はじめに

- 概要 （1 ページ）
- はじめに （2 ページ）
- 1.2（1）の新機能APIC （9 ページ）

概要

Cisco Application Centric Infrastructure (ACI) は、現代の IT 自動化と DevOps においてインフラストラクチャをダイナミックに管理する新しい強力な方法を提供します。インフラストラクチャの構築方法を変えるツールがあるということも重要ですが、有効性や効率性を長期的に向上させるためには、構築時（Day 0）のアクティビティ以上に、インフラストラクチャを効率的に運用する能力が欠かせません。ACI を効果的に活用するために、組織は ACI を日常業務に組み込む方法を理解する必要があります。本書では、インフラストラクチャを継続的に運用するために IT チームが実施する一般的な運用アクティビティのいくつかを検証します。また、ACI ベースのファブリックで構築後（Day 1 以降）の運用をサポートするために採用可能なツール、手法、プロセスを紹介します。

本書で使用したハードウェアとソフトウェア

Cisco Application Centric Infrastructure (ACI) は、ハードウェア、ソフトウェア、ASIC イノベーションを組み合わせて統合システムアプローチを実現し、ネットワーク、アプリケーション、セキュリティ、仮想化に共通する管理フレームワークを提供します。

本書の執筆にあたっては、以下のハードウェア デバイスを使用しました。

- Application Policy Infrastructure Controller（APIC）
- ACI スパイン スイッチ（Cisco Nexus 9508 および 9336PQ など）
- ACI リーフ スイッチ（Cisco Nexus 9396PX、9396TX、93128TX など）
- Cisco Application Virtual Switch（AVS）
- Cisco UCS B シリーズおよび C シリーズ サーバ
- 複数のスイッチとルータのモデル（Cisco Nexus 5000 スイッチ、Cisco サービス統合型ルータ（ISR）など）
- さまざまなハイパーバイザ（KVM、Microsoft Hyper-V、VMware vSphere など）

• IXIA IxVM 製品ファミリのトラフィック ジェネレータ

本書の記述は、ACI 1.2 ソフトウェア リリースに基づいています。

はじめに

ACME 社について

ACME 社は、ロケット動力付きローラー スケート、ジェット式一輪車、各種爆発物など、多種多様な製品ポートフォリオの製造、販売、流通を専門としている多国籍企業です。各製品グループは、社内で個々のビジネス グループとして活動しており、これまでは、個々にインフラストラクチャとアプリケーションを保持していました。これらのグループは市場への小売りルートに重点を置いていましたが、オンライン販売チャネルを占めている新たな競合他社の出現に強い危機感を覚え、最近、より直販型のビジネスモデルを推進することを決定しました。さらに競争力を高める一助として、ACMEはプロジェクトを立ち上げ、ポートフォリオ全体の顧客への製品提供に向けて、注文と流通をサポートするモバイル アプリケーション プラットフォームを構築することにしました。

従来、ACME の事業部門は IT 要求を満たすために、サードパーティのソフトウェア企業と市販のソフトウェアを利用していました。しかし、消費者とより親密な関係を築き、ユーザからのフィードバックをプラットフォームで直接得ることを望んでおり、また、市場の変動により俊敏に対応できるように、継続的な改善サイクルを組み込むことも望んでいます。これまで、カスタム ソフトウェアを使用していたときは、従来のインフラストラクチャおよびソフトウェア モデルを利用していたので、変化する要件に対応できませんでした。そのため、ACME はアプリケーションとインフラストラクチャ両方のライフサイクルを管理する新しいアプローチを探しています。アプリケーション開発者は、継続的デリバリや継続的インテグレーションなどの新たなアプリケーション開発傾向について調査し、新しいアプリケーションプラットフォームをこの方式で開発することにしました。これに対応するには、従来の概念では不可能な方法で、インフラストラクチャ コンポーネントをこれらの新しいパラダイムにマッピングできる必要があります。

ACMEがこれまでに直面した最も大きな課題の1つは、運用とインフラストラクチャが製品開発の付け足しであったことです。このことはいくつかの問題を引き起こしています。アプリケーションを導入する際に、チーム全員が週末に長い時間を費やしているため、顧客に影響するような停止が生じ、さらに、完成までにビジネス リーダーの希望以上の時間がかかっていました。そのため、ACME 社 は環境の構築による変革を決意しました。この環境では、インフラストラクチャのアーティファクトをアプリケーションの一部として扱い、バージョン管理によりチェックして、実際のアプリケーションと同時にテストし、継続的に向上させることができます。

ACME は、新しいアプリケーション プラットフォームをタイムリーに配置することに大きな重点を置いています。その一方で、拡張してインフラストラクチャの共有プールを提供できる基盤づくりにも関心を示しています。このプールは、効率を高めるために、すべてのビジネス グループで共有され、マルチテナント方式で運用されます。

エグゼクティブ ブリーフィングで、Cisco Systems の当時の CEO、John Chambers 氏は ACME に次のように説明しました。「世界は変化しています。あらゆる企業がテクノロジー企業となっています。そのことを受け入れないと取り残されてしまいます」

Amazon Web Services（AWS）や OpenStack などのクラウド プラットフォームの成功によって実証されているように、技術提供型の消費モデルは急激なビジネス要件の変化により迅速に適応できます。これこそ、ACME 社 のビジネス オーナーに必要な消費タイプです。運用の管理は運用グループが重点を置いていることですが、管理は純粋な消費モデルのフォールトとなる可能性があります。企業が自動化コンポーネントの消費を可能にするテクノロジーに投資をしない場合、成長するために残された唯一の方法は、人的レベルのコンポーネントを破棄することですが、そのような企業で働くことを選ぶ人間はあまりいません。

さまざまなテクノロジー ベンダーからの現在の提案を分析した結果、ACME 社は Cisco Application Centric Infrastructure (ACI)を選択しました。とりわけ必要なのは、すべての物理的および仮想的なインフラストラクチャ構成を、開発、テスト、実稼働の全環境にわたって一貫性のある 1 つの構成にまとめる能力、および、現在 ACME が保持しているさまざまなデータセンターのロケーション全体における互換性です。ACIは、ネットワーク デバイスとプロトコルの構築に使用される下部構造を変更するためにゼロから構築されています。このレベルのイノベーションは、ユーザの対話用ツールを拡張する機会を提供します。ここでは、IT とインフラストラクチャがより動的であることに力点を置いています。つまり、ビジネスの速度に合わせて IT を運用および管理できるようにすることです。ただし、この種の変化は恐れ、不安、疑念を引き起こします。本書では、ACIファブリックでの運用アクティビティにある程度の快適さと親しみやすさを感じてもらえるように図っています。

ACME社は架空の企業ですが、この事例はあらゆる企業に該当し、重要なことは、そのような企業の従業員の事例でもあることです。IT業界の従事者には、ビジネスの急激な変化についていく心構えが必要です。しかし、これは、ビジネスとテクノロジーの関係における大部分の運用グループの在り方に反しています。ほとんどの IT 運用グループは、現在のサービス提供に必要なツールにかなりの時間をかけているので、再投資には組織的な抵抗があります。考えるべきことは、「これまで機能してるものをなぜ変更するのか」ということです。

Why、Who、What、When、How

ACIについて、ACMEはインフラストラクチャの運用方法を単純化することに目を向けていますが、それは初歩に過ぎないと気づきました。このアプリケーションとインフラストラクチャは ACME 社にとって新しいものです。ACME は、誰が何を管理するのか、どのようにタスクに取り組むのかなど、基本的な問いに取り組む必要があります。さまざまなグループが通常操作を実行する時期や、それらの操作を実行する対象範囲についても検討する必要がありますが、これらにはより戦術的なポイントインタイムが関連します。ここでは以下のモニカに関連する事項について説明します。これらのモニカは、ACI ファブリックの運用、および ACME 社などの企業がワークロードを分割する方法に関連しています。

Why

「Why（理由）」は、ACIファブリックを運用可能にするために考慮すべきことの中で最も重要な部分です。ACME 社の場合、主要な成功基準は、アプリケーション イニシアティブのサポートに必要なインフラストラクチャ展開のプロセスと手順を合理化することです。目的とする結果を得るには、高度な自動化が必要です。自動化は、繰り返しタスクを高速化し、エラー

や工程漏れを排除します。当初、自動化は一部の仕事に対する脅威のように感じられるため、それらの関係者にとっては恐ろしい提案となる可能性があります。しかし、自動化はまったく逆のことをもたらします。チームのメンバー全員がより楽しく作業し、自由に価値を刷新して追加できるようになり、その一方で、日常的な繰り返しタスクがなくなります。ファブリックの自動化が組織にとって有益になるwhy（理由）を考えることは、期待投資利益率を設定する上で重要です。また、運用が特定の方法で実行されるwhy（理由）を考えることも、使用するプロセスやツールを構想する上で役立ちます。

Who

多くの組織と同様、元来、ACME 社にはIT イニシアティブの成功に関わっているさまざまなタイプの関係者がおり、それぞれが専門とするインフラストラクチャの特定要素を担当していました。これらのグループに対して明確な組織的境界を設けることもできますが、どのIT 組織でも、境界はある程度あいまいになっているようです。下記はこれらのグループの特徴の一部を示していますが、いくつの特徴が組み合わされている場合もあることに留意してください。マクロ レベルでは、さまざまな組織が存在しているということがエンドユーザにわからないようにするべきです。代わりに、組織全体が1つのチームとして、組織に価値をもたらす共通の目標に向かっているように映るべきです。

ACMEの開発応用チームは、社内で使用するソフトウェアとアプリケーション、および顧客に提供するソフトウェアに重点を置いています。チームのアプリケーション担当部署にはアプリケーション製品の責任者と各部門の専門家がおり、他のビジネス部門がビジネス アプリケーションを活用して仕事を遂行できるように尽力しています。チームの開発担当部署は、モバイル アプリケーション ソフトウェアのプラットフォームを作成します。アプリケーションの設計、パフォーマンス、可用性がエンドユーザにとって最適なものになるように、両部署は同じ部門の他のチームと緊密に連携する必要があります。

ACME のネットワーク チームは、レイヤ 2（MAC/スイッチング）とレイヤ 3（IP ルーティング）でパケットを転送する、ネットワーク構成の構築と管理に重点を置いています。チームの課題は、高い可用性を保ちながら、アプリケーション要件のやりくり、SLA の管理、情報セキュリティの実施支援を行うことです。このチームは、ネットワーク構成の設定方法、レイヤ 3 とレイヤ 2 の結合方法、転送の検証方法、およびファブリック内のネットワーク転送に関するトラブルシューティング方法を理解している必要があります。ACIconrefACIを使用すると、チームは、過負荷のネットワーク構成を分離したり、解決を目指していた特定のネットワークの問題に立ち返ることができ、一方、他のグループは特定のチームの専門知識を活用してセキュリティやアプリケーション レベルのポリシーを操作できます。また、チームは、ネットワーク転送のパフォーマンスにおいてさらに高い透過性を実現し、セルフサービス容量内でオンデマンドで利用可能な主要メトリックを作成できます。

ACME のストレージ チームは、組織にデータ ストレージ リソースを配布することに主な重点を置いています。ストレージチームは、可用性の面からデータの保護に取り組み、さらに、機密データの安全性も確保します。ストレージ チームは、非常に厳しい SLA の維持に大きな成功を収めており、これまで、ストレージアクセス用の個々のインフラストラクチャを管理していました。ACI ファブリックによって提供される機能を使用することで、チームは新しい IP ベースのストレージおよびクラスタリングテクノロジーを自信を持って展開できます。チームは、ストレージアクセスの実行の様子を確認できること、および競合の発生時に通知を受けることを望んでいます。チームは、主として、QoSの複数パスなどに関する特定の要件を抱えています。これまでは、ストレージ デバイスの管理に加えて、ストレージ ファブリックの配布

にも気を使わなければなりませんでした。ACIは、ストレージチームに必要とされる可視性をもたせます。これらの機能については、主にモニタリングの項で説明します。

ACME 社のコンピューティングおよび仮想化チームは、管理を担うサーバ ファームの仮想化という大きな取り組みを終えようとしています。最近、チームは、仮想化への取り組みとは別の新たなワークロードに対処し、仮想化への取り組みから得たのと同様のアジリティをベアメタル サーバにおいても実現するために、新しい設定管理ツールを採用しました。アプリケーションのロールアウトには仮想化と非仮想化の両方のワークロードがあるので、この採用はタイムリーです。また、アプリケーション開発者は、アプリケーションのポータビリティを大幅に向上させるために、Linux コンテナ テクノロジーの活用にますます関心を抱いています。コンピューティングおよび仮想化チームは、物理サーバと仮想サーバに共通のアクセスを提供する ACIconrefACI の機能に関心を示しています。この機能を使用すると、複数のハイパーバイザを集約した一か所から仮想化クラスタにエンドポイント グループをパブリッシュできます。これらの機能については、「ファブリック接続」の章で詳しく説明します。

ACME 社の情報セキュリティ チームは、従来、アプリケーション導入プロセスに関与し、脆弱性評価とデータの分類を担当していました。現在のプロジェクトでは、新しいアプリケーションにクレジット カード番号などの顧客機密情報が格納されます。この情報の機密性とACIconrefACI ファブリックのセキュリティ面から見て、情報セキュリティ チームはプロセスの初期に入力を行うことで、セキュリティやコンプライアンスの問題による作業のやり直しを回避できます。情報セキュリティ チームは、ACI セキュリティ モデルの運用面に関心を持っています。これには、テナント、ロール ベース アクセス コントロール（RBAC）、モニタリング、およびレイヤ 4 ～ レイヤ 7 サービスが関連しているからです。

What

「What（何を）」についてはさまざまな面から考察できますが、本書における主要コンセプトは、ACIファブリックの運用管理にどのようなツールを使用するかということです。これまでのネットワークでは、CLIやSNMPなどの従来のツールを使用してネットワークの運用を管理し、ツールを管理プラットフォームや設定/管理プロセスに統合していました。

ACIには従来のツールの要素もいくつかありますが、ファブリックの管理は、より柔軟なベースを提供する抽象化オブジェクトモデルに基づいて行われます。このベースによって、ファブリック オペレータは複数のモードから選択できます（GUI、CLI、API 統合、プログラム、スクリプティング、またはこれらの組み合わせなど）。ACIconrefACIでのツールの選択方法は、実行内容とツールの使用方法によって決まります。たとえば、運用スタッフが多数のインターフェイスとスイッチから情報を収集する場合や、さまざまなオブジェクトを同時に管理する場合は、スクリプティングを使用すると効率的です。一方、単純なダッシュボードのモニタリングには GUI の方が適しています。

When

「When（いつ）」は、上記のチームが計画に関与する時期を示します。ファブリックの実装および管理方法に関するポリシーとプロセスを作成する際は、早い段階でさまざまなチームを関与させることをお勧めします。ACIconrefACI のコラボレーション特性によって、ワークフローの高度な並列化を実現できます。これはACIと従来の処理との主要な相違点です。従来の処理は本質的に逐次的であるため、アプリケーションの開発に長い時間がかかり、問題が発生した場合の平均解決時間も長くなります。

How

「How（どのように）」は、以下の基本的な質問に対する回答です。

- ネットワーク担当者は、どのようにネットワーク転送の設定に取り組むのか。
- コンピューティング チームは、どのようにインフラストラクチャから情報を取得し、最適なワークロードの配置を決定するのか。
- アプリケーション チームは、どのようにパフォーマンスと使用メトリックを追跡するのか。
- ストレージ チームは、どのようにストレージ サブシステムへのアクセスを追跡し、それが性能基準を満たしていることを確認するのか。

「how（どのように）」に環境設定の変更が関連する場合は、変更の管理についても検討する必要があります。変更の管理は、ACIがサポート対象としているミッションクリティカルな環境において避けがたいことです。ACIポリシーモデルは、フォールトドメインの全体サイズを削減し、増分変更のメカニズムを提供するように設計されています。バックアップと復元用のメカニズムがありますが、これらについては以降の章で説明します。また、このモデルについて、およびテナントやファブリック全体に影響を及ぼすオブジェクトについても説明します。

運用手順の変化に伴い、現行の変更管理や継続的な統合/デリバリ戦略の評価が必要になります。本書では、全体を通じて、ファブリックのプロアクティブおよびリアクティブな管理を取り上げています。

その根拠となるのは、ビジネス リスクを軽減してシステムの可用性を高めるために、大部分の組織がある種の構造化された変更管理方式を実装しているということです。変更/IT 管理に関するいくつかの基本原則（Cisco Lifecycle Services、FCAPS、およびITIL）があるので、それらを適切な指針として開始することができます。変更管理や継続的統合に対する共通認識アプローチの基礎となるのは、ファブリックを処理する前の設計実装サイクルの初期に、日常的なメンテナンス、モニタリング、プロビジョニングを行う運用チームと話し合うことです。達成基準（本書の目標の 1 つ）に関する運用チームのトレーニングも重要です。5 年前のテクノロジーに基づく変更管理方針を適用している状況では、ACIが提供するテクノロジーを迅速に導入できません。

ACI ソリューション固有のマルチテナント機能とロール ベース アクセス コントロール機能により、変更の範囲と影響をクリーンボックスに入れて分離したり取り出すことができます。詳細については、ロールベース アクセス コントロールを参照してください。

最終的には、各変更の評価は基本的に業務に与えるリスクと価値の両方の観点から実施する必要があります。低オーバーヘッドの変更管理プロセスを可能にするための1つの方法は、それぞれの変更によるリスクを軽減し、価値を増大させることです。デリバリ プロセスの初期から定期的にリリースを実行し、ユーザからのフィードバックに基づいて、デリバリ チームが常に最も価値があることに取り組むことで、継続的デリバリにおいてこれを実現できます。

情報管理システムの分野では、3 種類の基本的変更があります。

- 緊急の変更
- 標準
- 規格

定義によると、緊急の変更はある種の技術的な機能停止（ハードウェア、ソフトウェア、インフラストラクチャ）への対応であり、影響を受けたシステムへのサービスを復旧するために実行されます。

通常の変更とは、変更要求の作成から始まり、検討、評価、承認または却下、計画と実装（承認された場合）という、一定の変換管理プロセスを経た変更です。ACI環境では、通常の変更は次の構成要素内の項目に適用できます。」

- ファブリック ポリシー（ファブリック内部とアクセスについては後述）。
- 他のすべてのテナントと共有される、共通テナント内のコンフィギュレーション オブジェクト（ファブリック全体に影響を与えるもの）
  - プライベート ネットワーク
  - ブリッジ ドメイン
  - Subnets
- Virtual Machine Manager（VMM）の統合
- レイヤ 4 ～ レイヤ 7 デバイス
  - デバイス パッケージ
  - 論理デバイスの作成
  - 具体的なデバイスの作成
- レイヤ 2 またはレイヤ 3 外部コンフィギュレーション
- 接続可能エンティティ プロファイル（AEP）の作成
- サーバまたは外部ネットワークの接続
- トラフィックが流れる方向を実質的に変化させる、現在展開されているコントラクトとフィルタへの変更

標準の変更とは、事前承認された低リスクの変更です。それぞれの組織が、許可する標準の変更の種類、承認者、「標準」と見なす変更の基準、および変更管理プロセスを決定します。通常の変更と同様に、記録して承認する必要があります。ACI環境における「標準」の変更の例は、次のとおりです。

- テナントの作成
- アプリケーション プロファイルの作成
- エンドポイント グループ（EPG）の作成
- テナント レベルでのコントラクト
- レイヤ 4 ～ レイヤ 7 サービス グラフ
- エンドポイント グループのドメインの関連付け

上記の項目はすべてのタスクを包括したものではなく、毎日または毎週実行される一般的なタスクを示しています。

環境に対する変更を監査する機能は、ACME 社にとって要件の 1 つです。 Application Policy Infrastructure Controller (APIC) はシステムに対するすべての設定変更の監査ログを保持します。これは、「何かが動作を停止した場合」に対処する主要なトラブルシューティング ツールです。緊急の対応として、監査ログを確認し、誰がどのような変更をいつ行ったかを調べ、その変更に起因するエラーと関連付けます。これにより、変更を迅速に元に戻すことができます。

インフラストラクチャの管理における継続的デリバリの詳細については、本書の範囲外です。

以降ではこれらの質問に回答しながら、コンセプトと手順の使用方法のフレームワーク、および組織内の同様の取り組みにそれらを適用する方法のフレームワークを示します。本書は一定

の順序でレイアウトされています。しかし、ACIを使用することで、ACME社は、全体を通じて取り上げられている関係者と並行してそれらのタスクを完了できます。また、本書では、関係者が以前よりも協力的な方法で連携して作業できる方法も示しています。本書全体を通じていくつかのスクリプト作成例が示されており、最後の項では、ACI APIを使用して大部分の運用作タスクを自動化する方法が詳しく説明されています。組織構造がこれらのチームにサイロ化してしまう可能性がありますが、顧客、ユーザ、そして最終的にはビジネスにより高い価値をもたらす上で最も重要なことは、グループが相互に協力（*insieme*（インスィエーメ））して作業することです。

図 *1 : ACI* は組織全体の *IT* 要件に対応

1.2（1）の新機能APIC

Application Policy Infrastructure Controller (APIC) リリース 1.2(1) で多数の新機能と機能拡張が採用されています。このセクションでは、新しい機能を強調し、概要を説明します。新しいハードウェア サポートを含む詳細については、Cisco Application Centric Infrastructure (ACI) ソフトウェアの使用しているバージョンのリリース ノートを参照してください。

基本 GUI

新しい「基本」GUI 動作モードが追加されました。APIC ログイン画面に、**[Basic]**または **[Advanced]** GUI モードを選択するオプションがあります。シンプル化された GUI の目的は、一般的なワークフローを実現するための簡単なインターフェイスを提供することです。GUIの動作モードを使用して、管理者はオブジェクト モデルについての最小限の知識で ACI を簡単に開始することができます。シンプル化されたGUIにより、スイッチプロファイル、インターフェイス プロファイル、ポリシー グループ、またはアクセス エンティティ プロファイル（AEP）などの、高度なポリシーを設定する必要なく、リーフポートとテナントを設定できます。ACI管理者は、必要に応じて、引き続き高度な（標準）GUIモードを使用できます。基本GUIはACIに新しく取り組むユーザにとっては有意義なものですが、シスコは大規模な運用、既存のファブリックの展開、およびより詳細なポリシー制御のためには、高度な GUI を活用することをお勧めします。

NX-OS スタイルの CLI

APIC の設定に対する既存のアプローチでは、ポリシー モデルのほとんどすべての側面へのユーザ アクセスが可能ですが、ポリシー モデルおよびフレームワークを包括的に把握する必要があります。NX-OS スタイルの CLI の前の APIC CLI 設定機能では ACI ポリシー モデルに関連するすべての管理対象オブジェクト（MO）の知識が必要で、CLI は **mocreate** および **moconfig** などのコマンドを使用して、UNIXファイルシステムとして表されるこれらの管理対象オブジェクトを作成、編集、保存することができました。このアプローチは、設定プロセスをできるだけ簡単にするために内部の詳細のほとんどを隠す Cisco IOS/NX-OS CLI 機能とは根本的に異なりました。既存の NX-OS スタイルのコマンド インターフェイスとより適切に連携するために、APIC の NX-OS スタイルの CLI が、ACI のポリシー モデルの詳細を知る負担なく、APIC の能力を利用する目的で導入されました。

APIC の新しい NX-OS スタイルの CLI は、使い慣れた NX-OS の構文をできるだけ多く使用します。NX-OS スタイルの CLI は、大規模にアプリケーションを展開する ACI ポリシー モデルの能力を犠牲にすることなく、必要に応じて基盤となる ACI ポリシー モデルを作成または変更するためのインテリジェンスを、ユーザ入力に提供します。

使用するモードにより、コマンドがその状況で有効ではない可能性があります。たとえば、ポッド設定モード [apic1(config-pod)#] の場合、**show running-config ntp** コマンドは、現在の NTP 設定を示しています。NTP 設定モード [apic1(config-ntp)#] の場合、**show running-config server** コマンドは、現在のNTP設定を示しています。現在のモードを調べるには、**where** コマンドを使用します。次に例を示します。

```
apic1# where
exec
```

```
apic1# configure
apic1(config)# where
configure
apic1(config)# pod 1
apic1(config-pod)# where
configure; pod 1
apic1(config-pod)# ntp
apic1(config-ntp)# where
configure; pod 1; ntp
```

（注） デフォルトでは、バージョン 1.2(1) 以降を実行している APIC への **ssh** の場合、以前のリリースのオブジェクト モデル CLI ではなく、NX-OS スタイルの CLI に自動的に配置されます。オブジェクト モデル CLI を使用するには、**bash** コマンドを使用します。次のコマンドを使用して、**bash** シェルで 1 つのコマンドを実行できます。

bash -c '*path/command*'

次に例を示します。

bash -c '/controller/sbin/acidiag avread'

レイヤ 4 ～ レイヤ 7 のサービスに対するロールベースのアクセス コントロール ルールの強化

マルチテナント環境のレイヤ 4 ～ レイヤ 7 のポリシー設定では、従来のロールベース アクセス コントロール（RBAC）ドメインおよびロールを使用して、テナント管理者が作成できない特定のオブジェクトを作成するのに、管理者の介入が必要でした。これは、ACI ポリシー モデルの、よりきめ細かな RBAC の権限の要件を採用します。テナント管理者は、グローバルな管理者の介入なしに、セルフサービスを介して RBAC ルールを作成し、テナント サブツリーの下にあるリソースの権限をシステム内の他のテナントやユーザに付与することもできるようになりました。

入力ベースの ACL

通常、ファブリックは、宛先エンドポイント グループが L3Out である場合、またはハードウェア プロキシ モードのブリッジ ドメインで、宛先エンドポイントがどのエンドポイント グループにあるかを入力リーフ スイッチが認識していない場合などを除き、ポリシー適用のために入力エンドポイント グループベースのアクセス コントロール リスト（ACL）を使用します。これらの例外が発生しても、ポリシーの適用は、パケットがファブリックから発信されているときに発生します。

ACI 管理者は、境界リーフ（L3Out 接続が配置され、入力/出力ポリシーがこれまで適用されてきた）から着信接続の送信元の非境界リーフへ、ポリシーの適用を移動できるようになりました。目標は、L3Out 接続を利用しているテナントの境界リーフでプログラムする必要がある ACL ルールの数を削減することと、代わりに接続元の入力リーフ スイッチへとそれらを移行することです。

「Policy Control Enforcement Direction」という名前の新しい設定プロパティが、レイヤ 3 External Outside エンドポイント グループに追加されました。このプロパティは、L3Out の出力トラフィックのポリシー適用の方向を定義するために使用されます。新しいデフォルト設定は、新しく作成されたレイヤ 3 External エンドポイント グループの入力ですが、このソフトウェアの

バージョンよりも前の既存のL3Outでは、以前の動作が変更されないように、古いデフォルトの動作が出力モードで継続されます。以前に作成したL3Outは ACI 管理者により、入力モードに手動で変更できます。

トラブルシューティング ウィザードの機能拡張

バージョン 1.1(1) で導入されたトラブルシューティング ウィザード（TSW）は、単一のテナント内からのエンドポイント接続のテストに限られていました。これでは、エンドポイントのいずれかがユーザテナントの外にある場合（共通テナントなど）、問題が表示されました。この機能は、テナント間のエンドポイントのテストをサポートするように改善されました。

APIC コンフィギュレーション ロールバック

設定のロールバック機能により、設定のスナップショットを作成でき、ローカルまたはリモートの場所に保存できます。2 つの保存されたスナップショットは、2 つの違いを特定するために使用することもできます。ファブリック ポリシーの変更が誤って行われた、またはそれにより問題が引き起こされた場合、スナップショットをロールバックして、変更されたポリシーのみを戻すことができます。既存かつ永続的なポリシーはこの操作中に影響を受けません。この機能には、スナップショットを自動化し、スケジュールする、組み込みの繰り返し機能が含まれています。スナップショットは、ファブリック全体またはユーザ テナント レベルで作成できます。

vRealize 統合

vRealize 自動化アプリケーションからAPICポリシーの管理を可能にする、VMware の vRealize スイート用のACI固有プラグインが導入されました。ユーザは、オーケストレーションおよび自動化ソフトウェアを使用して、仮想コンピューティングおよびサービスに加えて、基礎となるファブリックをプロビジョニングできるようになりました。プラグインは、定義済みのAPICポリシー、ワークフロー、ブループリントへのアクセスを提供します。

レイヤ 4 ～ レイヤ 7 サービス用のアンマネージド モード

レイヤ 4 ～ レイヤ 7 サービスの挿入機能によって、管理者は 1 つ以上のサービスを 2 つのエンドポイント グループ間に挿入できます。APIC はサービスのファブリック リソース（VLAN）を割り当て、サービス グラフで指定された設定に基づいてファブリック（リーフ）およびサービス アプライアンスをプログラムします。以前は、APIC には、サービス グラフの一部として使用するレイヤ 4 ～ レイヤ 7 のサービスに対するデバイス パッケージが必要でした。この処理の一部は、グラフのインスタンス化時のAPICのサービス アプライアンスのプログラミングを含んでいました。

一部の環境では、グラフのインスタンス化時に、APIC はサービス グラフのネットワーク リソースのみを割り当て、ファブリック側のみをプログラムすることが望ましい場合があります。これは、さまざまな理由で必要とされる可能性があります。たとえば、サービスアプライアンスをプログラムするために、既存のオーケストレータまたはDevOpsツールがすでにある環境の場合です。別の一般的な場合として、サービス アプライアンス用のデバイス パッケージがそのプラットフォームでは使用できない可能性がある場合です。

サービスのアンマネージド モードは必要な柔軟性を向上させます。有効にすると、サービス アプライアンス向けネットワーク リソースの割り当てと、ファブリック（リーフ）のプログラムのみに APIC を制限します。デバイスの設定は、外部でのお客様による実行に任せられます。

簡易ネットワーク管理プロトコル（SNMP）のサポート APIC

次の拡張機能が APIC とファブリック スイッチの既存の SNMP エージェントに追加されました。

- ISIS の隣接状態の変化トラップ
- 温度センサーのしきい値トラップ
- 電源インレット回線またはケーブルの状態変化トラップ
- CPU 使用率しきい値トラップ

vSphere 6 のサポート

VMM の vSphere 6.0 と vCenter 6.0 との統合が APIC バージョン 1.1(2) で導入されました。サポートには VMware Virtual Distributed Switch（vDS）の統合のみが含まれていました。Cisco AVS に対する追加のサポートは、このリリースに含まれています。リリース 1.2(1) での唯一のサポート制限は、vCenter 間と、vDS vMotion 間は AVS でサポートされないということです。これらの機能は、VMware vDS で完全にサポートされます。

共通パーベイシブ ゲートウェイ

複数のファブリックが展開されている ACI 展開で、1 つのファブリックから別のファブリックへのエンドポイントの移動には、ヘアピン トラフィックを回避するためにデフォルト ゲートウェイまたは IP アドレスを変更する必要がありました。この機能により、何も変更する必要なく、ファブリック間のエンドポイントのシームレスな移動が可能になります。

この機能を設定するには、各ファブリックに同様に設定された 2 つのブリッジ ドメインの設定が必要です。各ファブリックのブリッジ ドメインは、同じ仮想 IP アドレスと仮想 MAC アドレスを使用して設定され、それにより物理ファブリックがどこに存在しているかに関係なく、ブリッジ ドメインのエンドポイントからの到達可能性がもたらされます。

Microsoft マイクロセグメンテーション（uSeg）のサポート

APIC ソフトウェア リリース 1.1(1) では、ACI に属性ベースのエンドポイント グループ（別名 uSeg）の概念が導入されました。これにより、仮想マシン属性（VM 名、OS タイプ、およびハイパーバイザなど）、IP アドレスおよび仮想マシンと一致する MAC 設定を含む、さまざまな属性で定義された「uSeg EGP」と呼ばれる特別なエンドポイント グループが有効になります。属性の照合は、その uSeg エンドポイント グループのポリシーを仮想エンドポイントに動的に適用します。仮想ポート グループのバインディングを再度割り当てる必要はありません。このリリースより前では、VMware 仮想マシンのみがサポートされていました。現在は、Microsoft HyperV 仮想マシンにもサポートの対象が拡大されました。

Direct Server Return

エンドポイントがロード バランサの背後に配置されると、クライアントの要求はロード バランサに送信され、次に宛先サーバにリレーされます。サーバがクライアントに応答すると、同じパスを通過してロードバランサへ、さらにクライアントへと戻ります。これにより、しばしばロード バランサが通信のボトルネックとなり、ネットワーク パフォーマンスを低下させる可能性があります。Direct Server Return では、宛先サーバが直接クライアントに応答でき、ロード バランサを経由してリレーされる必要はありません。

共有レイヤ 3 Out

以前のソフトウェア リリースでは、レイヤ 3 Out 接続の導入方法と、複数のテナントによる使用に制限がありました。多くの場合、ユーザは同じゲートウェイデバイスを使用しているテナントにもかかわらず、テナントごとにレイヤ 3 Out のポリシーを定義する必要がありました。

このリリースではこの機能が改善され、テナントまたは VRF が、異なるテナントに設定されたレイヤ 3 Out 接続を使用できる機能が追加されました。この機能の一般的な使用例は、複数のユーザ テナントにより共有される「共通」テナントのレイヤ 3 Out を含むファブリックです。これは2つのテナント間で学習したルートをリーキングすることによって実現されます。

この機能の 1 つの制限は、中継ルーティングとも言われる、共有 L3Out 接続から渡される 1 つのテナントの学習ルートの交換がサポートされないことです。