
   c. コンピューティング ポリシー、ストレージ ポリシー、ネットワーク ポリシー、およびシステム ポリシーを追加します。必要に応じて、コスト モデルも追加できます。
   d. エンドユーザ セルフサービス ポリシーを追加し、セルフサービス オプションを設定します。
   e. サービス要求の一部として提供サービスをユーザに提供するために必要なコンテナ セットアップ ワークフローを追加します。ワークフローでは、コンテナのタイプとプロビジョニングするアプリケーションを考慮する必要があります。
5. コンテナ テンプレートに基づいてコンテナを作成します。

図は、Cisco UCS Director 内でのフェンスド仮想アプリケーション コンテナ テンプレートの作成を示しています。

図 *2*：フェンスド仮想アプリケーション コンテナ テンプレートの作成プロセス



フェンスド仮想コンテナの仮想インフラストラクチャポリシーの作成

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [仮想インフラストラクチャ ポリシー（Virtual Infrastructure Policies）] をクリックします。

ステップ 3 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 4 [仮想インフラストラクチャ ポリシー仕様（Virtual Infrastructure Policy Specification）] ページで、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ポリシーの名前。

名前	説明
[ポリシーの説明（Policy Description）] フィールド	ポリシーの説明。
[コンテナ タイプ（Container Type）] ドロップダウン リスト	[フェンスド仮想（Fenced Virtual）] をコンテナ タイプとして選択します。
[仮想アカウントの選択（Select Virtual Account）] ドロップダウン リスト	仮想インフラストラクチャ ポリシーを適用する仮想アカウントを選択します。

ステップ 5 [次へ（Next）] をクリックし、ウィザードのプロンプトに従います。

ステップ 6 [仮想インフラストラクチャ ポリシー：フェンシング ゲートウェイ（Virtual Infrastructure Policy - Fencing Gateway）] 画面で、次のフィールドに入力します。

名前	説明
[ゲートウェイが必要（Gateway Required）] チェックボックス	ゲートウェイ ポリシーを選択する場合は、このチェック ボックスをオンにします。選択しない場合は、[次へ（Next）] をクリックします。
[ゲートウェイ ポリシーの選択（Select Gateway Policy）] ドロップダウン リスト	[ゲートウェイが必要（Gateway Required）] チェック ボックスをオンにすると、このフィールドで、仮想インフラストラクチャ ポリシーに対してゲートウェイ ポリシーを選択できます。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [仮想インフラストラクチャ ポリシー：フェンシング ロード バランシング（Virtual Infrastructure Policy - Fencing Load Balancing）] 画面で、次のフィールドに入力します。

名前	説明
[F5 ロード バランサが必要（F5 Load Balancer Required）] チェックボックス	仮想インフラストラクチャ ポリシーに対して F5 ロード バランシングを選択するには、このチェック ボックスをオンにします。
[F5 ロードバランサ ポリシーの選択（Select F5 Load Balancer Policy）] ドロップダウン リスト	[F5 ロード バランサが必要（F5 Load Balancer Required）] チェック ボックスをオンにすると、このフィールドで F5 ロードバランシング ポリシーを選択できます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [概要（Summary）] ページで [送信（Submit）] をクリックします。

次の作業

フェンスド仮想コンテナを作成するための、アプリケーションコンテナテンプレートを作成します。

フェンスド仮想コンテナ用のアプリケーション コンテナ テンプレートの作成

アプリケーション コンテナのテンプレートを作成するには、次の要素に関する情報を提供する必要があります。この情報を使用して、コンテナを作成します。

- 仮想アカウント（クラウド）
- ネットワークの設定
- VM の設定
- コンテナのセキュリティ
- ネットワーク、ストレージ、コンピューティング、およびコスト モデルのポリシーの選択
- [ゲートウェイが必要（Gateway Required）] チェック ボックスが有効になっている場合はゲートウェイ ポリシーの選択（任意）
- サービス エンド ユーザのオプション

はじめる前に

仮想インフラストラクチャ ポリシーを作成します。フェンスド仮想コンテナの仮想インフラストラクチャ ポリシーの作成, （34 ページ）を参照してください。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 [テンプレートの追加（Add Template）] をクリックします。[アプリケーション コンテナ テンプレート（Application Container Template）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[テンプレート名（Template Name）] フィールド	新しいテンプレートの名前。

名前	説明
[テンプレートの説明（Template Description）] フィールド	テンプレートの説明。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [アプリケーション コンテナ テンプレート：仮想インフラストラクチャ ポリシーの選択（Application Container Template - Select a Virtual infrastructure policy）] 画面で、[仮想インフラストラクチャ ポリシーの選択（Select Virtual Infrastructure Policy）] ドロップダウン リストから、フェンスド仮想コンテナ タイプに対して作成された仮想インフラストラクチャ ポリシーを選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [アプリケーション コンテナ テンプレート：内部ネットワーク（Application Container Template - Internal Networks）] 画面で、コンテナに対して複数のネットワークを追加および構成できます。これらのネットワークは、このテンプレートを使用してプロビジョニングされる VM に適用されます。

ステップ 8 [追加（+）（Add (+)）] をクリックしてネットワークを追加します。[ネットワークへのエントリの追加（Add Entry to Networks）] 画面で、次のフィールドに値を入力します。

名前	説明
[ネットワーク名（Network Name）] フィールド	コンテナの一意のネットワーク名を入力します。最大 128 文字を使用できます。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	ネットワーク タイプを選択します。
[情報ソース（Information Source）] ドロップダウンリスト	情報ソースを選択します。この属性の種類は次のとおりです。 • インライン • 静的プール
[VLAN ID 範囲（VLAN ID Range）] フィールド	VLAN ID の範囲を入力します。
[ネットワーク IP アドレス（Network IP Address）] フィールド	ネットワークの IP アドレス（たとえば、10.10.10.0）。内部ネットワークごとに一意のサブネットが選択されます。
[ネットワークマスク（Network Mask）] フィールド	ネットワーク マスク アドレス（たとえば、255.255.255.0）。
[ゲートウェイ IP アドレス（Gateway IP Address）] フィールド	ネットワークのデフォルト ゲートウェイの IP アドレス。この IP アドレスの NIC が GW VM に作成されます。

ステップ 9 [送信（Submit）] をクリックします。
この後、アプリケーション コンテナでプロビジョニングされる VM を追加して設定できます。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [アプリケーション コンテナ テンプレート：VM（Application Container Template - VMs）] で、[追加（+）（Add (+)）] をクリックして VM を追加します。[仮想マシンへのエントリの追加（Add Entry to Virtual Machines）] ダイアログ ボックスが表示されます。次のフィールドに入力します。

名前	説明
[VM名（VM Name）] フィールド	VM の名前。
[説明（Description）] フィールド	VM の説明。
[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VMイメージテンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。
[VM イメージ（VM Image）] ドロップダウン リスト	このフィールドは、[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックス がオフになっている場合にのみ表示されます。展開するイメージを選択します。
[リンク済み複製の使用（Use Linked Clone）] チェック ボックス	このチェック ボックスは、スナップショットを使用する VMテンプレートを選択した場合のみ有効です。高速でストレージ効率の高いプロビジョニングが可能なリンク クローン機能を使用して新しいVMを展開するには、このボックスをオンにします。

名前	説明
[スナップショット（Snapshot）] フィールド	このフィールドは、[リンク クローンの使用（Use Linked Clone）] チェック ボックスがオンになっている場合にのみ表示されます。[選択（Select）] をクリックして、リンク クローン機能を使用して新しいVMをプロビジョニングするために使用する必要があるスナップショットを選択します。
[仮想 CPU の数（Number of Virtual CPUs）] ドロップダウン リスト	VM に割り当てる仮想 CPU の数。
[メモリ（Memory）] ドロップダウン リスト	割り当てるメモリ（MB 単位）。
[CPU予約(MHz)（CPU Reservation(MHz)）] フィールド	VM 用に予約する CPU。
[メモリ予約(MB)（Memory Reservation (MB)）] フィールド	VM のメモリ予約。
[ディスク サイズ（GB）（Disk Size (GB)）] フィールド	VM のカスタム ディスク サイズ。テンプレートのディスク サイズを使用するには、値に 0 を指定します。指定したディスク サイズで選択したイメージのディスク サイズが上書きされます。
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	VMのユーザ名とパスワードをエンドユーザと共有する方法のオプションを選択します。[パスワードのリセット後に共有（Share after password reset）] または [共有テンプレート クレデンシャル（Share template credentials）] を選択した場合、エンドユーザは選択したテンプレートのユーザ名とパスワードを指定する必要があります。
[イメージからのネットワーク設定の使用（Use Network Configuration from Image）] チェックボックス	オンにした場合は、イメージからのネットワーク設定がプロビジョニング済みのVMに適用されます。
[VM ネットワーク インターフェイス（VM Network Interface）] フィールド	VMネットワーク インターフェイス情報を入力します。
[最大数量（Maximum Quantity）] フィールド	作成後にこのコンテナで追加可能なインスタンスの最大数。
[初期数量（Initial Quantity）] フィールド	コンテナを作成する際にプロビジョニングするVMインスタンスの数。

ステップ 12 [送信（Submit）] をクリックします。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 [アプリケーション コンテナ テンプレート：外部ゲートウェイ セキュリティ設定（Application Container Template - External Gateway Security Configuration）] 画面で、[追加（+）（Add (+)）] をクリックして、ポート マッピングを追加します。[ポート マッピングへのエントリの追加（Add Entry to Port Mappings）] 画面で、次のフィールドに入力します。

名前	説明
[プロトコル（Protocol）] ドロップダウン リスト	プロトコルを選択します。この属性の種類は次のとおりです。 • TCP • UDP
[マッピングされたポート（Mapped Port）] フィールド	マッピングされたポートを入力します。
[リモート IP アドレス（Remote IP Address）] フィールド	IP アドレスを入力します。
[リモート ポート（Remote Port）] フィールド	リモート ポート フィールドを入力します。

ステップ 15 [アプリケーション コンテナ テンプレート：外部ゲートウェイ セキュリティ設定（Application Container Template - External Gateway Security Configuration）] 画面で、[追加（+）（Add (+)）] をクリックして、アウトバウンド ACL を追加します。[アウトバウンド ACL へのエントリの追加（Add Entry to Outbound ACLs）] 画面で、次のフィールドに入力します。

名前	説明
[プロトコル（Protocol）] ドロップダウン リスト	プロトコルを選択します。この属性の種類は次のとおりです。 • IP • TCP • UDP • ICMP
[ネットワークの選択（Select the Network）] ドロップダウン リスト	ネットワークを選択します。
[送信元アドレス（Source address）] フィールド	送信元アドレスを入力します。

名前	説明
[接続先アドレス（Destination address）] フィールド	接続先アドレスを入力します。
[アクション（Action）] フィールド	アクションを選択します。次のいずれかを設定できます。 • 承認（Accept） • 削除（Drop） • 却下（Reject）

ステップ 16 [送信（Submit）] をクリックします。

ステップ 17 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：展開ポリシー（Application Container Template - Deployment Policies）] 画面が表示されます。
VMのプロビジョニングに必要なコンピューティング、ストレージ、ネットワーク、システムポリシー、コスト モデルを選択する必要があります。ポリシーとは、アプリケーション コンテナ内で新しい VM を（システム リソースの可用性に基づいて）どこにどのようにプロビジョニングするかを決定するルールの集まりです。

- ネットワーク ポリシーは、仮想ファイアウォール（コンテナ ゲートウェイ）の外部インターフェイスの展開にのみ使用されます。

  （注） コンテナのゲートウェイ タイプが CISCO ASAv の場合は、ネットワーク ポリシーによって最初に ASAv 管理インターフェイスが追加されてから、同じ順序で VM ネットワークが外部インターフェイスが追加されます。

- 選択したネットワーク ポリシー内のポートグループは、ゲートウェイ VM がプロビジョニングされるホスト上に存在する必要があります。
- ネットワーク ポリシーは、スタティック *IP* プールまたは *DHCP* のいずれかを使用できます。ただし、コンテナ タイプが VSG の場合は、ネットワーク ポリシーはスタティック IP プールのみを使用する必要があります。VSG VM には IP アドレスが入力として必要です。現在、VSG VM の展開に DHCP を指定するプロビジョニングはありません。
- プロビジョニング済みの VM（コンテナ ゲートウェイ）のネットワーク アダプタ設定は、テンプレートの設定と同様である必要があります。このアプリケーション コンテナに使用されるネットワーク ポリシーで、[テンプレートからアダプタをコピーする（Copy Adapter from Template）] チェックボックスをオンにする場合としない場合があります。

次のフィールドに入力します。

名前	説明
[コンピューティング ポリシー（Compute Policy）] ドロップダウン リスト	コンピューティング ポリシーを選択します。

名前	説明
[ストレージ ポリシー（Storage Policy）] ドロップダウン リスト	ストレージ ポリシーを選択します。
[ネットワークポリシー（Network Policy）] ドロップダウン リスト	ネットワーク ポリシーを選択します。
[システム ポリシー（Systems Policy）] ドロップダウン リスト	システム ポリシーを選択します。
[コスト モデル（Cost Model）] ドロップダウン リスト	コスト モデルを選択します。

ステップ 18 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：オプション（Application Container Template - Options）] 画面が表示されます。
セルフサービス エンド ユーザの特定の権限を有効または無効にするオプションを選択できます。次のフィールドに入力します。

名前	説明
[エンドユーザ セルフサービス ポリシー（End User Self-Service Policy）] ドロップダウン リスト	エンドユーザのセルフサービス ポリシーを選択します。
[コンテナのセルフサービス削除の有効化（Enable Self-Service Deletion of Containers）] チェックボックス	オンにすると、このテンプレートを使用して作成したアプリケーション コンテナをエンドユーザが削除できるようになります。
[VNC ベースのコンソール アクセスの有効化（Enable VNC Based Console Access）] チェックボックス	オンにすると、コンテナ ホスト上の VM に VNC アクセスが許可されます。
[テクニカル サポート用の電子メール アドレス（Technical Support Email Addresses）] フィールド	電子メール アドレスのカンマ区切りのリストを入力します。自動化された通知がこれらの電子メールに送信されます。

ステップ 19 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：セットアップ ワークフロー（Application Container Template - Setup Workflows）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[コンテナ セットアップ ワークフロー（Container Setup Workflow）] ドロップダウン リスト	コンテナセットアップ ワークフローを選択します。デフォルトでは、ワークフローは選択されません。このコンテナに選択したゲートウェイ タイプが [Linux] で、コンテナに関連付けられたネットワーク ポリシーで [仮想マシン ポートグループ（Virtual Machine Portgroup）] を選択した場合は、このステップをスキップできます。コンテナ ゲートウェイとして CISCO ASA を選択するか、ネットワーク ポリシーとして [分散型仮想ポートグループ（Distributed Virtual Portgroup）] を選択した場合にのみ、特定のワークフローを選択する必要があります。CISCO ASAv ゲートウェイ タイプの場合は、[ASAv ゲートウェイを使用するアプリケーション コンテナ（Application Container with ASAv Gateway）] を選択します。 （注） アプリケーション コンテナ テンプレートを作成するためのタスクを開始する前に、いくつかの前提条件のステップを実行する必要があります。

ステップ 20 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：概要（Application Container Template - Summary）] 画面が表示され、現在の設定が示されます。

ステップ 21 [送信（Submit）] をクリックし、アプリケーション コンテナ テンプレートの作成を実行します。

次の作業

カスタム ワークフロータスクを使用して、テンプレートの特定の側面をカスタマイズできます。フェンスド仮想コンテナ用カスタム ワークフローの作成，（43 ページ）を参照してください。

フェンスド仮想コンテナ用カスタム ワークフローの作成

（注） ワークフローを実行するためのオーケストレーションの使用方法の詳細については、『Cisco UCS Director Orchestration Guide』を参照してください。

- **ゲートウェイ タイプ**：**CISCO ASA**：コンテナのゲートウェイ タイプが CISCO ASA の場合は、使用可能なワークフローのリストから [ASA ゲートウェイを使用するアプリケーション

コンテナ（Application Container with ASA Gateway）] を特に選択する必要があります。これを選択するために、ワークフローを検索してチェックボックスを確認することができます。

- **分散型仮想ポートグループ**：コンテナに関連付けられたネットワーク ポリシーで [分散型仮想ポートグループ（Distributed Virtual Portgroups）] を選択した場合は、次の手順を手動で実行する必要があります。

  1. [仮想ネットワーク タイプ（Virtual Network Type）] を選択し、名前を入力します。これは、コンテナに関連付けられたワークフローで必要になります。
  2. 特定のワークフローを選択します。このタイプのワークフローは、コンテナに関連付けたゲートウェイ タイプによって異なります。Linux ゲートウェイの場合は、[アプリケーション コンテナのセットアップ（Application Container Setup）] ワークフローを選択します。CISCO ASA ゲートウェイ タイプ場合は、[ASA ゲートウェイを使用するアプリケーション コンテナ（Application Container with ASA Gateway）] を選択します。
  3. Cisco UCS Director オーケストレーション アプリケーションに移動し、[ワークフロー デザイナ（Workflow Designer）] ページでワークフローを編集して、必要なワークフローを編集または複製します。
  4. ワークフローのウィンドウで、[コンテナ VM リソースの割り当て（Allocate Container VM Resources）] タスクをダブルクリックします。
  5. 必要なネットワーク タイプ（[分散型仮想ポートグループ（Distributed Virtual Portgroup）] または [分散型仮想ポートグループ N1K（Distributed Virtual Portgroup N1K）]）を選択します。
  6. プライマリ DVSwitch 名と代替 DVSwitch 名を指定します。
  7. [保存（Save）] をクリックし、ワークフローを保存します。

第 6 章

仮想セキュア ゲートウェイ アプリケーション コンテナの設定

この章は、次の項で構成されています。

仮想セキュア ゲートウェイ アプリケーション コンテナ

Cisco Virtual Secure Gateway（VSG）コンテナ タイプは、強化されたセキュリティを仮想環境で提供するために使用します。Cisco UCS Director を使用して、Prime Network Services Controller（PNSC）とともに、その内部ファイアウォール（Cisco Virtual Security Gateway）を設定できます。このファイアウォールは、設定後、アプリケーション コンテナに統合されます。

Cisco VSG は仮想ファイアウォール アプライアンスで、仮想データセンターおよびクラウド環境への信頼できるアクセスを提供します。Cisco VSG では、さまざまなセキュリティ プロファイルを持つ複数のテナント ワークロードの広範な組み合わせによって、仮想データセンターのプライベート クラウドまたはパブリック クラウドにおける共通のコンピューティング インフラストラクチャの共有を可能にします。1 つ以上の仮想マシン（VM）を固有の信頼ゾーンに割り当てることで、Cisco VSG は確立されたセキュリティ ポリシーを通じて信頼ゾーンへのアクセスを制御し、モニタするようにします。

Cisco VSG には次の利点があります。

- 信頼できるマルチテナント アクセス：マルチテナント（スケールアウト）環境で適用されたコンテキスト認識型セキュリティ ポリシーに基づいた、きめ細かいゾーンベースの管理およびモニタリングにより、法規制の遵守を強化し、監査を簡略化します。セキュリティ ポリシーはセキュリティ プロファイル テンプレートとして構成され、数多くの Cisco VSG にわたる管理と展開を簡略にします。

- 動的操作：セキュリティ テンプレートと信頼ゾーンの VM インストール時のオンデマンド プロビジョニング、トランスペアレント モビリティの強化、および VM のライブ マイグレーションとしてのモニタリングがさまざまな物理サーバで実行されます。
- 中断のない管理：セキュリティ チームとサーバ チームの分別管理により、コラボレーションを強化しながら、管理上のエラーを排除し、監査を簡略にします。

Cisco VSG は次を実行します。

- 業界規制への準拠の強化
- 仮想化環境の監査プロセスを簡略化します。
- 仮想データセンターか、プライベート/パブリック クラウド コンピューティング環境かにかかわらず、幅広い仮想化されたワークロード セットを共有コンピューティング インフラストラクチャ上の複数のテナントに安全に展開して、コストを削減します。

仮想セキュリティ ゲートウェイ アプリケーション コンテナの前提条件

以下に示すのは、VSG コンテナ設定の前提条件です。

- コンテナ VM リソースの割り当てタスクを実行する場合、デフォルトの仮想ネットワーク タイプは、VSG コンテナの分散仮想ポートグループ N1K です。VSG コンテナのプライマリ DVSwitch 名は必ず変更します。

仮想セキュリティ ゲートウェイ アプリケーション コンテナの制限

VSG アプリケーション コンテナの作成プロセス

PNSC アカウントの追加

PNSC は、Cisco 仮想サービスのデバイスおよびセキュリティ ポリシーを一元管理できる仮想アプライアンスで、Red Hat Enterprise Linux に基づいています。マルチテナント操作用に設計された PNSC は、シームレスで、拡張可能な自動化中心の管理を仮想データセンター環境およびクラウド環境で実現します。PNSC は基本的にセキュリティ コンポーネント（ファイアウォール）を VSG およびアプリケーション コンテナに提供し、VM を互いに分離します。PNSC は、管理者がシスコ仮想サービスの一元管理を Cisco UCS Director を通じて実行できるようにします。

（注） PNSC は特定のポッドに関連付けられていません。

ステップ 1 [管理（Administration）] > [物理アカウント（Physical Accounts）] を選択します。

ステップ 2 [物理アカウント（Physical Accounts）] ページで [マルチドメイン マネージャ（Multi-Domain Managers）] をクリックします。

ステップ 3 [追加（Add）]（+）をクリックします。

ステップ 4 [アカウントの追加（Add Account）] 画面で、次のフィールドに入力します。

名前	説明
[アカウントタイプ（Account Type）] フィールド	アカウント タイプとして PNSC を選択し、[送信（Submit）] をクリックします。
[アカウント名（Account Name）] フィールド	マルチドメイン アカウント名。
[説明（Description）] フィールド	マルチドメイン アカウントの説明。
[サーバ管理（Server Management）] ドロップダウン リスト	ドロップダウン リストから、[すべてのサーバ（All Servers）] または [選択したサーバ（Selected Servers）] を選択し、それに応じてサーバを管理します。
[サーバアドレス（Server Address）] フィールド	PNSC サーバの IP アドレス。
[クレデンシャル ポリシーの使用（Use Credential Policy）] チェック ボックス	手動で情報を入力する代わりに、このアカウントのクレデンシャル ポリシーを使用する場合は、このチェック ボックスをオンにします。
[クレデンシャルポリシー（Credential Policy）] ドロップダウン リスト	[クレデンシャルポリシーの使用（Use Credential Policy）] チェック ボックスをオンにした場合は、このドロップダウン リストから使用するクレデンシャル ポリシーを選択します。 このフィールドが表示されるのは、クレデンシャル ポリシーの使用を選択した場合のみです。
[ユーザ ID（User ID）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。アカウントにアクセスするユーザ ID。

名前	説明
[パスワード（Password）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。ユーザ名に関連付けられたパスワードです。
[共有秘密パスワード（Shared Secret Password）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。アカウントの事前共有秘密キー。
[通信タイプ（Transport Type）] ドロップダウン リスト	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェック ボックスがオフになっている場合にのみ表示されます。次の転送タイプを選択します。 • HTTP：標準プロトコル。 • HTTPS：標準セキュア プロトコル。
[ポート（Port）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。ポート番号（転送タイプに基づく）。
[連絡先の電子メール（Contact Email）] フィールド	このアカウントを使用する管理者または個人の電子メール アドレス。
[ロケーション（Location）] フィールド	アカウントと関連付けられたデバイスの場所。

ステップ 5 [送信（Submit）] をクリックします。

PNSC レポートの表示

PNSC アカウントを作成後に、Cisco UCS Director を使用して関連レポートを表示できます。

[物理（Physical）] > [ネットワーク（Network）] メニューから、次のレポートを使用できます。

- 要約
- Tenants
- vDC

- [vApps]
- [PNSC ファイアウォール ポリシー（PNSC Firewall Policy）]
- [VM マネージャ（VM Manager）]
- Clients
- [HA ID 使用状況レポート（HA ID Usage Report）]

ステップ 1 [物理（Physical）] > [ネットワーク（Network）] を選択します。

ステップ 2 [マルチ ドメイン マネージャ（Multi-domain Manager）] を展開します。
マルチドメイン マネージャのアカウントに追加された PNSC アカウントを表示できます。

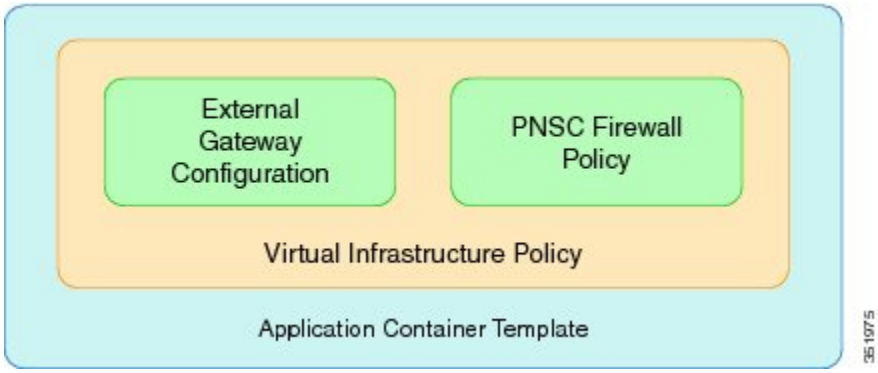
ステップ 3 PNSC のエントリをクリックし、使用可能なレポートを表示します。

アプリケーション コンテナへの VSG の統合

内部ファイアウォール（Cisco Virtual Security Gateway）に加えて PNSC を設定する Cisco UCS Director を使用し、アプリケーション コンテナに統合することができます。

統合プロセスには、いくつかの段階があります。

- Cisco UCS Director に OVA ファイルをアップロードします。
- PNSC ファイアウォール ポリシー（PNSC を使用したコンテナの作成に使用）を作成します。
- 仮想インフラストラクチャ ポリシーを作成します。使用する仮想アカウントと、プロビジョニングを行うコンテナのタイプをこのポリシーで定義します。
- アプリケーション コンテナ テンプレートを作成します。このテンプレートは、仮想インフラストラクチャ ポリシー、コンピューティング ポリシー、ストレージ ポリシー、およびネットワーク ポリシーをテンプレートへの入力として使用します。



OVA ファイルのアップロード

Cisco UCS Director では、管理者、グループ管理者、またはエンドユーザが事前に定義されたストレージの場所に OVA ファイルをアップロードできます。

（注） OVA ファイルをアップロードする権限のある唯一のタイプが、グループ管理者とエンドユーザです。

はじめる前に

適切なアクセス権があることを確認します。

ステップ 1 [管理（Administration）] > [統合（Integration）] を選択します。

ステップ 2 [統合（Integration）] ページで [ユーザ OVF 管理（User OVF Management）] をクリックします。

ステップ 3 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 4 [ファイルのアップロード（Upload File）] 画面で、次のフィールドに値を入力します。

名前	説明
[フォルダタイプ] ドロップダウン リスト	OVF ファイルを含んでいるフォルダのタイプ。次のいずれかを実行します。 • [パブリック（Public）] : パブリック ファイルのみを表示するには、このロールを選択します。 • [ユーザ（User）] : エンドユーザである場合は、このロールを選択します。エンド ユーザには広範囲の権限は付与されません。ユーザ ロールは第 1 レベルのサポートに適していますが、その主要な目的は問題の識別、修復、およびエスカレートにあります。 • [グループ（Group）] : このロールでは OVA ファイルを展開できます。
[ファイル名（File Name）] フィールド	アップロードし、表示する OVF ファイルの名前。
[ファイル（File）] フィールド	OVA ファイルをドロップするか、または [ファイルの選択（Select a File）] をクリックして、必要なファイルを参照して選択します。
[ファイルの説明（File Description）] フィールド	ファイルの説明（必要な場合）。

ステップ 5 [送信（Submit）] をクリックします。

PNSC ファイアウォール ポリシーの作成

ファイアウォール ポリシーを使用して Cisco VSG にネットワーク トラフィックを適用します。Cisco VSG は、PNSC の一環として使用される内部ファイアウォールです。Cisco VSG の主要コンポーネントはポリシー エンジンです。ポリシー エンジンは、Cisco VSG で受信するネットワーク トラフィックをフィルタする設定としてポリシーを使用します。

（注） PNSC ファイアウォール ポリシーはスタンドアロン モードと高可用性（HA）モードの両方をサポートします。

ステップ 1 [物理（Physical）] > [ネットワーク（Network）] を選択します。

ステップ 2 [マルチドメイン マネージャ（Multi-Domain Managers）] の下にリストされている [PNSC アカウント（PNSC accounts）] を展開します。

ステップ 3 ファイアウォール ポリシーを作成する PNSC アカウントをクリックします。

ステップ 4 [PNSC ファイアウォール ポリシー（PNSC Firewall Policy）] をクリックします。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [ファイアウォール ポリシーの作成（Create Firewall Policy）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ファイアウォール ポリシーの一意の名前。
[ポリシーの説明（Policy Description）] フィールド	ファイアウォール ポリシーの説明。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 PNSC ゾーンを展開し、[追加（+）（Add (+)）] をクリックしてゾーンを作成します。

ステップ 9 [PNSC ゾーンへのエントリの追加（Add Entry to PNSC Zones）] 画面で、次のフィールドに入力します。

名前	説明
[ゾーン名（Zone Name）] フィールド	ゾーンの一意の名前。
[ゾーンの説明（Zone Description）] フィールド	ゾーンの説明。
[ゾーン条件（Zone Conditions）]	[ゾーン条件（Zone Conditions）] を展開し、[追加（Add）] をクリックしてゾーン条件を追加します。

名前	説明
[属性タイプ（Attribute Type）] ドロップダウン リスト	属性のタイプとして [ネットワーク（Network）] または [VM] を選択します。
[属性名（Attribute Name）] ドロップダウン リスト	属性タイプに応じて異なるリストから属性を選択します。
[演算子（Operator）] ドロップダウン リスト	演算子のタイプを選択します。
[属性値（Attribute Value）] フィールド	選択した属性タイプに基づいて属性値を入力します。

ステップ 10 [送信（Submit）] をクリックします。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [PNSC ACL ルール（PNSC ACL Rules）] を展開し、[追加（+）（Add (+)）] をクリックして PNSC ACL ルール エントリを作成します。

ステップ 13 [PNSC ACL ルールへのエントリの追加（Add Entry to PNSC ACL Rules）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ACL ルールの名前。名前はコンテナに固有である必要があります。
[説明（Description）] フィールド	ACL ルールの説明。
[アクション（Action）] ドロップダウン リスト	ルールに許可されたアクションのタイプ。次のいずれかを実行します。 • [許可（Permit）] : 一致するトラフィックでの使用を許可します。 • [却下（Drop）] : 一致するトラフィックでの使用を却下します。 • [リセット（Reset）] : 一致するトラフィックでのルールをリセットします。
[条件一致基準（Condition Match Criteria）] ドロップダウン リスト	満たす必要がある条件を選択します。
[プロトコル/サービス（Protocol/Service）] ドロップダウン リスト	リストからプロトコルまたはサービスを選択します。

名前	説明
[任意のプロトコル（Any Protocol）] チェック ボックス	オンにした場合は、すべてのプロトコルにルールが適用されます。オフにした場合は、演算子（「equals」、「notequals」）およびプロトコル（たとえば、IP や EGP）を指定する必要があります。
[送信元の条件（Source Conditions）]	
[属性タイプ（Attribute Type）] ドロップダウン リスト	属性のタイプを選択します。
[属性名（Attribute Name）] ドロップダウン リスト	属性タイプに応じて異なるドロップ ダウン リストから、属性名を選択します。
[演算子（Operator）] ドロップダウン リスト	演算子のタイプを選択します。
[属性値（Attribute Value）] フィールド	属性値。
[送信先の条件（Destination Conditions）]	
[属性タイプ（Attribute Type）] ドロップダウン リスト	属性のタイプを選択します。
[属性名（Attribute Name）] ドロップダウン リスト	属性タイプに応じて異なるドロップ ダウン リストから、属性名を選択します。
[演算子（Operator）] ドロップダウン リスト	演算子のタイプを選択します。
[属性値（Attribute Value）] フィールド	属性値。

ステップ 14 [送信（Submit）] をクリックします。

ステップ 15 [次へ（Next）] をクリックします。

ステップ 16 [PNSC-VSG 設定（PNSC-VSG Configuration）] 画面で、次のフィールドに入力します。

名前	説明
[ユニファイド ファブリックの使用（Use Unified Fabric）] チェック ボックス	ユニファイドファブリックを使用するには、チェック ボックスをオンにします。
[VSG OVF URL] ドロップダウン リスト	Cisco UCS Director にアップロードされている OVA ファイルのリストから OVA ファイルを選択します。

名前	説明
[VSG の管理者パスワード（Admin Password for the VSG）] フィールド	VSG の管理者パスワード。
[ポリシー エージェントの共有シークレット パスワード（Policy agent shared secret Password）] フィールド	ポリシー エージェントの共有パスワード。
[展開モード（Deployment mode）] ドロップダウン リスト	展開のタイプ。次のいずれかを実行します。 • [スタンドアロン（Standalone）]：スタンドアロン モード。 • [HA]：高可用性モード。
[VSG HA Id] フィールド	VSG HA の ID。使用可能な範囲は 1 ～ 4095 です。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	リストからネットワーク タイプを選択します。
[VLAN ID 範囲（VLAN ID Range）] フィールド	VLAN ID の範囲（たとえば、100 ～ 199）。
[同じ VLAN/VXLAN の使用（Use same vlan/vxlan）] チェック ボックス	オンにした場合は、VSG HA とデータ ポート グループの両方に同じ VLAN ID または VXLAN ID を使用します。
[名前（Name）] フィールド	VSG の名前。
*[プライマリ VSG（Primary VSG）]*セクション（*HA* モードのみ）	
[名前（Name）] フィールド	プライマリ VSG の名前。
[展開設定（Deployment Configuration）] ドロップダウン リスト	展開設定。次のいずれかを実行します。 • [小 VSG の展開（Deploy Small VSG）] • [中 VSG の展開（Deploy Medium VSG）] • [大 VSG の展開（Deploy Large VSG）]

名前	説明
[ディスク形式（Disk Format）] ドロップダウンリスト	仮想ディスクを保存する形式。次のいずれかを実行します。 • [シック プロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）] • [シック プロビジョニング（Easy Zeroed）（Thick Provision Easy Zeroed）] • [シン プロビジョニング（Thin Provision）]
[セカンダリ VSG（Secondary VSG）]（HA モードのみ）	
[名前（Name）] フィールド	プライマリ VSG の名前。
[展開設定（Deployment Configuration）] ドロップダウン リスト	展開設定。次のいずれかを実行します。 • [小 VSG の展開（Deploy Small VSG）] • [中 VSG の展開（Deploy Medium VSG）] • [大 VSG の展開（Deploy Large VSG）]
[ディスク形式（Disk Format）] ドロップダウンリスト	仮想ディスクを保存する形式。次のいずれかを実行します。 • [シック プロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）] • [シック プロビジョニング（Easy Zeroed）（Thick Provision Easy Zeroed）] • [シン プロビジョニング（Thin Provision）]

ステップ 17 [送信（Submit）] をクリックします。

ステップ 18 [OK] をクリックします。

仮想インフラストラクチャ ポリシーの作成

仮想インフラストラクチャ ポリシーは、使用する VM やプロビジョニングするコンテナのタイプを定義します。また、このポリシーは、この特定のアカウントに関連付ける PNSC アカウントも定義します。

（注） ゲートウェイ関連の Linux ベースの VM イメージパラメータをこのポリシーに追加できます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [仮想インフラストラクチャ ポリシー（Virtual Infrastructure Policies）] をクリックします。

ステップ 3 [ポリシーを追加（+）（Add Policy (+)）] をクリックします。

ステップ 4 [仮想インフラストラクチャ ポリシーの作成（Create a virtual infrastructure policy）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	仮想インフラストラクチャ ポリシーの一意の名前。
[ポリシーの説明（Policy Description）] フィールド	仮想インフラストラクチャ ポリシーの説明。
[コンテナ タイプ（Container Type）] ドロップダウン リスト	VSG コンテナ タイプを選択します。
[仮想アカウントの選択（Select Virtual Account）] ドロップダウン リスト	仮想アカウント（クラウド）を選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [仮想インフラストラクチャ ポリシー：PNSC 情報（Virtual Infrastructure Policy - PNSC Information）] 画面で、次のフィールドに入力します。

名前	説明
[PNSC アカウント（PNSC Account）] フィールド	PNSC アカウントを展開し、PNSC アカウントを選択します。
[VSG テンプレート設定（VSG Template Configuration）] セクション	
[PNSC ファイアウォール ポリシー（PNSC Firewall Policy）] ドロップダウン リスト	ファイアウォール ポリシーを選択します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [仮想インフラストラクチャ ポリシー：フェンシング ゲートウェイ（Virtual Infrastructure Policy - Fencing Gateway）] 画面で、次のフィールドに入力します。

名前	説明
[ゲートウェイが必要（Gateway Required）] チェック ボックス	ゲートウェイが必要な場合は、このボックスをオンにします。
[ゲートウェイ ポリシーの選択（Select Gateway Policy）] ドロップダウン リスト	このフィールドは、[ゲートウェイが必要（Gateway Required）] チェック ボックスがオンになっている場合にのみ表示されます。ゲートウェイ ポリシーを選択します。
ゲートウェイの要約	仮想インフラストラクチャ ポリシーのゲートウェイ設定の概要が表示されます。

ステップ 9 [次へ（Next）] をクリックします。[仮想インフラストラクチャ ポリシー：概要（Virtual Infrastructure Policy - Summary）] 画面が表示され、現在の設定が示されます。

ステップ 10 [送信（Submit）] をクリックします。

VSG 用アプリケーション テンプレートの作成

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 [テンプレートの追加（Add Template）] をクリックします。[アプリケーション コンテナ テンプレートの追加（Add Application Container Template）] ページが表示されます。次のフィールドに入力します。

名前	説明
[テンプレート名（Template Name）] フィールド	新しいテンプレートの名前。
[テンプレートの説明（Template Description）] フィールド	テンプレートの説明。

ステップ 4 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：仮想インフラストラクチャ ポリシーの選択（Application Container Template - Select a Virtual Infrastructure policy）] 画面が表示されます。この画面で、アプリケーション コンテナを展開するクラウドを選択します。次のフィールドに入力します。

名前	説明
[仮想インフラストラクチャ ポリシーの選択（Select Virtual Infrastructure Policy）] ドロップダウン リスト	コンテナに展開する仮想インフラストラクチャ ポリシーを選択します。

ステップ 5 [次へ（Next）] をクリックします。[アプリケーション コンテナ：テンプレート：内部ネットワーク（Application Container Template - Internal Networks）] 画面が表示されます。

（注） VSG コンテナごとに 1 つのネットワークのみを設定できます。

ステップ 6 [追加（+）（Add (+)）] アイコンをクリックしてネットワークを追加します。[ネットワークへのエントリの追加（Add Entry to Networks）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[ネットワーク名（Network Name）] フィールド	ネットワーク名。この名前はコンテナで一意である必要があります。最大 128 文字を使用できます。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	ネットワーク タイプを選択します。
[情報ソース（Information Source）] ドロップダウン リスト	リストから情報ソースのタイプを選択します。
[VLAN ID 範囲（VLAN ID Range）] フィールド	VLAN ID の範囲。この値は、複製または作成できるコンテナの数を制御します。
[ネットワーク IP アドレス（Network IP Address）] フィールド	コンテナのネットワーク IP アドレス。
[ネットワークマスク（Network Mask）] フィールド	ネットワーク マスク。
[ゲートウェイ IP アドレス（Gateway IP Address）] フィールド	ネットワークのデフォルトゲートウェイの IP アドレス。この IP アドレスの NIC が GW VM に作成されます。 （注） ゲートウェイの内部インターフェイスにこの IP アドレスが設定されます。

ステップ 7 [送信（Submit）] をクリックします。

この後、アプリケーション コンテナでプロビジョニングされるゲートウェイ VM を追加および設定できます。

ステップ 8 [OK] をクリックします。

ステップ 9 [次へ（Next）] をクリックします。
[アプリケーション コンテナ テンプレート：VM（Application Container Template - VMs）] 画面が表示されます。

ステップ 10 [追加（+）（Add (+)）] をクリックして VM を追加します。次のフィールドに入力します。

名前	説明
[VM] フィールド	VM の名前。フルネームには、コンテナ名とこの名前が含まれます。
[説明（Description）] フィールド	VM の説明。
[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VM イメージ テンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。
[VM イメージ（VM Image）] ドロップダウン リスト	このフィールドは、[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックスがオフになっている場合にのみ表示されます。展開するイメージを選択します。
[仮想 CPU の数（Number of Virtual CPUs）] ドロップダウン リスト	VM に割り当てる仮想 CPU の数を選択します。
[メモリ（Memory）] ドロップダウン リスト	VM に割り当てるメモリの量（MB 単位）を選択します。
[CPU予約(MHz)] フィールド	VM に対する CPU 確保（Mhz 単位）。
[メモリ予約(MB)（Memory Reservation (MB)）] フィールド	VM のメモリ予約。

名前	説明
[ディスク サイズ（GB）（Disk Size (GB)）] フィールド	VM のカスタム ディスク サイズ。テンプレートのディスク サイズを使用するには、値にゼロを指定します。指定したディスク サイズで選択したイメージのディスク サイズが上書きされます。 （注） この値がテンプレート サイズ未満の場合、この値は無視されます。
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	VMのユーザ名とパスワードをエンドユーザと共有する方法のオプションを選択します。[パスワードのリセット後に共有（Share after password reset）] または [共有テンプレート クレデンシャル（Share template credentials）] を選択した場合、エンドユーザは選択したテンプレートのユーザ名とパスワードを指定する必要があります。
[イメージからのネットワーク設定の使用（Use Network Configuration from Image）] チェックボックス	オンにした場合は、イメージからのネットワーク設定がプロビジョニング済みの VM に適用されます。
[VM ネットワーク インターフェイス（VM Network Interfaces）] フィールド	VM ネットワーク インターフェイスを展開し、VM ネットワーク インターフェイス情報を選択します。別のネットワーク インターフェイスを追加する場合は、ステップ 11 に進みます。
[最大数量（Maximum Quantity）] フィールド	作成後にこのコンテナで追加可能なインスタンスの最大数。
[初期数量（Initial Quantity）] フィールド	コンテナを作成する際にプロビジョニングする VM インスタンスの数。 （注） 各 VM には一意の名前と IP アドレスが設定されます。

ステップ 11 （任意） [追加（+）（Add (+)）] をクリックして、新しい（複数の）VM ネットワーク インターフェイスを追加します。次のフィールドに入力します。

名前	説明
[VM ネットワーク インターフェイス名（VM Network Interface Name）] フィールド	VM ネットワーク インターフェイスの名前。
[ネットワークの選択（Select the Network）] ドロップダウン リスト	ネットワークを選択します。

名前	説明
[Ipアドレス（IP Address）] フィールド	ネットワークの IP アドレス。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 [OK] をクリックします。
[アプリケーション コンテナ テンプレート：外部ゲートウェイ セキュリティ設定（Application Container Template - External Gateway Security Configuration）] 画面が表示されます。ポート マッピングや発信アクセス制御リスト（ACL）などのセキュリティ設定コンポーネントを指定できます。

ステップ 14 [追加（+）（Add (+)）] をクリックし、ポート マッピングを追加します。次のフィールドに入力します。

名前	説明
[プロトコル（Protocol）] ドロップダウン リスト	ポート マッピング用のプロトコルを選択します。
[マッピングされたポート（Mapped Port）] ドロップダウン リスト	選択したプロトコルにマッピングされたポートを選択します。
[リモート IP アドレス（Remote IP Address）] フィールド	リモート マシンの IP アドレス。
[リモート ポート（Remote Port）] フィールド	リモート マシンのポート番号。

ステップ 15 [送信（Submit）] をクリックします。

ステップ 16 [OK] をクリックします。

ステップ 17 [アプリケーション コンテナ テンプレート：外部ゲートウェイ セキュリティの設定（Application Container Template - External Gateway Security Configuration）] 画面で、[追加（+）（Add (+)）] アイコンをクリックしてアウトバウンド ACL を追加します。次のフィールドに入力します。

名前	説明
[プロトコル（Protocol）] ドロップダウン リスト	プロトコルを選択します。
[ネットワークの選択（Select the Network）] ドロップダウン リスト	ルールを適用する必要があるネットワーク。
[ソースアドレス（Source Address）] フィールド	送信元のクラスレス ドメイン間ルーティング（CIDR）の IP アドレス。

名前	説明
[接続先アドレス（Destination Address）] フィールド	送信先 CIDR の IP アドレス。
[アクション（Action）] フィールド	一致するネットワーク トラフィックで適用されるアクション。

ステップ 18 [送信（Submit）] をクリックします。

ステップ 19 [OK] をクリックします。

ステップ 20 [次へ（Next）] をクリックします。

ステップ 21 [アプリケーション コンテナ テンプレート：ポリシーの展開（Application Container Template - Deployment Policies）] 画面で、次のフィールドに入力します。

名前	説明
[コンピューティング ポリシー（Compute Policy）] ドロップダウン リスト	仮想コンテナのすべてのコンピューティング コンポーネントを展開するポリシーを選択します。
[ストレージポリシー（Storage Policy）] ドロップダウン リスト	仮想コンテナのすべてのストレージ コンポーネントを展開するポリシーを選択します。
[ネットワーク ポリシー（Network Policy）] フィールド	コンテナ ゲートウェイに展開するポリシーを選択します。コンピューティングポリシーの一部とみなされるホストは、Cisco Nexus 1000（Cisco VSG の展開に使用）と関連付ける必要があります。 （注） このフィールドは、コンテナ ゲートウェイの外部インターフェイスのみに使用されます。また、リソース割り当ては Cisco Nexus 1000 シリーズ スイッチと関連付ける必要があります。
[システム ポリシー（Systems Policy）] フィールド	DNS とその他の OS ライセンスの設定に使用される値。
[コスト モデル（Cost Model）] フィールド	コスト モデルを選択します。
[共通のネットワークポリシーを使用します（Use common network policy）] チェックボックス	VSG 管理ネットワークに上記で定義した共通ネットワーク ポリシーを使用するには、このチェックボックスをオンにします。
[管理ネットワーク ポリシー（Management Network Policy）] ドロップダウン リスト	[共通のネットワーク ポリシーを使用します（Use common network policy）] をオンにしなかった場合は、VSG 管理ネットワークのネットワーク ポリシーを選択します。

ステップ 22 [次へ（Next）] をクリックします。

ステップ 23 [アプリケーション コンテナ テンプレート：オプション（Application Container Template - Options）] 画面で、次のフィールドに入力します。

名前	説明
[エンドユーザ セルフサービス ポリシー（End User Self-Service Policy）] ドロップダウン リスト	アプリケーション コンテナ テンプレートに該当するエンドユーザ セルフサービス ポリシーを選択します。
[コンテナのセルフサービス削除の有効化（Enable Self-Service Deletion of Containers）] チェックボックス	オンにした場合は、コンテナのセルフサービス削除が有効になります。
[VNC ベースのコンソール アクセスの有効化（Enable VNC Based Console Access）] チェックボックス	オンにした場合は、VNC ベースの VM へのコンソールアクセスが有効になります。
[テクニカル サポート用の電子メール（Technical Support Email Addresses）] フィールド	コンテナのプロビジョニングに関して電子メールを受け取る担当者の電子メール アドレスのカンマ区切りのリストを入力します。

ステップ 24 [次へ（Next）] をクリックします。

ステップ 25 コンテナをセットアップするワークフローを選択します。

ステップ 26 ワークフロー リストを展開し、ワークフロー（たとえば、ワークフロー ID 431 フェンスド コンテナ セットアップ：VSG（Workflow Id 431 Fenced Container Setup - VSG））を選択します。

（注） ワークフローには、割り当てられたリソースが含まれている必要があります。たとえば、VSG ワークフローの場合は、Cisco Nexus 1000 シリーズのリソースが含まれている必要があります。

ステップ 27 [選択（Select）] をクリックします。

ステップ 28 [送信（Submit）] をクリックします。

第 7 章

ファブリック コンテナの設定

この章は、次の項で構成されています。

ファブリック アプリケーション コンテナ

ファブリック アプリケーション コンテナタイプは Dynamic Fabric Automation（DFA）ネットワークの配備に使用します。Cisco Unified Fabric Automation は、接続されたすべてのデバイスが同じホップ数で到達可能な、マルチステージのスイッチング ネットワークです。Cisco Unified Fabric Automation 組織ファブリックにより、スケールアウト モデルを使用した最適な拡張が可能になります。

Cisco UCS Director はオーケストレーション エンジンとして機能し、最終的に仮想マシン（VM）仮想ネットワーク インターフェイス カード（vnic）が取り込まれるテナント（レイヤ 2 および 3）ネットワークの作成を担当します。Cisco Unified Fabric Automation は基本的に、新しく作成されたネットワーク用のスケーラブルなネットワーク インフラストラクチャを提供します。

Cisco Unified Fabric Automation は、統合によってデータセンターを最適化します。このアーキテクチャによって、物理サーバ環境と仮想マシン環境が統合された際にトラフィックの可視性や最適化を妨げ、拡張性を損なうオーバーレイ ネットワークが不要になります。また、ゼロ タッチのプロビジョニングや高度なオーケストレーションが可能になり、大規模なクラウド ネットワークで性能や遅延がより正確に予測できるようになります。

（注） DFA ネットワーク内のアプリケーション コンテナの詳細については、『Cisco UCS Director Unified Fabric Automation Management Guide』を参照してください。

ファブリック アプリケーション コンテナの制限

次に示すのはファブリック コンテナの制限です。

- F5 ロード バランシングは、ファブリック コンテナでのみサポートされます。

ファブリック アプリケーション コンテナ ポリシーの作成

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [仮想インフラストラクチャ ポリシー（Virtual Infrastructure Policies）] をクリックします。

ステップ 3 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 4 [仮想インフラストラクチャ ポリシー仕様（Virtual Infrastructure Policy Specification）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ポリシーの名前。
[ポリシーの説明（Policy Description）] フィールド	ポリシーの説明。
[コンテナ タイプ（Container Type）] ドロップダウン リスト	[ファブリック（Fabric）] を選択し、[次へ（Next）] をクリックして選択内容を確定し、ウィザードの指示に従います。 （注） Cisco Dynamic Fabric Automation 環境では、ゲートウェイの作成はオプションです。
[仮想アカウントの選択（Select Virtual Account）] ドロップダウン リスト	選択した仮想アカウント（ゲートウェイ VM を作成するクラウド）。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [仮想インフラストラクチャ ポリシー：ファブリック情報（Virtual Infrastructure Policy - Fabric Information）] 画面で、次のフィールドに入力します。

名前	説明
[VSG 使用（With VSG）] チェックボックス	VGSG をサポートするにはチェックボックスをオンにします。 オンになっている場合、[サービス ネットワーク設定（Service Network Configuration）] および [ホスト ネットワーク設定（Host Network Configuration）] の情報を入力します。
[ファブリック アカウント（Fabric Account）] ドロップダウン リスト	ファブリック アカウントを選択します。
[スイッチ タイプ（Switch Type）] ドロップダウン リスト	スイッチ タイプを選択します。
[スイッチ名（Switch Name）] ドロップダウン リスト	スイッチを選択します。
[代替スイッチ名（Alternate Switch Name）] ドロップダウン リスト	代替スイッチ名を選択します。
[サービス ネットワーク設定（Service Network Configuration）]	

名前	説明
[レイヤ 3（Layer 3）] チェックボックス	このフィールドは、[VSG の使用（With VSG）] チェック ボックスがオンになっている場合にのみ表示されます。レイヤ3をサポートするにはチェックボックスをオンにします。 （注） vPath パーティション、サービス、および分類子ネットワークのセットアップなどのレイヤ 3 サポートに必要な展開前セットアップを実行する必要があります。これを実行するには、次のタスクを含むオーケストレーション ワークフローをタスク ライブラリから作成し、実行します。 • ファブリック組織の作成（vPath 組織の作成） • ファブリック パーティションの作成（vPath パーティションの作成） • ファブリック ネットワークの作成（vPath 分類子ネットワークの作成） • AddHostVMKernelPortondvSwitch（N1kv VEM クラスタへの vmknics の追加） • ファブリック ネットワークの作成（vPath サービス ネットワークの作成）
[ファブリック組織（Fabric Organization）] ドロップダウン リスト	このフィールドは、[レイヤ 3（Layer 3）] チェックボックスがオンになっている場合にのみ表示されます。ファブリック組織を選択します。
[ファブリック パーティション（Fabric Partition）] ドロップダウン リスト	このフィールドは、[レイヤ 3（Layer 3）] チェックボックスがオンになっている場合にのみ表示されます。ファブリック パーティションを選択します。
[ファブリック サービス ネットワーク（Fabric Service Network）] フィールド	このフィールドは、[レイヤ 3（Layer 3）] チェックボックスがオンになっている場合にのみ表示されます。ファブリック サービス ネットワークのリストを展開し、ファブリック サービス ネットワークを選択します。

名前	説明
[モビリティ ドメイン ID（HA）（Mobility Domain Id (HA)）] フィールド	このフィールドは、[モビリティ ドメインID（HA）（Mobility Domain Id (HA)）] チェック ボックスがオンになっている場合にのみ自動的に入力されます。このチェック ボックスがオフになっている場合は、[モビリティ ドメイン ID（Mobility Domain ID）] リストを展開して、モビリティ ドメイン ID を選択します。
[自動選択モビリティ ドメイン ID（Auto Select Mobility Domain Id）] チェック ボックス	モビリティ ドメイン ID を自動的に選択するには、このボックスをオンにします。
[ホスト ネットワーク設定（Host Network Configuration）]	
[モビリティ ドメイン ID（サービス ネットワーク + HA）（Mobility Domain Id (Service Network + HA)）] フィールド	このフィールドは、[モビリティ ドメインID（HA）（Mobility Domain Id (HA)）] チェック ボックスがオンになっている場合にのみ自動的に入力されます。このチェック ボックスがオフになっている場合は、[モビリティ ドメイン ID（Mobility Domain ID）] リストを展開して、モビリティ ドメイン ID を選択します。 （注） レイヤ 2 の場合、サービス ネットワークと対応するホスト ネットワークのモビリティ ドメインは、サービスネットワークと同じである必要があります。あるいは、なしにすることもできます。
[自動選択モビリティ ドメイン ID（Auto Select Mobility Domain Id）] チェック ボックス	モビリティ ドメイン ID を自動的に選択するには、このボックスをオンにします。
[パーティション パラメータ（Partition Parameters）]	
[DCI ID] フィールド	DCI ID を入力します。
[ファブリックでパーティションを拡張する（Extend the partition across the fabric）] チェックボックス	チェックボックスをオンにし、ファブリックのパーティションを入力します。
[サービス ノード IP アドレス（Service Node IP Address）] フィールド	サービス ノードの IP アドレスを入力します。
[DNS サーバ（DNS Server）] フィールド	DNS サーバを入力します。
[セカンダリ DNS サーバ（Secondary DNS Server）] フィールド	セカンダリ DNS サーバを入力します。

名前	説明
[マルチキャスト グループ アドレス（Multi Cast Group Address）] フィールド	マルチキャスト グループ アドレスを入力します。
[プロファイル名（Profile Name）] フィールド	プロファイル名リストを展開し、プロファイル名を選択します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 コンテナのゲートウェイを追加する場合は、[仮想インフラストラクチャ ポリシー：ゲートウェイ（Virtual Infrastructure Policy - Gateway）] 画面で、[ゲートウェイが必要（Gateway required）] チェック ボックスをオンにします。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 コンテナのロード バランサを追加する場合は、[仮想インフラストラクチャ ポリシー：フェンシング ロード バランシング（Virtual Infrastructure Policy - Fencing Load Balancing）] 画面で、[F5 ロード バランサが必要（F5 Load Balancer Required）] チェック ボックスをオンにします。

ステップ 11 [概要（Summary）] 画面で、構成の概要を表示して [送信（Submit）] をクリックします。

ファブリック アプリケーション コンテナ テンプレートの作成

アプリケーション コンテナを作成する前に、テンプレートを作成する必要があります。

（注） このテンプレートでは、さまざまなネットワーク（DFA ネットワークを含む）で使用するアプリケーション コンテナを作成できます。テンプレートに行った変更は、そのテンプレートで作成された既存のアプリケーション コンテナには影響を与えません。

はじめる前に

アプリケーション コンテナ ポリシーを作成します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 [テンプレートの追加（Add Template）] をクリックします。[アプリケーション コンテナ テンプレート（Application Container Template）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[テンプレート名（Template Name）] フィールド	新しいテンプレートの名前。
[テンプレートの説明（Template Description）] フィールド	新しいテンプレートの説明。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [アプリケーション コンテナ テンプレート：仮想インフラストラクチャ ポリシーの選択（Application Container Template - Select a Virtual infrastructure policy）] 画面が表示されます。次の選択を実行します。

名前	説明
[仮想インフラストラクチャ ポリシーの選択（Select Virtual Infrastructure Policy）] ドロップダウン リスト	ポリシー（ファブリック環境で使用するために作成されたポリシー）を選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [アプリケーション コンテナ テンプレート：ファブリック ネットワーク（Application Container Template - Fabric Networks）] 画面で、[追加（+）（Add (+)）] をクリックしてファブリック ネットワークを追加します。次のフィールドに入力します。

名前	説明
[外部パーティション（External Partition）] チェックボックス	このフィールドは、選択した仮想インフラストラクチャ ポリシーでゲートウェイが選択されている場合にのみ表示されます。ASA 外部パーティションのホスト ネットワークを有効にするには、このチェックボックスをオンにします。
[ネットワーク名（Network Name）] フィールド	コンテナ内のネットワークの一意の名前。最大 128 文字を使用できます。

名前	説明
[ネットワーク ロール（Network Role）] ドロップダウン リスト	ネットワーク ロールを選択します。
[説明（Description）] フィールド	ネットワークの説明。
[マルチキャスト グループ アドレス（Multicast Group Address）] フィールド	マルチキャスト グループ アドレス。
[プロファイル名（Profile Name）] フィールド	プロファイル名リストを展開し、プロファイルを選択します。
[ゲートウェイ IP アドレス（Gateway IP Address）] フィールド	ネットワークのデフォルト ゲートウェイの IP アドレス。
[ネットワークマスク（Network Mask）] フィールド	ネットワーク マスク（たとえば、255.255.255.0）。
[DHCP サーバ アドレス（DHCP Server Address）] フィールド	DHCP サーバの IP アドレス。
[vrfdhcp] フィールド	VRF DHCP サーバの IP アドレス。
[mtuvalue] フィールド	最大伝送単位（MTU）値。
[dhcpServerv6Address] フィールド	DHCP サーバの IPv6 アドレス。
[vrfv6dhcp] フィールド	VRF DHCP サーバの IPv6 アドレス。
[ゲートウェイ IPv6 アドレス（Gateway IPv6 Address）] フィールド	ゲートウェイの IPv6 アドレス。
[プレフィクス長（Prefix Length）] フィールド	IPv6 アドレスによって使用されるプレフィックス長。
[DHCP スコープ（DHCP Scope）]	
[DHCP 有効（DHCP Enabled）] チェックボックス	DHCP を有効にするには、チェックボックスをオンにします。
[サービス構成パラメータ（Service Configuration Parameters）]	
[開始 IP（Start IP）] フィールド	ネットワークの開始 IP アドレス。
[終了 IP（End IP）] フィールド	ネットワークの終了 IP アドレス。

名前	説明
[セカンダリ ゲートウェイ（Secondary Gateway）] フィールド	セカンダリ ゲートウェイの IP アドレス。

ステップ 8 [送信（Submit）] をクリックします。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [アプリケーション コンテナ テンプレート：VM（Application Container Template - VMs）] 画面で、[追加（+）（Add (+)）] をクリックして VM を追加します。[仮想マシンへのエントリの追加（Add Entry to Virtual Machines）] ダイアログ ボックスが表示されます。次のフィールドに入力します。

名前	説明
[VM名（VM Name）] フィールド	VM の名前。
[説明（Description）] フィールド	VM の説明。
[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VMイメージテンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。
[VM イメージ（VM Image）] ドロップダウン リスト	このフィールドは、[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックス がオフになっている場合にのみ表示されます。展開するイメージを選択します。
[仮想 CPU の数（Number of Virtual CPUs）] ドロップダウン リスト	VM に割り当てる仮想 CPU の数。
[メモリ（Memory）] ドロップダウン リスト	割り当てるメモリ（MB 単位）。
[CPU予約(MHz)（CPU Reservation(MHz)）] フィールド	VM 用に予約する CPU。

名前	説明
[メモリ予約(MB)（Memory Reservation (MB)）] フィールド	VM のメモリ予約。
[ディスク サイズ（GB）（Disk Size (GB)）] フィールド	VM のカスタム ディスク サイズ。テンプレートのディスク サイズを使用するには、値に 0 を指定します。指定したディスク サイズで選択したイメージのディスク サイズが上書きされます。
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	VM のユーザ名とパスワードをエンドユーザと共有する方法のオプションを選択します。[パスワードのリセット後に共有（Share after password reset）] または [共有テンプレート クレデンシャル（Share template credentials）] を選択した場合、エンドユーザは選択したテンプレートのユーザ名とパスワードを指定する必要があります。
[イメージからのネットワーク設定の使用（Use Network Configuration from Image）] チェックボックス	オンにした場合は、イメージからのネットワーク設定が使用され、プロビジョニング済みの VM に設定が適用されます。
[VM ネットワーク インターフェイス（VM Network Interface）] フィールド	VM ネットワーク インターフェイスを展開し、VM ネットワーク インターフェイスを選択します。
[最大数量（Maximum Quantity）] フィールド	作成後にこのコンテナで追加可能なインスタンスの最大数。
[初期数量（Initial Quantity）] フィールド	コンテナを作成する際にプロビジョニングする VM インスタンスの数。

ステップ 11 [次へ] をクリックします。[アプリケーション コンテナ テンプレート：展開ポリシー（Application Container Template - Deployment Policies）] 画面が表示されます。
VM のプロビジョニングに必要なコンピューティング、ストレージ、ネットワーク、システムポリシー、コスト モデルを選択する必要があります。ポリシーとは、アプリケーション コンテナ内で新しい VM を（システム リソースの可用性に基づいて）どこにどのようにプロビジョニングするかを決定するルールの集まりです。

- ネットワーク ポリシーは、仮想ファイアウォール（コンテナ ゲートウェイ）の外部インターフェイスの展開にのみ使用されます。

  （注） コンテナのゲートウェイ タイプが CISCO ASAv の場合は、ネットワーク ポリシーによって最初に ASAv 管理インターフェイスが追加されてから、同じ順序で VM ネットワークが外部インターフェイスが追加されます。

- 選択したネットワーク ポリシー内のポートグループは、ゲートウェイ VM がプロビジョニングされるホスト上に存在する必要があります。
- ネットワーク ポリシーは、スタティック *IP* プールまたは *DHCP* のいずれかを使用できます。ただし、コンテナ タイプが VSG または ASA の場合は、ネットワーク ポリシーはスタティック IP プールのみを使用する必要があります。VSG または ASA VM には IP アドレスが入力として必要です。現在、VSG または ASA VM の展開に DHCP を指定するプロビジョニングはありません。
- プロビジョニング済みの VM（コンテナ ゲートウェイ）のネットワーク アダプタ設定は、テンプレートの設定と同様である必要があります。このアプリケーション コンテナに使用されるネットワーク ポリシーで、[テンプレートからアダプタをコピーする（Copy Adapter from Template）] チェックボックスをオンにする場合としない場合があります。

次のフィールドに入力します。

名前	説明
[コンピューティング ポリシー（Compute Policy）] ドロップダウン リスト	コンピューティング ポリシーを選択します。
[ストレージ ポリシー（Storage Policy）] ドロップダウン リスト	ストレージ ポリシーを選択します。
[ネットワークポリシー（Network Policy）] ドロップダウン リスト	ネットワーク ポリシーを選択します。
[システム ポリシー（Systems Policy）] ドロップダウン リスト	システム ポリシーを選択します。
[コスト モデル（Cost Model）] ドロップダウン リスト	コスト モデルを選択します。

ステップ 12 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：オプション（Application Container Template - Options）] 画面が表示されます。
このページでは、セルフサービス エンド ユーザの特定の権限を有効または無効にするオプションを選択できます。次のフィールドに入力します。

フィールド	説明
[エンドユーザ セルフサービス ポリシー（End User Self-Service Policy）] ドロップダウン リスト	エンドユーザのセルフサービス ポリシーを選択します。
[コンテナのセルフサービス削除の有効化（Enable Self-Service Deletion of Containers）] チェックボックス	オンにすると、このテンプレートを使用して作成したアプリケーション コンテナをエンドユーザが削除できるようになります。

フィールド	説明
[VNCベースのコンソールアクセスの有効化（Enable VNC Based Console Access）] チェックボックス	オンにすると、コンテナホスト上のVMに仮想ネットワーク コンピューティング（VNC）アクセスが許可されます。
[テクニカル サポート用の電子メール アドレス（Technical Support Email Addresses）] テキスト フィールド	電子メール アドレスのカンマ区切りのリストを入力します。自動化された通知がこれらの電子メールに送信されます。

ステップ 13 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：セットアップ ワークフロー（Application Container Template - Setup Workflows）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[コンテナ セットアップ ワークフロー（Container Setup Workflow）] ドロップダウン リスト	コンテナセットアップ ワークフローを選択します。デフォルトでは、ワークフローは選択されていません。このコンテナに選択したゲートウェイ タイプが [Linux] で、コンテナに関連付けられたネットワーク ポリシーで [仮想マシン ポートグループ（Virtual Machine Portgroup）] を選択した場合は、このステップをスキップできます。コンテナ ゲートウェイとして CISCO ASA を選択するか、ネットワーク ポリシーとして [分散型仮想ポートグループ（Distributed Virtual Portgroup）] を選択した場合にのみ、特定のワークフローを選択する必要があります。CISCO ASAv ゲートウェイ タイプの場合は、[ASAv ゲートウェイを使用するアプリケーション コンテナ（Application Container with ASAv Gateway）] を選択します。 （注） アプリケーションコンテナテンプレートを作成するためのタスクを開始する前に、いくつかの前提条件のステップを実行する必要があります。

ステップ 14 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：概要（Application Container Template - Summary）] 画面が表示され、現在の設定が示されます。

ステップ 15 [送信（Submit）] をクリックし、アプリケーション コンテナ テンプレートの作成を実行します。

第 8 章

CiscoApplicationPolicyInfrastructureController Container の設定

この章は、次の項で構成されています。

Cisco UCS Director およびシスコ アプリケーション セントリック インフラストラクチャ

Cisco UCS Director は、コンピューティング、ネットワーク、ストレージ、および仮想化の各階層に対し単一のインターフェイスから管理できる統合インフラストラクチャ管理ソリューションです。Cisco UCS Director では、コンピューティング、ネットワーク、ストレージ、および仮想化の各階層をサポートするワークフロー タスクで、ワークフロー オーケストレーション エンジンを使用します。Cisco UCS Director はマルチテナント機能をサポートするため、インフラストラクチャをポリシー ベースで共有することができます。

Cisco UCS Director は、異なるコンテナ階層の間でコントラクトを定義する機能をサポートするため、階層間にルールを適用することもできます。

シスコ アプリケーション セントリック インフラストラクチャ（ACI）では、アプリケーションの要件によってネットワークを定義できます。このアーキテクチャは、アプリケーションの導入サイクル全体を簡素化、最適化、加速化します。

Cisco UCS Director と Cisco ACI を組み合わせることにより、アプリケーション セントリック インフラストラクチャのプロビジョニングおよび提供を自動化できます。

（注） ACI 1.1(1*) を使用するには、TLSv1 が Cisco Application Policy Infrastructure Controller（APIC）で有効になっていることを確認します。APIC で、[ファブリック（Fabric）] > [ファブリック リソース（Fabric Resources）] > [Pod Polices（ポッド ポリシー）] > [通信（Communication）] > [デフォルト（Default）] を選択して、**TLSv1** を有効にします。

Cisco Application Policy Infrastructure Controller

Cisco Application Policy Infrastructure Controller（APIC）は、シスコ アプリケーション セントリック インフラストラクチャ（ACI）の自動化、管理、モニタリング、およびプログラム可能性の統合ポイントです。APIC は、インフラストラクチャの物理コンポーネントと仮想コンポーネントに対して統一された運用モデルを提供し、あらゆるアプリケーションをどこからでも展開、管理、モニタリングできるようにします。また、さらに大規模なクラウド ネットワークの中央制御エンジンとなります。APIC は、ユーザ定義のアプリケーション要件とポリシーに基づき、ネットワークのプロビジョニングと制御をプログラムによって自動化します。APIC の詳細については、このリリースの『Cisco UCS Director APIC Management Guide』を参照してください。

オーケストレーション機能を使用して、ワークフローの APIC 構成と管理タスクを自動化することができます。APIC のオーケストレーション タスクの完全なリストは、ワークフロー デザイナとタスク ライブラリで入手できます。Cisco UCS Director でのオーケストレーションの詳細については、このリリースの『Cisco UCS Director Orchestration Guide』を参照してください。

APIC アプリケーション コンテナ

Cisco UCS Director では、Cisco Application Policy Infrastructure Controller（APIC）をサポートするアプリケーション コンテナを作成できます。追加情報については、このリリースの『Cisco UCS Director APIC Management Guide』を参照してください。APIC アプリケーション コンテナでは、次を実行できます。

- WMware 環境でのネットワークの確立。
- 複数のネットワークからの VM のプロビジョニング。
- ゲートウェイ（ASAv など）を使用してネットワークを隔離する手段を提供する。
- VPX または SDX ロード バランサを使用したコンテナ ネットワークのロード バランシングを可能にする。
- Cisco Application Centric Infrastructure（ACI）の使用
- ベア メタル サーバ、または VM、あるいはその両方のプロビジョニング。

APIC アプリケーション コンテナの前提条件

APIC アプリケーション コンテナを作成する前に、次の Cisco UCS Director タスクを実行する必要があります。これらのタスクの追加情報については、このリリースの『Cisco UCS Director APIC Management Guide』を参照してください。

- APIC アカウントを追加し、設定します。
- リソース グループを追加します。
- 提供サービスを追加します。
- テナント プロファイルを追加します。
- タグ ライブラリを追加します。タグの作成については、このリリースの『Cisco UCS Director Administration Guide』を参照してください。
- ファイアウォール ポリシーを追加します（任意）。

APIC アプリケーション コンテナの制限

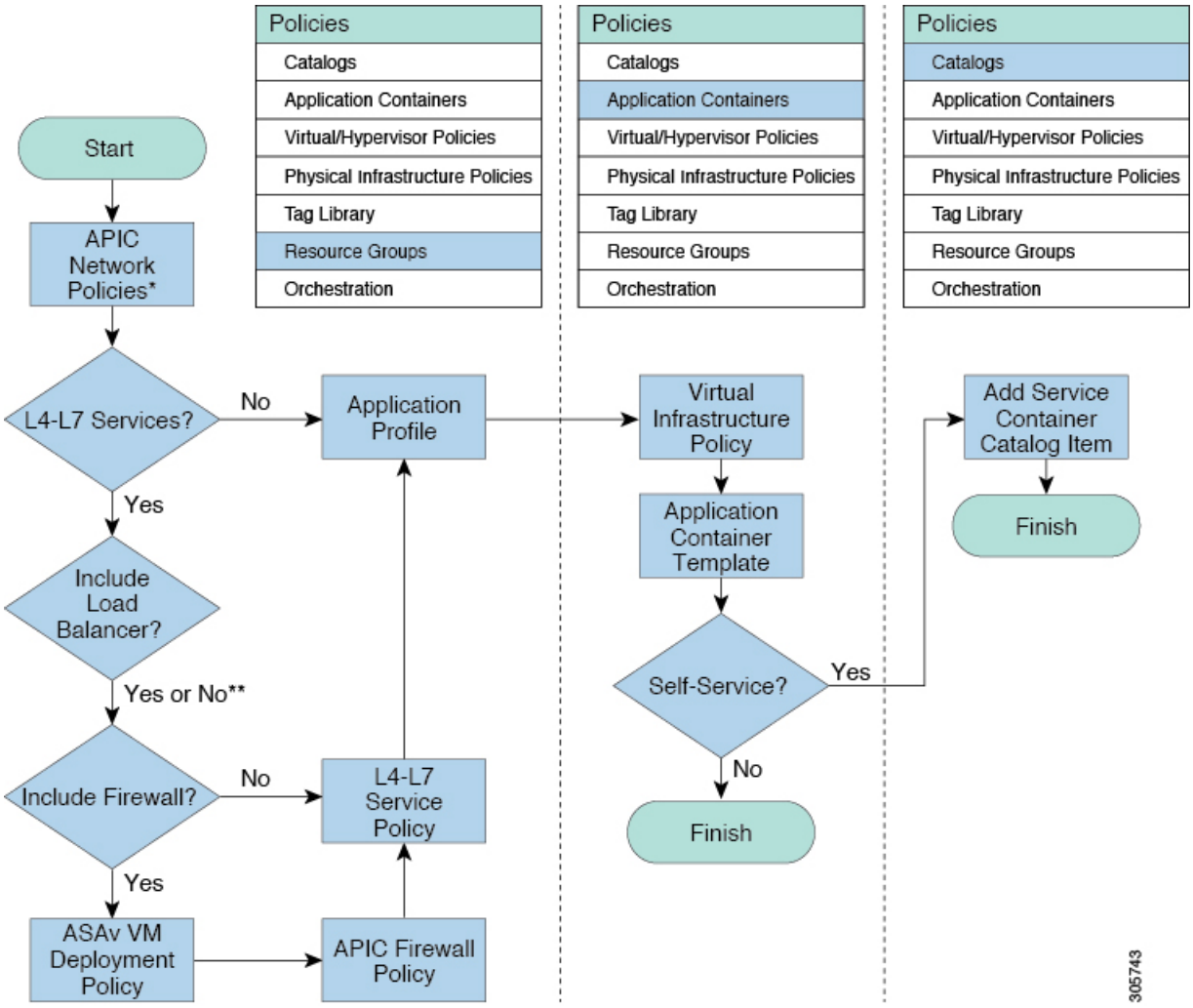
Cisco UCS Director APIC アプリケーション コンテナには次の制限があります。

- コンテナを作成し、使用する前に、テナントオンボーディングを実行する必要があります。
- リソースグループには、コンテナのリソースの管理に必要なアカウントが含まれている必要があります。これは、ストレージ、コンピューティング、ネットワーク、および仮想リソースを任意に組み合わせたものです。
- 物理サーバを必要とするアプリケーションコンテナ構成の場合、現在ではUCS管理対象サーバのみがサポートされています。

APIC アプリケーション コンテナの作成プロセス

次の図に、Cisco UCS Director 内での APIC アプリケーション コンテナの作成プロセスのフローを示します。

図 *3*：*APIC* アプリケーション コンテナの作成プロセス



* Optional. APIC Network Policies are only needed to override default APIC network entity properties.

** Load Balancer is an L4-L7 service but does not require a separate policy.

ASAv VM 導入ポリシー

適応型セキュリティ仮想アプライアンス（ASAv）は、仮想化環境に包括的なファイアウォール機能を提供し、データセンター トラフィックとマルチテナント環境のセキュリティを強化します。ASAv VM 導入ポリシーは、OVF からの ASAv VM の導入タスクで使用されます。

ASAv VM 導入ポリシーの追加

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [ASAv VM 導入ポリシー（ASAv VM Deployment Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ASAv VM 展開ポリシー（ASAv VM Deployment Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ASAv VM 導入ポリシーの名前を入力します。
[ASAv OVF] リスト	リストを展開してオープン仮想化フォーマット（OVF）のテンプレート ファイルを選択し、[選択（Select）] をクリックします。
[VM 名（VM Name）] フィールド	ASAv 仮想マシン（VM）インスタンスの名前を入力します。 このポリシーによって、この VM 名の前にコンテナ名が自動的に付与されます。
[ポート（Port）] フィールド	ファイアウォール アプライアンスのポート番号を入力します。 ポート 443 の使用をお勧めします。
[ユーザ名（Username）] フィールド	ファイアウォール アプライアンスへのアクセスに使用されるユーザ名を入力します。
[パスワード（Password）] フィールド	ファイアウォール アプライアンスへのアクセスに使用されるパスワードを入力します。
[ディスク形式（Disk Format）] ドロップダウンリスト	仮想ディスク フォーマットを選択します。プロビジョニングに使用可能なフォーマットは、[Thick Provision Lazy Zeroed]、[Thick Provision Eager Zeroed]、および [Thin Provision] です。

名前	説明
[導入オプション（Deployment Option）] ドロップダウン リスト	導入オプションを選択します。これは、VM を展開するために使用できる、事前定義済みの設定です。導入オプションは、ASAv 9.3.1、ASAv 9.3.2 以降の OVF に基づいて一覧表示されます。 導入オプションは、導入 vCPU カウントに基づいて、ASAv 9.3.1 用に一覧表示されます。このカウントは、ASAv VM の導入時に ASAv VM に搭載される vCPU の数を表します。 次の導入オプションが ASAv 9.3.2 以降用に一覧表示されます。 • [ASAv5]：ASAv を 100 Mbps の最大スループットで導入します（1 つの vCPU と 2 GB のメモリを使用します）。これがデフォルト値です。 • [ASAv10]：ASAv を 1 Gbps の最大スループットで導入します（1 つの vCPU と 2 GB のメモリを使用します）。 • [ASAvASAv30]：ASAv を 2 Gbps の最大スループットで導入します（4 つの vCPU と 8 GB のメモリを使用します）。 （注） バージョン ASAv 9.5.2 のリリースまで、OVA ファイルは VMware 環境の ASAv 導入用に提供されていました。バージョン ASAv 9.5.2 以降では、OVA ファイルは Cisco.com で入手できず、代わりに ZIP ファイルが表示されます。zip ファイルには、asav-esxi.ovf ファイルではなく asav-vi.ovf ファイルを選択できる 2 つの OVA ファイルが含まれています。

ステップ 5 [送信（Submit）] をクリックします。

APIC ファイアウォール ポリシー

オプションで、エンドポイント間の特定のポートを通過するネットワーク トラフィックを許可するファイアウォール ポリシー ルールを作成できます。

アプリケーション プロファイルを作成すると、アプリケーション プロファイル内の階層ごとにファイアウォールとロード バランサのどちらを使用するかを選択できます。L4-L7 ポリシーを作成する場合は、Cisco UCS Director で作成したファイアウォール ポリシーのいずれかを選択できます。

ファイアウォール ポリシーは、ファイアウォールをサービスとして選択した次の APIC タスクで使用されます。

- L4-L7 サービス グラフの作成
- L4-L7 サービス グラフへの機能ノードの追加

APIC ファイアウォール ポリシーの追加

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [APIC ファイアウォール ポリシー（APIC Firewall Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ファイアウォール ポリシーの作成（Create Firewall Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
ポリシーの詳細	
[名前（Name）] フィールド	ファイアウォール ポリシーの名前を入力します。
[説明（Description）] フィールド	ファイアウォール ポリシーの説明を入力します。
ACL の詳細	

名前	説明
[ACL（ACL(s)）] リスト	

名前	説明
	リストを展開して、ファイアウォール ポリシーに定義されているアクセス制御リスト（ACL）を選択します。 [+] をクリックして ACL を定義します。 [ACL へのエントリの追加（Add Entry to ACL(s)）] 画面で、次のフィールドに値を入力します。 • [既存のACLリスト名（Existing ACL List Name）] ドロップダウンリスト：既存の ACL のリストから ACL 名を選択します。 • [新しい ACL リスト（New ACL list?）] チェック ボックス：新しい ACL を作成する場合は、このボックスをオンにします。 • [新しい ACL リスト名（New ACL List Name）] フィールド：このフィールドは、[新しいACL リスト（New ACL list）] チェック ボックスをオンにすると表示されます。作成する ACL の名前を入力します。 • [ACL 名（ACL Name）] フィールド：ファイアウォール ポリシー用のルールを定義する ACL エントリ。 • [プロトコル（Protocol）] ドロップダウンリスト：通信用のプロトコルを選択します。 • [任意の送信元（Source Any）] チェック ボックス：すべての送信元ホストまたはネットワークを許可または拒否する場合は、このボックスをオンにします。デフォルトでは、このチェック ボックスはオンになっています。 • [送信元アドレス（Source Address）] フィールド：このフィールドは、[任意の送信元（Source Any）] チェックボックスをオフにすると表示されます。送信元アドレスとしてシングル ホストまたはそれらの範囲を指定するための IP アドレス、IP アドレス範囲、またはサブネット マスク付き IP アドレスを入力します。 • [任意の宛先（Destination Any）] チェック ボックス：すべての宛先アドレスに ACL エントリ ステートメントを適用するには、このボック

名前	説明
	スをオンにします。デフォルトでは、このチェック ボックスはオンになっています。 • [接続先アドレス（Destination Address）] フィールド：このフィールドは、[任意の接続先（Destination Any）] チェックボックスをオフにすると表示されます。接続先アドレスとしてシングル ホストまたはそれらの範囲を指定するための IP アドレス、IP アドレス範囲、またはサブネット マスク付き IP アドレスを入力します。 • [アクション（Action）] ドロップダウンリスト：ACL エントリのアクションとして [許可（Permit）] または [拒否（Deny）] を選択します。 • [順序（Order）] フィールド：許可ステートメントまたは拒否ステートメントを実行する必要のあるシーケンスを入力します。
[ブリッジ グループ インターフェイスの詳細（Bridge Group Interface Details）]：ブリッジ グループ インターフェイスは、ファイアウォールをトランスペアレント モードで実行している場合は必ず設定する必要があります。セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。 ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは ASA 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。	

名前	説明
[ブリッジグループインターフェイス（Bridge Group Interface(s)）] フィールド	ファイアウォール ポリシーに対して定義されたブリッジ グループ インターフェイスを入力します。 ブリッジ グループ インターフェイスのリストを展開し、[+] をクリックして、ブリッジ グループ ID を定義します。 [ブリッジ グループ インターフェイスへのエントリの追加（Add Entry to Bridge Group Interface(s)）] 画面で、次のフィールドに値を入力します。 • [ブリッジ グループ ID（Bridge Group ID）] フィールド：ブリッジ グループの一意の ID を入力します。ブリッジ グループ ID の値は 1 ～ 100 の整数です。 • [IPv4 アドレス値（IPv4 Address Value）] フィールド：ブリッジ グループの管理 IP アドレスを入力します。
インターフェイスの詳細（Interface Details）	

名前	説明
[インターフェイス（Interface(s)）] フィールド	

名前	説明
	ファイアウォール ポリシーに対して定義されたインターフェイスを入力します。 インターフェイスのリストを展開し、[+] をクリックして、インターフェイスを定義します。 [インターフェイスへのエントリの追加（Add Entry to Interface(s)）] 画面で、次のフィールドに値を入力します。 • [インターフェイス名（Interface Name）] フィールド：設定する必要のあるインターフェイスの名前を入力します。 • [仮想IPのIPプールオプション（IP Pool Option for Virtual IP）] ドロップダウンリスト：IP プール オプションを使用すると、仮想 IP アドレスが IP アドレスの範囲からインターフェイスに割り当てられます。インターフェイスに IP アドレスを自動的に割り当てるには、次のオプションのいずれかを選択します。 ◦ 既存のリストからIPプールを選択 ◦ IPプール範囲を指定 • [IP プール（IP Pool）] フィールド：インターフェイス用として予約されていない仮想 IP アドレスを選択する IP プールを入力します。 • [セキュリティレベル（Security Level）] フィールド：インターフェイスのセキュリティ レベルを入力します。セキュリティ レベルの値は 0 ～ 100 の整数です。 • [ブリッジグループID（Bridge Group ID）] ドロップダウンリスト：インターフェイスを割り当てる必要のあるブリッジグループ ID を選択します。 • [インバウンドACL（Inbound ACL）] ドロップダウンリスト：インターフェイスに入るときにトラフィックに適用するインバウンド アクセス リストとして ACL を選択します。 • [アウトバウンドACL（Outbound ACL）] ドロップダウンリスト：インターフェイスを出ると

名前	説明
	きにトラフィックに適用するアウトバウンド アクセス リストとして ACL を選択します。
インターフェイスの割り当て	
[外部インターフェイス（External Interface）] ドロップダウンリスト	外部インターフェイスとしてインターフェイスを選択します。
[内部インターフェイス（Internal Interface）] ドロップダウンリスト	内部インターフェイスとしてインターフェイスを選択します。

ステップ 5 [送信（Submit）] をクリックします。

APIC ネットワーク ポリシー

APIC ネットワーク ポリシーは、アプリケーション プロファイルのネットワーク（階層）設定で使用するオプションのポリシーです。APIC ネットワーク ポリシーは APIC アプリケーション コンテナのプロビジョニングに使用されるデフォルト設定を上書きします。テナントまたはコンテナのプライベート ネットワークを指定し、サブネットワークを作成し、エンド ポイント グループ（EPG）を作成するためのポリシーを作成できます。

APIC ネットワーク ポリシーの追加

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [APIC ネットワーク ポリシー（APIC Network Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ネットワーク ポリシーの作成（Create Network Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
ポリシー仕様	
[名前（Name）] フィールド	APIC ネットワーク ポリシーの名前を入力します。

名前	説明
[説明（Description）] フィールド	APIC ネットワーク ポリシーの説明を入力します。
プライベート ネットワーク仕様	
[プライベートネットワーク（Private Network）] ドロップダウンリスト	次のいずれかを実行します。 • [コンテナ（Container）] : プライベート ネットワークをコンテナ ワークフローから選択します。 • [テナント（Tenant）] : プライベート ネットワークをテナントから選択します。
サブネット仕様	
[サブネットの作成（Create Subnet）] チェックボックス	サブネットを作成する場合に、このボックスをオンにします。 [サブネットの作成（Create Subnet）] をオンにすると、次の追加のフィールドが表示されます。 • [共有サブネット（Shared Subnet）] ボックス：共有サブネットを使用してプライベート ネットワークを作成する場合に、このボックスをオンにします。 • [パブリック サブネット（Public Subnet）] チェック ボックス：パブリック サブネットを使用してプライベート ネットワークを作成する場合に、このボックスをオンにします。 • [プライベート サブネット（Private Subnet）] チェック ボックス：プライベート サブネットを使用してプライベート ネットワークを作成する場合に、このボックスをオンにします。
EPG 仕様	
[QOS] フィールド	EPGに割り当てる必要のあるQOS名を入力します。
[導入の緊急度（Deploy Immediacy）] ドロップダウンリスト	ドメインをすぐに導入するかまたは必要に応じて導入するかを選択します。

名前	説明
[解決の緊急度（Resolution Immediacy）] ドロップダウンリスト	ポリシーがリーフ ノードにどのように適用されるかを選択します。 • [緊急（Immediate）]：VLAN バインディング、NVGRE バインディング、VXLAN バインディング、契約、およびフィルタを含むすべてのポリシーがハイパーバイザの物理 NIC の接続時にリーフ ノードに適用されます。ハイパーバイザ/リーフ ノード間接続の解決には、リンク層検出プロトコル（LLDP）または OpFlex が使用されます。 • [オンデマンド（On Demand）]：物理 NIC を接続し、仮想 NIC とポート グループ（EPG）を関連付けたときにのみ、ポリシーがリーフ ノードに適用されます。 • [事前プロビジョニング（Pre-provision）]：VM コントローラが仮想スイッチ（たとえば、VMware VDS など）に接続される前でもポリシー（たとえば、VLAN、VXLAN バインディング、コントラクト、フィルタなど）をリーフ スイッチにダウンロードすることにより、スイッチの設定を事前プロビジョニングすることを指定します。
ブリッジ ドメイン仕様	
[フォワーディング（Forwarding）] ドロップダウンリスト	ブリッジ ドメインのフォワーディング方式（[最適化（Optimize）] または [カスタム（Custom）]）を選択します。
[L2不明なユニキャスト（L2 Unknown Unicast）] ドロップダウンリスト	不明な層宛先のフォワーディング方式を選択します。 このドロップダウンリストは、[フォワーディング（Forwarding）] ドロップダウンリストで [カスタム（Custom）] を選択すると表示されます。
[不明なマルチキャストフラッディング（Unknown Multicast Flooding）] ドロップダウンリスト	不明な層宛先のマルチキャスト トラフィックのフォワーディング方式を選択します。 このドロップダウンリストは、[フォワーディング（Forwarding）] ドロップダウンリストで [カスタム（Custom）] を選択すると表示されます。

名前	説明
[ARPフラッディング（ARP Flooding）]チェックボックス	ARP フラッディングを有効にする場合に、このボックスをオンにします。ARP フラッディングが無効になっている場合は、ユニキャスト ルーティングがターゲット IP アドレスで実行されます。 このチェックボックスは、[フォワーディング（Forwarding）] ドロップダウンリストで [カスタム（Custom）] を選択すると表示されます。
[ユニキャストルーティング（Unicast Routing）] チェックボックス	ユニキャスト ルーティングを有効にする場合に、このボックスをオンにします。ユニキャスト ルーティングは事前に定義されたフォワーディング基準（IP または MAC アドレス）に基づくフォワーディング方式です。 このチェックボックスは、[フォワーディング（Forwarding）] ドロップダウンリストで [カスタム（Custom）] を選択すると表示されます。このチェックボックスは、デフォルトでオンになっています。

ステップ 5 [送信（Submit）] をクリックします。

レイヤ 4 ～ レイヤ 7 サービス ポリシー

APIC は、ファブリック内のサービスをプロビジョニングできるだけでなく、ファブリックに接続するファイアウォールやロード バランサなどのレイヤ 4 ～レイヤ 7 のサービスもプロビジョニングできるようにするオープン ノースバウンド API を備えています。

レイヤ 4 ～レイヤ 7 サービス ポリシーの追加

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [L4-L7 サービス ポリシー（L4-L7 Service Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [L4-L7 サービスポリシーの追加（Add L4-L7 Service Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
L4-L7 サービスの仕様	
[名前（Name）] フィールド	レイヤ 4 ～レイヤ 7 サービス ポリシーの名前を入力します。
[説明（Description）] フィールド	レイヤ 4 ～レイヤ 7 サービス ポリシーの説明を入力します。

名前	説明
[ファイアウォールを許可（Allow Firewall）] チェックボックス	

名前	説明
	このボックスをオンにした場合は、ファイアウォール サービス サービスがレイヤ 4 ～レイヤ 7 サービスポリシーに適用可能になります。[ファイアウォールを許可（Allow Firewall）] を選択すると、次の追加のフィールドが表示されます。 • [ファイアウォール タイプ（Firewall Type）] ドロップダウン リスト：ファイアウォール タイプを選択します。 • [デバイスパッケージ（Device Package）] フィールド：リストを展開し、サポートされている APIC バージョンに基づいて正しいデバイス パッケージを選択します。 • [ファイアウォール ポリシー（Firewall Policy）] フィールド：リストを展開して、ファイアウォールポリシーを選択します。[+] をクリックして、ファイアウォール ポリシーを追加します。 ファイアウォール ポリシーの追加についての詳細は、APIC ファイアウォール ポリシーの追加, （84 ページ） を参照してください。 • [マルチ コンテキストの有効化（Multi Context Enabled）] チェック ボックス：複数のセキュリティ コンテキスト対応の ASA がファイアウォール設定に使用されているかどうかを確認するには、このチェック ボックスをオンにします。 このチェック ボックスは、[物理（PHYSICAL）] ファイアウォール タイプが選択されている場合にのみ表示されます。 このチェックボックスがオフの場合、物理 ASA アプライアンスを使用できます。 （注） VMware 環境に加え、Hyper-V 環境でも、コンテナのファイアウォールとして物理 ASA を使用することを選択できます。 • [ファイアウォール HA を有効にする（Enable Firewall HA）] チェックボックス—このチェックボックスは、[仮想（VIRTUAL）] ファイア

名前	説明
	ウォール タイプが選択されている場合にのみ表示されます。ファイアウォール サービスの高可用性を有効にする場合に、このボックスをオンにします。 • [ステートフル フェールオーバーの有効化（Enable Stateful Failover）] ドロップダウン リスト：このフィールドは、[ファイアウォール HA の有効化（Enable Firewall HA）] をオンにした場合に表示されます。高可用性モードで ASA のステートフル フェールオーバーを有効にするかまたは無効にするかを選択します。ステートフル フェールオーバーはデフォルトでは無効になっています。 ASAv でフェールオーバーが設定されている場合、Gig0/8 は failover_lan インターフェイスであり、Gig0/7 はステートフル フェールオーバー インターフェイス設定のオプションの failover_link です。 • [トランスペアレントモード（Transparent Mode）] チェック ボックス：トランスペアレント ファイアウォール モードを実行するには、このボックスをオンにします。 このチェック ボックスは、[仮想（VIRTUAL）] ファイアウォール タイプが選択されている場合にのみ表示されます。 （注） この機能は、管理対象のネットワーク サービスがある VDC でサポートされます。

名前	説明
[ロードバランサを許可（Allow Load Balancer）] チェックボックス	このボックスをオンにした場合は、ロード バランサ サービスがレイヤ4～レイヤ7サービス ポリシーに適用可能になります。[ロード バランサを許可（Allow Load Balancer）] を選択すると、次の追加のフィールドが表示されます。 • [ロード バランサ タイプ（Load Balancer Type）] ドロップダウン リスト：ロード バランサ タイプを選択します。 • [デバイス パッケージ（Device Package）] フィールド：リストを展開し、リストからデバイス パッケージを選択します。 • [ロード バランサ HA を有効にする（Enable Load Balancer HA）] チェック ボックス：ロード バランサ サービスのハイ アベイラビリティを有効にするには、このボックスをオンにします。 • [ネットワーク設定（Network Setting）] チェック ボックス：ロード バランサ デバイスの NTP と SNMP 構成を設定するには、このチェック ボックスをオンにします。 • [NTP および SNMP 設定（NTP and SNMP Configuration）] フィールド：このフィールドは、[ネットワーク設定（Network Setting）] チェック ボックスがオンである場合に表示されます。ネットワーク デバイス ポリシーを選択するリストを展開します。選択されたネットワーク デバイス ポリシーの NTP および SNMP 設定は、ロード バランサ デバイスに適用されます。 （注） ロードバランサ サービスは、複数のプライベート ネットワークが備わったテナントでサポート対象となる唯一のサービスです。
[概要（Summary）]：レイヤ 4 ～レイヤ 7 サービス ポリシーの概要が表示されます。	

ステップ 5 [送信（Submit）] をクリックします。

ネットワーク デバイス システム パラメータ ポリシー

ネットワーク デバイス システム パラメータ ポリシーは、ロード バランサ デバイス上で設定されている必要がある NTP および SNMP パラメータを設定します。ネットワーク デバイス システム パラメータ ポリシーは、レイヤ 4 からレイヤ 7 のサービス ポリシーの作成時に、LB デバイスを設定するための NTP および SNMP パラメータを定義するためにオプションで選択します。

APIC コンテナのプロビジョニング時に、対応する NTP および SNMP パラメータが APIC 内のデバイス クラスタに設定され、LB デバイスに設定されるように、アプリケーション プロファイルと作成したレイヤ 4 からレイヤ 7 のサービス ポリシーを選択する必要があります。

ネットワーク デバイス システム パラメータ ポリシーの追加

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [ネットワーク デバイス システム パラメータ ポリシー（Network Device System Parameters Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ネットワーク デバイス システム パラメータ ポリシーの作成（Create Network Device System Parameters Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
パラメータ ポリシー仕様	
[ポリシー名（Policy Name）] フィールド	ネットワーク デバイス システム パラメータ ポリシーの名前を入力します。
[説明（Description）] フィールド	ネットワーク デバイス システム パラメータ ポリシーの説明を入力します。
NTP パラメータ	
[NTP サーバ（NTP Server）] フィールド	NTP サーバのカンマ区切りの IP アドレスまたはホスト名を入力します。
SNMP パラメータ（SNMP Parameters）	

名前	説明
[トラップ クラス（Trap Class）] ドロップダウン リスト	トラップ クラスとして次のいずれかを選択します。 • [固有（Specific）] : デバイス固有のトラップを使用します。 • [汎用（Generic）] : コールドスタート、ウォームスタート、リンク ダウン、リンク アップ、認証失敗、EGP ネイバ ロスなど、定義済みのトラップを実装します。
[トラップ宛先（Trap Destination）] フィールド	管理対象デバイスが受信したトラップをアプライアンスが転送する宛先システムの IP アドレスを入力します。
[コミュニティ名（Community Name）] フィールド	SNMP トラップに関連付けられたグローバルコミュニティ文字列を入力します。デバイスから送信されるトラップは、この文字列をコミュニティ名として渡します。コミュニティ名には、任意の英数字形式を使用できます。ハイフン（-）、ピリオド（.）、シャープ記号（#）、スペース（）、アンパサンド（@）、等号（=）、コロン（:）、およびアンダースコア（_）などの特殊文字を使用できます。
[アクセス許可（Permissions）] ドロップダウン リスト	SNMP マネージャとエージェントの間で情報を伝送するための権限として、次のいずれかを選択します。 • get：SNMP エージェントにアクセスして、1 つ以上の MIB オブジェクトの現在の値を取得します。 • get_next：MIB オブジェクトのツリー全体を順番に参照します。 • get_bulk：メッセージ サイズに対する特定の制約内で、できるだけ大きな単位でデータを取得します。 • set：MIB オブジェクトの現在の値を更新します。 • all
[ユーザ名（User Name）] フィールド	SNMP ユーザの名前を入力します。

名前	説明
[グループ（Group）] フィールド	SNMP グループの名前を入力します。
[認証タイプ（Authentication Type）] ドロップダウン リスト	SNMPユーザの代わりに送信されるメッセージを認証するための認証プロトコルのタイプとして、MD5 または SHA を選択します。
[認証パスワード（Authentication Password）] フィールド	選択した認証タイプに使用するパスワードを入力します。
[プライバシー タイプ（Privacy Type）] ドロップダウン リスト	SNMPユーザの代わりに送信されるメッセージを暗号化するためのプライバシー タイプとして、AES または DES を選択します。
[プライバシー パスワード（Privacy Password）] フィールド	選択したプライバシー タイプに使用するパスワードを入力します。

ステップ 5 [送信（Submit）] をクリックします。

次の作業

レイヤ 4 からレイヤ 7 のサービス ポリシーの作成時には、LB デバイスを設定するための NTP および SNMP パラメータを定義するためのネットワーク デバイス ポリシーを選択します。

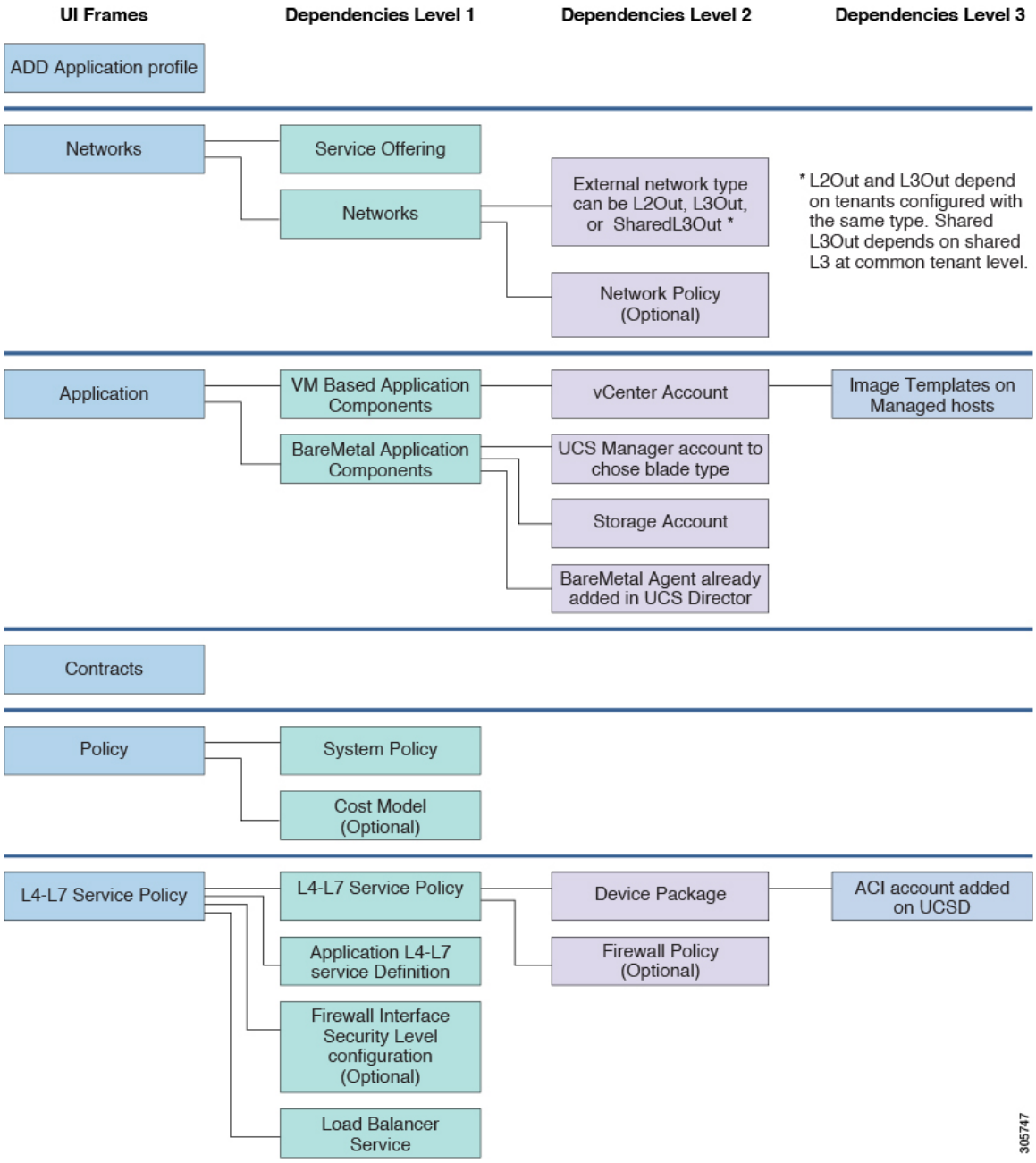
アプリケーション プロファイル

アプリケーション プロファイルは、アプリケーションの導入に必要なインフラストラクチャの説明です。これらのインフラストラクチャの要件には、ベア メタル設定、仮想マシン（VM）、L4-L7 ポリシー、および接続ポリシーが含まれます。

（注） コンテナのプロビジョニングは、VMware 環境または Hyper-V 環境で行うことができます。

次の図は、アプリケーション プロファイルの依存関係を示しています。

図 *4*：アプリケーション プロファイル：依存関係



アプリケーション プロファイルの追加

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [アプリケーション プロファイル（Application Profile）] をクリックします。

ステップ 3 アプリケーション プロファイルが含まれている行をクリックし、[その他のアクション（More Actions）] ドロップダウン リストから [表示（View）] を選択して、アプリケーション プロファイルの名前、説明、およびサービス オファリングを表示します。または [詳細の表示（View Details）] を選択して次を表示します。

名前	説明
[階層(Tiers)]	アプリケーション プロファイルの階層名、説明、物理ネットワーク サービスクラス、および仮想ネットワーク サービス クラスを表示します。
[VM（VMs）]	アプリケーション プロファイルの VM 名、説明、選択されているネットワーク、仮想コンピューティング サービス クラス、および仮想ストレージ サービス クラスが表示されます。
[BM(BMs)]	アプリケーション プロファイルの VM 名、説明、選択されているネットワーク、物理コンピューティング サービス クラス、および物理ストレージ サービス クラスが表示されます。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [プロファイル仕様（Profile Specification）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	アプリケーション プロファイルの名前を入力します。 名前は32 文字以下の英数字で構成する必要があり、_（アンダースコア）、-（ハイフン）、.（ピリオド）、:（コロン）などの特殊文字を使用できます。 追加後は名前を変更できません。
[説明（Description）] フィールド	アプリケーション プロファイルの説明を入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [ネットワーク（Networks）] 画面で、次のフィールドに値を入力します。

名前	説明
[サービス オファリング（Service Offering）] リスト	サービス オファリングを展開して、使用するサービス オファリングをオンにし、[検証（Validate）] をクリックします。提供サービスは、このアプリケーション プロファイルでコンテナを作成するテナントに属している必要があります。 [追加（Add）] をクリックして、サービス オファリングを追加します。『Cisco UCS Director APIC Management Guide』を参照してください。
[ネットワーク（Networks）] リスト	リストを展開し、[追加（Add）] をクリックしてネットワークを設定します。ネットワークの設定方法の詳細については、次の手順を参照してください。

ステップ 8 [追加（Add）] をクリックしてアプリケーションの層を設定します。
[ネットワークへのエントリの追加（Add Entry to Networks）] 画面で、次のフィールドに値を入力します。

名前	説明
[ネットワーク（Network）] フィールド	ネットワークの名前を入力します。
[説明（Description）] フィールド	ネットワークの説明を入力します。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	ネットワーク タイプを選択します。 • [内部（Internal）] • [外部（External）] • [インフラストラクチャ（Infrastructure）] • [フェールオーバー（Failover）] （注） テナントに複数のプライベート ネットワークが必要な場合は、[内部（Internal）] ネットワーク タイプと [外部（External）] ネットワーク タイプのみを定義する必要があります。

名前	説明
[関心のあるタグ値（Interested Tag Value）] リスト	関心のあるタグ値を展開し、使用するタグ値をオンにし、[検証（Validate）] をクリックして、各階層のタグ値を選択します。コンテナのプロビジョニング時に、階層に関連付けられたタグに基づいてリソースが選択されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [内部（Internal）] である場合にのみ表示されます。 （注） 複数のタグ（VMware クラスタまたはデータストア クラスタに使用されるタグ）を選択できます。たとえば、データストアのタグ（ds タグ - ゴールド）と VMware クラスタのタグ（クラスタ タグ - ESXi クラスタ タグ）を選択すると、データストアを選択する際に、ゴールド値のタグが付けられたデータストアが選択されます。 （注） 共有 L3Out のサポートを役立てるには、共通のテナントの外部ネットワークと契約にタグ付けするために使用されるタグ値を選択します。
[APICネットワークポリシー（APIC Network Policy）] ドロップダウンリスト	リストから APIC ネットワーク ポリシーを選択します。 このフィールドは、[ネットワーク タイプ（Network Type）] が [内部（Internal）]、[インフラストラクチャ（Infrastructure）]、または [フェールオーバー（Failover）] である場合にのみ表示されます。 [+] をクリックして、APIC ネットワーク ポリシーを追加します。APIC ネットワーク ポリシーの追加, （91 ページ）を参照してください。

名前	説明
[L2/L3選択（L2/L3 Selection）] ドロップダウンリスト	デフォルトでは、[L2Out] が選択されており、ACI ファブリックが外部レイヤ2ネットワークと統合されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [外部（External）] である場合にのみ表示されます。 次のいずれかを選択できます。 • L2Out：ACI ファブリックを外部レイヤ 2 ネットワークと統合します。 • L3Out：ACI ファブリックを外部レイヤ 3 ネットワークと統合します。 • [SharedL3Out]：ACI ファブリックを共有の外部レイヤ 3 ネットワークと統合します。ネットワークは、テナント vPOD で事前にタグ付けおよび更新されている必要があり、共有 L3Out の場合は、外部ネットワークに対して同じタグが選択されている必要があります。
[テナントで使用可能な既存のL2/L3アウト設定を使用する（Use Existing L2/L3 Out config available in the tenant）] チェックボックス	デフォルトでは、このボックスがオンになっており、コンテナの作成時にテナントで定義されている L2/L3 アウト設定が使用されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [外部（External）] である場合にのみ表示されます。 （注） アプリケーション プロファイルに基づいてコンテナを作成すると、アプリケーション プロファイルでの L2/L3 の選択に応じて、L2 アウトまたは L3 アウトの設定を持つテナントが表示されます。

ステップ 9 [送信（Submit）] をクリックします。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [アプリケーション（Application）] 画面で、次の操作を実行します。

a) [VM ベースのアプリケーション コンポーネント（VM Based Application Components）] を展開して、[+] をクリックします。

b) [VM ベースのアプリケーション コンポーネントへのエントリの追加（Add Entry to VM Based Application Components）] 画面で、次のフィールドに値を入力します。

名前	説明
[VM 名（VM Name）] フィールド	VM の名前を入力します。
[説明（Description）] フィールド	VM の説明を入力します。
[ネットワーク（Network）] ドロップダウン リスト	リストからネットワークを選択します。
[イメージ選択タイプ（Image Selection Type）] ドロップダウン リスト	イメージ選択に関して、次のいずれかを選択します。 • [すべてのイメージ(All Images)] • [イメージタグベースの選択（Image Tag based selection）] : イメージ タグ ベースの選択を選択すると、[タグ（Tag）] リストが表示されます。[+] をクリックして、タグを追加します。
[コンテンツ ライブラリ VM テンプレートを使用した新しい VM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VM イメージテンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。

名前	説明
[VM イメージ（VM Image）] リスト	このフィールドは、[コンテンツ ライブラリ VM テンプレートを使用した新しい VM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス がオフになっている場合にのみ表示されます。VM イメージを展開して、使用する VM イメージをオンにし、[検証（Validate）] をクリックします。リストは、[イメージ選択タイプ（Image Selection Type）] ドロップダウン リストで選択されたオプションによって異なります。 （注） クラウド タイプにかかわらず、すべての VM イメージが管理対象クラウドからリストされます。 （注） 次の基準を満たすイメージの選択肢が表示されます。 • VMware ツールがインストールされているイメージ。 • いずれのグループにも割り当てられていないイメージ。
[リンク済み複製の使用（Use Linked Clone）] チェック ボックス	このチェック ボックスは、スナップショットを使用する VM テンプレートを選択した場合のみ有効です。高速でストレージ効率の高いプロビジョニングが可能なリンク クローン機能を使用して新しい VM を展開するには、このボックスをオンにします。
[スナップショット（Snapshot）] フィールド	このフィールドは、[リンク クローンの使用（Use Linked Clone）] チェック ボックスがオンになっている場合にのみ表示されます。[選択（Select）] をクリックして、リンク クローン機能を使用して新しい VM をプロビジョニングするために使用する必要があるスナップショットを選択します。
[仮想コンピューティング サービス クラス（Virtual Compute Service Class）] ドロップダウン リスト	仮想コンピューティング カテゴリのサービス クラスを選択します。
[仮想ストレージ サービス クラス（Virtual Storage Service Class）] ドロップダウン リスト	仮想ストレージ カテゴリのサービス クラスを選択します。

名前	説明
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	ユーザと VM のルートまたは管理者パスワードを共有する方法を選択します。 • 共有しない • パスワード リセット後に共有する • テンプレート クレデンシャルを共有する パスワード共有オプションとして [パスワード リセット後に共有する（Share after password reset）] または [テンプレート クレデンシャルを共有する（Share template credentials）] を選択したときに表示されるテンプレートのルートログインIDとルート パスワードを指定します。
[VM ネットワーク インターフェイス（VM Network Interfaces）] リスト	リストを展開し、[+] をクリックして、VM ネットワーク インターフェイスを追加します。
[最大数量（Maximum Quantity）] フィールド	階層ごとの VM インスタンスの最大数を入力します。 （注） この数により、各階層のサブネット サイズを決定することができます。この数は、アプリケーション コンテナの導入時に定義される値で上書きされます。この値は、リソースの数がアプリケーション プロファイル内の最大数より少ない場合でも受け入れられます。
[初期数量（Initial Quantity）] フィールド	アプリケーションの作成時にプロビジョニングする VM インスタンスの数を入力します。

c) [送信（Submit）] をクリックします。

ステップ 12 [アプリケーション（Application）] 画面で、次の操作を実行します。

a) [ベア メタル アプリケーション コンポーネント（Bare Metal Application Components）] リストを展開して、[+] をクリックします。

b) [ベア メタル アプリケーション コンポーネントへのエントリの追加（Add Entry to Bare Metal Application Components）] 画面で、次のフィールドに値を入力します。

名前	説明
[インスタンス名（Instance Name）] フィールド	ベア メタル インスタンスの名前を入力します。

名前	説明
[説明（Description）] フィールド	ベア メタル インスタンスの説明を入力します。
[ブート LUN サイズ（GB）（Boot Lun Size (GB)）] フィールド	ブートの推奨 LUN サイズ。
[ネットワーク（Network）] ドロップダウン リスト	ネットワークを選択します。
[ターゲット BMA（Target BMA）] ドロップダウン リスト	PXE セットアップ用のベア メタル エージェント（BMA）を選択します。
[ベア メタルイメージ（Bare Metal Image）] ドロップダウン リスト	ベア メタル イメージを選択します。
[ブレードタイプ（Blade Type）] ドロップダウン リスト	APIC コンテナのブレード タイプとして次のいずれかを選択します。 • ハーフ幅（Half Width） • フル幅（Full Width）
[物理コンピューティング サービス クラス（Physical Compute Service Class）] ドロップダウン リスト	物理コンピューティング カテゴリのサービス クラスを選択します。
[物理ストレージサービスクラス（Physical Storage Service Class）] ドロップダウン リスト	物理ストレージ カテゴリのサービス クラスを選択します。

c) [送信（Submit）] をクリックします。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 [コントラクト（Contracts）] 画面で、多層アプリケーションの通信に関するルールを定義できます。コントラクトは、エンドポイント グループ間（EPG 間）通信を有効にするポリシーです。このポリシーは、アプリケーション層間の通信を指定するルールです。コントラクトが EPG に添付されていない場合は、EPG 間通信がデフォルトで無効になります。EPG 内通信は常に許可されるため、EPG 内通信にはコントラクトが必要ありません。

コントラクトに複数の対象を含めることができます。対象は、単方向または双方向フィルタの実現に使用できます。単方向フィルタは、コンシューマからプロバイダー方向（IN）フィルタとプロバイダーからコンシューマ方向（OUT）フィルタのどちらかの方向で使用されます。双方向フィルタは同じフィルタが両方の方向で使用されます。これは、再帰的ではありません。

新しいコントラクトはソース ネットワークと宛先ネットワークのペアごとに作成されます。たとえば、ソース ネットワークとしての Web 層と宛先ネットワークとしてのアプリケーション層間で複数のルール

が定義されている場合は、ソース ネットワークとしての Web 層と宛先ネットワークとしてのアプリケーション層間のコントラクト情報を保持する単一のコントラクトが APIC 上で作成されます。

コントラクトでは、ルールで単方向または双方向フィルタが定義されている場合に新しい対象が作成されます。対象は、ルールに単方向フィルタと双方向フィルタのどちらが含まれているかによって同じコントラクトの複数のルールで再利用されます。

新しいフィルタは、特定のルールに対して作成されます。新しいフィルタ ルールは、ネットワーク間で定義されたすべてのルールに対して作成されます。

ステップ 15 契約を展開し、[+] をクリックして、通信プロトコルの詳細を追加します。

a) [契約へのエントリの追加（Add Entry to Contracts）] 画面で、次のフィールドに値を入力します。

名前	説明
[ルール名（Rule Name）] フィールド	ルールの名前を入力します。
[ソース ネットワークの選択（Select Source Network）] ドロップダウン リスト	コントラクトルールを適用するソースネットワークを選択します。 送信元ネットワークとして外部ネットワークが選択されている場合、[ルール名（Rule Name）] フィールド、[送信元ネットワークの選択（Select Source Network）] ドロップダウン リスト、および [宛先ネットワークの選択（Select Destination Network）] ドロップダウン リストのみを設定に使用できます。Cisco UCS Director は、選択した外部ネットワークで使用されているタグに基づいて、アプリケーションプロファイルを設定する前に、テナントの vPOD 内で、既存の契約をタグ付きおよび更新済みとして使用します。
[宛先ネットワークの選択（Select Destination Network）] ドロップダウン リスト	コントラクトルールを適用する宛先ネットワークを選択します。
[ルール説明（Rule Description）] フィールド	ルールの説明を入力します。
[プロトコル（Protocol）] ドロップダウン リスト	通信用のプロトコルを選択します。
[双方向を適用する（Apply Both Directions）]チェックボックス	送信元から宛先へのトラフィック（またはその逆のトラフィック）に対して同じ契約を適用する場合には、このボックスをオンにします。
以下のフィールドは、TCP または UDP プロトコルを選択した場合にのみ表示されます。	
[送信元ポートの開始（Source Port Start）] フィールド	送信元ポート番号の開始範囲を入力します。

名前	説明
[送信元ポートの終了（Source Port End）] フィールド	送信元ポート番号の終了範囲を入力します。
[送信先ポートの開始（Destination Port Start）] フィールド	宛先ポート番号の開始範囲を入力します。
[送信先ポートの終了（Destination Port End）] フィールド	宛先ポート番号の終了範囲を入力します。
[ステートフル（Stateful）] チェック ボックス	このチェック ボックスは、TCP プロトコルを選択した場合に表示されます。チェック ボックスをオンにして、ステートフル接続を有効にします。
[アクション（Action）] ドロップダウン リスト	通信に対して実行するアクションを選択します。 • 承認（Accept） • 削除（Drop） • 却下（Reject）

b) [送信（Submit）] をクリックします。

ステップ 16 [次へ（Next）] をクリックします。

ステップ 17 [ポリシー（Policy）] 画面で、次の手順を実行します。

a) [VMware システムポリシー（VMware System Policy）] ドロップダウンリストからポリシーを選択します。

b) これはオプションです。[システム ポリシー（System Policy）] ドロップダウン リストに新しいポリシーを追加するには、[+] をクリックします。

c) [システム ポリシー情報（System Policy Information）] 画面で、次のフィールドに値を入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	システム ポリシーの名前を入力します。
[ポリシーの説明（Policy Description）] フィールド	システム ポリシーの説明を入力します。
[VM名のテンプレート（VM Name Template）] フィールド	VM 名に使用するテンプレートを入力します。 （注） 名前テンプレートが指定されない場合、ユーザが入力する名前が VM 名として使用されます。

名前	説明
[VM 名の一意性チェックの無効化（Disable VM Name Uniqueness Check）] チェック ボックス	VM 名の一意性の検証をスキップするには、このチェック ボックスをオンにします。
[VM名の検証ポリシー（VM Name Validation Policy）] ドロップダウンリスト	VM 名を検証するポリシーを選択します。
[エンドユーザVM名またはVMプレフィクス（End User VM Name or VM Prefix）] チェックボックス	ユーザに VM の名前またはプレフィックスの指定を許可する場合に、このボックスをオンにします。
[導入後に電源をオンにします（Power On after deploy）] チェック ボックス	プロビジョニング後に VM の電源をオンにする場合に、このボックスをオンにします。
[ホスト名のテンプレート（Host Name Template）] フィールド	ホスト名のテンプレートを入力します。
[ホスト名の一意性のチェックの無効化（Disable Host Name Uniqueness Check）] チェック ボックス	ホスト名の一意性の検証をスキップするには、このチェック ボックスをオンにします。
[ホスト名の検証ポリシー（Host Name Validation Policy）] ドロップダウンリスト	ホスト名を検証するポリシーを選択します。
[Linuxタイムゾーン（Linux Time Zone）] ドロップダウン リスト	Linux VM のタイム ゾーンを選択します。
[Linux VM最大ブート待機時間（Linux VM Max Boot Wait Time）] ドロップダウン リスト	VM が起動中に一時停止する最大時間の値を選択します。
[DNSドメイン（DNS Domain）] フィールド	DNS ドメインの名前を入力します。
[DNSサフィックスリスト（DNS Suffix List）] フィールド	DNS に付加するドメイン名サフィックスのリストを入力します。
[DNSサーバリスト（DNS Server List）] フィールド	DNS サーバのリストを入力します。
[VMイメージのタイプ（VM Image Type）] ドロップダウン リスト	VM イメージ タイプとして次のいずれかを選択します。 • Windows と Linux • Linux のみ

名前	説明
[VMアノテーションの定義（Define VM Annotation）] チェックボックス	注釈は、アプリケーション/Web階層が、APICネットワーク ポリシーを通じて、サブネットを共有およびパブリックとして作成することを許可することを示します。VM アノテーションを定義する場合に、このボックスをオンにします。
[VM の注記（VM Annotation）] フィールド	このフィールドは、[VM アノテーションの定義（Define VM Annotation）] チェック ボックスをオンにしている場合に表示されます。VM の注釈を入力します。
[カスタム属性（Custom Attributes）] フィールド	このフィールドは、[VM アノテーションの定義（Define VM Annotation）] チェック ボックスをオンにしている場合に表示されます。カスタム属性を展開し、[+] をクリックしてカスタム属性を追加します。

d) [送信（Submit）] をクリックします。
e) [コスト モデル（Cost Model）] ドロップ ダウン リストで、チャージバックを計算するコスト モデルを選択します。
f) [HyperV 展開ポリシー（HyperV Deployment Policy）] を展開し、HyperV コンテナ プロビジョニング用の HyperV 展開ポリシーを調べます。
g) [次へ（Next）] をクリックします。

ステップ 18 [L4-L7 サービスポリシー（L4-L7 Service Policy）] 画面で、[L4-L7 サービスの設定（Configure L4-L7 Service）] チェック ボックスをオンにし、アプリケーション プロファイルにレイヤ 4 ～レイヤ 7 サービスを設定します。[L4-L7 サービスの設定（Configure L4-L7 Service）] チェック ボックスがオンになっている場合には、次のフィールドに値を入力します。

a) [L4-L7サービスポリシー（L4-L7 Service Policy）] ドロップダウンリスト：リストからレイヤ 4 ～レイヤ 7 サービス ポリシーを選択します。[+] をクリックして、レイヤ 4 ～レイヤ 7 サービス ポリシーを追加します。レイヤ 4 ～レイヤ 7 サービス ポリシーの追加, （94 ページ）を参照してください。
b) [アプリケーション L4-L7 サービス定義（Application L4-L7 Service Definition）] リスト：アプリケーション L4-L7 サービス定義を展開して、[+] をクリックします。[アプリケーション L4-L7 サービス定義へのエントリの追加（Add Entry to Application L4-L7 Service Definition）] 画面で、次のフィールドに値を入力します。

名前	説明
[サービス名（Service Name）] フィールド	サービスの名前を入力します。

名前	説明
[コンシューマ（Consumer）] ドロップダウン リスト	内部階層を選択します。 （注） 階層間でASA/ASAvを展開する場合は、レイヤ2ネットワークがあるテナントに依存せずに、共有レイヤ3ネットワークがある VDC を作成できます。
[プロバイダー（Provider）] ドロップダウン リスト	外部階層を選択します。
[プロトコル（Protocol）] ドロップダウン リスト	プロトコルを選択します。 （注） このフィールドは、ロード バランサ サービスのみに表示されます。
[ポート（Port）] ドロップダウン リスト	選択したプロトコルのポート番号を選択します。 （注） このフィールドは、ロード バランサ サービスのみに表示されます。

名前	説明
[サービス（Services）] リスト	リストを展開して、次のボックスのいずれかをオンにしてサービス タイプを選択します。 • [ファイアウォール（FIREWALL）]：コンシューマとプロバイダー間にファイアウォール サービスを提供します。 • [LB_SINGLE_ARM]：シングルアーム モードのコンシューマとプロバイダー間にロード バランサ サービスを設定します。シングルアーム モードでは、1つのインターフェイスを通じてロード バランサがネットワークに接続します。 （注） シングルアーム ロード バランサ サービスは、複数のプライベート ネットワークが備わったテナントでサポート対象となる唯一のサービス タイプです。 • [FW_LB_ONE_ARM]：コンシューマとプロバイダー間にファイアウォールとシングルアーム ロード バランサ サービスを設定します。シングルアーム モードでは、1つのインターフェイスを通じてロードバランサがネットワークに接続します。 • [LB_DUAL_ARM]：デュアルアーム モードのコンシューマとプロバイダー間にロード バランサ サービスを設定します。デュアルアーム モードでは、2つの異なるインターフェイスを持つコンシューマとプロバイダーにロード バランサが接続されます。 • FW_LB_SSL_OFFLOAD：コンシューマとプロバイダーの間に、SSL オフロードのサポートと共に、ファイアウォールとロード バランサ サービスの両方を設定します。

c) アプリケーション プロファイルでネットワーク階層のファイアウォール セキュリティをカスタマイズするには、[階層のファイアウォール セキュリティをカスタマイズする（Customize Firewall Security For Tiers）] ボックスをオンにします。

d) [階層のファイアウォール セキュリティをカスタマイズする（Customize Firewall Security For Tiers）] チェック ボックスがオンになっている場合に表示されるファイアウォールセキュリティ レベルを展開します。セキュリティ レベルを変更するには、階層を選択し、[編集（Edit）] をクリックします。

ステップ 19 [送信（Submit）] をクリックします。

アプリケーション プロファイルの複製

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [アプリケーション プロファイル（Application Profile）] をクリックします。

ステップ 3 複製するアプリケーション プロファイルを含む行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [複製（Clone）] を選択します。

ステップ 5 [プロファイル仕様（Profile Specification）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	アプリケーション プロファイルの名前を入力します。 名前は32文字以下の英数字で構成する必要があり、_（アンダースコア）、-（ハイフン）、.（ピリオド）、:（コロン）などの特殊文字を使用できます。 追加後は名前を変更できません。
[説明（Description）] フィールド	アプリケーション プロファイルの説明を入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [ネットワーク（Networks）] 画面で、次のフィールドに値を入力します。

名前	説明
[サービス オファリング（Service Offering）] リスト	サービス オファリングを展開して、使用するサービス オファリングをオンにし、[検証（Validate）] をクリックします。提供サービスは、このアプリケーション プロファイルでコンテナを作成するテナントに属している必要があります。 [追加（Add）] をクリックして、サービス オファリングを追加します。『Cisco UCS Director APIC Management Guide』を参照してください。
[ネットワーク（Networks）] リスト	リストを展開し、[追加（Add）] をクリックしてネットワークを設定します。ネットワークの設定方法の詳細については、次の手順を参照してください。

ステップ 8 [追加（Add）] をクリックしてアプリケーションの層を設定します。
[ネットワークへのエントリの追加（Add Entry to Networks）] 画面で、次のフィールドに値を入力します。

名前	説明
[ネットワーク（Network）] フィールド	ネットワークの名前を入力します。
[説明（Description）] フィールド	ネットワークの説明を入力します。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	ネットワーク タイプを選択します。 • [内部（Internal）] • [外部（External）] • [インフラストラクチャ（Infrastructure）] • [フェールオーバー（Failover）] （注） テナントに複数のプライベート ネットワークが必要な場合は、[内部（Internal）] ネットワーク タイプと [外部（External）] ネットワーク タイプのみを定義する必要があります。

名前	説明
[関心のあるタグ値（Interested Tag Value）] リスト	関心のあるタグ値を展開し、使用するタグ値をオンにし、[検証（Validate）] をクリックして、各階層のタグ値を選択します。コンテナのプロビジョニング時に、階層に関連付けられたタグに基づいてリソースが選択されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [内部（Internal）] である場合にのみ表示されます。 （注） 複数のタグ（VMware クラスタまたはデータストア クラスタに使用されるタグ）を選択できます。たとえば、データストアのタグ（ds タグ - ゴールド）と VMware クラスタのタグ（クラスタ タグ - ESXi クラスタ タグ）を選択すると、データストアを選択する際に、ゴールド値のタグが付けられたデータストアが選択されます。 （注） 共有 L3Out のサポートを役立てるには、共通のテナントの外部ネットワークと契約にタグ付けするために使用されるタグ値を選択します。
[APICネットワークポリシー（APIC Network Policy）] ドロップダウンリスト	リストから APIC ネットワーク ポリシーを選択します。 このフィールドは、[ネットワーク タイプ（Network Type）] が [内部（Internal）]、[インフラストラクチャ（Infrastructure）]、または [フェールオーバー（Failover）] である場合にのみ表示されます。 [+] をクリックして、APIC ネットワーク ポリシーを追加します。APIC ネットワーク ポリシーの追加, （91 ページ）を参照してください。

名前	説明
[L2/L3選択（L2/L3 Selection）] ドロップダウンリスト	デフォルトでは、[L2Out] が選択されており、ACI ファブリックが外部レイヤ2ネットワークと統合されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [外部（External）] である場合にのみ表示されます。 次のいずれかを選択できます。 • L2Out：ACI ファブリックを外部レイヤ 2 ネットワークと統合します。 • L3Out：ACI ファブリックを外部レイヤ 3 ネットワークと統合します。 • [SharedL3Out]：ACI ファブリックを共有の外部レイヤ 3 ネットワークと統合します。ネットワークは、テナント vPOD で事前にタグ付けおよび更新されている必要があり、共有 L3Out の場合は、外部ネットワークに対して同じタグが選択されている必要があります。
[テナントで使用可能な既存のL2/L3アウト設定を使用する（Use Existing L2/L3 Out config available in the tenant）] チェックボックス	デフォルトでは、このボックスがオンになっており、コンテナの作成時にテナントで定義されている L2/L3 アウト設定が使用されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [外部（External）] である場合にのみ表示されます。 （注） アプリケーション プロファイルに基づいてコンテナを作成すると、アプリケーション プロファイルでの L2/L3 の選択に応じて、L2 アウトまたは L3 アウトの設定を持つテナントが表示されます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [アプリケーション（Application）] 画面で、VM ベースのアプリケーション コンポーネントを追加します。

a) [+] をクリックします。

b) [VM アプリケーション コンポーネントへのエントリの追加（Add Entry to VM Application Components）] 画面で、次のフィールドに値を入力します。

名前	説明
[VM 名（VM Name）] フィールド	VM の名前を入力します。
[説明（Description）] フィールド	VM の説明を入力します。
[ネットワーク（Network）] ドロップダウン リスト	リストからネットワークを選択します。
[イメージ選択タイプ（Image Selection Type）] ドロップダウン リスト	イメージ選択に関して、次のいずれかを選択します。 • [すべてのイメージ(All Images)] • [イメージ タグ ベースの選択（Image Tag based selection）] : イメージ タグ ベースの選択を選択すると、[タグ（Tag）] リストが表示されます。[+] をクリックして、タグを追加します。
[コンテンツ ライブラリ VM テンプレートを使用した新しい VM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VM イメージ テンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。

名前	説明
[VM イメージ（VM Image）] リスト	このフィールドは、[コンテンツ ライブラリ VM テンプレートを使用した新しい VM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス がオフになっている場合にのみ表示されます。VM イメージを展開して、使用する VM イメージをオンにし、[検証（Validate）] をクリックします。リストは、[イメージ選択タイプ（Image Selection Type）] ドロップダウン リストで選択されたオプションによって異なります。 （注） クラウド タイプにかかわらず、すべての VM イメージが管理対象クラウドからリストされます。 （注） 次の基準を満たすイメージの選択肢が表示されます。 • VMware ツールがインストールされているイメージ。 • いずれのグループにも割り当てられていないイメージ。
[リンク済み複製の使用（Use Linked Clone）] チェック ボックス	このチェック ボックスは、スナップショットを使用する VM テンプレートを選択した場合のみ有効です。高速でストレージ効率の高いプロビジョニングが可能なリンク クローン機能を使用して新しい VM を展開するには、このボックスをオンにします。
[スナップショット（Snapshot）] フィールド	このフィールドは、[リンク クローンの使用（Use Linked Clone）] チェック ボックスがオンになっている場合にのみ表示されます。[選択（Select）] をクリックして、リンク クローン機能を使用して新しい VM をプロビジョニングするために使用する必要があるスナップショットを選択します。
[仮想コンピューティング サービス クラス（Virtual Compute Service Class）] ドロップダウン リスト	仮想コンピューティング カテゴリのサービス クラスを選択します。
[仮想ストレージ サービス クラス（Virtual Storage Service Class）] ドロップダウン リスト	仮想ストレージ カテゴリのサービス クラスを選択します。

名前	説明
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	ユーザと VM のルートまたは管理者パスワードを共有する方法を選択します。 • 共有しない • パスワード リセット後に共有する • テンプレート クレデンシャルを共有する パスワード共有オプションとして [パスワード リセット後に共有する（Share after password reset）] または [テンプレート クレデンシャルを共有する（Share template credentials）] を選択したときに表示されるテンプレートのルートログインIDとルート パスワードを指定します。
[VM ネットワーク インターフェイス（VM Network Interfaces）] リスト	リストを展開し、[+] をクリックして、VM ネットワーク インターフェイスを追加します。
[最大数量（Maximum Quantity）] フィールド	階層ごとの VM インスタンスの最大数を入力します。 （注） この数により、各階層のサブネット サイズを決定することができます。この数は、アプリケーション コンテナの導入時に定義される値で上書きされます。この値は、リソースの数がアプリケーション プロファイル内の最大数より少ない場合でも受け入れられます。
[初期数量（Initial Quantity）] フィールド	アプリケーションの作成時にプロビジョニングする VM インスタンスの数を入力します。

c) [送信（Submit）] をクリックします。

ステップ 11 [アプリケーション（Application）] 画面で、ベア メタル アプリケーション コンポーネントを追加します。

a) [+] をクリックします。

b) [ベア メタル アプリケーション コンポーネントへのエントリの追加（Add Entry to Bare Metal Application Components）] 画面で、次のフィールドに値を入力します。

名前	説明
[インスタンス名（Instance Name）] フィールド	ベア メタル インスタンスの名前を入力します。
[説明（Description）] フィールド	ベア メタル インスタンスの説明を入力します。

名前	説明
[ブート LUN サイズ（GB）（Boot Lun Size (GB)）] フィールド	ブートの推奨 LUN サイズ。
[ネットワーク（Network）] ドロップダウン リスト	ネットワークを選択します。
[ターゲット BMA（Target BMA）] ドロップダウン リスト	PXE セットアップ用のベア メタル エージェント（BMA）を選択します。
[ベア メタルイメージ（Bare Metal Image）] ドロップダウン リスト	ベア メタル イメージを選択します。
[ブレードタイプ（Blade Type）] ドロップダウン リスト	APIC コンテナのブレード タイプとして次のいずれかを選択します。 • ハーフ幅（Half Width） • フル幅（Full Width）
[物理コンピューティング サービス クラス（Physical Compute Service Class）] ドロップダウン リスト	物理コンピューティング カテゴリのサービス クラスを選択します。
[物理ストレージ サービス クラス（Physical Storage Service Class）] ドロップダウン リスト	物理ストレージ カテゴリのサービス クラスを選択します。

c) [送信（Submit）] をクリックします。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 通信プロトコルの詳細を追加するには、[契約（Contracts）] 画面で [+] をクリックします。

a) [契約へのエントリの追加（Add Entry to Contracts）] 画面で、次のフィールドに値を入力します。

名前	説明
[ルール名（Rule Name）] フィールド	ルールの名前を入力します。

名前	説明
[ソース ネットワークの選択（Select Source Network）] ドロップダウン リスト	コントラクトルールを適用するソースネットワークを選択します。 送信元ネットワークとして外部ネットワークが選択されている場合、[ルール名（Rule Name）] フィールド、[送信元ネットワークの選択（Select Source Network）] ドロップダウン リスト、および [宛先ネットワークの選択（Select Destination Network）] ドロップダウン リストのみを設定に使用できます。Cisco UCS Director は、選択した外部ネットワークで使用されているタグに基づいて、アプリケーションプロファイルを設定する前に、テナントの vPOD 内で、既存の契約をタグ付きおよび更新済みとして使用します。
[宛先ネットワークの選択（Select Destination Network）] ドロップダウン リスト	コントラクトルールを適用する宛先ネットワークを選択します。
[ルール説明（Rule Description）] フィールド	ルールの説明を入力します。
[プロトコル（Protocol）] ドロップダウン リスト	通信用のプロトコルを選択します。
[双方向を適用する（Apply Both Directions）]チェックボックス	送信元から宛先へのトラフィック（またはその逆のトラフィック）に対して同じ契約を適用する場合には、このボックスをオンにします。
以下のフィールドは、TCP または UDP プロトコルを選択した場合にのみ表示されます。	
[送信元ポートの開始（Source Port Start）] フィールド	送信元ポート番号の開始範囲を入力します。
[送信元ポートの終了（Source Port End）] フィールド	送信元ポート番号の終了範囲を入力します。
[送信先ポートの開始（Destination Port Start）] フィールド	宛先ポート番号の開始範囲を入力します。
[送信先ポートの終了（Destination Port End）] フィールド	宛先ポート番号の終了範囲を入力します。
[ステートフル（Stateful）] チェック ボックス	このチェック ボックスは、TCP プロトコルを選択した場合に表示されます。チェック ボックスをオンにして、ステートフル接続を有効にします。

名前	説明
[アクション（Action）] ドロップダウン リスト	通信に対して実行するアクションを選択します。 • 承認（Accept） • 削除（Drop） • 却下（Reject）

b) [送信（Submit）] をクリックします。

ステップ 14 [次へ（Next）] をクリックします。

ステップ 15 [ポリシー（Policy）] 画面で、次の手順を実行します。

a) [VMware システムポリシー（VMware System Policy）] ドロップダウンリストからポリシーを選択します。

b) これはオプションです。[システム ポリシー（System Policy）] ドロップダウン リストに新しいポリシーを追加するには、[+] をクリックします。

c) [システム ポリシー情報（System Policy Information）] 画面で、次のフィールドに値を入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	システム ポリシーの名前を入力します。
[ポリシーの説明（Policy Description）] フィールド	システム ポリシーの説明を入力します。
[VM名のテンプレート（VM Name Template）] フィールド	VM 名に使用するテンプレートを入力します。 （注） 名前テンプレートが指定されない場合、ユーザが入力する名前が VM 名として使用されます。
[VM 名の一意性チェックの無効化（Disable VM Name Uniqueness Check）] チェック ボックス	VM 名の一意性の検証をスキップするには、このチェック ボックスをオンにします。
[VM名の検証ポリシー（VM Name Validation Policy）] ドロップダウンリスト	VM 名を検証するポリシーを選択します。
[エンドユーザVM名またはVMプレフィクス（End User VM Name or VM Prefix）] チェックボックス	ユーザに VM の名前またはプレフィックスの指定を許可する場合に、このボックスをオンにします。
[導入後に電源をオンにします（Power On after deploy）] チェック ボックス	プロビジョニング後に VM の電源をオンにする場合に、このボックスをオンにします。

名前	説明
[ホスト名のテンプレート（Host Name Template）] フィールド	ホスト名のテンプレートを入力します。
[ホスト名の一意性のチェックの無効化（Disable Host Name Uniqueness Check）] チェック ボックス	ホスト名の一意性の検証をスキップするには、このチェック ボックスをオンにします。
[ホスト名の検証ポリシー（Host Name Validation Policy）] ドロップダウンリスト	ホスト名を検証するポリシーを選択します。
[Linuxタイムゾーン（Linux Time Zone）] ドロップダウン リスト	Linux VM のタイム ゾーンを選択します。
[Linux VM最大ブート待機時間（Linux VM Max Boot Wait Time）] ドロップダウン リスト	VM が起動中に一時停止する最大時間の値を選択します。
[DNSドメイン（DNS Domain）] フィールド	DNS ドメインの名前を入力します。
[DNSサフィックスリスト（DNS Suffix List）] フィールド	DNSに付加するドメイン名サフィックスのリストを入力します。
[DNSサーバリスト（DNS Server List）] フィールド	DNS サーバのリストを入力します。
[VMイメージのタイプ（VM Image Type）] ドロップダウン リスト	VMイメージタイプとして次のいずれかを選択します。 • Windows と Linux • Linux のみ
[VMアノテーションの定義（Define VM Annotation）] チェックボックス	注釈は、アプリケーション/Web階層が、APICネットワーク ポリシーを通じて、サブネットを共有およびパブリックとして作成することを許可することを示します。VM アノテーションを定義する場合に、このボックスをオンにします。
[VM の注記（VM Annotation）] フィールド	このフィールドは、[VM アノテーションの定義（Define VM Annotation）] チェック ボックスをオンにしている場合に表示されます。VM の注釈を入力します。

名前	説明
[カスタム属性（Custom Attributes）] フィールド	このフィールドは、[VM アノテーションの定義（Define VM Annotation）] チェック ボックスをオンにしている場合に表示されます。カスタム属性を展開し、[+] をクリックしてカスタム属性を追加します。

d) [送信（Submit）] をクリックします。
e) [コスト モデル（Cost Model）] ドロップ ダウン リストで、チャージバックを計算するコスト モデルを選択します。
f) [HyperV 展開ポリシー（HyperV Deployment Policy）] を展開し、HyperV コンテナ プロビジョニング用の HyperV 展開ポリシーを調べます。
g) [次へ（Next）] をクリックします。

ステップ 16 [L4-L7 サービスポリシー（L4-L7 Service Policy）] 画面で、[L4-L7 サービスの設定（Configure L4-L7 Service）] チェック ボックスをオンにし、アプリケーション プロファイルにレイヤ 4 ～レイヤ 7 サービスを設定します。[L4-L7 サービスの設定（Configure L4-L7 Service）] チェック ボックスがオンになっている場合には、次のフィールドに値を入力します。

a) [L4-L7サービスポリシー（L4-L7 Service Policy）] ドロップダウンリスト：リストからレイヤ 4 ～レイヤ 7 サービス ポリシーを選択します。[+] をクリックして、レイヤ 4 ～レイヤ 7 サービス ポリシーを追加します。レイヤ 4 ～レイヤ 7 サービス ポリシーの追加, （94 ページ）を参照してください。
b) [アプリケーション L4-L7 サービス定義（Application L4-L7 Service Definition）] リスト：アプリケーション L4-L7 サービス定義を展開して、[+] をクリックします。[アプリケーション L4-L7 サービス定義へのエントリの追加（Add Entry to Application L4-L7 Service Definition）] 画面で、次のフィールドに値を入力します。

名前	説明
[サービス名（Service Name）] フィールド	サービスの名前を入力します。
[コンシューマ（Consumer）] ドロップダウン リスト	内部階層を選択します。 （注） 階層間で ASA/ASAv を展開する場合は、レイヤ 2 ネットワークがあるテナントに依存せずに、共有レイヤ 3 ネットワークがある VDC を作成できます。
[プロバイダー（Provider）] ドロップダウン リスト	外部階層を選択します。
[プロトコル（Protocol）] ドロップダウン リスト	プロトコルを選択します。 （注） このフィールドは、ロード バランサ サービスのみに表示されます。

名前	説明
[ポート（Port）] ドロップダウン リスト	選択したプロトコルのポート番号を選択します。 （注） このフィールドは、ロード バランサ サービスのみに表示されます。
[サービス（Services）] リスト	リストを展開して、次のボックスのいずれかをオンにしてサービス タイプを選択します。 • [ファイアウォール（FIREWALL）]：コンシューマとプロバイダー間にファイアウォール サービスを提供します。 • [LB_SINGLE_ARM]：シングルアーム モードのコンシューマとプロバイダー間にロード バランサ サービスを設定します。シングルアーム モードでは、1 つのインターフェイスを通じてロード バランサがネットワークに接続します。 （注） シングルアーム ロード バランサ サービスは、複数のプライベート ネットワークが備わったテナントでサポート対象となる唯一のサービス タイプです。 • [FW_LB_ONE_ARM]：コンシューマとプロバイダー間にファイアウォールとシングルアーム ロード バランサ サービスを設定します。シングルアーム モードでは、1 つのインターフェイスを通じてロードバランサがネットワークに接続します。 • [LB_DUAL_ARM]：デュアルアーム モードのコンシューマとプロバイダー間にロード バランサ サービスを設定します。デュアルアーム モードでは、2 つの異なるインターフェイスを持つコンシューマとプロバイダーにロード バランサが接続されます。 • FW_LB_SSL_OFFLOAD：コンシューマとプロバイダーの間に、SSL オフロードのサポートと共に、ファイアウォールとロード バランサ サービスの両方を設定します。

c) アプリケーション プロファイルでネットワーク階層のファイアウォール セキュリティをカスタマイズするには、[階層のファイアウォール セキュリティをカスタマイズする（Customize Firewall Security For Tiers）] ボックスをオンにします。

d) [階層のファイアウォール セキュリティをカスタマイズする（Customize Firewall Security For Tiers）] チェック ボックスがオンになっている場合に表示されるファイアウォール セキュリティ レベルを展開します。セキュリティ レベルを変更するには、階層を選択し、[編集（Edit）] をクリックします。

ステップ 17 [送信（Submit）] をクリックします。

アプリケーション プロファイルの編集

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [アプリケーション プロファイル（Application Profile）] をクリックします。

ステップ 3 編集するアプリケーション プロファイルを含む行をクリックします。

ステップ 4 [編集（Edit）] をクリックします。

ステップ 5 [プロファイル仕様（Profile Specification）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	アプリケーション プロファイルの名前を入力します。 名前は32文字以下の英数字で構成する必要があり、_（アンダースコア）、-（ハイフン）、.（ピリオド）、:（コロン）などの特殊文字を使用できます。 追加後は名前を変更できません。
[説明（Description）] フィールド	アプリケーション プロファイルの説明を入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [ネットワーク（Networks）] 画面で、次のフィールドに値を入力します。

名前	説明
[提供サービス（Service Offering）] フィールド	アプリケーション プロファイルの作成時に選択されたサービス オファリングが表示されます。これは変更できません。

名前	説明
[ネットワーク（Networks）] フィールド	リストを展開して、アプリケーションで必要なネットワーク タイプとネットワークの数を定義します。ネットワークの設定方法の詳細については、次の手順を参照してください。

ステップ 8 [追加（Add）] をクリックしてアプリケーションの層を設定します。
[ネットワークへのエントリの追加（Add Entry to Networks）] 画面で、次のフィールドに値を入力します。

名前	説明
[ネットワーク（Network）] フィールド	ネットワークの名前を入力します。
[説明（Description）] フィールド	ネットワークの説明を入力します。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	ネットワーク タイプを選択します。 • [内部（Internal）] • [外部（External）] • [インフラストラクチャ（Infrastructure）] • [フェールオーバー（Failover）] （注） テナントに複数のプライベート ネットワークが必要な場合は、[内部（Internal）] ネットワーク タイプと [外部（External）] ネットワーク タイプのみを定義する必要があります。

名前	説明
[関心のあるタグ値（Interested Tag Value）] リスト	関心のあるタグ値を展開し、使用するタグ値をオンにし、[検証（Validate）] をクリックして、各階層のタグ値を選択します。コンテナのプロビジョニング時に、階層に関連付けられたタグに基づいてリソースが選択されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [内部（Internal）] である場合にのみ表示されます。 （注） 複数のタグ（VMware クラスタまたはデータストア クラスタに使用されるタグ）を選択できます。たとえば、データストアのタグ（ds タグ - ゴールド）と VMware クラスタのタグ（クラスタ タグ - ESXi クラスタ タグ）を選択すると、データストアを選択する際に、ゴールド値のタグが付けられたデータストアが選択されます。 （注） 共有 L3Out のサポートを役立てるには、共通のテナントの外部ネットワークと契約にタグ付けするために使用されるタグ値を選択します。
[APIC ネットワークポリシー（APIC Network Policy）] ドロップダウンリスト	リストから APIC ネットワーク ポリシーを選択します。 このフィールドは、[ネットワーク タイプ（Network Type）] が [内部（Internal）]、[インフラストラクチャ（Infrastructure）]、または [フェールオーバー（Failover）] である場合にのみ表示されます。 [+] をクリックして、APIC ネットワーク ポリシーを追加します。APIC ネットワーク ポリシーの追加, （91 ページ） を参照してください。

名前	説明
[L2/L3選択（L2/L3 Selection）] ドロップダウンリスト	デフォルトでは、[L2Out] が選択されており、ACI ファブリックが外部レイヤ2ネットワークと統合されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [外部（External）] である場合にのみ表示されます。 次のいずれかを選択できます。 • L2Out：ACI ファブリックを外部レイヤ 2 ネットワークと統合します。 • L3Out：ACI ファブリックを外部レイヤ 3 ネットワークと統合します。 • [SharedL3Out]：ACI ファブリックを共有の外部レイヤ 3 ネットワークと統合します。ネットワークは、テナント vPOD で事前にタグ付けおよび更新されている必要があり、共有 L3Out の場合は、外部ネットワークに対して同じタグが選択されている必要があります。
[テナントで使用可能な既存のL2/L3アウト設定を使用する（Use Existing L2/L3 Out config available in the tenant）] チェックボックス	デフォルトでは、このボックスがオンになっており、コンテナの作成時にテナントで定義されている L2/L3 アウト設定が使用されます。 このフィールドは、[ネットワーク タイプ（Network Type）] が [外部（External）] である場合にのみ表示されます。 （注） アプリケーション プロファイルに基づいてコンテナを作成すると、アプリケーション プロファイルでの L2/L3 の選択に応じて、L2 アウトまたは L3 アウトの設定を持つテナントが表示されます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [アプリケーション（Application）] 画面で、VM ベースのアプリケーション コンポーネントを追加します。

a) [+] をクリックします。

b) [VM アプリケーション コンポーネントへのエントリの追加（Add Entry to VM Application Components）] 画面で、次のフィールドに値を入力します。

名前	説明
[VM 名（VM Name）] フィールド	VM の名前を入力します。
[説明（Description）] フィールド	VM の説明を入力します。
[ネットワーク（Network）] ドロップダウン リスト	リストからネットワークを選択します。
[イメージ選択タイプ（Image Selection Type）] ドロップダウン リスト	イメージ選択に関して、次のいずれかを選択します。 • [すべてのイメージ(All Images)] • [イメージ タグ ベースの選択（Image Tag based selection）] : イメージ タグ ベースの選択を選択すると、[タグ（Tag）] リストが表示されます。[+] をクリックして、タグを追加します。
[コンテンツ ライブラリ VM テンプレートを使用した新しい VM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VM イメージテンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。

名前	説明
[VM イメージ（VM Image）] リスト	このフィールドは、[コンテンツ ライブラリ VM テンプレートを使用した新しい VM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス がオフになっている場合にのみ表示されます。VM イメージを展開して、使用する VM イメージをオンにし、[検証（Validate）] をクリックします。リストは、[イメージ選択タイプ（Image Selection Type）] ドロップダウン リストで選択されたオプションによって異なります。 （注） クラウド タイプにかかわらず、すべての VM イメージが管理対象クラウドからリストされます。 （注） 次の基準を満たすイメージの選択肢が表示されます。 • VMware ツールがインストールされているイメージ。 • いずれのグループにも割り当てられていないイメージ。
[リンク済み複製の使用（Use Linked Clone）] チェック ボックス	このチェック ボックスは、スナップショットを使用する VM テンプレートを選択した場合のみ有効です。高速でストレージ効率の高いプロビジョニングが可能なリンク クローン機能を使用して新しい VM を展開するには、このボックスをオンにします。
[スナップショット（Snapshot）] フィールド	このフィールドは、[リンク クローンの使用（Use Linked Clone）] チェック ボックスがオンになっている場合にのみ表示されます。[選択（Select）] をクリックして、リンク クローン機能を使用して新しい VM をプロビジョニングするために使用する必要があるスナップショットを選択します。
[仮想コンピューティング サービス クラス（Virtual Compute Service Class）] ドロップダウン リスト	仮想コンピューティング カテゴリのサービス クラスを選択します。
[仮想ストレージ サービス クラス（Virtual Storage Service Class）] ドロップダウン リスト	仮想ストレージ カテゴリのサービス クラスを選択します。

名前	説明
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	ユーザと VM のルートまたは管理者パスワードを共有する方法を選択します。 • 共有しない • パスワード リセット後に共有する • テンプレート クレデンシャルを共有する パスワード共有オプションとして [パスワード リセット後に共有する（Share after password reset）] または [テンプレート クレデンシャルを共有する（Share template credentials）] を選択したときに表示されるテンプレートのルート ログイン ID とルート パスワードを指定します。
[VM ネットワーク インターフェイス（VM Network Interfaces）] リスト	リストを展開し、[+] をクリックして、VM ネットワーク インターフェイスを追加します。
[最大数量（Maximum Quantity）] フィールド	階層ごとの VM インスタンスの最大数を入力します。 （注） この数により、各階層のサブネット サイズを決定することができます。この数は、アプリケーション コンテナの導入時に定義される値で上書きされます。この値は、リソースの数がアプリケーション プロファイル内の最大数より少ない場合でも受け入れられます。
[初期数量（Initial Quantity）] フィールド	アプリケーションの作成時にプロビジョニングする VM インスタンスの数を入力します。

c) [送信（Submit）] をクリックします。

ステップ 11 [アプリケーション（Application）] 画面で、ベア メタル ベースのアプリケーション コンポーネントを追加します。

a) [+] をクリックします。

b) [ベア メタル アプリケーション コンポーネントへのエントリの追加（Add Entry to Bare Metal Application Components）] 画面で、次のフィールドに値を入力します。

名前	説明
[インスタンス名（Instance Name）] フィールド	ベア メタル インスタンスの名前を入力します。

名前	説明
[説明（Description）] フィールド	ベア メタル インスタンスの説明を入力します。
[ブート LUN サイズ（GB）（Boot Lun Size (GB)）] フィールド	ブートの推奨 LUN サイズ。
[ネットワーク（Network）] ドロップダウン リスト	ネットワークを選択します。
[ターゲット BMA（Target BMA）] ドロップダウン リスト	PXE セットアップ用のベア メタル エージェント（BMA）を選択します。
[ベア メタル イメージ（Bare Metal Image）] ドロップダウン リスト	ベア メタル イメージを選択します。
[ブレードタイプ（Blade Type）] ドロップダウン リスト	APIC コンテナのブレード タイプとして次のいずれかを選択します。 • ハーフ幅（Half Width） • フル幅（Full Width）
[物理コンピューティング サービス クラス（Physical Compute Service Class）] ドロップダウン リスト	物理コンピューティング カテゴリのサービス クラスを選択します。
[物理ストレージ サービス クラス（Physical Storage Service Class）] ドロップダウン リスト	物理ストレージ カテゴリのサービス クラスを選択します。

c) [送信（Submit）] をクリックします。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 通信プロトコルの詳細を追加するには、[+] をクリックします。

a) [契約へのエントリの追加（Add Entry to Contracts）] 画面で、次のフィールドに値を入力します。

名前	説明
[ルール名（Rule Name）] フィールド	ルールの名前を入力します。

名前	説明
[ソース ネットワークの選択（Select Source Network）] ドロップダウン リスト	コントラクトルールを適用するソース ネットワークを選択します。 送信元ネットワークとして外部ネットワークが選択されている場合、[ルール名（Rule Name）] フィールド、[送信元ネットワークの選択（Select Source Network）] ドロップダウン リスト、および [宛先ネットワークの選択（Select Destination Network）] ドロップダウン リストのみを設定に使用できます。Cisco UCS Director は、選択した外部ネットワークで使用されているタグに基づいて、アプリケーションプロファイルを設定する前に、テナントの vPOD 内で、既存の契約をタグ付きおよび更新済みとして使用します。
[宛先ネットワークの選択（Select Destination Network）] ドロップダウン リスト	コントラクトルールを適用する宛先ネットワークを選択します。
[ルール説明（Rule Description）] フィールド	ルールの説明を入力します。
[プロトコル（Protocol）] ドロップダウン リスト	通信用のプロトコルを選択します。
[双方向を適用する（Apply Both Directions）] チェックボックス	送信元から宛先へのトラフィック（またはその逆のトラフィック）に対して同じ契約を適用する場合には、このボックスをオンにします。
以下のフィールドは、TCP または UDP プロトコルを選択した場合にのみ表示されます。	
[送信元ポートの開始（Source Port Start）] フィールド	送信元ポート番号の開始範囲を入力します。
[送信元ポートの終了（Source Port End）] フィールド	送信元ポート番号の終了範囲を入力します。
[送信先ポートの開始（Destination Port Start）] フィールド	宛先ポート番号の開始範囲を入力します。
[送信先ポートの終了（Destination Port End）] フィールド	宛先ポート番号の終了範囲を入力します。
[ステートフル（Stateful）] チェック ボックス	このチェック ボックスは、TCP プロトコルを選択した場合に表示されます。チェック ボックスをオンにして、ステートフル接続を有効にします。

名前	説明
[アクション（Action）] ドロップダウン リスト	通信に対して実行するアクションを選択します。 • 承認（Accept） • 削除（Drop） • 却下（Reject）

b) [送信（Submit）] をクリックします。

ステップ 14 [次へ（Next）] をクリックします。

ステップ 15 [ポリシー（Policy）] 画面で、次の手順を実行します。

a) [VMware システムポリシー（VMware System Policy）] ドロップダウンリストからポリシーを選択します。

b) これはオプションです。[システム ポリシー（System Policy）] ドロップダウン リストに新しいポリシーを追加するには、[+] をクリックします。

c) [システム ポリシー情報（System Policy Information）] 画面で、次のフィールドに値を入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	システム ポリシーの名前を入力します。
[ポリシーの説明（Policy Description）] フィールド	システム ポリシーの説明を入力します。
[VM名のテンプレート（VM Name Template）] フィールド	VM 名に使用するテンプレートを入力します。 （注） 名前テンプレートが指定されない場合、ユーザが入力する名前が VM 名として使用されます。
[VM 名の一意性チェックの無効化（Disable VM Name Uniqueness Check）] チェック ボックス	VM 名の一意性の検証をスキップするには、このチェック ボックスをオンにします。
[VM名の検証ポリシー（VM Name Validation Policy）] ドロップダウンリスト	VM 名を検証するポリシーを選択します。
[エンドユーザVM名またはVMプレフィクス（End User VM Name or VM Prefix）] チェックボックス	ユーザに VM の名前またはプレフィックスの指定を許可する場合に、このボックスをオンにします。
[導入後に電源をオンにします（Power On after deploy）] チェック ボックス	プロビジョニング後に VM の電源をオンにする場合に、このボックスをオンにします。

名前	説明
[ホスト名のテンプレート（Host Name Template）] フィールド	ホスト名のテンプレートを入力します。
[ホスト名の一意性のチェックの無効化（Disable Host Name Uniqueness Check）] チェック ボックス	ホスト名の一意性の検証をスキップするには、このチェック ボックスをオンにします。
[ホスト名の検証ポリシー（Host Name Validation Policy）] ドロップダウンリスト	ホスト名を検証するポリシーを選択します。
[Linuxタイムゾーン（Linux Time Zone）] ドロップダウン リスト	Linux VM のタイム ゾーンを選択します。
[Linux VM最大ブート待機時間（Linux VM Max Boot Wait Time）] ドロップダウン リスト	VM が起動中に一時停止する最大時間の値を選択します。
[DNS ドメイン（DNS Domain）] フィールド	DNS ドメインの名前を入力します。
[DNSサフィックスリスト（DNS Suffix List）] フィールド	DNS に付加するドメイン名サフィックスのリストを入力します。
[DNSサーバリスト（DNS Server List）] フィールド	DNS サーバのリストを入力します。
[VMイメージのタイプ（VM Image Type）] ドロップダウン リスト	VM イメージ タイプとして次のいずれかを選択します。 • Windows と Linux • Linux のみ
[VMアノテーションの定義（Define VM Annotation）] チェックボックス	注釈は、アプリケーション/Web 階層が、APIC ネットワーク ポリシーを通じて、サブネットを共有およびパブリックとして作成することを許可することを示します。VM アノテーションを定義する場合に、このボックスをオンにします。
[VM の注記（VM Annotation）] フィールド	このフィールドは、[VM アノテーションの定義（Define VM Annotation）] チェック ボックスをオンにしている場合に表示されます。VM の注釈を入力します。

名前	説明
[カスタム属性（Custom Attributes）] フィールド	このフィールドは、[VM アノテーションの定義（Define VM Annotation）] チェック ボックスをオンにしている場合に表示されます。カスタム属性を展開し、[+] をクリックしてカスタム属性を追加します。

d) [送信（Submit）] をクリックします。
e) [コスト モデル（Cost Model）] ドロップ ダウン リストで、チャージバックを計算するコスト モデルを選択します。
f) [HyperV 展開ポリシー（HyperV Deployment Policy）] を展開し、HyperV コンテナ プロビジョニング用の HyperV 展開ポリシーを調べます。
g) [次へ（Next）] をクリックします。

ステップ 16 [L4-L7サービスポリシー（L4-L7 Service Policy）] 画面で、レイヤ 4 ～レイヤ 7 サービス設定を編集します。

ステップ 17 [送信（Submit）] をクリックします。

アプリケーション プロファイルの削除

（注） 使用中のアプリケーション プロファイルは削除できません。

ステップ 1 [ポリシー（Policies）] > [リソース グループ（Resource Groups）] を選択します。

ステップ 2 [リソース グループ（Resource Groups）] ページで [アプリケーション プロファイル（Application Profile）] をクリックします。

ステップ 3 削除するアプリケーション プロファイルを含む行をクリックします。

ステップ 4 [削除（Delete）] をクリックします。

ステップ 5 [アプリケーション プロファイル（Application Profile）] 確認画面で、[削除（Delete）] をクリックします。

仮想インフラストラクチャ ポリシーの作成

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [仮想インフラストラクチャ ポリシー（Virtual Infrastructure Policies）] をクリックします。

ステップ 3 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 4 [仮想インフラストラクチャ ポリシー仕様（Virtual Infrastructure Policy Specification）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ポリシーの一意の名前を入力します。
[ポリシーの説明（Policy Description）] フィールド	仮想インフラストラクチャ ポリシーの説明を入力します。
[コンテナ タイプ（Container Type）] ドロップダウン リスト	コンテナ タイプを選択します。[APIC] を選択して APIC コンテナの仮想インフラストラクチャ ポリシーを作成します。 （注） [ゲートウェイなし（No Gateway）] オプションを使用してアプリケーション コンテナ ポリシーを作成した場合は、（コンテナ タイプに関係なく）ゲートウェイ VM はプロビジョニングされません。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [仮想インフラストラクチャ ポリシー：APIC 情報（Virtual Infrastructure Policy - APIC Information）] 画面で、次のフィールドに入力します。

（注） [ゲートウェイなし（No Gateway）] オプションを使用してアプリケーション コンテナ ポリシーを作成した場合は、ゲートウェイ VM はプロビジョニングされません。

名前	説明
[アプリケーション プロファイル（Application Profile）] ドロップダウン リスト	アプリケーション プロファイルを選択します。
+	クリックして、新しいアプリケーション プロファイルを作成します。『Cisco UCS Director APIC Management Guide』の説明に従って、新しいアプリケーション プロファイルを作成するように求められます。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [仮想インフラストラクチャ ポリシー：概要（Virtual Infrastructure Policy - Summary）] 画面に現在の設定が表示されます。

ステップ 9 [送信（Submit）] をクリックします。

アプリケーション コンテナ テンプレートの作成

APIC アプリケーション コンテナを作成する前に、テンプレートを作成する必要があります。

はじめる前に

仮想インフラストラクチャ ポリシーを作成します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 [テンプレートの追加（Add Template）] をクリックします。

ステップ 4 [アプリケーション コンテナ テンプレートの追加（Add Application Container Template）] 画面で、次のフィールドに入力します。

名前	説明
[テンプレート名（Template Name）] フィールド	新しいテンプレートの名前を入力します。
[テンプレートの説明（Template Description）] フィールド	テンプレートの説明を入力します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [アプリケーション コンテナ テンプレート：仮想インフラストラクチャ ポリシーの選択（Application Container Template - Select a Virtual infrastructure policy）] 画面で、次のフィールドに入力します。

名前	説明
[仮想インフラストラクチャ ポリシーの選択（Select Virtual Infrastructure Policy）] ドロップダウン リスト	APIC ポリシーを選択します。

名前	説明
+	クリックして、新しいインフラストラクチャ ポリシーを作成します。仮想インフラストラクチャ ポリシーの作成, （143 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [アプリケーション コンテナ テンプレート：オプション（Application Container Template - Options）] 画面で、次のフィールドに入力します。

名前	説明
[エンド ユーザ セルフサービス ポリシー（End User Self-Service Policy）] ドロップダウン リスト	エンドユーザ ポリシーを選択します。参照先 エンド ユーザ ポータルでのオプションの設定, （181 ページ）
[コンテナのセルフサービス削除の有効化（Enable Self-Service Deletion of Containers）] チェックボックス	ユーザがアプリケーション コンテナを削除できるようにするには、このボックスをオンにします。
[VNC ベースのコンソール アクセスの有効化（Enable VNC Based Console Access）] チェックボックス	このボックスをオンにすると、ユーザはブラウザで VM に対して VNC コンソールを開くことができます。
[テクニカル サポート用の電子メール（Technical Support Email Addresses）] フィールド	テクニカル サポート担当者の電子メール アドレスのカンマ区切りのリストを入力します。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [アプリケーション コンテナ テンプレート：設定ワークフロー（Application Container Template - Setup Workflows）] 画面で、コンテナ設定ワークフロー リストからワークフローを選択します。

ステップ 11 [次へ（Next）] をクリックし、[概要（Summary）] 画面を表示します。

ステップ 12 [送信（Submit）] をクリックし、アプリケーション コンテナ テンプレートの作成を実行します。

（注） アプリケーション コンテナ テンプレートのワークフロー作成は、定義されていない場合でも VMware ベースのコンテナに対して自動的にフェッチされます。HyperV ベース コンテナの特定のワークフローを設計および選択する必要があります。

APIC アプリケーション コンテナの作成

アプリケーションコンテナテンプレートを作成した後は、テンプレート管理機能を使用してアプリケーション コンテナを作成するサービス リクエストを開始できます。

はじめる前に

アプリケーション コンテナ テンプレートを作成します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 APIC テンプレートを選択します。

ステップ 4 [コンテナの作成（Create Container）] をクリックします。

ステップ 5 [テンプレートからのコンテナの作成（Create Container from Template）] 画面で、次のフィールドに入力します。

名前	説明
[コンテナ名（Container Name）] フィールド	コンテナの名前を入力します。この名前は一意である必要があります。
[コンテナ ラベル（Container Label）] フィールド	コンテナのラベルを入力します。
[テナント（Tenant）] リスト	[テナント（Tenant）] を展開し、使用するテナントを選択して [検証（Validate）] をクリックします。 （注） アプリケーション テンプレートにレイヤ 2 またはレイヤ 3 の階層要件がある場合は、レイヤ 2 またはレイヤ 3 が設定されているテナントのみがリストに表示されます。
[顧客組織（Customer Organizations）] ドロップダウン リスト	（任意）。テナント内の組織を選択します。
[リソースの制限の有効化（Enable Resource Limits）] チェック ボックス	リソース制限を有効にするには、このチェック 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、コンテナの vCPU の数、メモリ、最大ストレージサイズ、ハーフ幅物理サーバの最大数、およびフル幅物理サーバの最大数を指定するための追加のフィールドが表示されます。

名前	説明
[ネットワーク管理の有効化（Enable Network Management）] チェックボックス	コンテナを APIC 管理下に置くには、このチェックボックスをオンにします。
[ネットワーク スループット（Network Throughput）] ドロップダウン リスト	ドロップダウン リストからネットワーク スループットを選択します。
[階層ラベルのカスタマイズ（Tier Label Customization）] 領域	階層ラベルのカスタマイズされた名前。この領域は、複数のプライベート ネットワークを備えたテナントには表示されません。

ステップ 6 [送信（Submit）] をクリックします。

（注） [送信結果（Submit Result）] プロンプトに表示されたサービス リクエストを書き留めます。サービス リクエストの詳細情報を表示することで、作成されたコンテナの経過を表示できます。

ステップ 7 [アプリケーション コンテナ（Application Containers）] をクリックします。

[アプリケーション コンテナ（Application Containers）] ペインに新しいコンテナが表示されます。

（注） サービス リクエストは実行に時間がかかることがあります。コンテナを使用する前に、サービス リクエストの進捗を確認してワークフロー全体が正常に実行されたかを判断します。

サポートされているレイヤ 4 からレイヤ 7 のデバイス

APIC アプリケーション コンテナは、次のレイヤ 4 からレイヤ 7 のデバイスをサポートします。

- ファイアウォール：物理的な ASA と Cisco ASAv。
- ロード バランサ：VPX または SDX ロード バランサ。

サポートされているファイアウォールおよびロード バランサの詳細については、『Cisco UCS Director Compatibility Matrix』を参照してください。

L4-L7 サービスの設定

APIC アプリケーション コンテナは L4-L7 サービスをサポートします。この手順では、L4-L7 サービスを既存のコンテナに設定する方法を説明します。userAPIAddLBService API を使用してロード バランサ サービスを追加できます。

はじめる前に

APIC アプリケーション コンテナを作成します。

（注） ここでは、L4-L7 サービスを既存のアプリケーション コンテナに追加する方法を説明します。また、APIC アプリケーション プロファイルに L4-L7 サービスを設定できます。その場合は、そのプロファイルを使用してすべてのアプリケーション コンテナに L4-L7 サービスが展開されます。アプリケーション プロファイルでの L4-L7 サービスの設定の詳細については、レイヤ 4 ～ レイヤ 7 サービス ポリシー，（94 ページ）を参照してください。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 L4-L7 サービスを設定するアプリケーション コンテナを選択します。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから、[L4-L7 サービスの設定（Configure L4-L7 Service）] を選択します。

ステップ 5 [L4-L7 設定（L4-L7 Configuration）] 画面で、次のフィールドに値を入力します。

名前	説明
[サービス タイプ（Service Type）] ドロップダウン リスト	

名前	説明
	アプリケーション コンテナの設定に基づいて表示される、次のいずれかのサービス タイプを選択します。 • [ファイアウォール（Firewall）] • [ロード バランサ（ワン アーム）（Load Balancer (One Arm)）] • [ロードバランサ（ワン アーム、SSL オフロード）（Load Balancer (One Arm, SSL Offload)）] （注） このサービス タイプは、コンテナが [ファイアウォールおよびロード バランサ（ワン アーム、SSL オフロード使用）（Firewall and Load Balancer (One Arm, with SSL Offload)）] チェーンを使用してすでに設定されている場合のみ表示されます。 • [ロード バランサ（ツー アーム）（Load Balancer (Two Arm)） • [ファイアウォールおよびシングル アームのロード バランサ（Firewall and Single Arm Load Balancer）] • [ファイアウォールおよびロード バランサ（ワン アーム、SSL オフロード使用）（Firewall and Load Balancer (One Arm, with SSL Offload)）] （注） アプリケーション プロファイルで [L4-L7 サービスの設定（Configure L4-L7 Service）] チェック ボックスがオンになっている場合、次の条件下で対応するサービス タイプがリストされます。 • [L4-L7 サービス ポリシーの追加（Add L4-L7 Service Policy）] ダイアログ ボックスで [ファイアウォールを許可（Allow Firewall）] チェック ボックスがオンになっている場合、ファイアウォール サービス タイプのみがリストされます。 • [L4-L7 サービス ポリシーの追加（Add L4-L7 Service Policy）] ダイアログ ボックスで [ロード バランサを許可（Allow Load Balancer）] チェック ボックスがオンになっている場合、ロード バランサ サービス タイプのみがリストされます。 • [L4-L7 サービス ポリシーの追加（Add L4-L7 Service Policy）] ダイアログ ボックスで [ファイアウォールの許可（Allow Firewall）] および [ロード バランサの許可（Allow Load Balancer）] チェック ボックスがオンになっている場合、ファイアウォールとロードバランサのサービス タイプがリストされます。

名前	説明
	（注） 選択されたコンテナが L4-L7 サービスをサポートしていない場合、サービス タイプは [サービスタイプ（Service Type）] ドロップダウン リストに表示されません。
[サービス名（Service Name）] フィールド	サービスの一意の名前を入力します。
[コンシューマ（Consumer）] ドロップダウン リスト	サービス コンシューマとしてネットワーク（階層）を選択します。
[プロバイダー（Provider）] ドロップダウン リスト	サービス プロバイダーとしてネットワーク（階層）を選択します。
ロード バランサ サービス タイプを [サービス タイプ（Service Type）] ドロップダウン リストから選択した場合は、次のフィールドが表示されます。	
[LB サーバ（LB Servers）]	LB サーバを展開し、ロード バランシングする必要があるサーバを選択します。 このフィールドは、複数のプライベート ネットワークを備えたテナント用のコンテナが選択された場合には表示されません。ロードバランサ サーバそれぞれの IP アドレスをカンマで区切って入力します。
[プロトコル（Protocol）] ドロップダウン リスト	プロトコルを選択します。
[ポート] フィールド	このフィールドは、複数のプライベート ネットワークを備えたテナント用のコンテナが選択された場合には表示されません。選択したプロトコルのポート番号。
次のフィールドは、[サービスタイプ（Service Type）] ドロップダウン リストから [ロード バランサ（ワン アーム、SSL オフロード）（Load Balancer (One Arm, SSL Offload)）] が選択された場合にのみ表示されます。	
[SSL ポート（SSL Port）] フィールド	SSL が有効な vServer のポート番号。
[証明書（Certificate）] フィールド	有効な SSL 証明書。
[キー（Key）] フィールド	SSL 証明書の一意のキー。
以下のフィールドは、複数のプライベート ネットワークを備えたテナント用のコンテナが選択された場合にのみ表示されます。	

名前	説明
[フロント エンド ポート（Front End Port）]	フロント エンド ポート番号。
[バック エンド ポート（Back End Port）]	バック エンド ポート番号。
[cookie 名（CookieName）]	cookie の名前を入力します。
[LB 方式（LB Method）]	ロード バランサの方式を選択します。
[永続化タイプ（PersistenceType）]	永続化のタイプを選択します。

ステップ 6 [送信（Submit）] をクリックします。

ファイアウォール ルールの追加

はじめる前に

Cisco UCS Director では、管理者またはエンドユーザが L4-L7 サービスを備えた APIC アプリケーション コンテナを作成できます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 既存のアプリケーション コンテナをダブルクリックします。

ステップ 4 ファイアウォール サービス タイプの L4-L7 サービスを選択します。
[ファイアウォール ルール（Firewall Rules）] 画面が表示されます。

ステップ 5 新規出力エントリを追加するには、[ルールの追加（+）（Add Rule (+)）] をクリックします。

ステップ 6 [ファイアウォール ルールの追加（Add Firewall Rule）] 画面で、次のフィールドに入力します。

名前	説明
[インターフェイス名（Interface Name）] ドロップダウンリスト	インターフェイスの名前を選択します。

名前	説明
[ACL の方向（ACL Direction）] ドロップダウン リスト	[着信（Inbound）] または [発信（Outbound）] を ACL の方向として選択します。
[ACE 名（ACE Name）] フィールド	ファイアウォール ルールを定義する ACE 名を入力します。
[プロトコル（Protocol）] ドロップダウン リスト	通信用のプロトコルを選択します。
[送信元ポートの範囲（Source Port Range）] フィールド	このフィールドは、TCP または UDP プロトコルを選択した場合にのみ表示されます。送信元ポートの範囲を入力します。
[送信先ポートの範囲（Destination Port Range）] フィールド	このフィールドは、TCP または UDP プロトコルを選択した場合にのみ表示されます。送信先ポートの範囲を入力します。
[すべての送信元（Source Any）] チェックボックス	すべての送信元ホストまたはネットワークを許可するには、このチェックボックスをオンにします。
[ソースアドレス（Source Address）] フィールド	このフィールドは、[すべての送信元（Source Any）] チェックボックスがオフになっている場合にのみ表示されます。送信元アドレスとしてシングル ホストまたはそれらの範囲を指定するための IP アドレス、IP アドレス範囲、またはサブネット マスク付き IP アドレス。
[すべての送信先（Destination Any）] チェックボックス	宛先アドレスで ACE エントリ ステートメントを適用するには、このチェックボックスをオンにします。
[接続先アドレス（Destination Address）] フィールド	このフィールドは、[すべての送信先（Destination Any）] チェックボックスがオフになっている場合にのみ表示されます。接続先アドレスとしてシングル ホストまたはそれらの範囲を指定するための IP アドレス、IP アドレス範囲、またはサブネット マスク付き IP アドレス。
[アクション（Action）] ドロップダウン リスト	[許可（Permit）] または [拒否（Deny）] を ACE エントリのアクションとして選択します。
[順序] フィールド	拒否ステートメントまたは許可ステートメントを実行する必要がある順序。

ステップ 7 [送信（Submit）] をクリックします。

ファイアウォール ルールを変更するには、ファイアウォール ルールを選択して [ルールの変更（Modify Rule）] クリックします。ファイアウォール ルールを削除するには、ファイアウォール ルールを選択して [ルールの削除（Delete Rule）] クリックします。

ロード バランサ サービスへの実サーバの追加

はじめる前に

Cisco UCS Director では、管理者またはエンドユーザが L4-L7 サービスを備えた APIC アプリケーション コンテナを作成できます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 既存のアプリケーション コンテナをダブルクリックします。

ステップ 4 ロード バランサ サービス タイプの L4-L7 サービスを選択します。
[LB サーバ（LB Servers）] 画面が表示されます。

ステップ 5 [サーバの追加（Add Servers）] をクリックします。

ステップ 6 [サーバの追加（Add Servers）] 画面で、[VM（VMs）] を展開して、使用する VM をオンにします。

ステップ 7 [ポート（Port）] フィールドにポート番号を入力します。
選択した VM がこのポート番号で設定されます。

ステップ 8 [送信（Submit）] をクリックします。

ロード バランサ サーバを削除するには、[サーバの削除（Remove Servers）] をクリックします。

L4-L7 サービスの削除

はじめる前に

既存のアプリケーション コンテナを 1 つ以上の L4-L7 サービスを使用して作成し、展開します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナをダブルクリックします。

ステップ 4 [L4-L7 サービス（L4 L7 Services）] をクリックします。

ステップ 5 L4-L7 サービスのリストから、削除するサービスをクリックします。

ステップ 6 [削除（Delete）] をクリックします。

ステップ 7 確認ダイアログで、[削除（Delete）] をクリックします。

契約の追加

Cisco UCS Director で各アプリケーション コンテナ用に作成された契約またはセキュリティ ルールを表示できます。セキュリティ ルールは、そのテナント内の同じコンテナまたは異なるコンテナの階層の間に追加できます。

はじめる前に

APIC アプリケーション コンテナを作成します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 既存のアプリケーション コンテナをダブルクリックします。

ステップ 4 [コントラクト（Contracts）] をクリックします。

ステップ 5 [契約の追加（+）（Add Contract (+)）] をクリックし、新しい契約を追加します。

ステップ 6 [契約へのエントリの追加（Add Entry to Contracts）] 画面で、次のフィールドに値を入力します。

名前	説明
[ソース ネットワークの選択（Select Source Network）] フィールド	[ソース ネットワークの選択（Select Source Network）] を展開し、契約を適用するソース/宛先コンテナのソース ネットワークをオンにし、[検証（Validate）] をクリックします。
[宛先ネットワークの選択（Select Destination Network）] フィールド	[宛先ネットワークの選択（Select Destination Network）] を展開して、契約を適用するソース/宛先コンテナ内の宛先ネットワークを選択し、[検証（Validate）] をクリックします。
（注） 契約が同じコンテナの階層の間にある場合は、同じコンテナに属する階層を選択できますが、そうでない場合は、異なるコンテナから階層を選択できます。	
[ルールの作成（Create Rulet）] チェックボックス	ルールを作成する場合に、このチェックボックスをオンにします。 チェックボックスをオンにすると、契約とフィルタルールが作成されます。 チェックボックスがオフの場合は、空の契約のみが作成されます。
以下のフィールドは、[ルールの作成（Create Rule）] チェックボックスをオンにした場合に表示されます。	
[ルール名（Rule Name）] フィールド	ルールの名前。
[ルール説明（Rule Description）] フィールド	ルールの説明。
[プロトコル（Protocol）] ドロップダウン リスト	通信用のプロトコルを選択します。
[双方向を適用する（Apply Both Directions）] チェックボックス	送信元ら宛先へのトラフィックと、宛先から送信元へのトラフィックに対して、同じ契約を適用する場合に、このチェックボックスをオンにします。
以下のフィールドは、TCP または UDP プロトコルを選択した場合にのみ表示されます。	
[送信元ポートの開始（Source Port Start）] フィールド	送信元ポート番号の開始範囲を入力します。
[送信元ポートの終了（Source Port End）] フィールド	送信元ポート番号の終了範囲を入力します。
[送信先ポートの開始（Destination Port Start）] フィールド	宛先ポート番号の開始範囲を入力します。

名前	説明
[送信先ポートの終了（Destination Port End）] フィールド	宛先ポート番号の終了範囲を入力します。
[アクション（Action）] ドロップダウン リスト	通信に対して実行するアクションを選択します。 • 承認（Accept） • 削除（Drop） • 却下（Reject）
[ステートフル（Stateful）] チェック ボックス	このチェック ボックスは、TCP プロトコルを選択した場合に表示されます。チェック ボックスをオンにして、ステートフル接続を有効にします。

ステップ 7 [送信（Submit）] をクリックします。
各契約をドリル ダウンし、以下のレポートを表示することができます。

- セキュリティ ルール：異なるコンテナの階層間のすべてのルールを一覧表示します。
- 契約の詳細：その契約の契約名、対象、フィルタ、ルールが表示されます。

（注） 契約の最後のルールを削除すると、各契約が削除されます。

セキュリティ ルールの追加

Cisco UCS Director で各アプリケーション コンテナ用に作成されたすべてのセキュリティ ルールを表示するには、各契約をドリル ダウンする必要があります。

はじめる前に

Cisco UCS Director では、管理者およびエンド ユーザが APIC アプリケーション コンテナを作成し、各アプリケーション コンテナ用に作成したセキュリティ ルールを追加できます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナをダブルクリックします。

ステップ 4 [コントラクト（Contracts）] をクリックします。

ステップ 5 セキュリティ ルールを追加する契約が含まれている行をクリックして、[詳細の表示（View Details）] をクリックします。

ステップ 6 [セキュリティ ルール（Security Rules）] をクリックします。

ステップ 7 [追加（Add）] をクリックしてセキュリティ ルールを追加します。

ステップ 8 [契約の追加（Add Contract）] 画面で、次のフィールドに入力します。

名前	説明
[ソース ネットワークの選択（Select Source Network）] フィールド	契約のソース ネットワークを表示します。
[宛先ネットワークの選択（Select Destination Network）] フィールド	契約の宛先ネットワークが表示されます。
[ルール名（Rule Name）] フィールド	ルールの名前。
[ルール説明（Rule Description）] フィールド	ルールの説明。
[プロトコル（Protocol）] ドロップダウン リスト	通信用のプロトコルを選択します。
[双方向を適用する（Apply Both Directions）] チェックボックス	送信元から宛先へのトラフィック（およびその逆のトラフィック）に対して同じ契約を適用する場合に、このチェック ボックスをオンにします。
以下のフィールドは、TCP または UDP プロトコルを選択した場合にのみ表示されます。	
[送信元ポートの開始（Source Port Start）] フィールド	送信元ポート番号の開始範囲を入力します。
[送信元ポートの終了（Source Port End）] フィールド	送信元ポート番号の終了範囲を入力します。
[送信先ポートの開始（Destination Port Start）] フィールド	宛先ポート番号の開始範囲を入力します。

名前	説明
[送信先ポートの終了（Destination Port End）] フィールド	宛先ポート番号の終了範囲を入力します。
[アクション（Action）] ドロップダウン リスト	通信に対して実行するアクションを選択します。 • 承認（Accept） • 削除（Drop） • 却下（Reject）
[ステートフル（Stateful）] チェックボックス	このチェック ボックスは、TCP プロトコルを選択した場合に表示されます。チェック ボックスをオンにして、ステートフル接続を有効にします。

ステップ 9 [送信（Submit）] をクリックします。
セキュリティ ルールがアプリケーション コンテナ用に作成されます。

セキュリティ ルールの削除

Cisco UCS Director で各アプリケーション コンテナ用に作成されたすべてのセキュリティ ルールを表示するには、各契約をドリルダウンする必要があります。セキュリティ ルールの追加, （157 ページ）を参照してください。

はじめる前に

APIC アプリケーション コンテナを作成します。

ステップ 1 削除する既存のセキュリティ ルールを選択します。

ステップ 2 選択したセキュリティ ルールを削除するには、[削除（Delete）] をクリックします。
確認用のダイアログボックスが表示されます。

ステップ 3 [削除（Delete）] をクリックします。
セキュリティ ルールが削除されます。

サービス チェーニング

APIC コンテナでは、2 つのネットワーク間にファイアウォールとロード バランサの両方を連続して作成できます。このプロセスは L4-L7 サービス チェーニングまたは単にサービス チェーニングと呼ばれ、その結果の一連のファイアウォールとロード バランサはサービス チェーンと呼ばれます。

APIC コンテナでサービス チェーンを作成する方法は 2 つあります。

- 既存のコンテナでサービス チェーンを作成します。L4-L7 サービスの設定, （147 ページ）を参照してください。
- ファイアウォールとロード バランサの両方をコンテナのアプリケーション プロファイルの一部として作成します。この場合は、コンテナの作成時に両方のサービスがプロビジョニングされます。アプリケーション プロファイルの追加, （104 ページ）およびレイヤ 4 ～ レイヤ 7 サービス ポリシーの追加, （94 ページ）を参照してください。

（注） サービス チェーンは、物理と仮想の両方のゲートウェイを使用するアプリケーション コンテナ内には作成できません。

VDC で [ネットワーク管理を有効にする（Enable Network Management）] が無効として表示される場合は、次の設定がデフォルトで実行されます。

- インフラストラクチャ ネットワークを使用してロード バランサをファイアウォールにリンクします。
- デフォルトにより、インフラストラクチャ ネットワークのいずれかの IP アドレスを使用してロード バランサに SNIP が作成されます。
- ファイアウォールを指すデフォルト ルートがロード バランサに追加されます。

既存コンテナへの VM の追加

他のタイプのコンテナに VM を追加する場合と同じ方法で、既存の APIC コンテナへ VM を追加できます。VM の追加, （170 ページ）を参照してください。

（注） イメージを使用して既存のコンテナに VM を追加する場合は、1 つのネットワーク アダプタのみを追加できます。アプリケーション プロファイルでテンプレートを定義して作成した場合は、複数のアダプタでそのテンプレートを使用できます。

（注） [APIC コンテナへの VM の追加（Add VMs to APIC Container）] ワークフローを使用して VM をコンテナに追加することはできません。VM を追加するには、[VM の追加（Add VMs）] をクリックするか、API を使用してください。

はじめる前に

APIC アプリケーション コンテナを作成します。

階層/ネットワークの追加

はじめる前に

APIC アプリケーション コンテナを作成します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから、[階層/ネットワークの追加（Add Tier/Network）] を選択します。

ステップ 5 [階層/ネットワークの追加（Add Tier/Network）] 画面で、次のフィールドに入力します。

名前	説明
[階層/ネットワーク名（Tier/Network Name）] フィールド	階層またはネットワークの名前。
[階層ラベル（Tier Label）] フィールド	階層のラベル。

名前	説明
[ネットワークの分離（Isolate Network）] チェックボックス	このチェックボックスをオンにすると、新しい階層が作成され、選択した階層に関連付けられます。 （注） 分離された階層の場合、サブネットはパブリック サブネット プール ポリシーに加えて、テナントの作成時に指定されたプライベート IP サブネット ポリシーから取得されます。 チェックボックスがオフの場合は、新しい階層の作成のみが行われます。 （注） 分離されていない階層の場合、サブネットはテナントが割り当てられたサブネットから取得されます。選択されたコンテナの数が、許可されている階層の最大数に到達した場合、分離されていない階層を作成することはできません。
[親の階層（Parent Tier）] ドロップダウン リスト	このフィールドは、[ネットワークの分離（Isolate Network）]チェックボックスがオンになっている場合にのみ表示されます。 親の階層を選択します。

ステップ 6 [送信（Submit）] をクリックします。
新しい階層またはネットワークが作成されます。仮想マシンを選択して、コンテナ ネットワークに vNIC を追加できます。

VM への仮想ネットワーク インターフェイス カードの追加

はじめる前に

既存のアプリケーション コンテナを 1 つ以上の VM を使用して作成し、展開します。VM に仮想ネットワーク インターフェイス カード（vNIC）を追加する前に、コンテナにプロビジョニング

されている VM で VMware ツールが起動され、イーサネット インターフェイスがアップ状態になっている必要があります。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナをダブルクリックします。

ステップ 4 [仮想マシン（Virtual Machines）] をクリックします。

ステップ 5 vNIC を追加する VM を含む行をクリックします。

ステップ 6 [その他のアクション（More Actions）] ドロップダウン リストから [vNIC の追加（Add vNICs）] を選択します。

ステップ 7 [コンテナ ネットワークへの vNIC の追加（Add vNIC to Container Network）] 画面で、次のフィールドに値を入力します。

名前	説明
[ネットワーク（Network）] ドロップダウン リスト	VM が存在するのと同じアプリケーション コンテナ内の階層/ネットワークを選択します。 （注） 分離されていない階層/ネットワークのうち VM がすでに接続されているものは、フィルタによってリストから除外されます。 （注） 分離された階層/ネットワークのうち、選択された VM がその階層/ネットワークの一部であるものも、フィルタによってリストから除外されます。
[VM クレデンシャル（VM Credentials）]	
[ユーザ名（Username）]	VM のユーザ名を入力します。
[パスワード（Password）]	VM のパスワードを入力します。

ステップ 8 [送信（Submit）] をクリックします。
コンテナ VM に vNIC を追加するため、VM の電源がオフになります。vNIC がコンテナ ネットワークに追加されると、VM の電源がオンになります。

仮想ネットワーク インターフェイス カードの削除

はじめる前に

既存のアプリケーション コンテナを 1 つ以上の VM を使用して作成し、展開します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナをダブルクリックします。

ステップ 4 [仮想マシン（Virtual Machines）] をクリックします。

ステップ 5 削除する vNIC の VM を含む行をクリックします。

ステップ 6 [vNIC の削除（Delete vNICs）] をクリックします。

ステップ 7 [VM vNIC の削除（Delete VM vNICs）] 画面で、削除する vNIC を選択します。

ステップ 8 [削除（Delete）] をクリックします。
VM vNIC が削除されます。

既存コンテナへのベアメタル サーバの追加

（注） ベア メタル サーバは、APIC コンテナでのみサポートされます。

はじめる前に

ベアメタル サーバをコンテナに追加する前に、Bare Metal Agent を Cisco UCS Director に追加する必要があります。このリリースの『Cisco UCS Director Bare Metal Agent Installation and Configuration Guide』を参照してください。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 BM を追加するコンテナを選択します。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [BM の追加（Add BMs）] を選択します。

ステップ 5 [BM の追加（Add BMs）] 画面で、[ベア メタル アプリケーション コンポーネント（Bare Metal Application Components）] を展開し、[追加（+）（Add (+)）] をクリックして新規 BM を追加します。

ステップ 6 [エントリの追加（Add Entry）] 画面で、次のフィールドに入力します。

名前	説明
[インスタンス名（Instance Name）] フィールド	BM インスタンスに割り当てる名前を入力します。
[説明（Description）] フィールド	（任意）説明を入力します。
[ネットワーク（Network）] ドロップダウン リスト	BM コンポーネントを追加するネットワーク（階層）を選択します。
[ベア メタル イメージ（Bare Metal Image）] ドロップダウン リスト	使用する BM イメージ。このリストは、ベア メタル エージェントから取得されます。
[ブレードタイプ（Blade Type）] ドロップダウン リスト	コンテナのブレード タイプとして次のいずれかを選択します。 • ハーフ幅（Half Width） • フル幅（Full Width）
[ブート LUN サイズ（GB）（Boot Lun Size (GB)）] フィールド	ブートの推奨 LUN サイズ。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 BM をさらに追加するには、ステップ 5 からの手順を繰り返します。

ステップ 9 必要なすべての BM を定義したら、[BM の追加（Add BMs）] 画面の [送信（Submit）] をクリックします。

ディスクの追加

はじめる前に

既存のアプリケーション コンテナを 1 つ以上のベアメタル サーバを使用して作成し、展開します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナをダブルクリックします。

ステップ 4 [ベアメタル（Bare Metals）] をクリックします。

ステップ 5 ディスクを追加するベアメタル サーバを選択します。

ステップ 6 [ディスクの追加（Add Disk）] をクリックします。

ステップ 7 [BM へのディスクの追加（Add Disk to BM）] 画面で、ディスク サイズを GB 単位で入力します。

ステップ 8 [送信（Submit）] をクリックします。

ディスクの削除

はじめる前に

既存のアプリケーション コンテナをベアメタル サーバに関連付けられた 1 つ以上のディスクを使用して作成し、展開します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナをダブルクリックします。

ステップ 4 [ベアメタル（Bare Metals）] をクリックします。

ステップ 5 ディスクを削除するベア メタル サーバを選択します。

ステップ 6 [ディスクの削除（Add Delete）] をクリックします。

ステップ 7 テーブルから削除する BM の LUN ID 番号を選択します。

ステップ 8 [送信（Submit）] をクリックします。
確認画面で、削除を確認します。

ベア メタル サーバの削除

はじめる前に

既存のアプリケーション コンテナを 1 つ以上のベアメタル サーバを使用して作成し、展開します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナをダブルクリックします。

ステップ 4 [ベアメタル（Bare Metals）] をクリックします。

ステップ 5 ベアメタル サーバのリストから、削除するベアメタル サーバを選択します。

ステップ 6 [BM の削除（Delete BM）] をクリックします。
ベアメタル サーバと、関連付けられたディスクが削除されます。

第 9 章

アプリケーション コンテナの管理

この章は、次の項で構成されています。

アプリケーション コンテナの管理

管理者として、アプリケーション コンテナで次の管理アクションを実行できます。

- VM の追加
- コンソールのオープン
- テンプレートのクローン
- コンテナ電源の管理
- コンテナの削除
- レポートの表示

コンテナ アクションの表示

コンテナに適用するために使用可能なアクションは、状況によって異なります。[アプリケーション コンテナ（Application Containers）] ページの上部にあるアクション アイコン、または [その他

のアクション（More Actions）] ドロップダウン リストを使用して、それらのアクションを実行します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 使用可能なすべてのアクションを表示するためのコンテナを選択します。

（注） セルフサービス ユーザがコンテナに対してアクションを実行できるようにするには、コンテナ テンプレートの作成時に [セルフサービスの有効化（Enable Self-Service）] をオンにして、セルフサービス ユーザ権限を付与します。

VM の追加

（注） [コンテナへの VM の追加（Add VMs to Container）] ワークフローを使用して VM をコンテナに追加することはできません。VM を追加するには、[VM の追加（Add VMs）] をクリックするか、API を使用してください。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [VM の追加（Add VMs）] を選択します。

ステップ 5 [VM の追加（Add VMs）] 画面で、仮想マシンのリストを展開して、[追加（Add）] をクリックします。次のいずれかの方法で仮想マシンを定義します。

- VM イメージを使用し、手動でパラメータを設定します。ステップ 6 を参照してください。
- アプリケーション プロファイルで定義されたテンプレートを使用します。ステップ 7 を参照してください。

ステップ 6 [仮想マシンへのエントリの追加（Add Entry to Virtual Machines）] 画面で、[事前定義テンプレートの使用（Use Predefined Template）] チェック ボックスをオフのままにして、次のフィールドに入力します。

名前	説明
[ネットワーク（Network）] ドロップダウン リスト	VM を追加するネットワーク（階層）を選択します。

名前	説明
[VM 名（VM Name）] フィールド	VM に割り当てる名前を入力します。 アプリケーションコンテナの展開時に、アプリケーションプロファイルで定義されている内容からプレフィックスを更新できます。
[コンテンツ ライブラリ VMテンプレートを使用した新しい VM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VM イメージ テンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VMテンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキストライブラリ VMテンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。
[VM イメージ（VM Image）] リスト	このフィールドは、[コンテンツ ライブラリ VMテンプレートを使用した新しいVM のプロビジョニング（Provision new VM using Content Library VM Template）] チェック ボックス がオフになっている場合にのみ表示されます。リストを展開し、使用するVM イメージを選択します。 クラスタ用の vCenter でこれらの VM を定義します。
[リンク済み複製の使用（Use Linked Clone）] チェック ボックス	このチェック ボックスは、スナップショットを使用する VM テンプレートを選択した場合のみ有効です。高速でストレージ効率の高いプロビジョニングが可能なリンク クローン機能を使用して新しいVMを展開するには、このボックスをオンにします。
[スナップショット（Snapshot）]フィールド	このフィールドは、[リンク クローンの使用（Use Linked Clone）] チェック ボックスがオンになっている場合にのみ表示されます。[選択（Select）]をクリックして、リンク クローン機能を使用して新しい VM をプロビジョニングするために使用する必要があるスナップショットを選択します。
[vCPU 数（Number of vCPUs）] ドロップダウン リスト	VM の仮想 CPU の数を選択します。
[メモリ（MB）（Memory (MB)）] ドロップダウン リスト	VM メモリのサイズを選択します。

名前	説明
[ディスク サイズ（GB）（Disk Size (GB)）] フィールド	VM ディスクのサイズを入力します。 0 を入力すると、VM はイメージで定義されているディスク サイズを使用します。
[DRS ルールの選択（Select DRS Rule）] リスト	リストを展開し、分散リソーススケジューラ（DRS）ルール（アフィニティ ルールとも呼ばれる）を選択します。
[ストレージ DRS ルールの選択（Select Storage DRS Rule）] リスト	リストを展開し、ストレージ分散リソーススケジューラ（DRS）ルールを選択します。 （注） このフィールドは、[DRS ルールの選択（Select DRS Rule）] から DRS ルールを選択した場合にのみ表示されます。
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	この VM のパスワード共有ポリシーを選択します。 デフォルトでは、ルート パスワードは共有されません。
[ネットワーク アダプタ タイプ（Network Adapter Type）] ドロップダウン リスト	VM のネットワーク アダプタを選択します。
[初期数量（Initial Quantity）] ドロップダウン リスト	アプリケーション起動時に作成する VM の数を選択します。

ステップ 8 に進みます。

ステップ 7 [仮想マシンへのエントリの追加（Add Entry to Virtual Machines）] 画面で、[事前定義テンプレートの使用（Use Predefined Template）] チェック ボックスをオンにして、次のフィールドに入力します。

名前	説明
[ネットワーク（Network）] ドロップダウン リスト	VM を追加するネットワーク（階層）を選択します。
[VM 名（VM Name）] ドロップダウン リスト	アプリケーション プロファイルで定義された VM の名前を選択します。
[DRS ルールの選択（Select DRS Rule）] リスト	リストを展開し、DRS ルール（アフィニティ ルールとも呼ばれる）を選択します。

名前	説明
[インスタンスの数（No Of Instances）] ドロップダウン リスト	プロビジョニングする VM インスタンスの数を選択します。 アプリケーション プロファイルで定義された VM の最大数を超えないように、ドロップダウン リストは選択肢を制限します。

ステップ 8 [送信（Submit）] をクリックします。

ステップ 9 VM をさらに追加するには、ステップ 5 からのこの手順を繰り返します。

ステップ 10 VM の追加が終了したら、[VM の追加（Add VMs）] 画面で、[送信（Submit）] をクリックします。

アプリケーション コンテナからの VM の削除

はじめる前に

- 既存のアプリケーション コンテナを 1 つ以上の VM を使用して作成し、展開します。
- 削除する VM の電源をオフにします。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 アプリケーション コンテナを選択します。

ステップ 3 [その他のアクション（More Actions）] ドロップダウン リストから、[コンテナのデコミッション（Decommission Container）] を選択します。

ステップ 4 VM のリストから、削除する VM を持つ行をクリックします。

（注） 電源がオフになっている VM のみがリストに表示されます。

ステップ 5 [送信（Submit）] をクリックします。

選択したコンテナから VM が削除されます。

VM コンソールへのアクセス

はじめる前に

VNC を使用してアクセスする個々の VM に対する適切なコンソール アクセス権を有効にする必要があります。「VNC コンソール アクセスの有効化」を参照してください。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [コンソールを開く（Open Console）] を選択します。

ステップ 5 [VM コンソールへのアクセス（Access VM Console）] 画面で、[VM の選択（Select VM）] ドロップダウン リストから VM を選択します。

ステップ 6 [送信（Submit）] をクリックします。
選択した VM のコンソールが新しいブラウザ ウィンドウで開きます。

（注） コンテナでの VNC の自動設定については、アプリケーション コンテナ テンプレートを作成するときに [VNC ベースのコンソール アクセスの有効化（Enable VNC Based Console Access）] チェックボックスをオンにし、権限を付与する必要があります。

VNC コンソール アクセスの有効化

個々の VM のコンソール アクセスを有効にできます。

ステップ 1 [仮想（Virtual）] > [コンピューティング（Compute）] を選択します。

ステップ 2 [コンピューティング（Compute）] ページで [VM（VMs）] をクリックします。

ステップ 3 コンソール アクセスを有効にする VM を含む行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [VNC の設定（Configure VNC）] を選択します。

ステップ 5 [VNC 要求の設定（Configure VNC Request）] 画面で、[キーボード マッピング（Key Board Mapping）] ドロップダウン リストから、マッピングを選択します。

ステップ 6 [送信（Submit）] をクリックします。

既存コンテナの複製

管理者として既存コンテナを複製できます。複製はすべての設定と設定データを元のコンテナに含まれている VM から転送します。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [コンテナの複製（Clone Container）] をクリックして、次のフィールドに値を入力します。

名前	説明
[コンテナ名（Container Name）] フィールド	コンテナの名前を入力します。
[コンテナ ラベル（Container Label）] フィールド	固有のコンテナ ラベルを入力します。
[テナント（Tenant）] リスト	リストを展開してテナントを選択し、[選択（Select）] をクリックします。

ステップ 5 [送信（Submit）] をクリックします。

コンテナ電源の管理

管理者は、コンテナの電源をオンまたはオフにすることができます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [コンテナの電源をオンにする（Power On Container）] または [コンテナの電源をオフにする（Power Off Container）] をクリックします。

ステップ 5 リストから、電源をオンまたはオフにする VM を選択します。

ステップ 6 [送信（Submit）] をクリックします。

アプリケーション コンテナの表示

Cisco UCS Director でアプリケーション コンテナを表示するには、[ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

[ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。
アプリケーション コンテナは、カラー スキームを使用してコンテナのステータスを識別します。

- 緑：すべての VM およびベア メタル サーバ（BM）の電源がオンの状態です。コンテナ設定に GW が含まれている場合は、ゲートウェイ（GW）もオンになっています。
- 黄色：要求されたいずれかの BM がまだ進行中/エラー状態であるか、またはいずれかのアプリケーション VM がダウンしています。
- 青：コンテナのプロビジョニングが進行中です。
- グレー：VM と BM がコンテナにありません。
- 赤：GW を含めて、すべての VM および BM の電源がオフになっています。

アプリケーション コンテナの削除

コンテナを削除すると、そのコンテナにプロビジョニングされたリソースも削除されます。[コンテナの削除（delete container）] アクションを開始すると、Cisco UCS Director がアプリケーション コンテナのセットアップをロールバックします。サービス リクエストが作成され、ロールバック ステータスが反映されます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [コンテナの削除（Delete Container）] を選択します。

（注） 関連 L4-L7 サービスがあるアプリケーション コンテナの削除を選択した場合は、コンテナ用にプロビジョニングされたすべてのリソースを削除するかどうかの確認が求められます。

ステップ 5 メッセージが表示され、L4-L7 サービスをコンテナとともに削除する場合は、[送信（Submit）] をクリックします。
サービス リクエストが生成されたことを確認する通知が表示されます。

ステップ 6 [組織（Organizations）] > [サービス リクエスト（Service Requests）] を選択します。

ステップ 7 [サービス リクエスト（Service Requests）] ページで [サービス リクエスト（Service Requests）] をクリックします。

ステップ 8 削除サービス リクエストが含まれている行をクリックします。

ステップ 9 [詳細の表示（View Details）] をクリックします。

レポートの表示

各コンテナについての概要レポート、クレデンシャルによる詳細レポート、およびクレデンシャルなしでの詳細レポートを生成できます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [レポートの表示（View Reports）] をクリックします。

ステップ 5 [コンテナ レポートの表示（View Container Reports）] 画面で、[レポート タイプの選択（Select Report Type）] ドロップ ダウン リストから、表示するレポートを選択します。
「クレデンシャル付き」のレポートには、プレーン テキストでパスワードが表示されます。「クレデンシャルなし」のレポートは、レポートにパスワードは表示されません。

管理者用のレポートには、セルフサービスユーザに関するレポートで指定されていないポリシー情報が含まれています。

ステップ 6 [送信（Submit）] をクリックします。
このレポートには、レポート ヘッダーでアプリケーション コンテナを作成するために使用されるサービス要求の ID が表示されます。

アプリケーション コンテナ情報の表示

アプリケーションコンテナのダッシュボードには、アプリケーションコンテナのすべての情報が表示されます。選択したアプリケーション コンテナについての情報がさまざまなページに表示されます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナ（Application Containers）] をクリックします。

ステップ 3 アプリケーション コンテナを選択します。

ステップ 4 [詳細の表示（View Details）] をクリックします。

ステップ 5 次の情報が表示されます。

ページ	説明
要約	• [概要（Overview）] : アプリケーション コンテナの次のような概要を表示します。コンテナ名と ID。DR が有効である場合には、グループ名、アプリケーション プロファイル、使用されているアプリケーション コンテナ テンプレート。管理対象ネットワーク サービスがある場合には、階層数、VM 数、および BM 数。リソース プール。 • [リソース制限（Resource Limits）] : 使用可能なリソースの概要と、リソースの制限を表示します。これには CPU、メモリ、データストア サイズ、ネットワーク スループット、およびサーバなどが含まれます。

ページ	説明
仮想マシン	アプリケーション コンテナに対してプロビジョニングされたVMに関する詳細を表示します。これにはVMのID、名前、およびタイプ、ステータス、IPアドレス、ゲストOS、およびVMがプロビジョニングされた時刻などが含まれます。 （注） 以下のアクションでは、VM名について特定の命名規則に従います。 • プライベート ネットワークに対するアプリケーション プロビジョニング：<コンテナ作成時に指定されたVM名><階層ごとのVMのインデックス> • APIC コンテナへのVMの追加：<[VMの追加（Add VM）] アクションで指定されたVM名><階層ごとのVMのインデックス>
[ベアメタル（Bare Metals）]	ベア メタルに関する詳細を表示します。これにはベア メタル名、OSタイプ、IPアドレス、およびサービス リクエスト（SR）IDなどが含まれます。 ベア メタルは、アプリケーション コンテナの一部としてプロビジョニングされた物理サーバです。
[階層マッピング（Tier Mapping）]	階層に関する情報を表示します。これには各階層のVMとBM、リソース名とタイプ、およびIPアドレスが含まれます。 アプリケーション コンテナ テンプレートを作成したときに定義したネットワークに対応する階層。通常のアプリケーションの階層には、Web、アプリケーション、およびデータベースが含まれます。階層には、VMとBMが含まれます。

ページ	説明
[L4-L7 サービス（L4 L7 Services）]	L4-L7 サービスに関する情報を表示します。これにはサービス リクエスト（SR）ID、サービス名、プライマリ IP アドレス、サービス タイプ、デバイス タイプ、コンシューマ層とプロバイダー層、ロード バランサの VIP と SNIP、サービス チェーンのフラグとタイプ、プロトコル、ポート、SSL 対応かどうかなどが含まれます。 （注） サービス名をドリル ダウンして、実際のサーバのリストを表示することができます。
契約	多層アプリケーションでの通信のルールを定義する契約に関する情報を表示します。これには契約、ソース コンテナとネットワーク、宛先コンテナとネットワークなどが含まれます。 （注） 各契約をドリル ダウンし、セキュリティ ルールを表示することができます。

第 10 章

セルフサービス管理のオプション

この章は、次の項で構成されています。

エンド ユーザ ポータルでのオプションの設定

管理アクションは、管理者がアプリケーション コンテナ テンプレートの作成プロセス時にオプションを有効にした場合にのみ、実行できます。次のリストに、アプリケーション コンテナで（管理者によって）有効または無効にできるエンドユーザ オプションを示します。

- VM へのアクセス
- vNIC の追加または削除
- リース時間の設定
- ディスクの追加または削除
- スナップショットの追加、削除、または復元
- VM 電源のオンまたはオフ
- VM のリブート、リセット、または一時停止
- VM のサイズ変更
- ゲストのシャットダウン

アプリケーション コンテナを最初に作成した場合は、グループ（顧客組織）に関連付けられます。そのグループに関連付けられたユーザは、コンテナ上で有効になっている管理アクションを表示および実行できます。

エンドユーザ ポータルを使用してアプリケーション コンテナを管理する方法については、『Cisco UCS End User Portal Guide』を参照してください。

ステップ 1 [ポリシー（Policies）] > [仮想/ハイパーバイザ ポリシー（Virtual/Hypervisor Policies）] > [サービスの提供（Service Delivery）] の順に選択します。

ステップ 2 [サービスの提供（Service Delivery）] ページで [エンドユーザ セルフサービス ポリシー（End User Self-Service Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [エンドユーザ ポリシーの追加（Add End User Policy）] 画面の、[アカウント タイプ（Account Type）] で、クラウド タイプを選択します。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 [エンド ユーザ ポリシー（End User Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	エンド ユーザ ポリシーの名前を入力します。
[ポリシーの説明（Policy Description）] フィールド	エンド ユーザ ポリシーの説明を入力します。
[エンドユーザ セルフサービス オプション（End User Self-Service Options）] チェックボックス	エンド ユーザに付与するアクションのボックスをオンにします。 （注） 選択したクラウド タイプによっては、その他のオプションも利用できます。

ステップ 7 [送信（Submit）] をクリックします。