

Cisco CloudCenter ソリューションと Cisco ACI: 一般的な使用例

概要

Cisco CloudCenter™ ソリューションは、アプリケーション セントリックなハイブリッドクラウド管理プラットフォームです。インフラストラクチャリソースのプロビジョニングを安全に実施し、19 を超えるデータセンター、プライベート クラウド、およびパブリッククラウド環境にアプリケーション コンポーネントを導入することができます。Cisco CloudCenter のアプリケーション セントリックで、ポリシーベースのハイブリッドクラウド管理機能は、Cisco® Application Centric Infrastructure (Cisco ACI) およびポリシーベースのネットワーク管理に最適です。

ハイブリッド IT 戦略を求める IT 部門は、アプリケーションをデータセンター、プライベート クラウド、およびパブリッククラウド環境に導入するための方法や場所を柔軟に選択できることを求めています。Cisco CloudCenter では、セルフサービス システムを利用して、アプリケーションをあらゆる環境にオン デマンドで導入することができます。Cisco ACI 管理型ネットワークを利用すれば、アプリケーション全体を導入する場合だけでなく、単一階層のみを導入する場合でも、パブリッククラウド単体の導入時に比べて、パブリッククラウドの俊敏性の活かしながら、ネットワークの安全性やコスト効果の高い導入オプションを選択できるというメリットがあります。

Cisco CloudCenter と Cisco ACI は、連携して 1 つのソリューションを提供します。このソリューションを利用することで、IT 組織は、さまざまなエンタープライズ IT ネットワークに対する最適な導入オプションを、これまでにないほど柔軟に選択できます。Cisco CloudCenter と Cisco ACI を利用することにより、セキュリティを確保しながらインフラストラクチャをプロビジョニングし、目的や必要性に応じてアプリケーションを導入することができます。Cisco CloudCenter では、アプリケーションの導入プロセスがすべて自動化されており、Cisco ACI API と直接通信して、



Cisco ACI のポリシー オブジェクトを自動的に作成します。作成されるオブジェクトには、アプリケーション ネットワーク プロファイル (ANP)、エンドポイント グループ (EPG)、コントラクト、フィルタ、および(マイクロセグメント化された安全なコミュニケーションに必要な)他のオブジェクトが含まれます。

IT 部門にとっては、最適なネットワーク セキュリティと業務の効率化を実現するチャンスとなります。ポリシーの作成や維持を手動で行ったり、プログラム言語を新たに学んだりする必要はありません。ユーザは、ネットワーク スキルやクラウド環境の詳細に関する知識がなくても、オンデマンドで柔軟にセルフサービスを利用することができます。拡張やサポート終了に対するアクションが自動化されており、ネットワーク ポリシーの更新や終了処理も自動で行われます。

このドキュメントでは、Cisco CloudCenter と Cisco ACI の導入による、3 つの効果的な使用例の概要を紹介します。

はじめに

Cisco ACI は、ネットワーク セキュリティの強化、ビジネス関連アプリケーションの要件に基づく通信ポリシーの自動化、開発者の待機時間の削減を実現し、次世代のデータセンターにおけるアプリケーションの導入を高速化します。

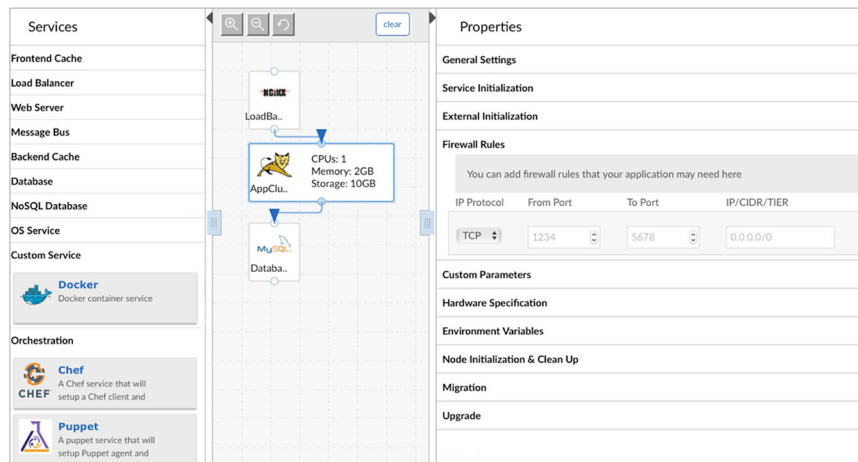
根幹となる Cisco ACI アプリケーション ポリシーは、ゼロトラスト モデルのホワイト リストです。ネットワーク上に配置できるオブジェクト、およびそのオブジェクトが通信できる他のオブジェクトや通信内容をポリシーに指定しない限り、アプリケーション階層間での通信を遮断することができます。Cisco ACI は、論理的なビジネススペースのポリシー定義を具体的なインフラストラクチャ設定へと変換して適用します。

Cisco CloudCenter は、アプリケーション セントリックなハイブリッドクラウド管理プラットフォームです。このプラットフォームを使用することで、インフラストラクチャ リソースのプロビジョニングを行い、19 を超えるデータセンター、プライベート クラウド、およびパブリック クラウド環境にアプリケーション コンポーネントを安全に導入できます。ユーザは、セルフサービス システムを使用してモデリングと導入を簡単に行い、新しいアプリケーションと既存のアプリケーションの両方を管理することができます。基盤となる環境、クラウド サービス、API についての詳細な知識は必要ありません。

Cisco CloudCenter ソリューションのドラッグアンドドロップ モデラー (図 1) で作業することにより、あらゆる環境に導入できる、クラウドに依存しないポータブル アプリケーション プロファイルを作成できます。簡単にカスタマイズできる OS イメージ、アプリケーション サービス、クラウドサービス、コンテナ、設定管理ツールを柔軟に組み合わせることで、新規や既存のアプリケーションをシンプルから複雑なものまでモデリングすることができます。

各アプリケーション プロファイルでは、インフラストラクチャの自動化レイヤとアプリケーションの自動化レイヤが、導入が容易な 1 つのブループリントに統合されています。Cisco CloudCenter のアプリケーション プロファイルにより、1 つの Cisco CloudCenter プラットフォームからあらゆるモデリング済みアプリケーションを導入し、管理することができます。これは、どのようなデータセンターやクラウド環境内であっても、一貫性のある予測可能な方法で行うことができます。

図 1. アプリケーション プロファイル トポロジのモデラー



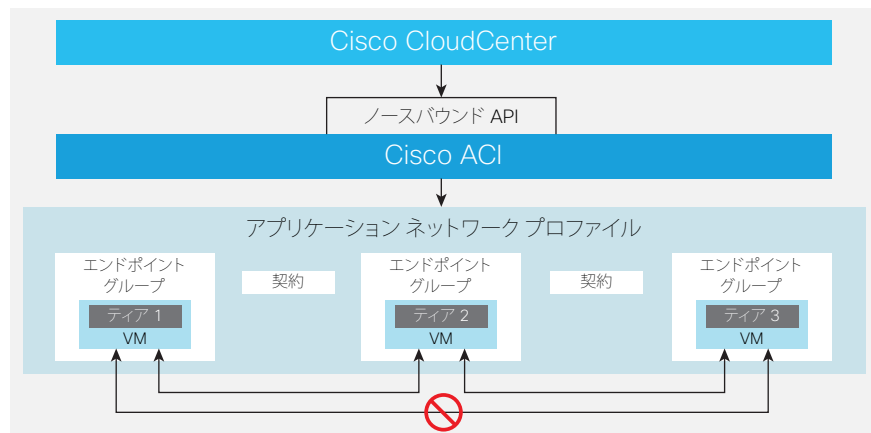
このソリューションのクラウドに依存しないアプリケーション プロファイルとクラウド固有のオーケストレータを組み合わせることで、アプリケーションのニーズを解釈し、それらのニーズをクラウド固有の API コールに変換して、クラウドからアプリケーションを抽象化します。その結果、Cisco CloudCenter では、開発者と IT 部門両方の作業効率を低下させる要因となることが多い、クラウド固有のスクリプティングとクラウドによる囲い込みを回避することができます。

Cisco ACI の活用

Cisco CloudCenter は、透過的に維持しつつ Cisco ACI と統合されます。Cisco ACI によって管理される環境にアプリケーション プロファイルを導入することを選択した場合、ユーザやネットワーク管理者が追加の作業を行う必要はありません。Cisco CloudCenter はアプリケーションのニーズを解釈し、Cisco ACI ノースバウンド API を呼び出して、ソフトウェア定義型ネットワーク (SDN) を最大限に活用するネットワーク ポリシー オブジェクトを自動化します。

図 2 に示すとおり、Cisco CloudCenter および Cisco ACI は、VMware や OpenStack API を使用する環境に導入されることが多くあります。

図 2. Cisco CloudCenter と Cisco ACI および VMware vCenter



Cisco CloudCenter と Cisco ACI は、プラグインをインストールせずに連携できます。環境固有のスクリプトを作成したり、アプリケーション コードを変更したりする必要はありません。ネットワーク管理者は、プログラミング言語を学習せずに、Cisco ACI のプログラム可能なインターフェイスを最大限に活用することができます。

Cisco CloudCenter によって管理されるオーケストレーションのフローには、以下の要素が含まれます。

- アプリケーション プロファイルのモデリング: サービス マネージャは Cisco CloudCenter の GUI を使用して、クラウドに依存しないアプリケーション プロファイルを作成し、特定のユーザと共有したり、マーケットプレイスに公開したりすることができます。
- セルフサービス導入を利用: ロール ベースおよびユーザ ベースのアクセス制御と、タグ ベースのガバナンスを組み合わせることで、適切な導入環境を選択できます (オプションで Cisco ACI を含めることも可能)。
- Cisco Application Policy Infrastructure Controller (APIC) ポリシー オブジェクトの作成と導入: ユーザが Cisco ACI ファブリックに含まれる環境を選択すると、Cisco CloudCenter によって適切なポリシー オブジェクトが自動的に作成され、APIC ノースバウンド REST API が呼び出されて、アプリケーション独自のネットワークが作成されます。
- インフラストラクチャのプロビジョニング: Cisco CloudCenter はインフラストラクチャ API (OpenStack や vCenter など) を呼び出し、適切なネットワークセグメント内で、コンピューティング、メモリ、およびストレージ リソースをプロビジョニングします。

- アプリケーション層の導入: Cisco CloudCenter では、アプリケーション プロファイルでモデリングされたトポロジと依存関係に基づいて、すべてのアプリケーション コンポーネントの導入とオーケストレーションが行われます。
- 継続的な管理: ユーザと管理者は、導入の進行状況を確認し、適切に設定するための操作を行うことができます。
- 水平方向のトラフィックをブロック: ある層が手動または自動でスケーリングされると、Cisco CloudCenter は Cisco ACI ポリシーを更新して水平方向のトラフィックをブロックします。デバイスが被害を受けても、侵害をそのデバイス内に留めます。
- サポート終了アクションの実行: インフラストラクチャ ポリシーおよびネットワーク ポリシー オブジェクトが自動的に削除されるため、ネットワークの完全性を保持し、インフラストラクチャ リソースを保護することができます。

Cisco CloudCenter と Cisco ACI を使用することで、IT 部門は、セキュリティの強化、アプリケーション導入のシンプル化、DevOps とネットワーク管理の効率向上を実現する強力なソリューションを利用できるようになります。

このドキュメントの後半では、Cisco CloudCenter と Cisco ACI を利用する 3 つの主要な使用例について紹介します。

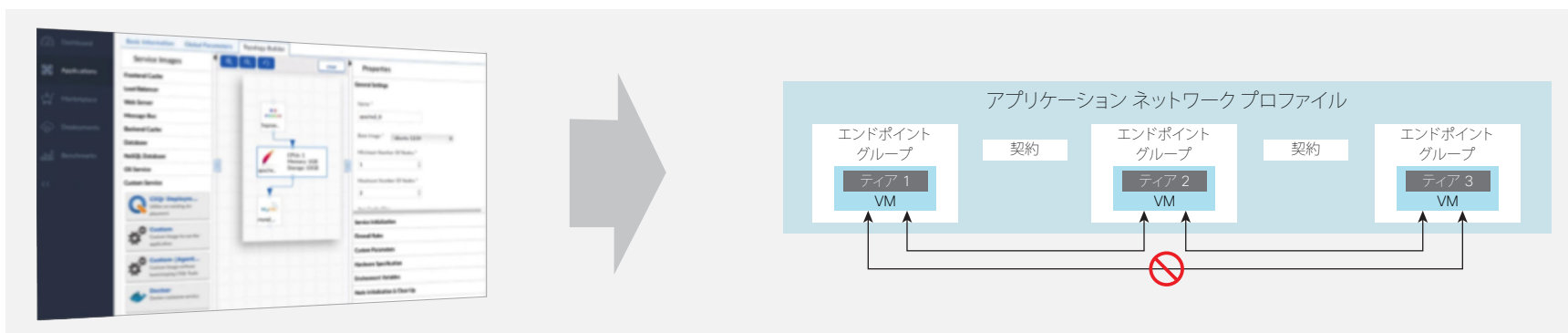


使用例 1: N 層アプリケーションの安全な導入

Cisco CloudCenter は、ガバナンス ルールをプログラミングすることでアプリケーションの導入をシンプル化・効率化します。ガバナンス ルールのプログラミングでは、インフラストラクチャの配置やセキュリティ プロファイルなどのポリシーを記述します。これらのルールによって、ますます多様化するインフラストラクチャ環境の複雑さを意識しなくてもすむようになります。

ユーザは、オンデマンドのセルフサービス導入によって柔軟性を確保します。ネットワーク管理者は、ポート設定やその他のセキュリティ設定パラメータを管理することができます。公開またはユーザと共有される Cisco CloudCenter の各アプリケーション プロファイルには、セキュリティやネットワークに関する指示が含まれます (図 3)。

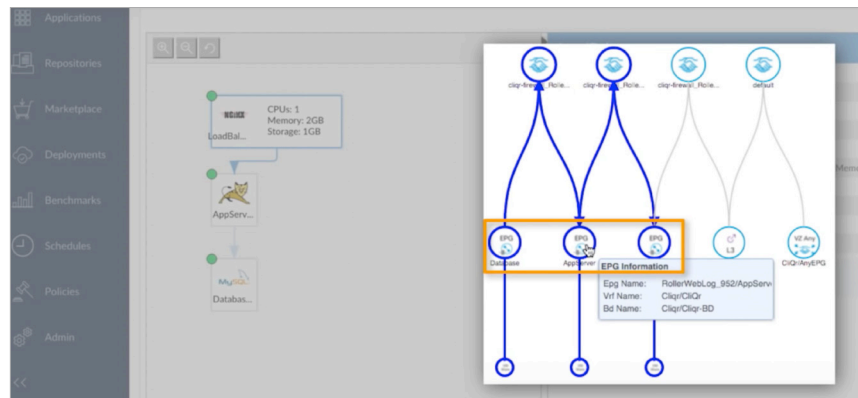
図 3. Cisco CloudCenter アプリケーション プロファイルに基づいて Cisco ACI のアプリケーション ネットワーク プロファイル オブジェクトを判断



Cisco CloudCenter Manager を介して導入を始めると (図 3)、Cisco CloudCenter Orchestrator は、アプリケーション プロファイルのトポロジとネットワーク設定情報を利用して Cisco ACI 用のポリシー オブジェクトを自動的に作成します。オーケストレータは、アプリケーション プロファイルのトポロジ要件やセキュリティ要件に基づき、ローカルの APIC API を呼び出して、Cisco ACI ANP、EPG、コンシューマとプロバイダー間のコントラクトのインスタンスを作成します。各アプリケーション層は、分離した独自のアプリケーション層ネットワークに配置されます。アプリケーション層ネットワーク間の接続は、アプリケーションのトポロジに基づいて自動的に確立されます。

図 4 では、Cisco ACI のユーザ インターフェイスに導入済みの 3 階層アプリケーションが表示されており、Cisco CloudCenter のインターフェイスにも同じアプリケーションの導入が表示されています。この横に並んだダイアグラムには 3 つの EPG と、その間のネットワークトラフィックを管理するコントラクトが表示されています。

図 4. Cisco CloudCenter Orchestration と Cisco ACI のセグメンテーション



Cisco CloudCenter は、Cisco CloudCenter アプリケーション プロファイルに含まれるアプリケーション スタック サービスの要件に応じて、アプリケーション階層ネットワークでプロトコルおよびポート アクセスを制限するコントラクトとフィルタを自動生成します。

Cisco CloudCenter と Cisco ACI とを統合することで、アプリケーションの導入と各アプリケーション階層の両方を対象として、アプリケーション トポロジ、アプリケーション スタック サービス、ネットワーク設定、およびエンドツーエンドのネットワーク分離を組み合わせたことができます。統合ソリューションでは、ユーザと管理者の両方が導入の進捗を確認できる、直感的なインターフェイスが提供されています。また、両方のプラットフォームで命名規則の一貫性を維持することもできます。

アプリケーションが終了すると、自動でプロビジョニングされた、アプリケーションに関連付けられているインフラストラクチャ オブジェクトが削除され、アプリケーション ライフサイクルの整合性が維持されます。また、セキュリティ脅威の原因となり得る不要なポリシーが削除され、貴重なメモリ リソースを節約することもできます。

使用例 2: 拡張アプリケーションの導入

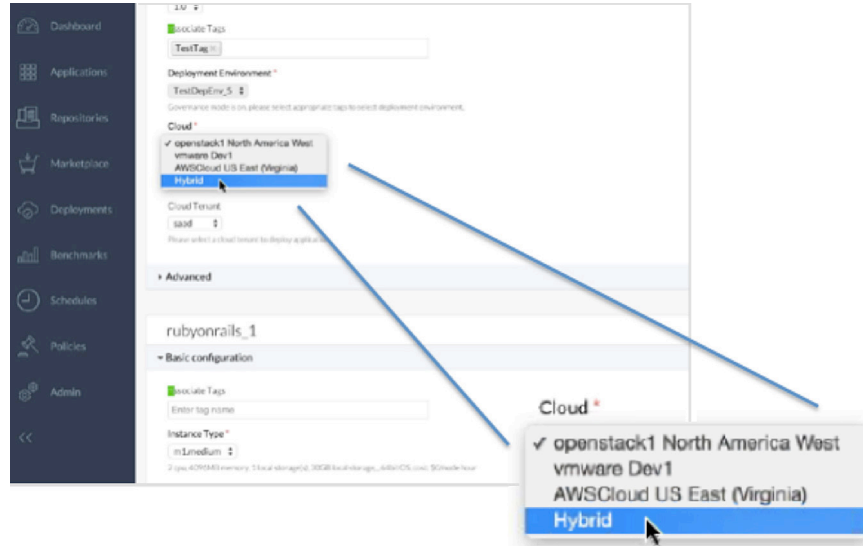
Cisco CloudCenter では、異なる環境の異なる階層を使用するアプリケーションの導入がサポートされています。ユーザがアプリケーションを導入する場合、通常は、ロールやガバナンス ルールなどの制御方法に応じて、ユーザが使用できるデータセンター、プライベート クラウド、またはパブリック クラウドの場所から 1 つが導入対象として選択されます。しかし、ユーザは拡張導入オプションを選択することもできます。拡張導入では、アプリケーション内の各階層で特定の対象サイトを選択することができます。

アプリケーションの拡張導入には、以下のようないくつかの利点があります。

- **コスト:** クラウドの従量課金制および拡張性は、ワークロードが変化する状況に適しています。ただし、インフラストラクチャのレンタルが長期間のワークロードに適していない場合もあります。そのため、Web アプリケーションやモバイル アプリケーションのユーザ インターフェイス層にはパブリック クラウドなどの従量課金制環境が適している場合がある一方で、アプリケーション サーバやデータベース サーバなどの固定的で長期間稼働させる層は、Cisco ACI で管理するプライベート クラウドやデータセンター内のネットワークに導入した方がコスト効率が良い場合もあります。
- **セキュリティおよびコンプライアンス:** アプリケーション サーバ層やロード バランサ層が各種の環境に導入できる場合でも、データベース層は、セキュリティ要件やコンプライアンス要件に対応するために、Cisco ACI で管理する、プライベート クラウドやデータセンター内のネットワークに導入するのが適しています。
- **高可用性およびディザスタ リカバリのマスター/スレーブ設定:** クラウドの異なる可用性ゾーンや異なるデータセンターおよびクラウドに導入された、マスターとスレーブ両方のコンポーネントが含まれるアプリケーション プロファイルをモデリングすることができます。高可用性およびディザスタ リカバリ性を備えた完全なアプリケーション スタックを、異なる可用性ゾーンないし異なるデータセンターやクラウドにワン クリックで導入できるのであれば、さまざまなフェイルオーバー シナリオをコスト効率良く簡単にテストし、テストが済んだら設定全体を削除することができます。さらに、完全にテスト済みの設定と同じ設定を、実稼働ワークロードにも自動的に導入することができます。

Cisco CloudCenter を使用することで、複数の導入環境が使用できる場合に、拡張されたアプリケーション トポロジを簡単に導入することができます。図 5 に示すように、ユーザは、導入時に対象クラウドとして [ハイブリッド (Hybrid)] を選択するだけです。選択すると、ユーザ インターフェイスでは、アプリケーション プロファイルでモデリングされた各階層のクラウド導入ドロップダウン メニューがそれぞれ表示されます。

図 5. ユーザーが [ハイブリッド (Hybrid)] を選択して、アプリケーションの拡張導入機能を有効化



スタック全体、または個々の階層の配置は、Cisco CloudCenter のタギングおよびルール エンジンに従って決定されます。たとえば、医療保険の相互運用性と説明責任に関する法令 (HIPPA) 準拠のアプリケーションにタグを付与することで、他の階層が導入されている場所に関係なく、Cisco ACI が管理するデータセンターのみをデータベース層として選択することができます。

Cisco CloudCenter と Cisco ACI では、拡張された 3 つのアプリケーション導入トポロジがサポートされています。どのトポロジを使用する場合でも、各アプリケーション階層に適した導入環境を選択することができます。アプリケーションのアーキテクチャや属性を変更する必要はなく、Cisco ACI や SDN に関するドメインの知識も必要ありません。階層を特定の環境に固定する、環境に固有のスクリプトやワークフローはありません。

- 複数のポッド: Cisco CloudCenter は、複数の Cisco ACI ポッドが存在するデータセンターに N 層のアプリケーションを導入できます。このシナリオでは、アプリケーションを 1 つのデータセンター内で別々のポッドに分散できます。エンタープライズ Web アプリケーションの各層は、異なる VLAN の各ネットワークに配置されます。ラベルベースで動的に方向を制限する、Cisco ACI 独自のルーティング機能により、コンシューマの仮想マシンは、ラベルが一致するプロバイダーの仮想マシンのみ接続されます。このアプローチによって、アプリケーション内の階層ごとにネットワークが完全に分離されます。
- 拡張されたファブリック: Cisco CloudCenter は、地理的に分散した拠点や距離が離れた拠点に広がる Cisco ACI ファブリックに N 層のアプリケーションを導入できます。このシナリオでは、1 つの拡張されたネットワークファブリックによって提供されるネットワーク サービスを利用しながら、アプリケーションを別々のデータセンターの異なるポッドに分散することができます。たとえば、ロード バランサおよびアプリケーション サーバをデータセンター A に配置し、データベースをデータセンター B に配置することができます。拡張されたファブリック トポロジにより、Cisco ACI のレイヤ 4 ~ レイヤ 7 (L4-L7) のサービスとの統合機能が強化されます。
- 複数のクラウド: Cisco CloudCenter は、Cisco ACI ポッドとパブリック クラウド全体に N 層アプリケーションを導入できます。アプリケーションの一部を、Cisco ACI が管理するネットワークのあるデータセンターやプライベート クラウドに導入し、一部をパブリック クラウドに配置することができます。このシナリオは、複数の分散したクラウド ロケーションにエッジのキャッシュがある Web アプリケーションや、アプリケーション層やデータセンター層が安全なデータセンターにあるモバイル アプリケーションに適しています。

Cisco CloudCenter と Cisco ACI は、完全に独自で柔軟なソリューションを連携して提供することで、複雑さを増すエンタープライズ ワークロードのコスト、セキュリティ、俊敏性の要件に対応します。「一度のプロファイル設定で、あらゆる場所に導入可能」という Cisco CloudCenter の機能が、拡張型導入トポロジにも利用できるようになりました。

すべての拡張型アプリケーション導入トポロジでは、Cisco CloudCenter アプリケーション プロファイルを変更する必要はなく、環境またはトポロジ固有のスクリプトを記述したり保守したりする必要もありません。アプリケーションも移行可能です。

使用例 3: Cisco ACI 環境へのアプリケーションの移行

パブリック クラウド環境内にある、Cisco ACI 未対応のデータセンターに導入済みのアプリケーションを取得し、Cisco ACI が管理する、より安全なデータセンターへと移行することができます。統合ソリューションにより、関連する Cisco ACI ポリシー オブジェクトの移行と作成が完全に自動化されます。

Cisco CloudCenter で管理される、導入されたアプリケーションのワークロードは、移行機能を利用することで、異なるクラウドに移行することができます。Cisco CloudCenter のアプリケーション プロファイルはポータブルで、クラウドに依存しません。つまり、単一の環境に限定されないことを意味します。そのため、Cisco CloudCenter と Cisco ACI ではハイブリッドな IT 戦略がサポートされ、ユーザはビジネス ニーズに応じてワークロードの配置を最適化することができます。さらに、使用状況、ガバナンス ルール、コストおよびパフォーマンスの要件、そしてアプリケーションのライフサイクル フェーズに応じて、異なるデータ センター、プライベート クラウド、およびパブリック クラウド間での移行を簡単に選択することができます。

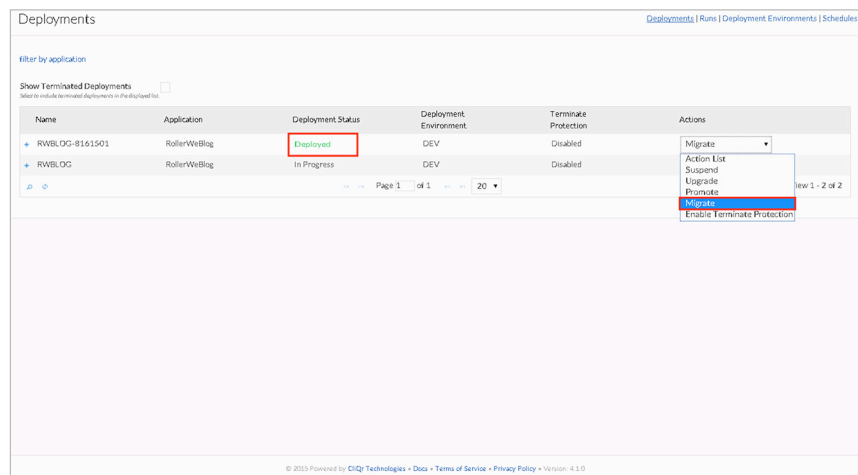
このソリューションでは、クラウドからの再移行、クラウド間でのソフトウェア開発ライフサイクル (SDLC) の移行、およびデータセンターの移行という主要な移行シナリオがサポートされています。

クラウドからの再移行

IT 組織の多くはクラウド戦略の一環としてアプリケーションを導入していますが、パブリック クラウドの月単位コストがかさむことから、こうした戦略を再考しつつあります。パブリック クラウドが自社のセキュリティおよびコンプライアンス要件に適合しているかどうかを懸念している組織もあります。Cisco CloudCenter を利用することで、パブリック クラウド内のアプリケーションを、Cisco ACI 管理型ネットワークを備えたデータセンターやプライベート クラウドへと再移行することができます。

図 6 に示すように、ユーザは既存の導入を選択して、移行を含むさまざまな管理アクションを選択できます。Cisco ACI 環境が移行対象として選択されている場合は、Cisco CloudCenter によってポリシー オブジェクトが自動的に作成され、APIC API を使用したネットワーク設定のインスタンス化が行われます。

図 6. ユーザが既存の導入に対して [移行 (Migrate)] を選択



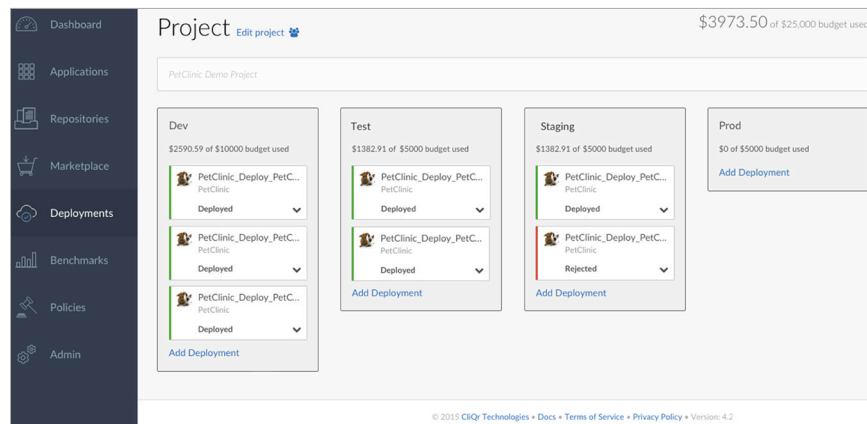
クラウド間でのソフトウェア開発ライフサイクルの移行

最も一般的なハイブリッド クラウドの使用例は、開発およびテスト アクティビティにパブリック クラウドを使用し、実稼働環境にデータセンターまたはプライベート クラウドを使用するというものです。Cisco CloudCenter では、統合された強力な CliQr® Continuous Integration and Continuous Delivery (CI/CD) プロジェクト ボード機能を使用したシナリオがサポートされています。この機能は、ソフトウェア開発ライフサイクル全体を管理します。

管理者は、自社のソフトウェア開発ライフサイクルを反映した Cisco CloudCenter 内でプロジェクトを作成することができます。リソースや予算は、プロジェクト全体に割り当てることも、特定のフェーズに割り当てることもできます。ライフサイクルのステージに沿ってコードのレベルを上げられるユーザや、各フェーズに最適なクラウドは、ユーザのアクセス制御およびポリシーで定義します。

図 7 に、各ステージの CI/CD プロジェクト ボードを示します。各ボードにはそれぞれのオーナーとプロジェクト予算が割り当てられています。

図 7. 実稼働用の CI/CD プロジェクト ボードと Cisco ACI 環境



開発およびテスト環境では Cisco ACI が使用されていないが、実稼働環境では Cisco ACI が使用されている DevOps シナリオの場合は、環境をまたがるワークフローを使用して CI/CD プロジェクト ボードを設定することができます。開発者は、実稼働前の環境ではある程度自由に選択できますが、最終的な実稼働環境(より安全な Cisco ACI 管理ネットワーク環境)では選択幅が制限されます。

Cisco CloudCenter には、強力なタギングおよびガバナンス エンジンが含まれています。これにより、フェーズに応じてセキュリティ設定を変更することができます。そのため、開発フェーズでの導入では、特定のポートがオープンになった状態で設定される可能性があります。ただし、アプリケーションが実稼働フェーズに移行されると、Cisco ACI ポリシーに基づいて適用されるマイクロセグメンテーションの効果が得られ、クラウドもこれらのポートを自動的に閉じます。一方、実稼働フェーズに昇格することで、実稼働ネットワーク内のネットワーク ポートやセキュリティ モニタリング エージェントのポートがオープンになる可能性があります。

Cisco CloudCenter と Cisco ACI は連携して、パブリック クラウド環境での導入では不可能な、卓越した柔軟性とセキュリティ制御を実現します。

データセンターの移行

多くの IT 組織では、自組織のハイブリッド IT 戦略の進化、合併および買収の遂行といった、さまざまなビジネス上の理由に応じて、データセンターのフットプリントを継続的に変更しています。Cisco CloudCenter はこのプロセスをシンプル化し、ワークロードを Cisco ACI 環境へと移行して SDN のメリットを得られるようにします。

移行のシナリオでは、IT 組織は一般に移行対象を詳細に調査し、継続的にアップグレードしながら、既存のワークロードを各フェーズの Cisco ACI 環境に移行します。各アプリケーションのプロファイルを設定することで、Cisco CloudCenter は VLAN ポートを Cisco ACI 管理ポートに変換し、トラフィックのモニタリング、およびパケット損失、遅延、ネットワーク ループの可視化という Cisco ACI のメリットを提供することができます。

まとめ

Cisco CloudCenter は、アプリケーションセントリックなハイブリッド クラウド管理プラットフォームです。このプラットフォームを使用することで、アプリケーション データセンター、プライベート クラウド、およびパブリック クラウド環境の導入と管理が簡単になります。Cisco CloudCenter と Cisco ACI は、連携して 1 つのソリューションを提供します。このソリューションを利用することで、IT 組織は、さまざまなエンタープライズ IT ネットワークに対する最適な導入オプションを、これまでにないほど柔軟に選択できます。この統合されたソリューションにより、パブリック クラウド単体では達成不可能な、俊敏性、安全性および効率性も得られます。

Cisco CloudCenter と Cisco ACI は連携して、複数階層アプリケーションを安全にプロビジョニングする機能、アプリケーション、ブループリントや導入スクリプトを変更せずにアプリケーションの拡張導入を自動化する機能、そしてアプリケーションを Cisco ACI 環境へ効率的に移行する機能といった独自の機能を提供します。