Cisco Cloud ACI on AWS

目次

Cisco Cloud Application Centric Infrastructure（Cisco Cloud ACI）の概要

企業に昨今強く求められるようになってきたのは、すばやくイノベーションを起こし、競合他社に後れを取らないように IT の俊敏性を高めることで顧客の要求を満たすことです。この目的を達成するためには、アプリケーションを展開する際、そのタイプに応じたインフラストラクチャ環境を選択しなければなりません。オンプレミスでホストするのが最適なアプリケーションもあれば、パブリッククラウドでホストするのが最適なアプリケーションもあります。さらに言えば、ハイブリッド展開に利点があるアプリケーションもあります。実際、ハイブリッドクラウドは多くの企業にとって新たな標準になりつつあります。

ただし、ハイブリッドクラウド環境の場合、均質なエンタープライズ運用モデルを維持すること、社内セキュリティポリシーを遵守すること、ハイブリッド環境全体で可視化を実現するのは容易なことではありません。Cisco Cloud Application Centric Infrastructure（Cisco Cloud ACI）は、運用のシンプル化、一貫性のあるポリシー管理に加え、複数のオンプレミスデータセンター環境とパブリッククラウドの可視化や、ハイブリッドクラウド環境の可視化を実現する包括的なソリューションです。オンプレミスのデータセンターで Cisco ACI™ を実行しているお客様は、Cisco Cloud ACI により、Cisco ACI ポリシーをパブリッククラウドにも適用できるようになります。

オンプレミスの Cisco ACI データセンターでは、データセンターに展開されているすべての Cisco ACI スイッチのポリシーを Cisco Application Policy Infrastructure Controller（APIC）から一元的に構成して管理できます。Cisco ACI を活用した複数のデータセンターをシームレスに相互接続し、Cisco ACI の構造とポリシーをサイト全体に選択的に適用する必要があるときは、Cisco ACI Multi-Site Orchestrator（MSO）の出番です。MSO は、地理的に分散した複数の ACI サイト全体でポリシーのオーケストレーションと可視化を一元的に行えるソフトウェアソリューションです。

Cisco ACI リリース 4.1 ではこうした新しい Cisco Cloud ACI 機能が利用可能になっており、オンプレミスの複数の Cisco ACI データセンターとパブリッククラウド全体でポリシーを管理することができます。MSO で構成したポリシーを、さまざまなオンプレミス Cisco ACI サイトとクラウドサイトにプッシュできます。オンプレミスで実行されている Cisco APIC コントローラは、MSO から受け取ったポリシーをローカルでレンダリングして適用します。Cisco ACI をパブリッククラウドに拡張するときにも似たようなモデルが使用されます。ただちょっとしたひねりがあります。Cisco ACI は、パブリッククラウドベンダーにとってネイティブの言語ではありません。エンドポイントグループ（EPG）やコントラクトといった概念になじみがないのです。そのため、MSO ポリシーをクラウドネイティブのポリシー構造に変換しなければなりません。たとえば Cisco ACI EPG 間のコントラクトの場合、AWS ではまずセキュリティグループに変換してから AWS クラウドインスタンスに適用することになります。このようにクラウド環境でポリシーを変換してプログラミングするには、Cisco Cloud ACI ソリューションの新しいコンポーネントを使用します。それが、Cisco Cloud Application Policy Infrastructure Controller です（以降、Cisco Cloud APIC または Cloud APIC と表記します）。

Cisco Cloud APIC は、サポートされているパブリッククラウドでネイティブに実行されます[1]。これにより、パブリッククラウドで接続を自動化し、ポリシーを変換して、ワークロードを高度に可視化できます。Cisco Cloud APIC は、MSO から受け取ったすべてのポリシーを変換して、VPC（仮想プライベートクラウド）、セキュリティグループ、セキュリティグループルールなどクラウドネイティブの構造にプログラミングします。

[1] パブリッククラウド環境のサポート情報については、データシートとリリースノートを参照してください。

この新しいソリューションに含まれる一連の機能により、アプリケーションの配置先に関係なくポリシーと運用の一貫性を高め、オンプレミスのデータセンターを真のハイブリッド クラウド アーキテクチャに拡張できます。また、ハイブリッド環境全体でのポリシーのオーケストレーション、一貫性のある運用、クラウド全体での可視化を一元的に行えます。

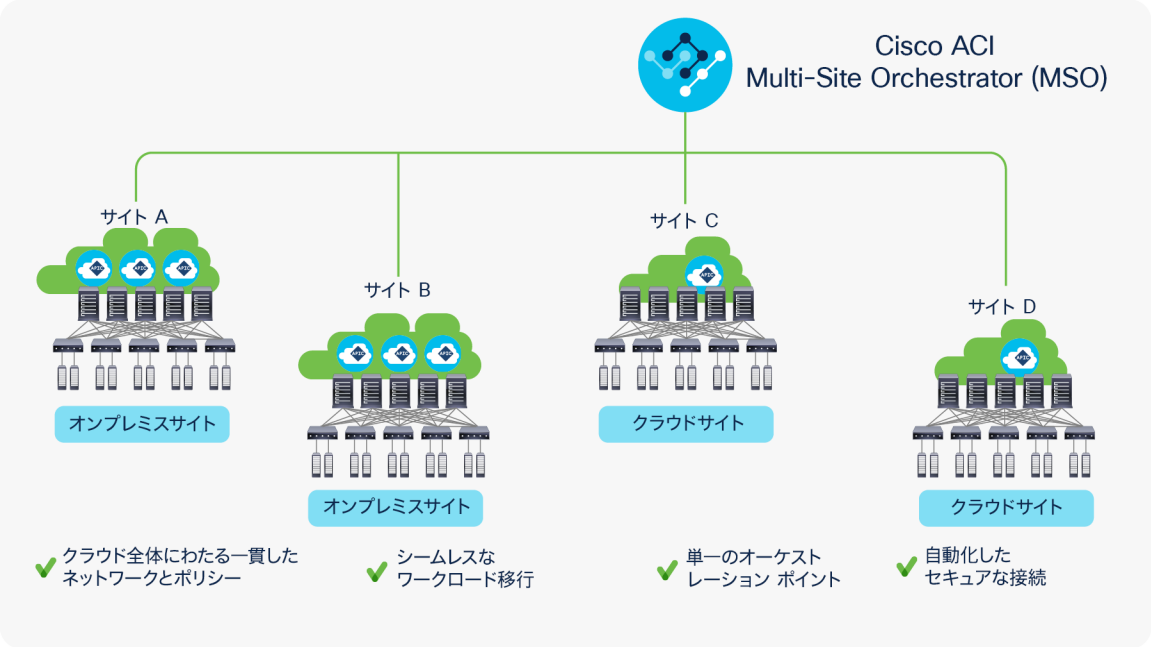


図 1.
Cisco Cloud ACI のアーキテクチャの概要

図 1 は、Cisco Cloud ACI のアーキテクチャ全体の概要を示しています。Cisco ACI Multi-Site Orchestrator がポリシーを一元管理するコントローラとして機能し、オンプレミスの複数の Cisco ACI データセンターとハイブリッド環境全体でポリシーを管理します。各クラウドサイトは、それぞれの Cloud APIC で抽象化されています。このホワイトペーパーではこの後、Cisco Cloud ACI on AWS のアーキテクチャ、利点、ユースケース、展開について説明します。

ハイブリッドクラウド環境の課題

ハイブリッドクラウド戦略の採用が進む中、シンプルで一貫した運用モデルを構築して、場所を問わず一貫性のあるポリシー、セキュリティ、可視化を実現することが求められています。それとともに、ハイブリッドクラウドの利点を得るためにソリューションの総費用を抑える必要があります。

ハイブリッドクラウド環境を構築して運用する際の主な課題は次のとおりです。

1. オンプレミスとパブリッククラウド間で安全な相互接続を自動的に確立する必要がある
2. オンプレミスのプライベートクラウドとパブリッククラウド全体での多様で一貫性のない機能に対処する必要がある
3. ハイブリッドクラウド インスタンスを管理、モニタリング、運用するには複数のツールを使用しなければならない
4. オンプレミスとパブリッククラウドでは、セキュリティ セグメンテーション機能に一貫性がない

5. パブリッククラウド環境の運用については学習曲線の問題がある
6. ハイブリッドクラウド環境の展開では、一貫した L4 ~ L7 サービスの統合を活用できない

Cisco ACI はアプリケーションを忠実に模倣したネットワークポリシーに基づく制御と可視化を可能にすることで、Software-Defined Networking（SDN）の約束であったインテントベースでのネットワークの構成と自動化を実現し、運用をさらにシンプルにしました。次に必要なのは、こうしたポリシーに基づく自動化をハイブリッド環境に拡張することです。Cisco Cloud ACI ソリューションは、自動化、セキュリティ、シンプル化を重要な柱とする首尾一貫したハイブリッドクラウド戦略を提供します。

Cisco Cloud ACI on AWS のアーキテクチャの概要

これまでの簡単な説明に加え、図 2 にも示すように、MSO のインスタンスは一貫したポリシーモデルを使用して複数の独立したサイトとのオーケストレーションを行うため、管理と可視性を一目で把握できます。これを、APIC クラスタがローカルに存在するオンプレミスの Cisco ACI ファブリックサイトでも、Cloud APIC で管理する AWS のクラウドサイトでも実現できます。通常の Cisco ACI マルチサイトアーキテクチャと同じく、すべてのサイトが「プレーンな」IP ネットワークで相互接続されます。その際、IP マルチキャストや Dynamic Host Configuration Protocol（DHCP）リレーは必要ありません。IP 接続を確立するだけでよく、その先は MSO によってサイト間オーバーレイ接続が確立されます。

Cisco ACI マルチサイトソリューションの詳細については、次のホワイトペーパーを参照してください。
https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.pdf

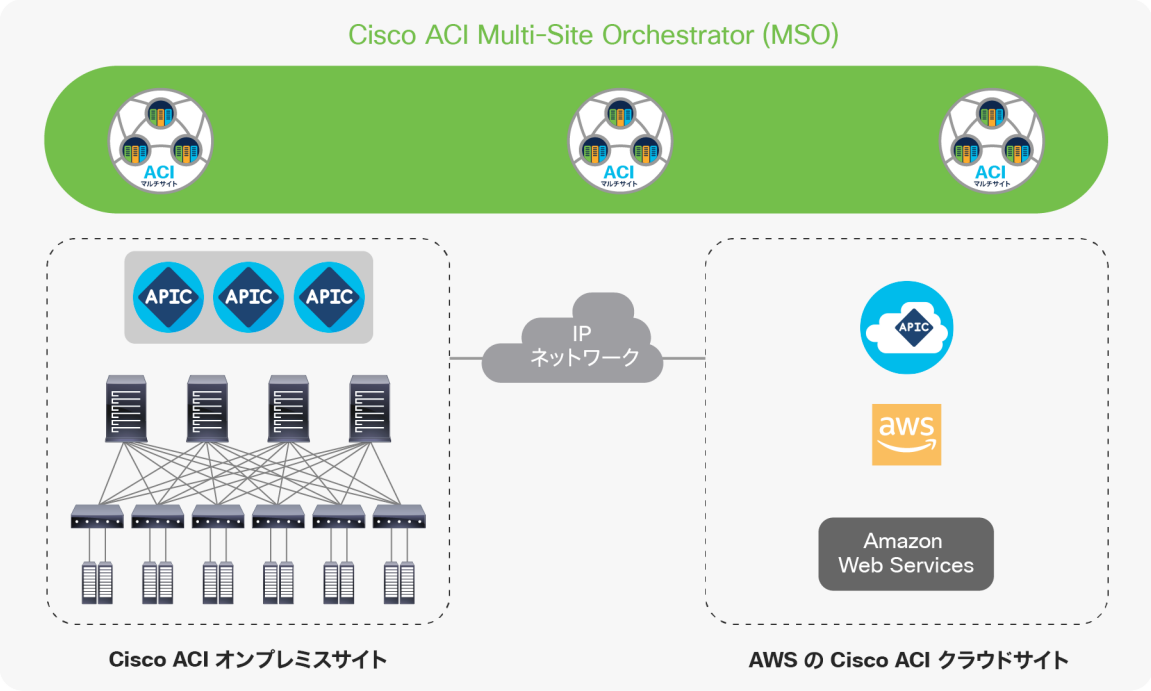


図 2.
Cisco Cloud ACI on AWS アーキテクチャ

Cisco Cloud ACI アーキテクチャの主な構成要素には、Cisco ACI リリース 4.1 ソフトウェアを実行し、第 2 世代のスパインモデル（EX、FX、C、または GX）を少なくとも 1 つ搭載しているオンプレミスの Cisco ACI サイト、Cisco ACI Multi-Site Orchestrator（MSO）、Cisco Cloud APIC、オンプレミスとクラウドサイトとのサイト間接続、オンプレミスの Cisco ACI サイトとクラウドサイト間のネットワーク ポリシー マッピングなどがあります。Cisco ACI リリース 4.2 以降、オンプレミスの Cisco ACI サイトは必須ではなくなりました。これにより、クラウド環境のみのお客様にも、ポリシーを 1 つだけ管理すればよい、クラウドサイトを自動的にプロビジョニングできる、可視性と相関関係を一元的に把握できるといった Cloud ACI の利点がもたらされます。

Cisco ACI Multi-Site Orchestrator（MSO）

Cisco ACI マルチサイトアーキテクチャの場合、相互接続されたすべてのサイトを Cisco ACI Multi-Site Orchestrator（MSO）から一元管理できます。すべてのサイト間ポリシーを 1 箇所で定義して、個々の Cisco ACI サイトに公開できます。個々のサイトでは、ローカルに存在する APIC が、ファブリックを構築する物理スイッチでそれぞれのポリシーをレンダリングします。

Cisco Cloud ACI を導入すると、MSO のオーケストレーション機能をクラウドサイトでも利用できるようになります。オンプレミスの Cisco ACI データセンターのサイト登録もクラウドサイトの登録も、MSO によって行われます。また、すべてのサイト（オンプレミスとクラウド）間にオーバーレイ接続が自動的に確立されます。MSO は、引き続きサイト間ポリシーの中心的なオーケストレータとして機能するほか、オンプレミスの Cisco ACI データセンターサイトだけでなく、AWS のクラウドサイトにも同じポリシーをプッシュできるようになりました。また、関連するサイトにのみポリシーを選択的に配布することで、オンプレミスとクラウドサイト間でポリシー展開をインストゥルメント化することもできます。たとえば MSO の場合、コンピューティング層とデータベース層をオンプレミスサイトに保持しながら、アプリケーションの Web フロント層を AWS のクラウドサイトに展開できます。ネットワーク管理者は、アプリケーションのリクエストに応じて、MSO のインターフェイスからオンプレミスサイトと AWS 間の通信フローを調整することもできます。

Cisco Cloud APIC on AWS

Cisco Cloud APIC は、Cisco Cloud ACI のアーキテクチャに新たに導入された重要なソリューション コンポーネントです。クラウドサイトの APIC に相当します。オンプレミスの Cisco ACI サイト向けの APIC と同じく、Cloud APIC はポリシーインテントを記述した Cisco ACI ネットワークポリシーモデルを使用して、クラウドサイトで実行されているネットワークポリシーを管理します。Cloud APIC はソフトウェア専用のソリューションであり、クラウドネイティブのインストゥルメント（AWS CloudFormation テンプレートなど）を使用して展開されます。ネットワークポリシーとセキュリティポリシーは、クラウドサイトの Cloud APIC でローカルに定義することも、MSO でグローバルに定義してから Cloud APIC に配布することもできます。オンプレミスの APIC が目的のポリシーをクラウドサイトの Cisco ACI スイッチにレンダリングし、Cloud APIC がそのポリシーを AWS クラウド ネットワーク インフラストラクチャにレンダリングします。このレンダリングは、Cisco ACI ネットワークポリシーを AWS ネイティブのネットワークポリシーに変換し、必要とされている AWS ネイティブのクラウドリソースを AWS ネイティブのポリシー API を使用して自動的にプロビジョニングすることで行われます。必要とされているリソースとは、VPC、クラウドルータ（Cisco® CSR 1000V シリーズと AWS Virtual Private Gateway（VGW））、セキュリティグループ、セキュリティグループルールなどです。簡単にまとめると、Cloud APIC の主な機能は次のとおりです。

1. ノースバウンド REST インターフェイスからクラウド展開を構成できます。
2. Cisco ACI ポリシーモデルとその他のクラウド固有のポリシーを直接または MSO から受け入れます。
3. クラウドサイトでエンドポイントの検出を行います。
4. Cisco ACI クラウドポリシーの変換を実行します。

5. クラウドルータのコントロールプレーンを構成します。
6. Cisco ACI ファブリックとクラウドサイト間のデータパスを構成します。

Cisco Cloud APIC は、APIC コントローラソフトウェアをマイクロサービスベースで展開するものです。Cisco Cloud APIC on AWS は、Amazon Elastic Block Store（Amazon EBS）の永続ブロック ストレージ ボリュームを使用して Amazon Elastic Compute Cloud（Amazon EC2）インスタンスとして展開され、動作します。AWS マーケットプレイスで Cisco Cloud APIC 向けの Amazon マシンを入手し、そのライセンスとして所有ライセンス持ち込み（BYOL）モデルを使用できます。

オンプレミスの ACI ファブリック向けの ACI APIC として機能する場合、ACI Cloud APIC はポリシーのみを扱い、データ転送パスには関与しません。Cloud APIC でダウンタイムが発生しても、クラウドサイト内のネットワーク転送機能やパフォーマンスに影響はありません。Cloud APIC の Amazon EC2 インスタンスは、Amazon EBS に組み込みのストレージボリュームの冗長性、高可用性、耐久性を利用します。Amazon EC2 インスタンスで障害が発生した場合はいつでも再起動（永続ストレージから構成と状態を再構築して以前の状態に復元）することができ、Cloud APIC の機能をシームレスに利用できます。したがって Cisco Cloud ACI on AWS の初期リリースでは、シンプルさと費用対効果の点から、Cloud APIC は単一の Amazon EC2 インスタンスとして展開されます。将来的には複数の仮想インスタンスのクラスタリングを導入して、Cloud APIC の拡張性とインスタンスレベルの冗長性を高める予定です。

Cisco Cloud ACI を使用する主な利点

Cisco Cloud ACI ソリューションの主な利点は次のとおりです。

オンプレミスとクラウドの相互接続の自動化

Cisco Cloud ACI on AWS は、オンプレミスの Cisco ACI ファブリックと AWS との間にエンドツーエンド接続を自動的に構成します。この接続は、IPsec VPN または AWS Direct Connect を使用してインターネット経由で行うことができます。Cisco Cloud APIC は、AWS に Cisco CSR 1000V シリーズ ルータをペアで展開して、オンプレミスにインストールされている IPsec ターミネータへの IPsec トンネルを形成するように各ルータをプログラミングします[2]。IPsec トンネルが稼働したら、MSO はオンプレミスの第 2 世代の Cisco ACI スパインと、AWS に展開された Cisco CSR 1000V シリーズ ルータとの間に BGP EVPN コントロールプレーンを設定します。これで、オンプレミスのデータセンターと AWS との間にエンドツーエンドの VXLAN トンネルが確立されます。このようにエンドツーエンドが自動化されるので、ハイブリッドクラウド接続をシームレスに確立できます。設定に要する時間が短くなり、エラーのリスクが減って、展開と変化のペースが向上します。このドキュメントの後半では、サイト間接続の自動化について技術的に詳しく説明します。

ユニバーサルポリシーモデル

Cisco ACI と AWS の両方とも、グループベースのネットワークポリシーモデルとセキュリティポリシーモデルを使用します。簡単に言えば、Cisco ACI ネットワークポリシーモデルの論理的なネットワーク構造は、テナント、ブリッジドメイン（BD）、ブリッジドメインサブネット、エンドポイントグループ（EPG）、コントラクトで構成されています。AWS の構造は若干異なり、ユーザーアカウント、Virtual Private Cloud（VPC）、セキュリティグループ、セキュリティグループルール、ネットワークアクセスリストを使用します。図 3 に示すように、Cisco ACI はエ

[2] ターミネータの設置はお客様の責任で行ってください。Cisco ACI リリース 5.1 の時点では、Cisco CSR 1000V のみが認定されています。

ンドポイントを EPG に分類し、コントラクトを使用してこれらの EPG 間に通信ポリシーを適用します。AWS は、分類とポリシーの適用にセキュリティグループ（SG）とセキュリティグループルールを使用します。図 4 は、セキュリティグループとセキュリティグループルールを使用して、AWS セキュリティポリシーを適用する一例を示しています。

図 3.
Cisco ACI の EPG ベースのネットワークモデル

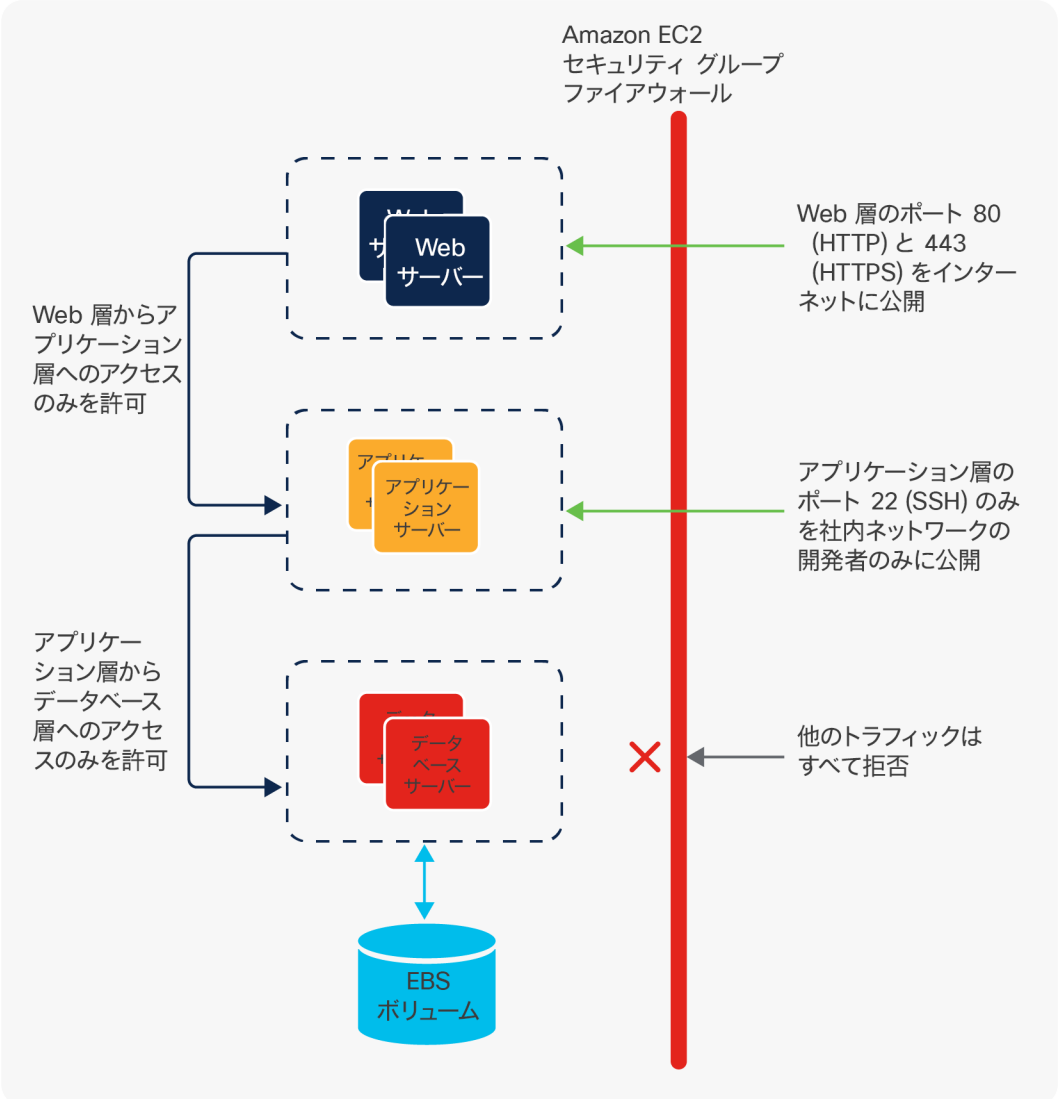


図 4.
AWS の SG ベースのネットワークモデル

*この図は、AWS のホワイトペーパー「Web Application Hosting in the AWS Cloud」[英語] から引用しました。

Cisco ACI と AWS 全体にネットワークポリシーを適切に展開するには、この 2 つのネットワークポリシーモデル間に細かく正確なマッピングを設定することが非常に重要です。図 5 は、Cloud APIC がこのポリシーマッピングをどのように処理するかを示しています。

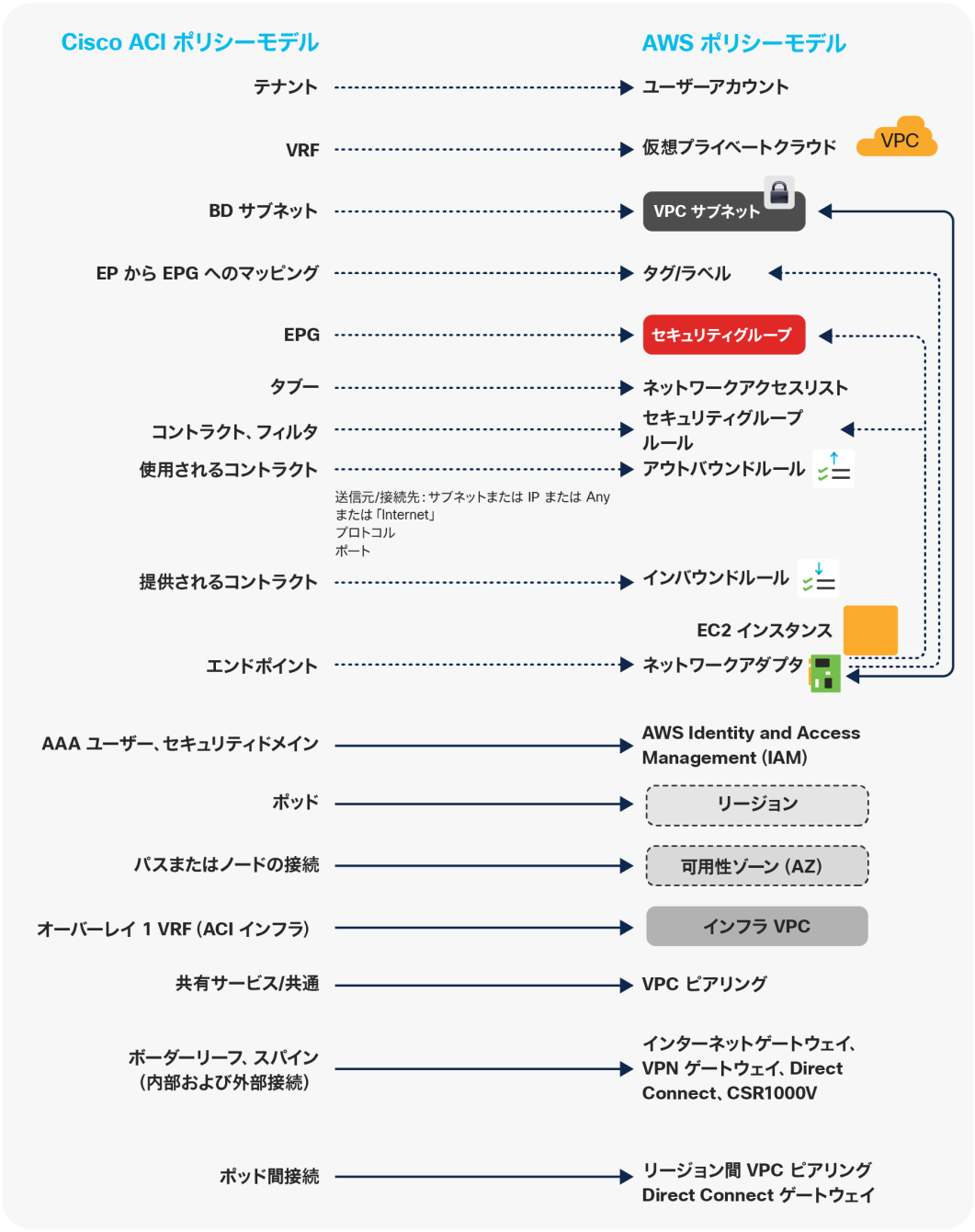


図 5.
Cisco ACI ポリシーモデルから AWS へのマッピング

統一されたネットワーク管理と運用

Cisco ACI Multi-Site Orchestrator（MSO）は、オンプレミス環境とパブリッククラウド環境におけるすべての管理対象エンドポイントをエンドツーエンドで可視化して各エンドポイントの正常性を把握できるようにするものです。MSO により、ハイブリッドクラウド環境の正常性、パフォーマンス、運用ステータスの一元的なモニタリングが可能になります。MSO から一元的にポリシーの構成とオーケストレーションが可能になるため、ハイブリッド環境全体で運用の複雑さが大幅に軽減されます。

クラウドネイティブサービスの利用

Cisco Cloud ACI は、クラウドネイティブの構造に従ってセキュリティポリシーとワークロード セグメンテーション ポリシーを適用します。そのため、Cisco Cloud ACI で管理されるワークロードからクラウドネイティブサービスを簡単に利用できます。管理者は、MSO でポリシーを定義して、どのワークロードがどのクラウドネイティブサービスにアクセスできるかを制限できます。AWS 環境内では、こうしたポリシーはワークロードから特定のサービスへのアクセスを許可または拒否するセキュリティグループルールとしてプログラミングされます。APIC 管理者にとって、アプリケーションの一部がオンプレミスで展開され、一部がクラウドで展開されることは重要ではありません。アプリケーションの通信を制御するのは、おなじみの EPG とコントラクトだからです。このソリューションの主な利点としては、クラウドバーストが簡単になることがあります。

さらに詳しく：ACI クラウドサイトの内部を見る

インフラ VPC によるハブアンドスポークトポロジ

Cisco Cloud ACI を実行すると、ハブアンドスポーク型の Amazon Virtual Private Cloud（VPC）トポロジが AWS ネイティブのネットワーク インフラストラクチャに展開されます。これは、Cisco ACI ポリシーを AWS ネイティブのポリシーに変換することで行われます。ハブはインフラ VPC であり、スポークはアプリケーションのエンドポイントが展開されるユーザー VPC です。この概念を、図 6 では AWS Virtual Private Gateway（VGW）と IPsec を使用して示し、図 7 では AWS Transit Gateway を使用して示しています。[3]

[3] AWS Transit Gateway（https://aws.amazon.com/jp/transit-gateway/）は、Cisco ACI リリース 5.0 以降でサポートされています。

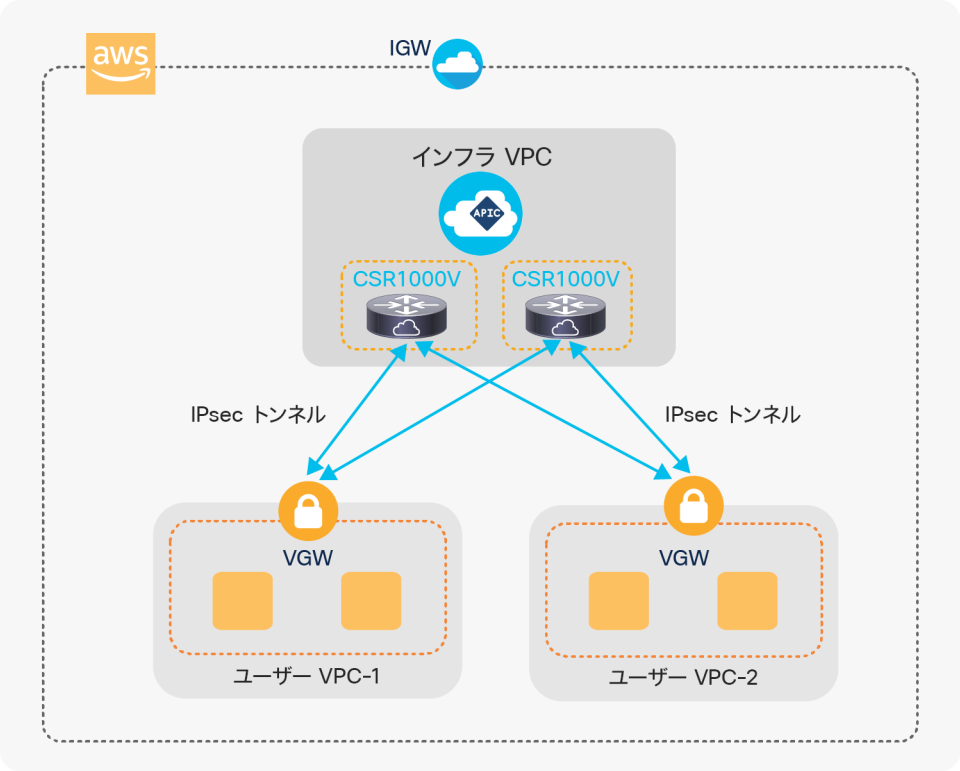


図 6.
VGW と IPsec トンネルを使用したクラウド

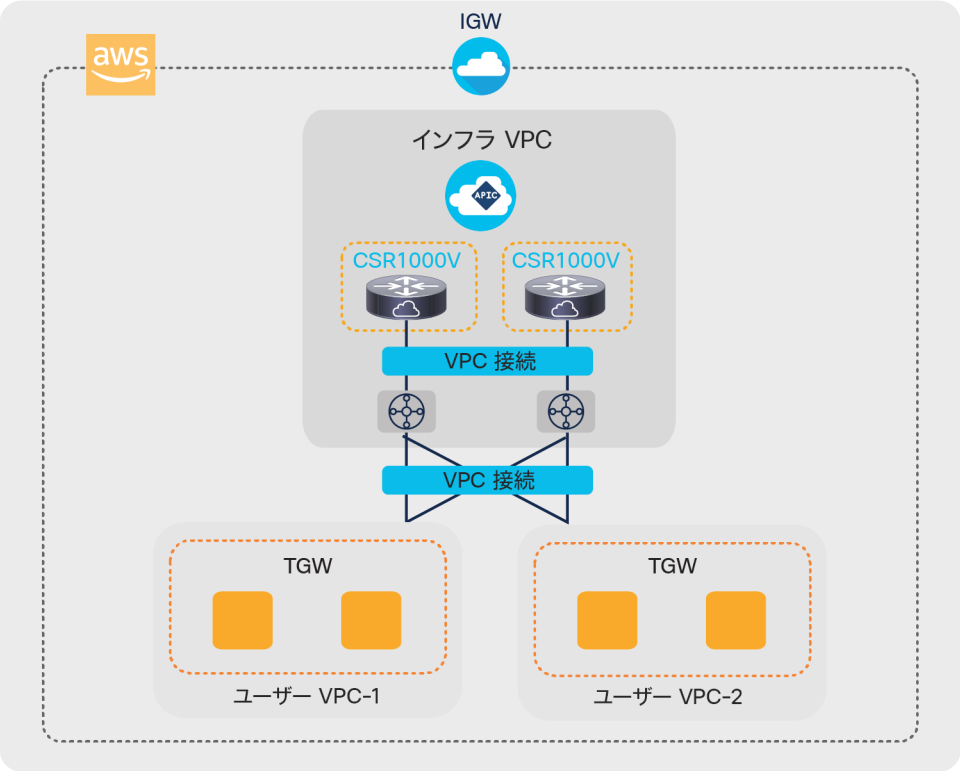


図 7.
AWS Transit Gateway を使用したクラウド（Cisco ACI リリース 5.0 以降）

インフラ VPC は、オンプレミスの Cisco ACI インフラ VRF の論理部分を担います。Cloud APIC が展開されて実行されている部分です。Cloud APIC の展開時に自動的に作成されます。Cloud APIC は続いて、仮想アンダーレイ接続を実現するクラウドルータとして、このインフラ VPC に Cisco CSR 1000V シリーズ ルータをペアで展開します。仮想アンダーレイ接続とは、クラウドサイト内の内部接続や、オンプレミスの Cisco ACI サイトへのサイト間接続などです。図 7 に示した AWS Transit Gateway を使用している例の場合、AWS Transit Gateway のペアもインフラ VPC に自動的に作成されます。

ユーザー VPC は、Cisco ACI ネットワークポリシーモデルのテナント VRF に相当します。Cloud APIC は、ACI テナント VRF をクラウドサイトに展開または拡張する必要がある場合にユーザー VPC を作成します。ユーザー VPC 内で、Cloud APIC はインフラ VPC に接続するように AWS Virtual Private Gateway（VGW）をプロビジョニングするか、他の VPC に接続するように AWS Transit Gateway への VPC 接続を構成して、適切なエンドツーエンド接続を確立します。

図 6 に示した VGW と IPsec トンネルを使用している例の場合、IPsec トンネルは自動的にプロビジョニングされ、インフラ VPC の Cisco CSR 1000V シリーズ ルータとユーザー VPC の AWS VGW との間に確立されます。これにより、インフラ VPC が中継 VPC として機能するようになり、オーバーレイ IPsec トンネルを介してユーザー VPC 間でルートを交換できるようになります。VPC 間のエンドポイント通信と、ユーザー VPC とオンプレミスサイト間のエンドポイント通信は、ユーザー VPC の VGW とインフラ VPC の CSR1000V を経由します。

図 7 に示した AWS Transit Gateway を使用している例の場合、ユーザー VPC 間のエンドポイント通信は AWS Transit Gateway を経由し、ユーザー VPC とオンプレミスサイト間のエンドポイント通信は AWS Transit Gateway とインフラ VPC の Cisco CSR 1000V シリーズのルータを経由します。そのためには、リージョンごとにローカルな Cisco CSR 1000V がインフラ VPC 内に必要になります。Cloud APIC は、テナントごとに Transit Gateway ルートドメインを 1 つ作成します。また、Cloud APIC での VRF とコントラクトの構成に基づいて、各 VPC から AWS Transit Gateway への VPC 接続、VPC ルートテーブル、Transit Gateway ルートドメインを自動的に構成します。VPC の EPG に別の VPC の EPG とのコントラクトがある場合、Cloud APIC がリモート VPC の CIDR ルートを VPC 出力ルートテーブルに自動的に追加します。Cloud APIC は、Transit Gateway のいずれかをネクストホップ先として使用するため、クラウド内の VPC 間トラフィックを適宜 AWS Transit Gateway 経由で転送できます。

一般に、次のような利点があるため、AWS Transit Gateway の使用をお勧めします。

- **パフォーマンスが高い：**AWS Transit Gateway では、VPC 間の他の通信方法よりもはるかに多くの帯域幅を利用できます。たとえば AWS Transit Gateway の場合、VPC 接続ごとに最大 50 Gbps の帯域幅を利用できます。一方、インターネット プロトコル セキュリティ（IPsec）トンネル経由の VPN 接続の場合、帯域幅は 1.5 Gbps に制限されます。
- **シンプルである：**AWS Transit Gateway は、複数の AWS VPC を相互接続するネットワーク中継ハブです。AWS Transit Gateway の導入前は、複数の AWS VPC 間を相互接続する場合、フルメッシュ VPC ピアリングか中継 VPC のいずれかを使用していました。どちらも、運用するのが複雑な設計です。一方 AWS Transit Gateway では、VPC 間の接続が大幅にシンプルになります。
- **コストを抑えられる：**同じ AWS リージョン内の VPC を接続する場合、AWS Transit Gateway を使用すればシスコ クラウド サービス ルータ（CSR）やライセンスは必要ありません。

  オンプレミスサイトや他のクラウドサイトへの接続には、引き続き CSR が必要です。Transit Gateway ピアリングをサポートしない AWS リージョン間にリージョン間接続が必要な場合は、引き続き接続に VGW と CSR を使用する必要があります。

- **拡張性がある：**VPN トンネルを使用した場合、BGP ルートの数が制限されます。一方、AWS Transit Gateway は VPC に直接接続するため BGP を使用する必要がなく、サポートできる接続の数が多くなります。

AWS Transit Gateway ごとに 5,000 の VPC を接続できます。AWS Transit Gateway グループ（Cisco Cloud APIC ソリューションで言うところのハブネットワーク）は、リージョンごとに 5,000 の VPC 接続をサポートします。

複数の AWS リージョンにまたがる ACI クラウドサイト

AWS の ACI クラウドサイトは複数の AWS リージョンにまたがることができます。クラウドサイト全体が同じ Cloud APIC によって管理されますが、各リージョンに独自のインフラ VPC を設置して Cisco CSR 1000V シリーズルータをペアにしたネットワークを実現できます（図 8 と 9 を参照）。VGW で IPsec トンネルを使用する場合は、インフラ VPC を他のリージョンと共有することもできます（図 10 を参照）。ユーザー VPC は、どのリージョンにも展開できます。いずれのユーザー VPC も、IPsec トンネルまたは AWS Transit Gateway を介してすべてのインフラ VPC に接続されています。

VGW で IPsec トンネルを使用する場合、各ユーザー VPC の AWS VGW とインフラ VPC のすべての Cisco CSR 1000V ルータ間に IPsec トンネルが確立されます。これにより、インフラ VPC とユーザー VPC 間にスパインリーフ CLOS アーキテクチャを仮想的に構築してリージョン内およびリージョン間を完全に接続できます。VPC、クラウドルータ、IPsec トンネルのプロビジョニングは、Cloud APIC によって完全に自動化されます。一方、MSO はオンプレミスとクラウドサイト間のオーバーレイネットワーク接続のプロビジョニングを自動化します。

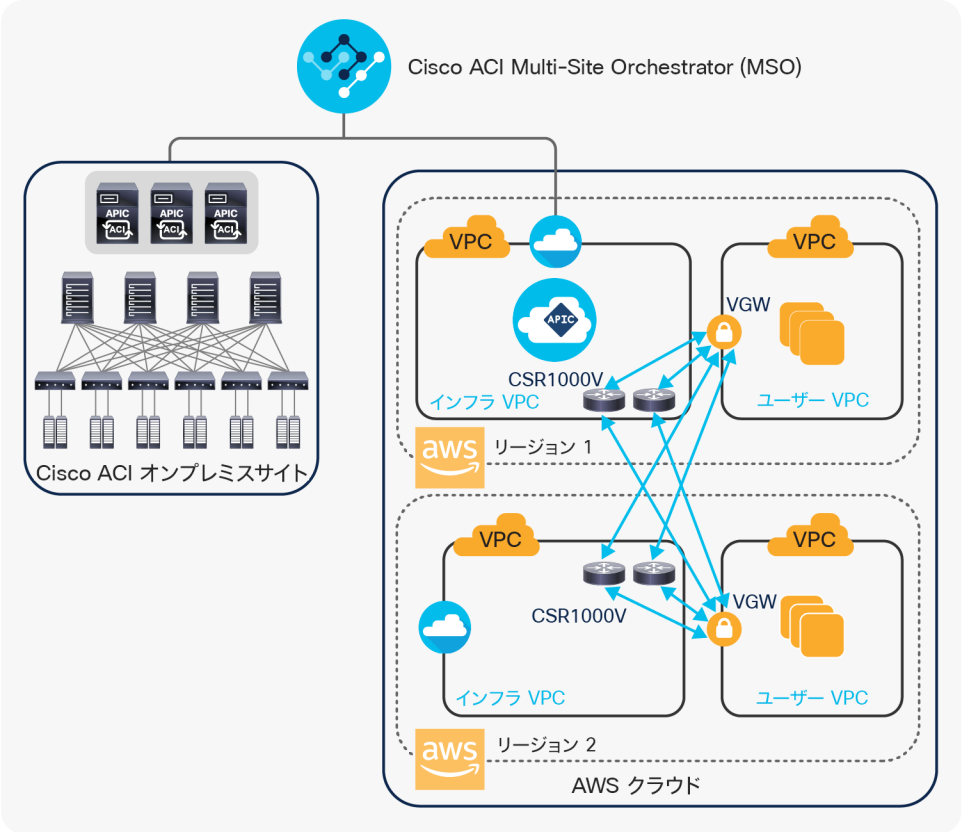


図 8.
リージョン専用のインフラ VPC を設置し、VGW で IPsec トンネルを使用している Cisco Cloud ACI AWS マルチリージョンサイト

AWS Transit Gateway を使用する場合、各ユーザー VPC から AWS Transit Gateway への VPC 接続とルートテーブル構成に加えて、AWS Transit Gateway 間のリージョン間ピアリングも Cloud APIC によって自動的に構成されます。これにより、フルメッシュ VPC ピアリングや中継 VPC を設計することなく、インフラ VPC とユーザー VPC の間にリージョン内接続とリージョン間接続を確立できます。リージョン間接続は、AWS Transit Gateway ピアリングを経由します。リージョン内の VPC 間の通信は、ローカルの AWS Transit Gateway を経由します。

この場合、オンプレミスとクラウドサイト間のトラフィック用に、リージョンごとに Cisco CSR 1000V シリーズルータが必要です。トラフィックは、AWS Transit Gateway とインフラ VPC の CSR 1000V ルータを経由します。VPC のエンドポイントが別のクラウドサイトまたはオンプレミスのエンドポイントと通信する必要がある場合、リモートサイトのプレフィックスルートが Cloud APIC によって VPC 出力ルートテーブルにプログラミングされ、AWS Transit Gateway がネクストホップ先として使用されます。次に、テナントの Transit Gateway ルートドメインが、インフラ VPC 接続を 0.0.0.0/0 サブネットのネクストホップ先として使用します。インフラ VPC のルートテーブルは、インフラ VPC の CSR 1000V ルータの ENI を 0.0.0.0/0 サブネットのネクストホップ先として使用します。そのため、各リージョンのインフラ VPC に CSR 1000V ルータが必要になります。目的の ENI が動作していない場合は、インフラ VPC ルートテーブルが残りの CSR 1000V ルータの ENI をネクストホップ先として自動的に使用します。

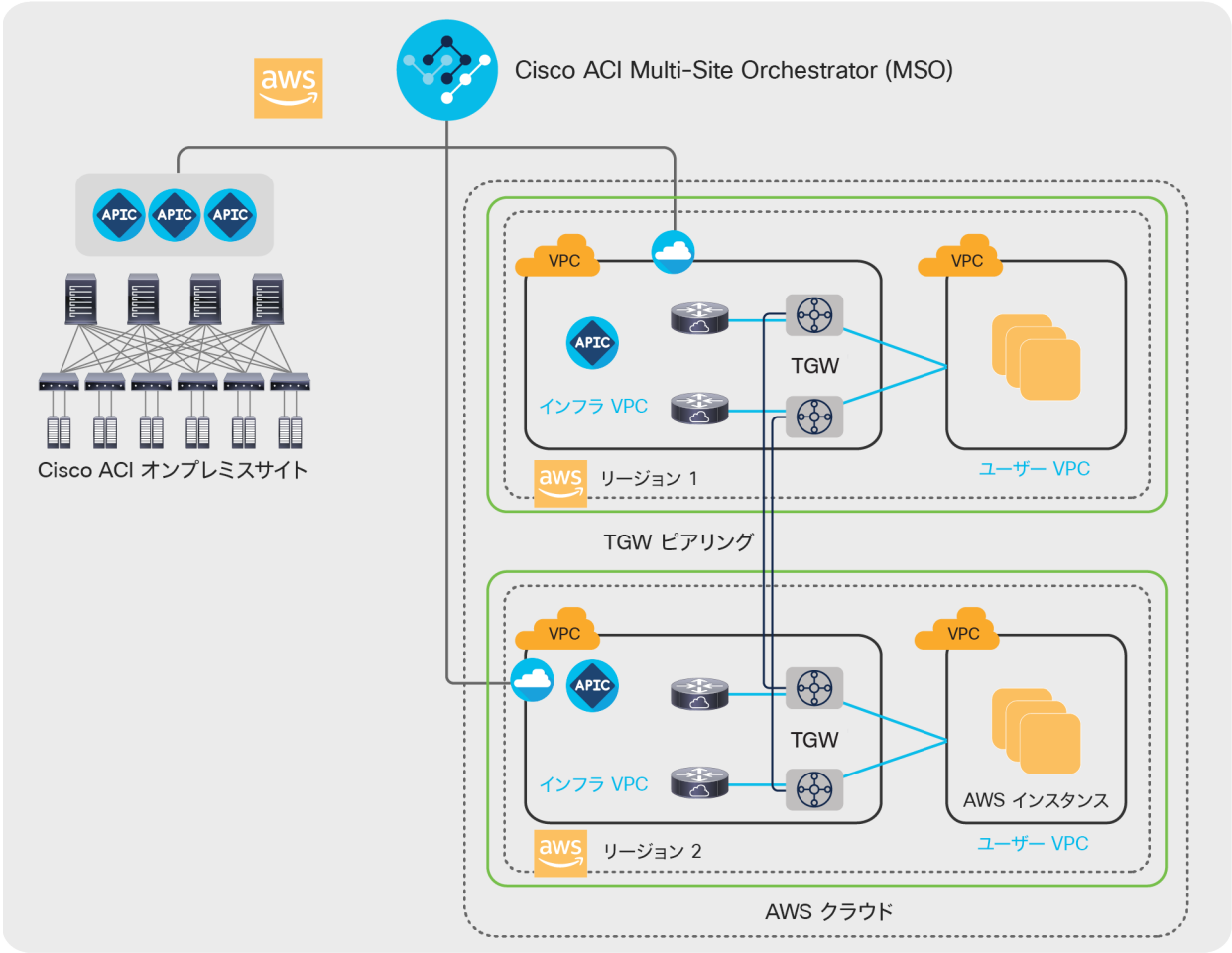


図 9.
リージョン専用のインフラ VPC を設置し、AWS Transit Gateway を使用している Cisco Cloud ACI AWS マルチリージョンサイト

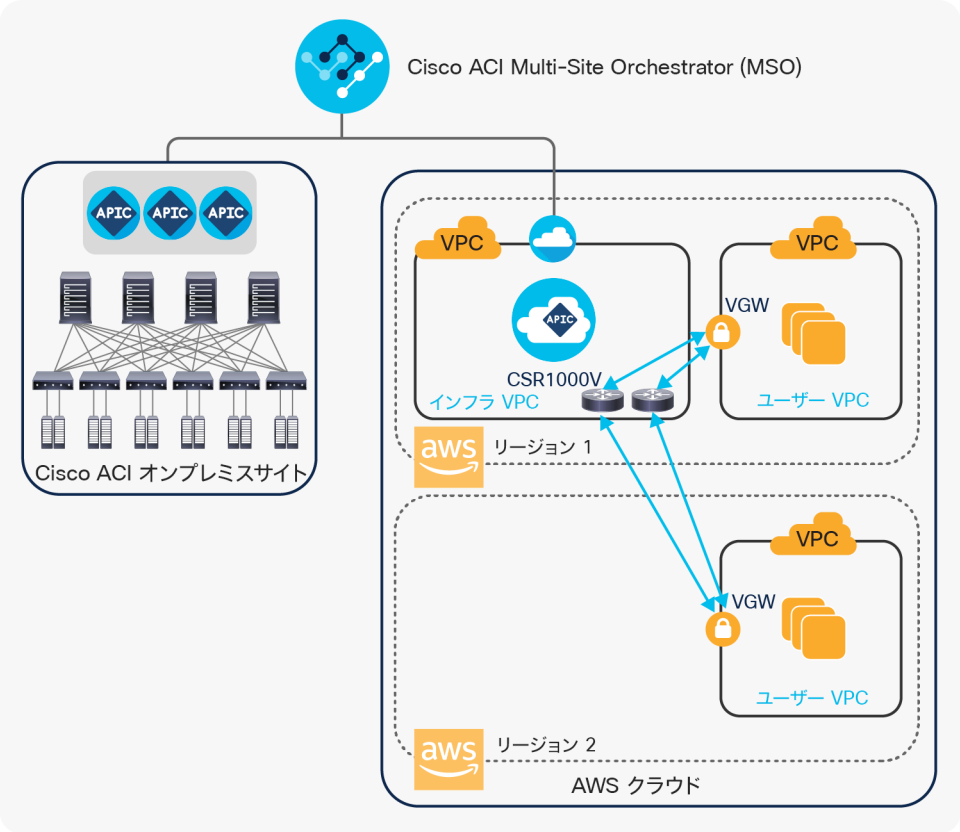


図 10.
共有インフラ VPC を設置し、VGW で IPsec トンネルを使用している Cisco Cloud ACI AWS マルチリージョンサイト

クラウドサイト内のトラフィックフロー

同じ VPC にある 2 つのエンドポイント間のトラフィックは、VPC 内でローカルに転送されます。インフラ VPC を経由する必要はなく、オンプレミスへのヘアピントラフィックも発生しません。別の VPC に存在する 2 つのエンドポイント間のトラフィックは、インフラ VPC または AWS Transit Gateway 内の Cisco CSR 1000V シリーズ ルータを介してルーティングする必要があります。クラウドサイトのエンドポイントとオンプレミスのエンドポイント間のトラフィックは、インフラ VPC の Cisco CSR 1000V シリーズ ルータを介してルーティングする必要があります。

サイト間接続

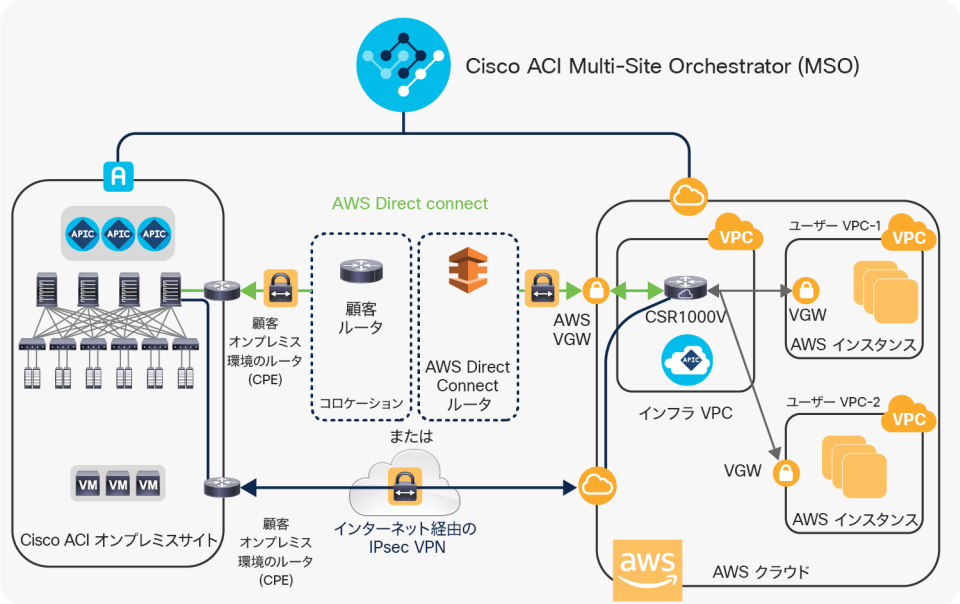
オンプレミスとクラウドサイト間のアンダーレイネットワーク

オンプレミスの Cisco ACI サイトと AWS の ACI クラウドサイトは、両サイト間のアンダーレイ IP ネットワーク上に構築された IPsec トンネルを介して接続されます。ACI クラウドサイトの IPsec トンネルは、インフラ VPC のクラウド Cisco CSR 1000V シリーズ ルータで自動的にプログラミングされます。サイト間 IPsec トンネルの終端となるオンプレミスの IPsec デバイスについては、お客様が管理する必要があります。アンダーレイ IP ネットワークは、インターネットのほか、AWS Direct Connect[4] で構成されているプライベートパスを経由できます。このアン

[4] Cisco ACI リリース 5.1 では、このソリューションは AWS Direct Connect の自動作成と管理には対応していませんが、AWS Direct Connect との連携は可能です。

ダーレイネットワークは、2 つのサイト間のオーバーレイ コントロールプレーンとデータプレーンの IP 到達可能性を提供します。これを図 11 に示します。

VPC 間の接続の場合、図 11 に示すように、ユーザー VPC の VGW または AWS Transit Gateway で構築した IPsec トンネルと、インターネット経由の IPsec VPN を使用した AWS Direct Connect のサイト間接続とを連携させることができます。



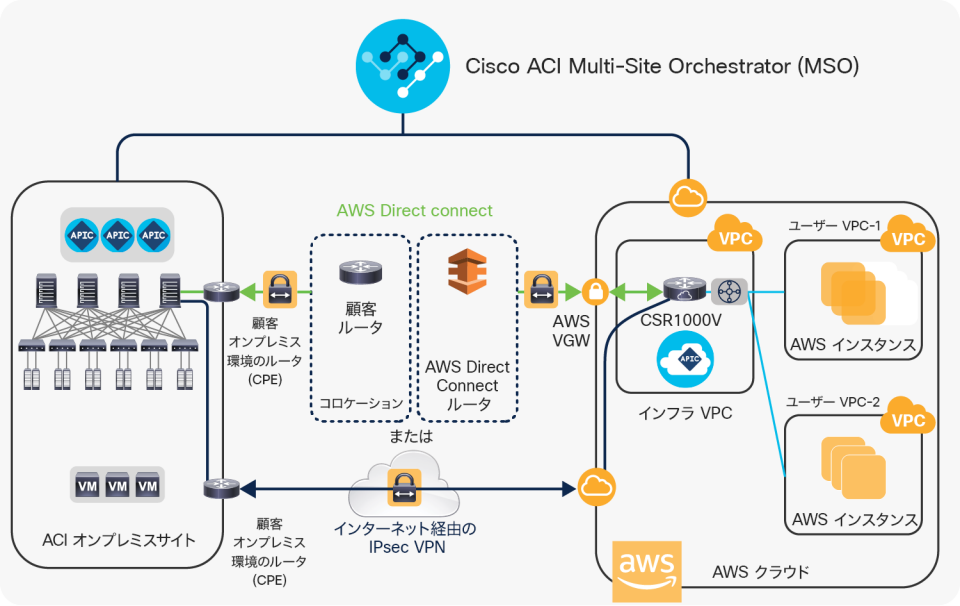


図 11.
オンプレミスとクラウドサイト間のアンダーレイネットワーク

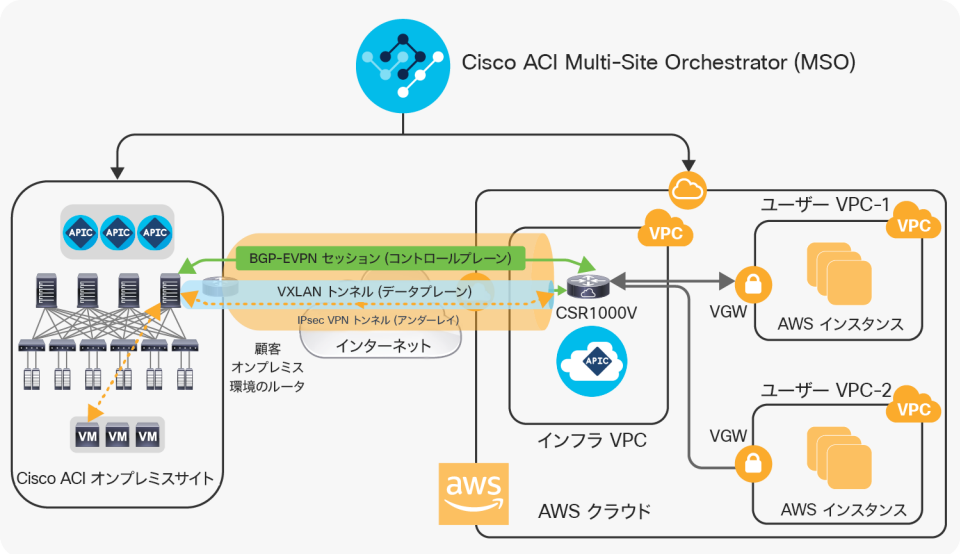
オンプレミスとクラウドサイト間のオーバーレイネットワーク

オンプレミスサイトとクラウドサイト間のオーバーレイネットワークは、コントロールプレーンとして BGP EVPN を実行し、データプレーンとして VXLAN カプセル化とトンネリングを使用します。アーキテクチャの観点から、このオーバーレイネットワークは Cisco ACI GOLF 機能[5]（ファブリック WAN のレイヤー 3 EVPN サービスとも呼ばれます）を使用します。

オンプレミスの Cisco ACI スパインスイッチとクラウドサイトのインフラ VPC の Cisco CSR 1000V シリーズ クラウドルータとの間に、BGP EVPN セッションが確立されます。テナントホストルートとプレフィックスルートは、2 つのサイト間で BGP EVPN ルートタイプ 2（ホスト）およびタイプ 5（プレフィックス）として交換されます。このオーバーレイネットワーク接続のプロビジョニングは、MSO によって自動的に行われます。

図 12 は、この論理/物理アーキテクチャを拡大表示したものです。オンプレミスのスパインがサイト間ネットワークに接続します（ポッド間ネットワークの場合は ISN または IPN と呼ばれます）。続いてその IPN レイヤーがオンプレミスの IPsec ルータに接続し、このルータが AWS インフラ VPC の Cisco CSR 1000V シリーズ ルータへの IPsec トンネルを開始します。ACI スパインスイッチと AWS インフラ VPC の Cisco CSR 1000V シリーズ ルータとの間には、IPN ネットワークと IPsec トンネルを介して MP-BGP EVPN セッションが確立されます。VPC 間接続の場合、ユーザー VPC の VGW または AWS Transit Gateway で構築した IPsec トンネルを使用できます。

IPsec トンネルと VXLAN カプセル化のオーバーヘッドが原因で断片化が発生しないように、場合によっては BGP EVPN コントロールプレーンの ACI コントロールプレーン MTU ポリシーとデータプレーンのエンドポイントで最大伝送ユニット（MTU）サイズを調整する必要があります。このサイズ調整を行わないと、ネットワーク内のデバイスによる断片化が原因で全体のパフォーマンスが低下する可能性があります。たとえば関連するエンドポイントの MTU が 1,300 バイトに調整されているとします。このサイズは、インターネットを経由するために（一般的にインターネットの MTU は 1,500 バイト）、VXLAN から 50 バイト、IPsec オーバーヘッドとして約 100 バイトを追加で考慮したものです。エンドポイントで MTU サイズを調整できない場合、あるいはサイズ調整を推奨されていない場合は、cAPIC から Cisco CSR 1000V シリーズ ルータに TCP の最大セグメントサイズ（MSS）調整を構成する必要があります。この構成オプションは、Cisco Cloud APIC リリース 4.2(4q)、4.2(5n)、5.0(2i) 以降で使用できます。



[5] https://www.cisco.com/c/ja_jp/td/docs/switches/datacenter/aci/apic/sw/2-x/L3_config/b_Cisco_APIC_Layer_3_Configuration_Guide/b_Cisco_APIC_Layer_3_Configuration_Guide_chapter_010010.html

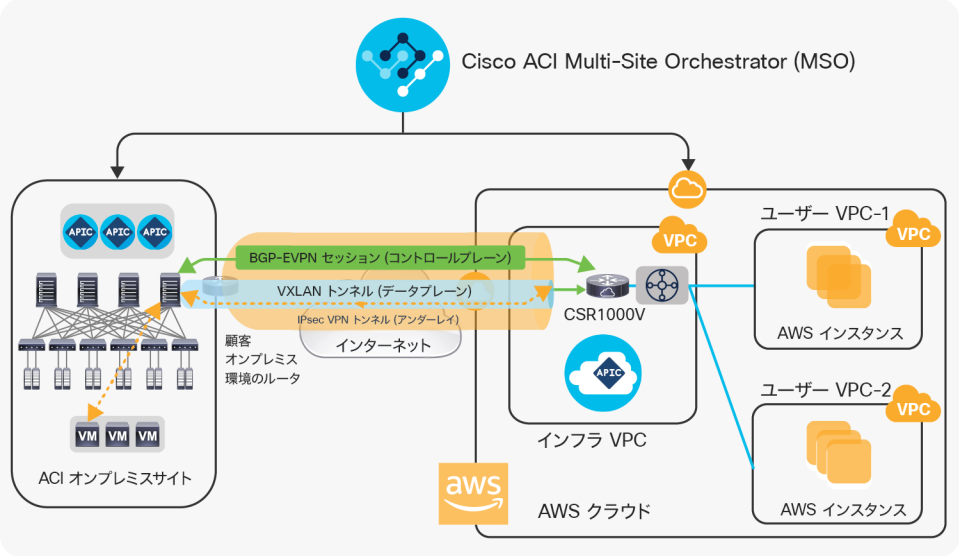


図 12.
オンプレミスとクラウドサイト間のオーバーレイネットワーク

ユースケースのシナリオ

Cisco Cloud ACI では、以下のシナリオを実現できます。

オンプレミスとクラウドサイト全体でのアプリケーションの高可用性

Cisco Cloud ACI では、オンプレミスとクラウドサイトにアプリケーションを展開することで、アプリケーションの高可用性を実現できます。これにより、同じ仮想ルーティングおよび転送ドメイン（VRF）内のハイブリッドクラウド環境全体に多層アプリケーションを展開できます。[6]

オンプレミスの Cisco ACI サイトにアプリケーション層を展開していたお客様は、一貫したポリシーでオンプレミスの層とやり取りできる新たなアプリケーション層をクラウドサイトに追加できるようになりました。

ディザスタリカバリ時にオンプレミスの Cisco ACI サイトと ACI クラウドサイトとの間でアプリケーションをフェールオーバーできます。アクティブ/アクティブモードでアプリケーションを展開することも可能です。このモードの場合、オンプレミスのアプリケーション層とクラウドの層の両方がアクティブになります。2 つのサイトにトラフィックが分散するように、グローバルロードバランサを構成することができます。

たとえばオンプレミスの Cisco ACI データセンターでアプリケーションの Web 層とアプリケーション層（2 つの EPG）が同じ VRF で動作しているとします。その VRF をクラウドサイトに拡張することで、クラウドサイトに Web 層とアプリケーション層を展開して、オンプレミスとクラウドサイト間にアクティブ/アクティブとして構成できます。また、オンプレミスの Web 層とアプリケーション層をアクティブとして展開し、クラウドの層をスタンバイとして機能させて、ディザスタリカバリ時にクラウドの層にフェールオーバーすることも可能です。

[6] 注：オンプレミスサイトとクラウド間にブロードキャストドメインを拡張することはできません。クラウドベンダーは通常、ブロードキャストやマルチキャストを実行しません。ユニキャストの宛先が不明になることもありません。

このような構成は MSO から一元的にオーケストレーションを行うことで実現できます。ハイブリッドクラウド環境にまたがるこうした層の間にコントラクトを構成することが可能です。このポリシーを MSO から両方のサイトに公開するだけで、ワークロード セグメンテーション ポリシーの実装に必要なエンドツーエンドの構造がプログラミングされます。これを図 13 に示します。

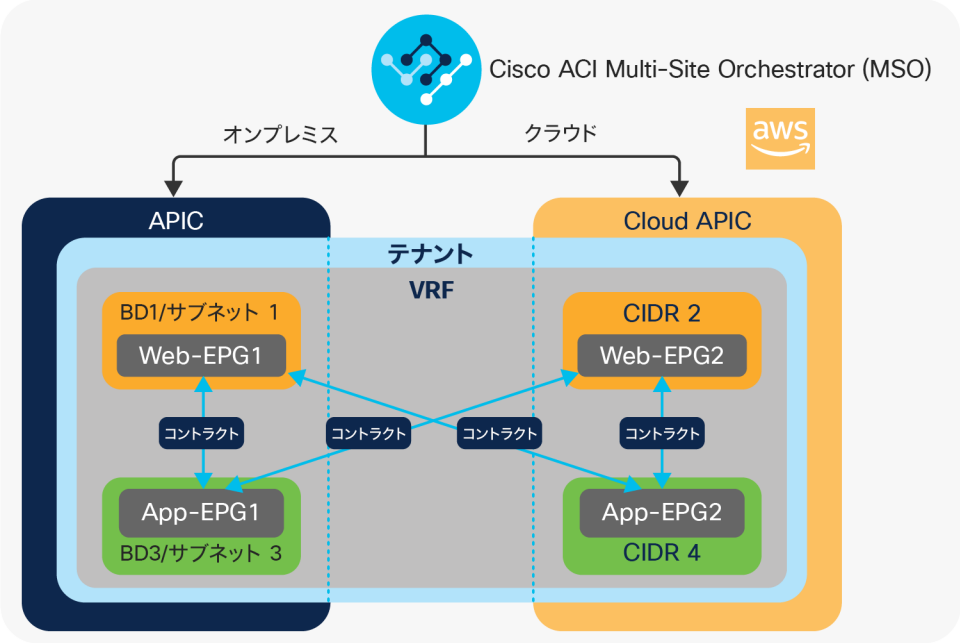


図 13.
オンプレミスの Cisco ACI とクラウドサイトに拡張されたアプリケーションの例

クラウドバースト：アプリケーション層（EPG）を一貫したセグメンテーションでクラウドに拡張

Cisco Cloud ACI では、オンプレミスと AWS のクラウドサイト全体にアプリケーション層を拡張できます。つまり、オンプレミスと AWS サイト全体に ACI EPG を拡張できるということです。これにより、ピーク負荷時にアプリケーションの 1 つの層を AWS クラウドにバーストし、他の層には安全なセグメンテーションポリシーに従ってオンプレミスでアクセスできます。複数の層を AWS 内のクラウドサイトにバーストすることもできます。この場合も、ワークロードの展開先に関係なく、同じレベルのポリシーと一貫したセグメンテーションが維持されます。

MSO から、新しい EPG を作成して後で拡張することも、オンプレミスサイトから既存の EPG をインポートして AWS に拡張することもできます。通常の Cisco ACI マルチサイトと同じように、テンプレートとスキーマを使用して拡張します。それが完了したら、サイトにローカルなプロパティを構成します。このプロパティでは、EPG でメンバーのエンドポイントをどのように分類するかを定義します。

EPG をオンプレミスの ACI サイトに関連付ける場合、EPG を Virtual Machine Manager（VMM）ドメインに関連付けるか、静的ポートまたは VLAN/ポートの組み合わせに関連付けて、オンプレミスのエンドポイントを分類できます。MSO から同じ EPG を AWS のクラウドサイトに関連付けた場合、AWS タグ、AWS IP サブネット、AWS IP アドレス、または AWS リージョンに基づいて EPG メンバーを分類できます。

EPG を拡張するというのは、オンプレミスサイトからクラウドにブロードキャストドメインを拡張するということではなく、さまざまなサブネットを使用してオンプレミスとクラウドのメンバーで EPG を作成できるということにすぎません。複数のエンドポイントを同じ EPG に含めると、その EPG 内を通信フローが自由に流れるようになります。

たとえば、Web 層とアプリケーション層で構成されるアプリケーションをオンプレミスの ACI サイトに展開したとします。ピーク負荷時に、Web 層だけ、または Web 層とアプリケーション層の両方を AWS 内のクラウドサイトにバーストします。これを、Cisco ACI MSO からボタンを数回クリックするだけでシームレスに行うことができます。各層は、オンプレミスワークロードと同じレベルのセキュリティとセグメンテーションで AWS に拡張されます。オンプレミス ACI でいつも行っているように、拡張した Web EPG とオンプレミス EPG あるいはクラウド EPG との間にコントラクトを構成できるようになっています。クラウドバーストはこれ以上なく簡単です。これを図 14 に示します。

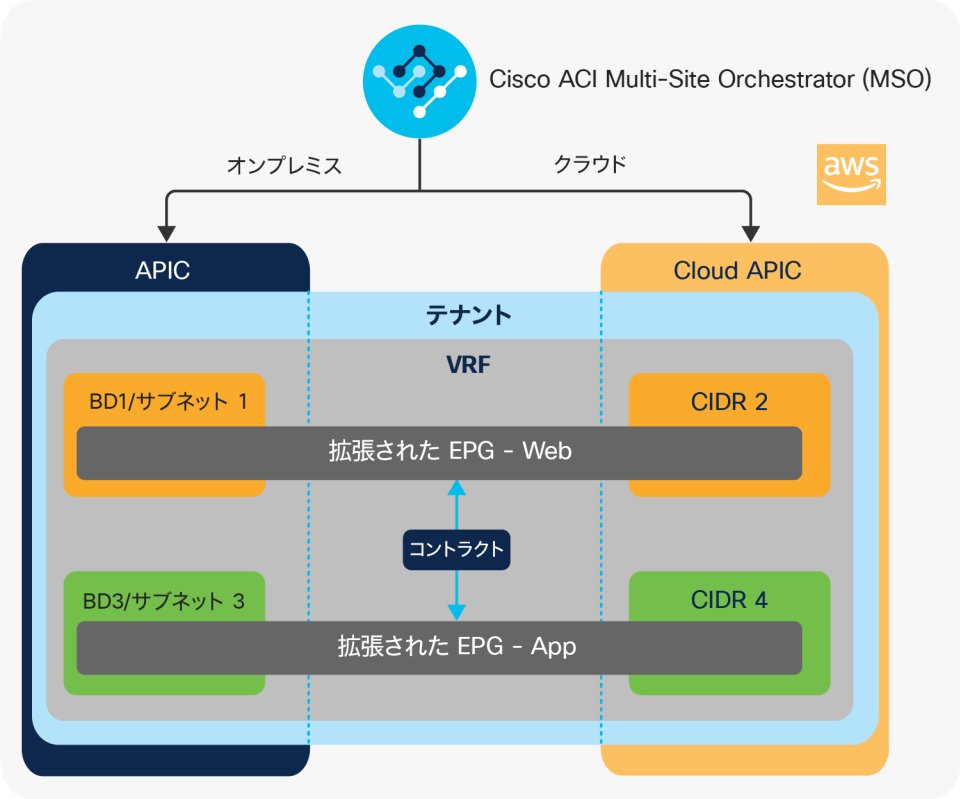


図 14.
サイト全体に拡張された EPG の例

ハイブリッドクラウド全体でのサービスの共有

オンプレミスの ACI サイト内のテナントに展開されている共有サービス（DNS、Active Directory（AD）、その他の認証サービスなど）は、他の Cisco ACI サイトと AWS サイトに展開されている別のテナント内のエンドポイントから安全に利用できます。これにより、オンプレミスの単一のプロバイダーテナントが提供するサービスを、オンプレミスの ACI サイトと AWS のクラウドサイトにまたがる複数のコンシューマテナントから利用できます*。

そのため、クラウドに新しいアプリケーションを展開し、オンプレミスのブラウンフィールド ネットワークから共有サービスを利用することが簡単になります。クラウドにホストされているアプリケーション向けに共有サービスを再展開する必要はありません。

* Cisco ACI リリース 5.1 では、テナント間共有サービスはサポートされていません。たとえば EPG が別々のテナントにある場合、クラウドのプロバイダー EPG とオンプレミスのコンシューマ EPG との間にコントラクトを展開することはできません。

たとえば、テナント 1（オンプレミスの ACI サイト）に DNS サーバーが展開されているとします。クラウドサイト（AWS のテナント 1）に Web-EPG が展開されている場合、Web-EPG 内のワークロードは、オンプレミスの ACI サイトから DNS-EPG と Web-EPG との間にある VRF 間コントラクトを介してオンプレミスの DNS 共有サービスにアクセスできます。これを図 15 に示します。

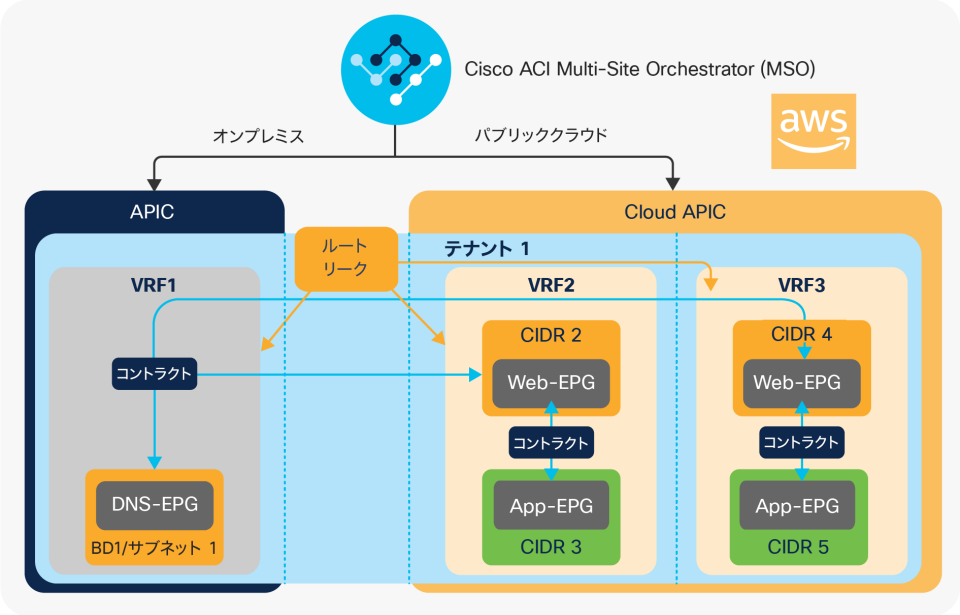


図 15.
サイト間共有サービスの例

クラウドまたはオンプレミスを介したインターネットへの外部接続

AWS クラウドのワークロードがインターネットに外部接続できるように構成するには、次の 2 つの方法があります。

1. Cloud L3Out：AWS に展開したワークロードに対して、クラウドローカルのインターネット接続（Cisco ACI で言うところの L3Out）を定義できます。そのためには、MSO で AWS のクラウドサイトに対してクラウド外部 EPG を構成します。クラウド外部 EPG は、インターネットゲートウェイ（IGW）を作成して、AWS サイト内のすべての VPC に接続します。これで、適切なルートが VPC ルートテーブルにプログラミングされます。
2. オンプレミス L3Out：お使いの環境によっては、AWS の VPC からオンプレミスサイトにすべてのトラフィックを送信し、オンプレミスのファイアウォール/IDS/IPS で検査したうえで、トラフィックがインターネットに出入りするようにする必要があります。これは、オンプレミス L3Out をトラフィックのインターネット出口として定義し、コントラクトを介してクラウドエンドポイントにその EPG を関連付けることでも行えます。

クラウドに展開したワークロードの外部ネットワーク接続オプションは、完全に制御できます。検査のためにトラフィックをリダイレクトすることも可能です。検査には、Cisco ACI サービスグラフを使用してオンプレミスに展開した各種サービスを利用できます。ここに挙げたことは、いずれも単一のポリシーで行えます。Cisco ACI Multi-Site Orchestrator によってエンドツーエンド接続の自動化とオーケストレーションが可能になるため、運用ワークフローが大幅にシンプルになります。

たとえば、AWS 環境にクラウド L3Out を構成すると（図 16 を参照）、各 AWS の VPC に AWS インターネットゲートウェイ（IGW）が接続され、定義されたポリシーに基づいて VPC の Amazon EC2 インスタンスがインターネットと直接通信できるようになります。

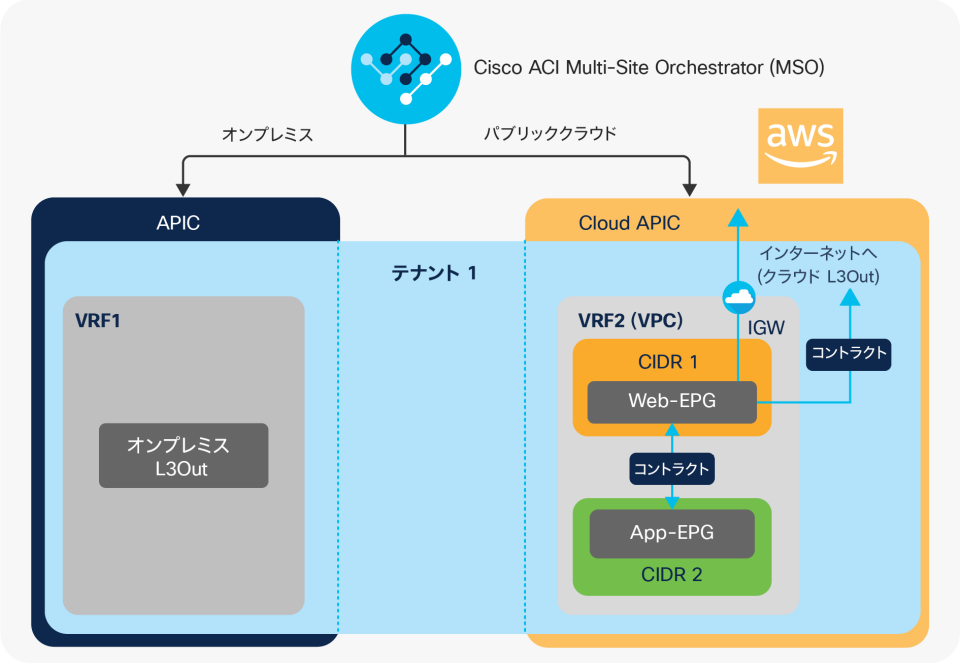


図 16.
クラウド L3Out の例

オンプレミスの Cisco ACI L3Out を定義し（図 17 を参照）、その L3Out を使用するようにクラウドインスタンスを設定すると、Amazon EC2 インスタンスのすべてのトラフィックが VPN トンネル経由で Cisco CSR 1000V シリーズ ルータに到達します。その後、IPsec トンネル上で動作する VXLAN トンネル経由でオンプレミスに送信されます。AWS インターネットゲートウェイを直接使用するのではなく、オンプレミスの Cisco ACI L3Out を介してトラフィックを送り出すことができます。

トラフィックがオンプレミスの Cisco ACI サイトに到達したら、Cisco ACI のサービスチェーンオプションを使用してそのトラフィックをさまざまな検査にかけてから、トラフィックをインターネットに送り出すことができます。

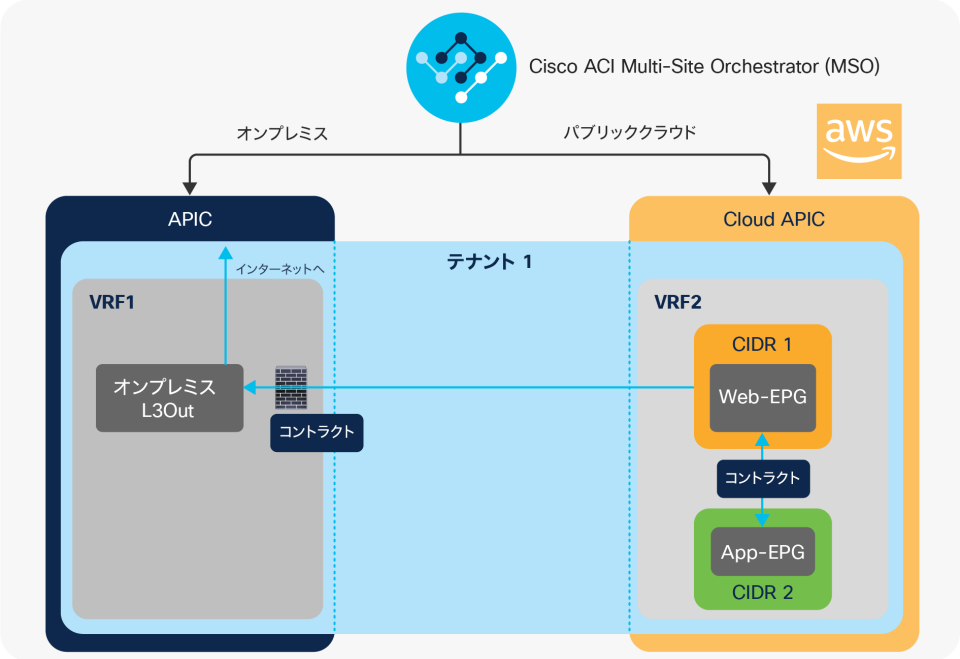


図 17.
クラウドエンドポイントのオンプレミス L3Out の例

クラウドネイティブおよびオンプレミスのサービス

Cisco Cloud ACI では、簡単な操作で AWS のクラウドネイティブのサービスまたはオンプレミスのサービスを安全に利用できます。

1. AWS Application Load Balancer：サービスグラフというオンプレミス ACI とよく似た概念を使用して、AWS Application Load Balancer（ALB）などのクラウドネイティブサービスをアプリケーションスタックとシームレスに統合できます。これは、MSO から完全に構成できます。Cloud APIC が VPC に ALB をエンドツーエンドで自動的に展開および構成して、特定のエンドポイントグループ内のエンドポイントに関連付けます。
2. オンプレミスサービス：オンプレミスと AWS サイトにまたがるアプリケーション層の場合、オンプレミスサービス（ロードバランサやファイアウォールなど）をシームレスに導入できます。そのためには、MSO から ACI サービスグラフを構成します。

たとえば、オンプレミスに展開したデータベース層とハイブリッドクラウド環境全体に広がる Web 層との間に East-West ファイアウォールが必要になったとします。図 18 に示すように、MSO から ACI サービスグラフを使用すると、これを非常に簡単に構成できます。データベース層と Web 層との間のトラフィックは、Web 層のエンドポイントがハイブリッドクラウドのどこに配置されているかに関係なく、常にこのファイアウォールを通過します。

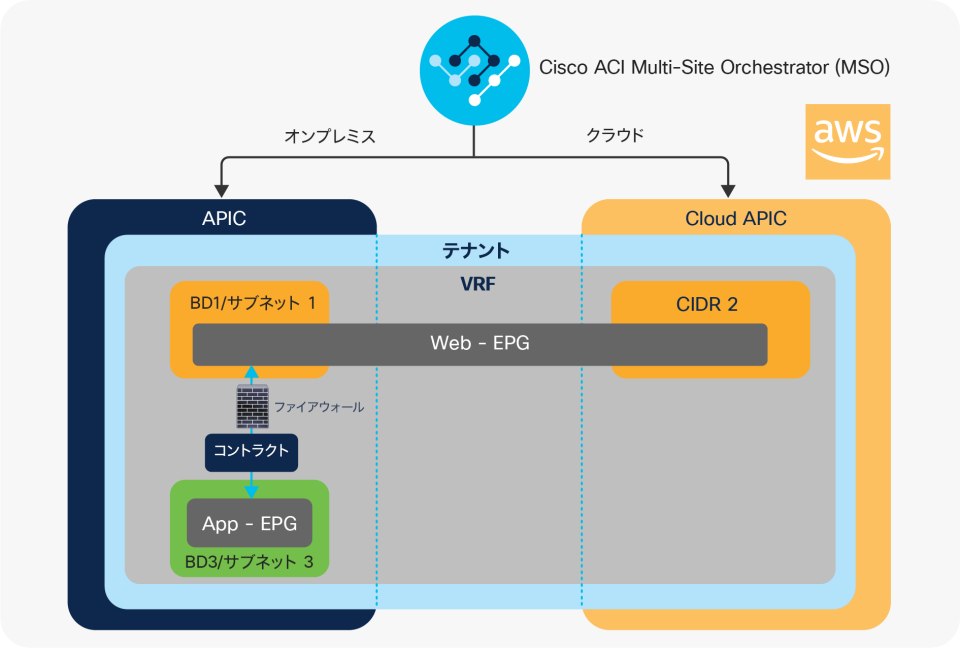


図 18.
拡張されたアプリケーション層のオンプレミス サービス チェーン

ソリューションを展開する方法

Cisco Cloud APIC とインフラ VPC の展開

Cisco Cloud APIC 向けの AWS AMI イメージは、AWS マーケットプレイスで入手できます。本ホワイトペーパーの執筆時点では、BYOL モデルのライセンスを使用できます。他のオプションについては、注文ガイドを参照してください。

Cisco Cloud ACI を展開するための最初のステップは、インフラ VPC を構成し、AWS で Cisco Cloud APIC を起動することです。こうしたステップの実行には、シスコが提供する AWS CloudFormation テンプレートを使用します。これにより、スタックと呼ばれる自動化ワークフローを作成して、一連のステップを自動的に実行できます。

CloudFormation では、JSON または YAML テンプレートを使用して自動化ワークフローを記述します。シスコは、Cisco Cloud ACI 統合の構成に必要なステップを実行するための CloudFormation テンプレートを提供しています。CloudFormation テンプレートは AWS マーケットプレイスで入手し、そこから実行できます。図 19 に示すように、シスコの公開 Web サイトからダウンロードして使用し、CloudFormation スタックを開始することも可能です。このスタックを開始すると、テンプレートに定義されている必須パラメータの入力を求められます。入力が完了すると、ワークフローに定義されたタスクが実行されます。AWS に Cisco Cloud APIC を展開する手順の詳細については、https://www.cisco.com/c/m/en_us/products/data-center/software-demos/aci/cloud-apic-deployment-walkthrough.html のウォークスルーをご覧ください。

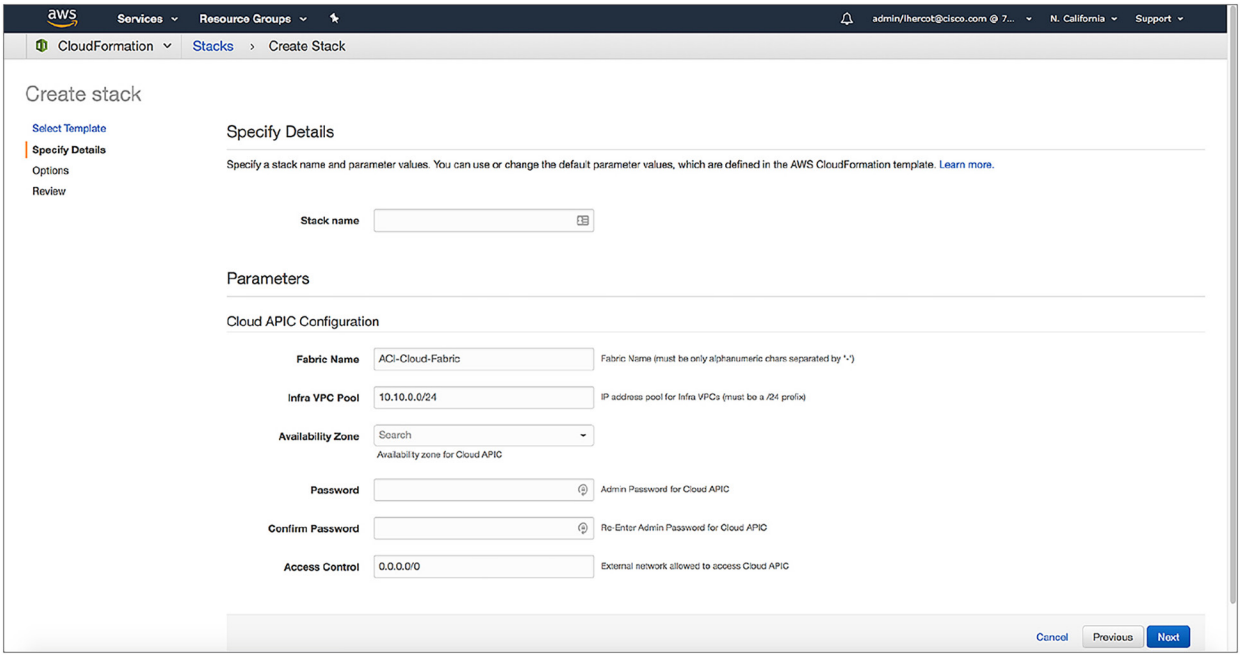


図 19.
AWS で Cisco Cloud APIC を起動するための CloudFormation スタックの作成

CloudFormation テンプレートが正常に展開されると、Cisco Cloud APIC に Web UI と API を介してアクセスできるようになります。図 18 に示すように、Cisco Cloud APIC のパブリック IP アドレスを確認するには、CloudFormation テンプレート出力を表示するか、Cloud APIC Amazon EC2 インスタンスに割り当てられている Elastic IP アドレスを調べます。Cisco Cloud APIC の UI に接続し、スタートアップウィザードに従ってインストールを完了します。

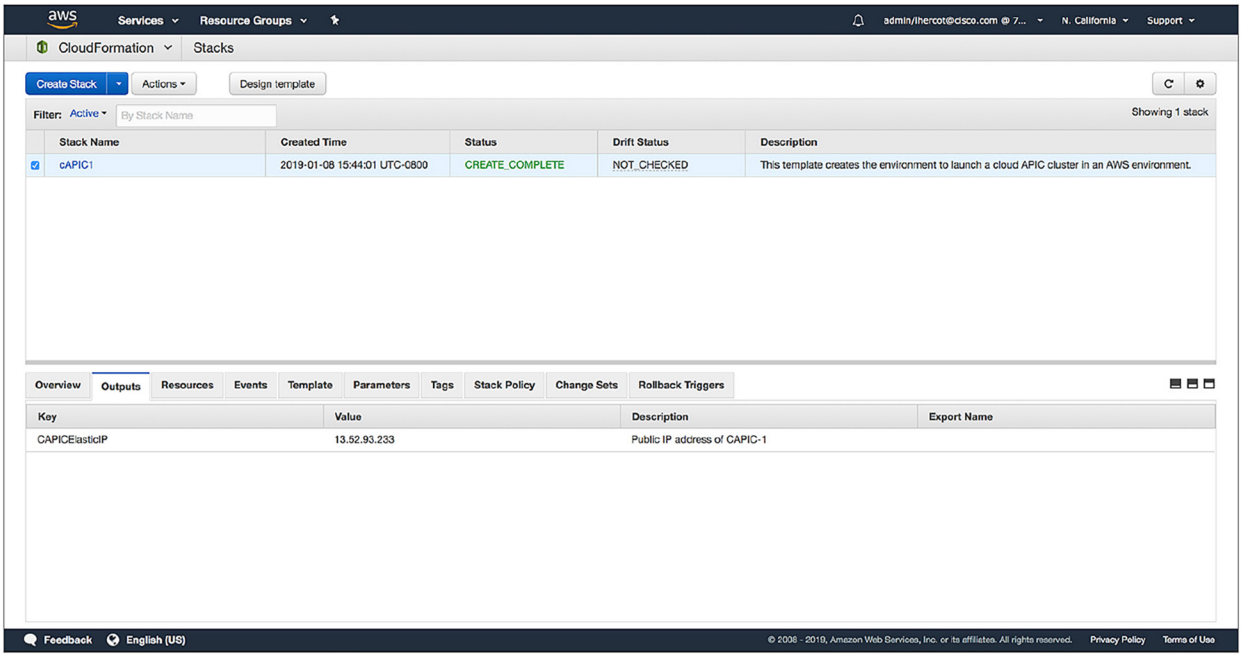


図 20.
Cisco Cloud APIC パブリック IP アドレスが記載された CloudFormation テンプレート出力

Cisco Cloud APIC の初回セットアップウィザード

Cisco Cloud APIC の UI に初めて接続すると、初回セットアップウィザード（図 21 を参照）が自動的に開始されます。このウィザードでは、Cisco Cloud APIC で必要とされる設定の一部（DNS、TEP プール、管理対象のリージョン、IPsec 接続オプションなど）を構成できます。初回セットアップウィザードの最後に、Cisco Cloud APIC が完全に動作するために必要な AWS インフラストラクチャ（Cisco CSR 1000V シリーズ ルータのペアなど）が構成されます。AWS インフラストラクチャのプロビジョニングは完全に自動化されており、Cisco Cloud APIC によって実行されます。このステップの後、AWS に Cisco ACI ポリシーを展開できるようになります。

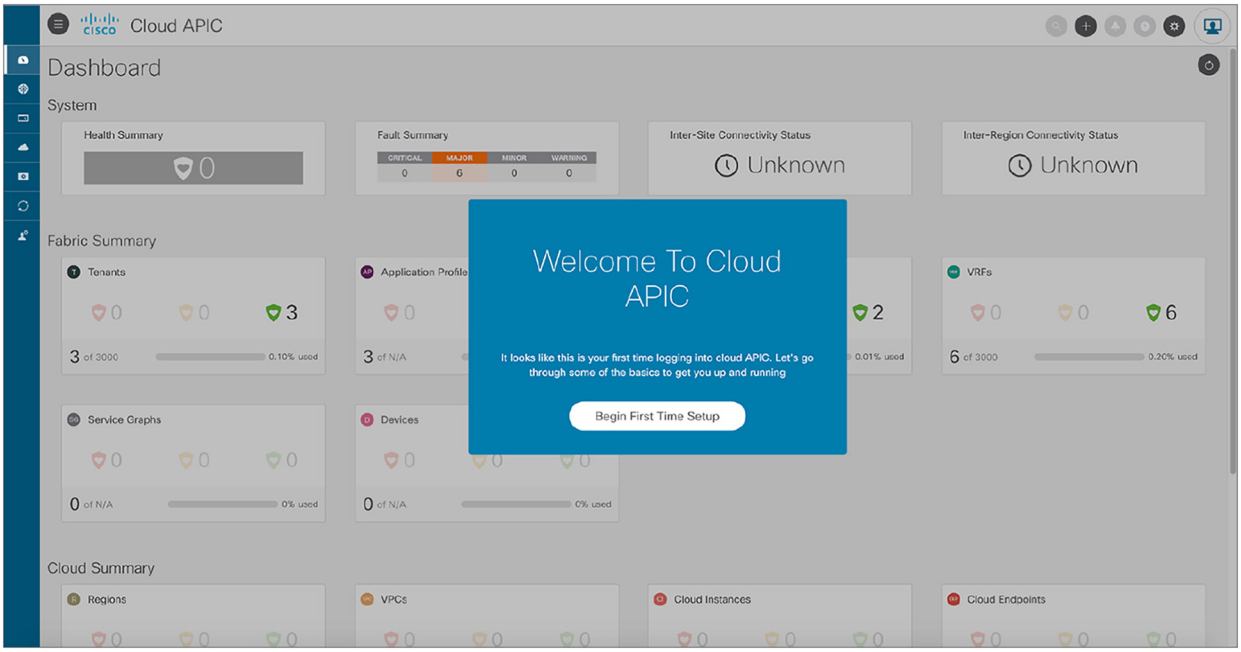


図 21.
Cisco Cloud APIC の初回セットアップウィザード

MSO での Cisco ACI クラウドサイトの登録

Cisco Cloud APIC のそれぞれが Cisco ACI サイトを表します。ポリシーをサイト全体に適用する場合、Cisco ACI は Cisco ACI Multi-Site Orchestrator（MSO）を使用します。図 22 に示すように、MSO で Cisco Cloud APIC を登録すると、それが新しいサイトとして表示され、AWS に既存または新規のスキーマを展開できるようになります。MSO により、サイト固有の必須オプション（サブネットと EPG メンバーの分類条件など、サイトごとに異なるオプション）を確実に指定できます。

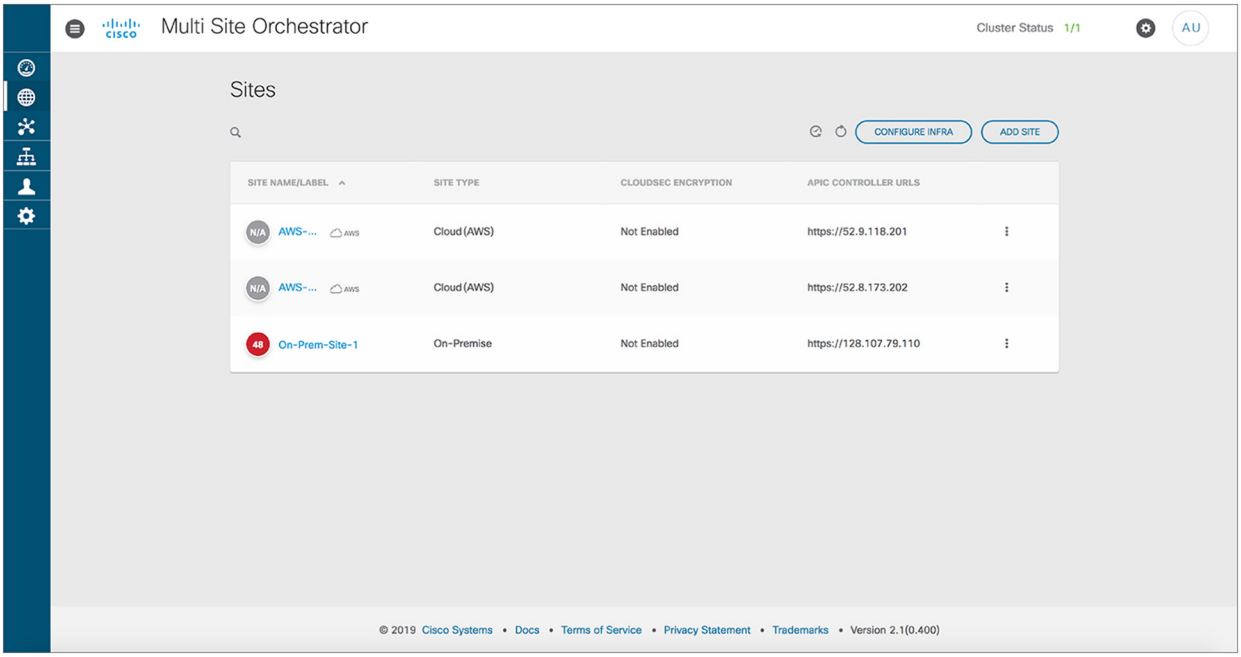


図 22.
MSO での Cisco ACI クラウドサイトの登録

Cisco Cloud APIC では、Cisco ACI オブジェクトモデル表現を使用して、AWS 上にネットワークを構築できます。バックエンドで、Cisco Cloud APIC は Cisco ACI オブジェクトを AWS ネイティブの構造に変換します。つまり、Cisco Cloud ACI は AWS ネットワーキング仕様に準拠しています。とはいえ Cisco ACI でよく使用される仕様とは若干異なるため、以下で詳しく説明します。

図 23 に示すように、AWS ではサブネットは VPC の可用性ゾーン（AZ）にバインドされています。VPC 自体はリージョンにバインドされています。

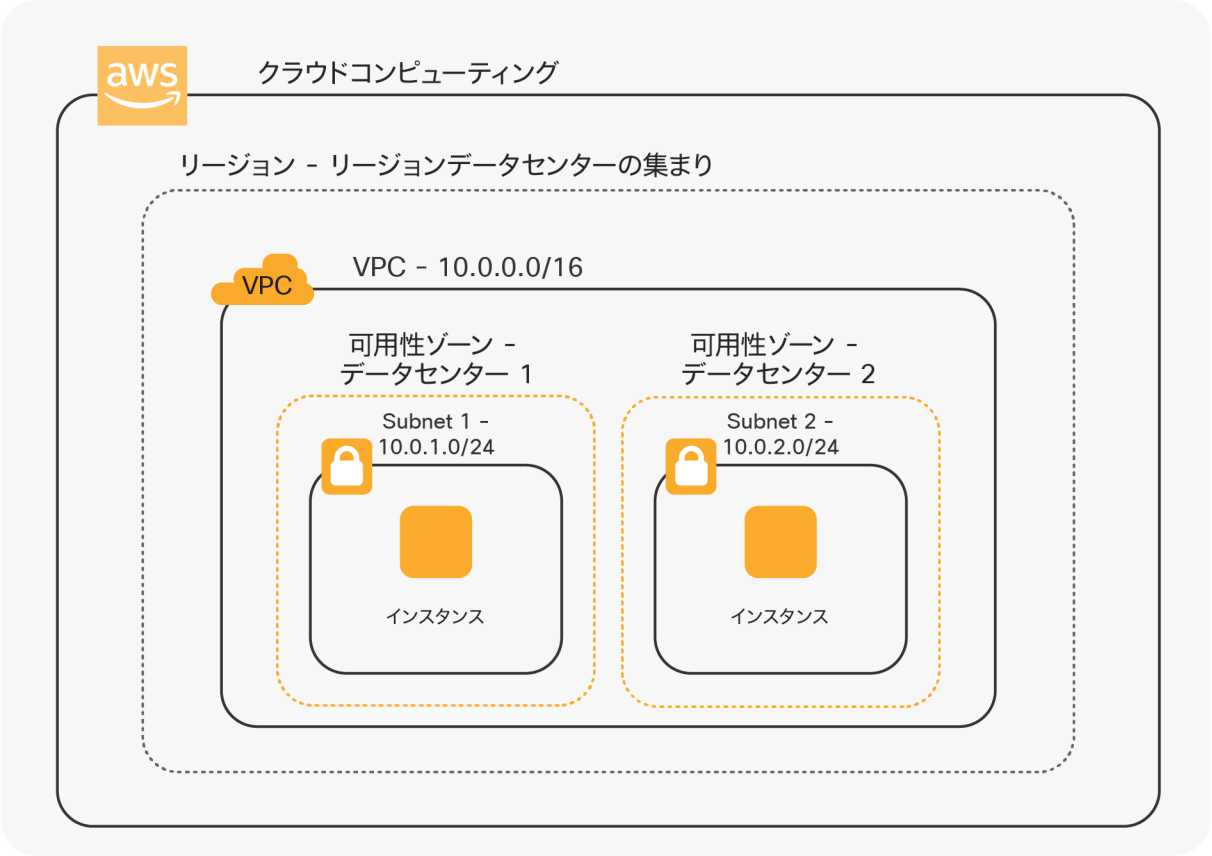


図 23.
AWS ネイティブのネットワーク構造

つまり、トラフィックは AZ 間、VPC 間、またはリージョン間でルーティングされます。VPC 間、またはオンプレミスサイトから AWS の VPC に L2 を拡張するという概念はありません。この設計理念を尊重して、Cisco Cloud ACI は L3 のみを使用してオンプレミスネットワークを拡張します。

Cisco Cloud APIC ではこのほか、Cisco ACI ポリシーの表現に使用されている AWS ネイティブの構造をまとめて参照することもできます。そのため、ネットワーク管理者は徐々に AWS ネットワーク構造の理解を深めていくことができます。以下の図 24 は、Cloud APIC の UI からネイティブのクラウドリソースを表示している様子を示しています。例では、クラウドサイトにプロビジョニングした AWS の VPC を表示しています。

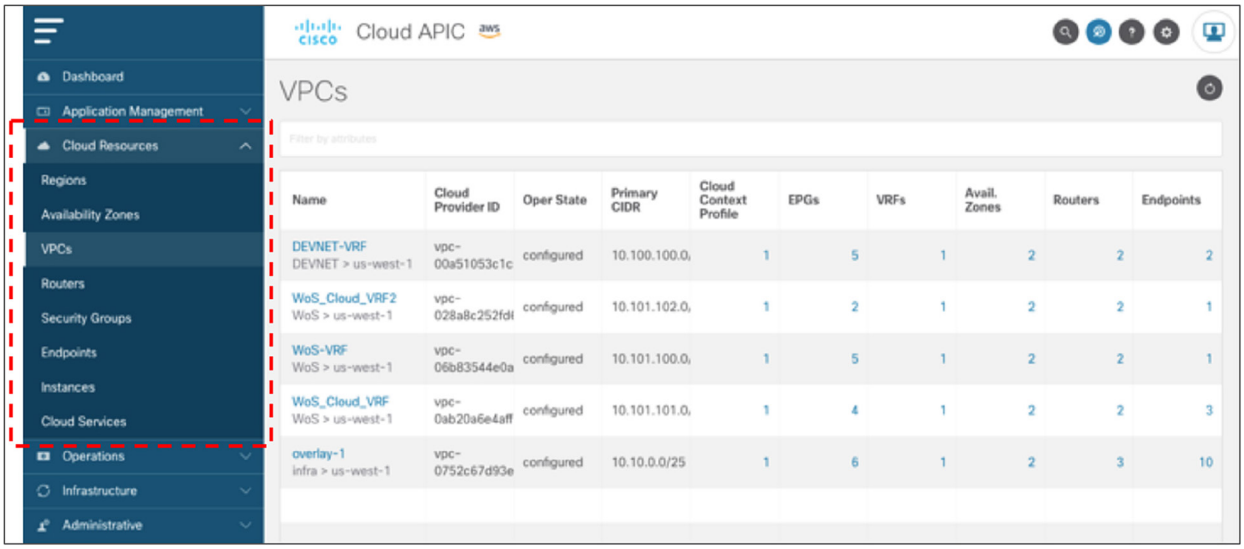


図 24.
Cloud APIC の UI からネイティブのクラウドリソースを表示

ハイブリッドシナリオでの多層アプリケーションの展開

このセッションでは、例として従来の 3 層アプリケーションを使用しています。アプリケーションは、データベース（DB）層、アプリケーション層、Web 層の 3 層で構成されています。Cisco Cloud ACI 統合を使用して、これをオンプレミスのデータセンターと AWS クラウド全体に展開するには、MSO でこのポリシーを表すスキーマを構成する必要があります。図 25 に示すように、少なくとも 1 つの VRF、1 つのアプリケーション プロファイル、3 つの EPG（アプリケーションの層ごとに 1 つの EPG）が含まれている必要があり、各層の間にはコントラクトも必要です。たとえばアプリケーション層とデータベース層は、オンプレミスと AWS の Web 層に展開できます。あるいは、このセットの並びを任意に変えることも可能です。前述のように、オンプレミスのデータセンターとクラウドとの間で 1 つ以上の EPG を拡張するオプションなどがあります。

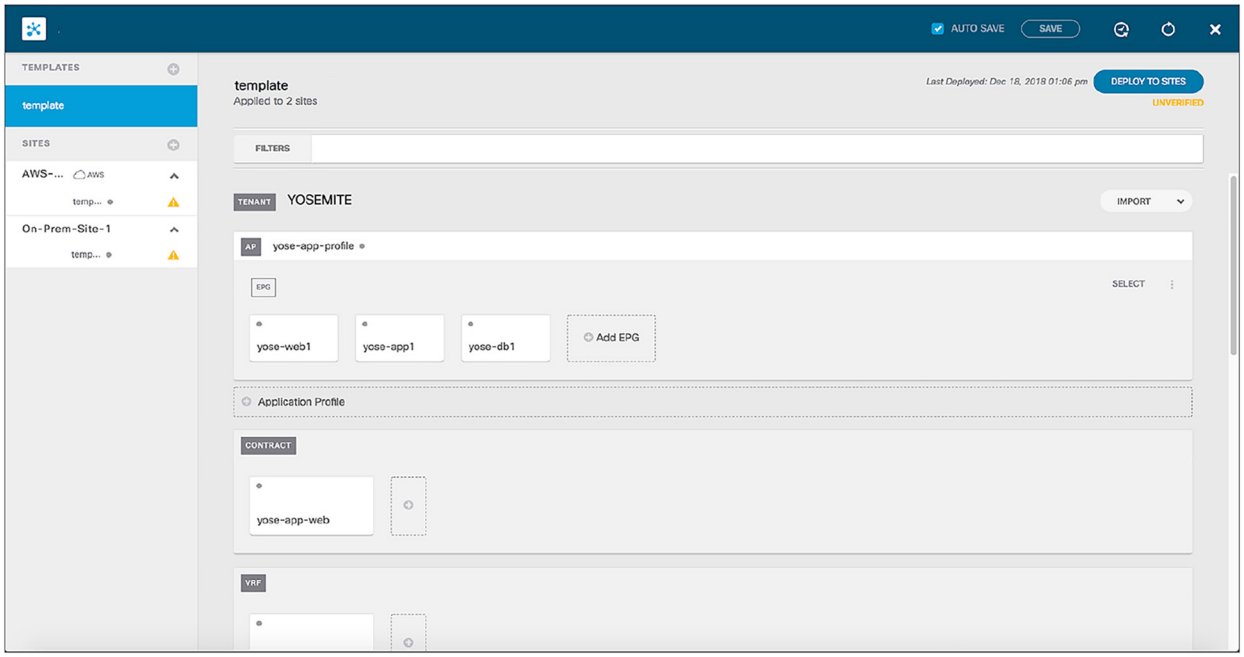


図 25.
MSO での 3 層アプリケーションスキーマ

構成したスキーマは、オンプレミスサイトと Cisco Cloud ACI サイトに関連付けることができます。関連付けを行ったら、AWS の VRF に使用するサブネットを定義します。Cisco Cloud APIC モデルでは、サブネットが VRF に関連付けられます。AWS では VRF が VPC にマップされ、サブネットが VPC の可用性ゾーン（AZ）にマップされるからです。つまり、AWS クラウドにのみ存在する Web EPG ごとにサブネットを定義する必要があります。また、クラウドインスタンスが Web EPG に加わるためのメンバー条件も定義します。図 26 に示すように、MSO スキーマに問題がなく、サイト固有の必須の構成ステップが完了したら、MSO から展開ボタンを 1 回クリックするだけで両方の Cisco ACI サイトに構成を展開できます。

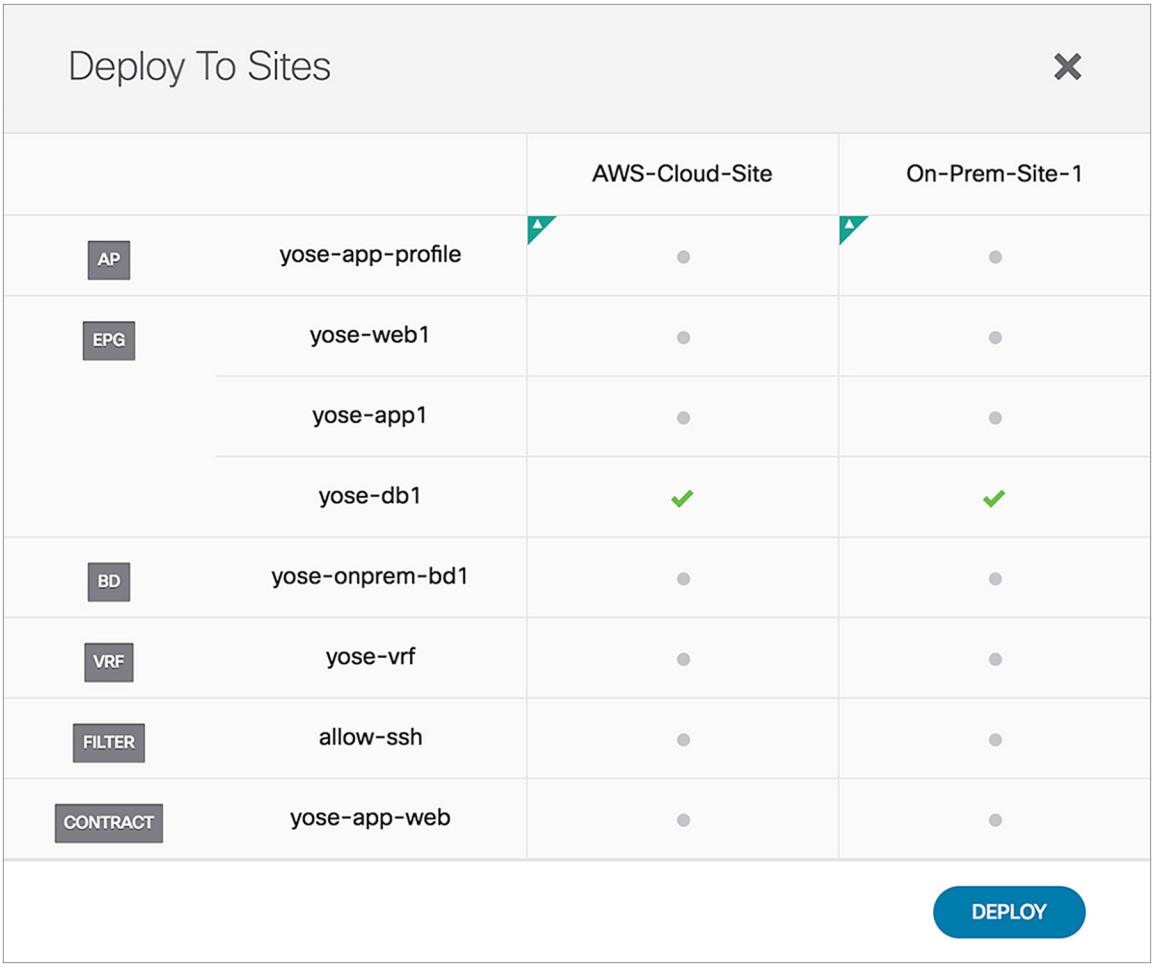


図 26.
オンプレミスと AWS 内のクラウドサイトへのアプリケーションの展開

図 27 に示すように、Cisco Cloud ACI を使用すると、AWS に存在する App EPG と Web EPG とが通信できるように、AWS クラウドとオンプレミス ACI が適切に構成されます。

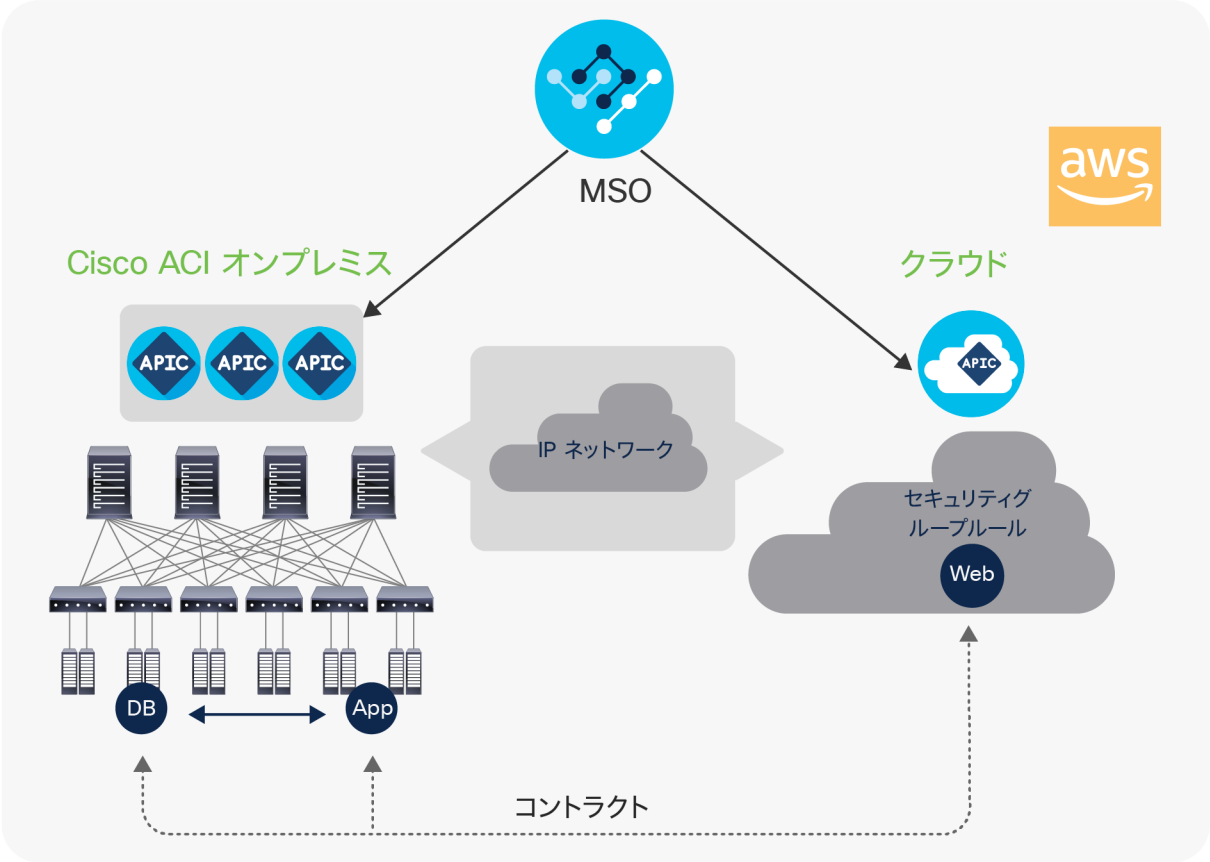


図 27.
オンプレミスと AWS 内のクラウドサイトに展開された 3 層アプリケーション

ニーズに応じて AWS に新しい Web インスタンスを展開できるようになっています。

まとめ

Cisco ACI リリース 4.1 で提供される Cisco Cloud ACI の新機能により、ネットワーク管理者は絶えず進化し続けるビジネス要件に合わせてすばやくインフラストラクチャを調整できます。極めて簡単な操作でハイブリッドクラウド環境の構成と Day 2 運用が行えるようになっており、IT の俊敏性が最大限に高まります。Cisco Cloud ACI では、オンプレミスとパブリッククラウドサイトにまたがる複雑なネットワークトポロジとセキュリティポリシーを設計できます。ネットワーク接続とワークロード セグメンテーション ポリシーのクロスサイト オーケストレーションは、Cisco ACI Multi-Site Orchestrator が Cisco Cloud APIC およびオンプレミスの APIC と連携して動作することで実現されます。

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

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
cisco.com/jp

0322-2023-000-X