概要

Cisco ACI ファブリックをパブリック クラウドに拡張する

Cisco Application Centric Infrastructure （ACI）プライベート クラウドを所有しているお客様は、パブリック クラウドでワークロードの一部を実行することがあります。ただし、ワークロードをパブリック クラウドに移行するには、別のインターフェイスを操作し、接続を設定してセキュリティ ポリシーを定義するさまざまな方法を学習する必要があります。これらの課題に対処すると、運用コストが増加し、一貫性が失われる可能性があります。

Cisco ACI は、Cisco Cloud Network Controller を使用して、マルチサイト ファブリックを Amazon Web Services（AWS）、Microsoft Azure、および Google Cloud パブリック クラウドに拡張できます。

Cisco Cloud Network Controller とは

Cisco Cloud Network Controller は、クラウドベース仮想マシン（VM）で展開可能な Cisco APIC のソフトウェア コンポーネントです。Cisco Cloud Network Controller は、次の機能を提供します。

- Amazon AWS、Microsoft Azure、または Google Cloud パブリック クラウドと対話するための既存の Cisco APIC インターフェイスと同様のインターフェイスを提供します。
- クラウド接続の展開と設定を自動化します。
- クラウド ルータ コントロール プレーンを設定します。

- オンプレミス Cisco ACI ファブリックとクラウドサイト間のデータ パスを設定します。
- Cisco ACI ポリシーをクラウド ネイティブ ポリシーに変換します。
- エンドポイントを検出します。

Cisco ACI Extension からパブリック クラウドへのメリットを享受するには

Cisco Cloud Network Controller は、パブリック クラウドへの Cisco ACI 拡張の重要な部分です。Cisco Cloud APICは、オンプレミスのデータセンターまたはパブリック クラウドの両方またはいずれかに展開されたワークロードに対して一貫したポリシー、セキュリティ、および分析を提供します。

パブリック クラウドへの Cisco ACI 拡張は、オンプレミスのデータセンターとパブリック クラウド間の自動接続を提供し、プロビジョニングとモニタリングを容易にします。また、オンプレミスのデータセンターとパブリック クラウド間、またはクラウド サイト間でポリシーを管理、監視、およびトラブルシューティングするための単一のポイントを提供します。

Azureガバメントサポート

Cisco Cloud Network Controller は、オンプレミスからクラウドへの接続（ハイブリッド クラウドおよびハイブリッド マルチクラウド）、クラウド サイトからクラウドへの接続（マルチクラウド）、およびシングルクラウドの構成（クラウドファースト）について、Azure Government をサポートしています。

Cisco Cloud Network Controller は次の Azure Government リージョンをサポートします。

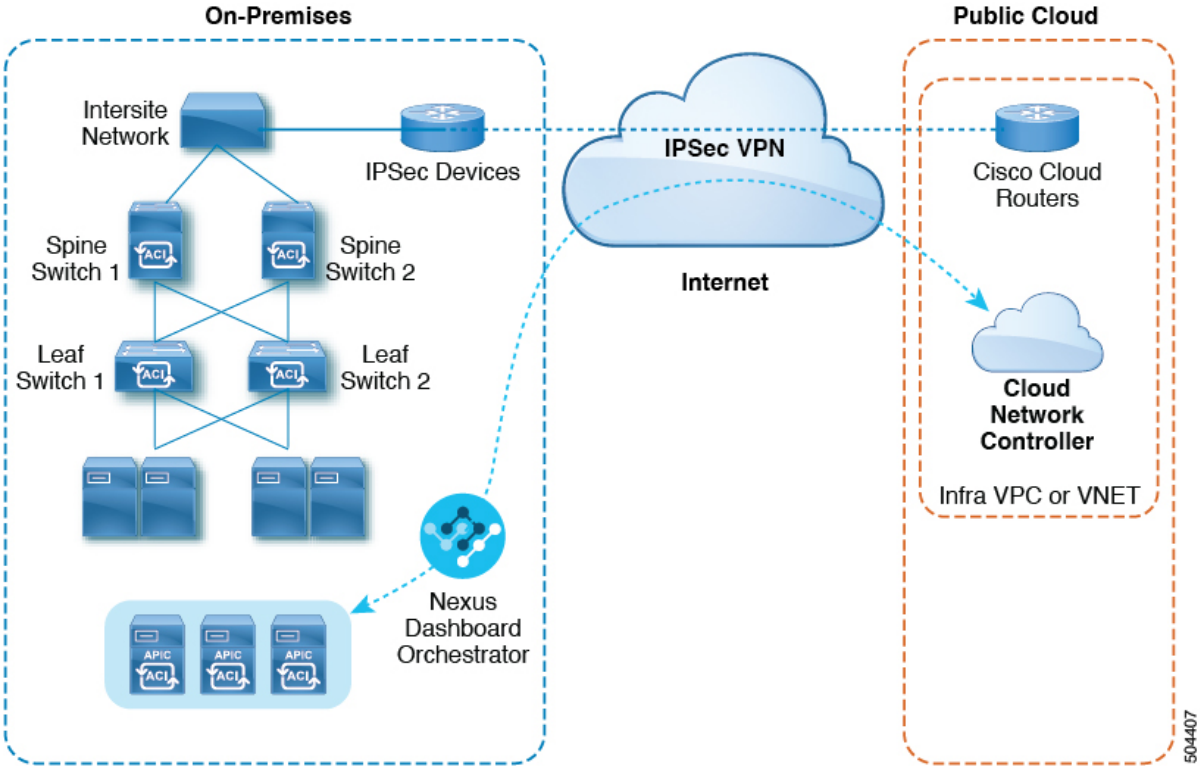
- US DoD セントラル
- US DoD 東部
- 米国政府、アリゾナ州
- 米国政府、テキサス州
- 米国政府、バージニア州

Cisco ACI ファブリックをパブリック クラウドに拡張するためのコンポーネント

マルチサイト ファブリックを Microsoft Azure パブリック クラウドに拡張するには、それぞれに固有のロールを持つ複数のコンポーネントが必要です。

次の図は Cisco Cloud Network Controller のアーキテクチャの内容を示しています。

図 *1 : Cisco Cloud Network Controller* のアーキテクチャ



オンプレミスデータセンターコンポーネント

Cisco ACI ファブリックおよび Cisco APIC

Cisco ACI では、アプリケーション要件でネットワークを定義できます。このアーキテクチャにより、アプリケーションの導入ライフサイクル全体がシンプルになって最適化され、短時間で完了します。Cisco Application Policy Infrastructure Controller（APIC）の主要コンポーネントです。Cisco ACIこれにより、アプリケーションは、ネットワーク、コンピューティング、およびストレージ機能を含むセキュアで共有された高性能リソース プールに直接接続できます。

マルチサイト およびマルチサイト オーケストレータ/Cisco Nexus Dashboard Orchestrator

マルチサイトは、プログラムを利用してアプリケーションがネットワーク要件を定義することを可能にするアーキテクチャです。このアーキテクチャにより、アプリケーションの展開が簡素化・最適化され、そして促進されます。Cisco Cloud Network Controller を使用してファブリックをパブリッククラウドに拡張するには、マルチサイトをインストールする必要があります。

詳細については、Cisco.com のマルチサイトのマニュアルおよびこのガイドのマルチサイトの構成情報を参照してください。

Cisco Nexus Dashboard Orchestrator （NDO）は、複数のファブリック（サイト）で複数の Cisco Application Policy Infrastructure Controller（APIC）のインスタンスを管理します。

Cisco ACI ファブリックをパブリック クラウドに拡張すると、Cisco Nexus Dashboard Orchestrator はオンプレミスのデータセンターとパブリック クラウド間の接続を作成します。マルチサイト

を使用して、オンプレミスのデータセンターとパブリック クラウド全体にテナントを作成します。

（注） オンプレミス Cisco ACI ファブリックを設定する必要があります。ファブリック外部接続ポリシーを作成し、マルチサイトに必要なオーバーレイTEPおよびその他の情報を定義します。また、マルチサイト アーキテクチャにオンプレミス Cisco ACI ファブリックを追加する必要があります。Cisco.com で『*Cisco ACI* マルチサイト構成ガイド』を参照してください。

詳細については、Cisco.comのマルチサイトのマニュアルおよびこのガイドのマルチサイトの構成情報を参照してください。

IP セキュリティ（IPSec）ルータ

Microsoft Azureのオンプレミスサイトとクラウドサイトの間でIPsec接続を確立するには、インターネットプロトコルセキュリティ（IPsec）対応のルータが必要です。

Azureパブリッククラウドコンポーネント

Cisco Cloud Network Controller

Cisco Cloud Network Controller は次のアクションを実行します。

- パブリッククラウド上のサイトを定義し、クラウドインフラ仮想ネットワーク（VNET）をプロビジョニングし、すべてのリージョンで CCR を管理します。
- パブリッククラウドでポリシーモデルをレンダリングし、クラウドの健全性を管理します。Cisco ACI

詳細については、*Cisco Cloud Network Controller* リリース ノート を参照してください。

CCR

CCR は、仮想およびクラウド環境で包括的な WAN ゲートウェイとネットワークサービスを提供します。CCR により、企業はWANをプロバイダーがホストするクラウドに拡張できます。Cisco Cloud Network Controller ソリューションには 2 つの CCR が必要です。

Cisco Cloud Network Controller は、クラウド サービス ルータとして **Cisco Catalyst 8000V** を使用します。この CCR の詳細については、Cisco CSR 8000v のマニュアル を参照してください。

Microsoft Azure パブリック クラウド

Microsoft Azureは、コンピューティング、ストレージ、ネットワーク、データベースなどのオンデマンドサービスを提供するクラウドベースのプラットフォームです。Azureのサブスクライバは、ワークロードを実行できる仮想コンピュータにインターネット経由でアクセスできます。

詳細については、Microsoft Azure の Web サイトのマニュアルを参照してください。

オンプレミスデータセンターとパブリッククラウド間の接続

IPsec VPN

パブリックにルーティング可能なIPアドレスを含み、Microsoft Azure接続に十分な帯域幅を持つ、IPsecルータからのVPNとのインターネット接続が必要です。

管理接続

オンプレミスのデータ センターの Nexus Dashboard Orchestrator と Microsoft Azure パブリック クラウドの Cisco Cloud Network Controller の間に管理接続が必要です。

サポートされているクラウドコンピューティング プラットフォームと接続オプション

Cisco Nexus Dashboard Orchestrator を使用して、次のコンポーネント間の接続を確立することガできます。

- オンプレミスからクラウドへの接続：
  - 次のパブリッククラウドサイトの接続：
    - オンプレミス Cisco ACI および Amazon AWS パブリック クラウド サイト
    - オンプレミスおよびMicrosoft Azureパブリッククラウドサイト Cisco ACI
    - オンプレミス Cisco ACI と Google Cloud パブリック クラウド サイト
  - オンプレミスからシングルクラウドサイトへの接続（ハイブリッドクラウド）
  - オンプレミスから複数のクラウドサイトへの接続（ハイブリッドマルチクラウド）
- クラウドサイト間接続（マルチクラウド）：
  - Amazon AWSパブリッククラウドサイト間（Amazon AWSパブリッククラウドサイトからAmazon AWSパブリッククラウドサイト）
  - Microsoft Azureパブリッククラウドサイト間（Microsoft Azureパブリッククラウドサイトから Microsoft Azureパブリッククラウドサイト）
  - Google Cloud パブリック クラウド サイト間（Google Cloud パブリック クラウド サイトから Google Cloud パブリック クラウド サイトへ）
  - Amazon AWS 、Microsoft Azure、および Google Cloud パブリック クラウド サイト間

さらに、シングルクラウド設定（Cloud First）もサポートされます。

ポリシーの用語

Cisco Cloud Network Controller の主要な機能は、 Cisco Application Centric Infrastructure（ACI）ポリシーのパブリック クラウドのネイティブ コンストラクトへの変換です。

Cisco ACI と Microsoft Azure 間のポリシー マッピング

次の表に、Microsoft Azure のポリシー用語と同等の用語を示します。Cisco ACI

Cisco ACI	Azure
テナント（リージョン、VRF）	リソース グループ
Virtual Routing and Forwarding（VRF）	仮想ネットワーク
BD サブネット	サブネット
契約、フィルタ	アウトバウンドルール、インバウンドルール
EP から EPG へのマッピング	アプリケーション セキュリティ グループ（ASG）、ネットワーク セキュリティ グループ（NSG）
エンドポイント	VM インスタンスのネットワーク アダプタ

テナント、ID、およびサブスクリプションについて

AzureにはActive Directory構造があります。最上位レベルの構造は組織であり、その下にディレクトリ（Azureテナントとも呼ばれます）があります。ディレクトリ内には、1つ以上のAzureサブスクリプションを設定できます。

特定のAzureコンポーネント間の関係は次のとおりです。

テナントサブスクリプションリソースグループリソース ＞＞＞

それぞれの説明は次のとおりです。

- 1つのテナントは複数のサブスクリプションを持つことができますが、各サブスクリプションは1つのテナントにのみ属することができます。
- 1つのサブスクリプションに複数のリソースグループを含めることができますが、各リソースグループは1つのサブスクリプションにのみ属することができます。
- 1つのリソースグループは複数のリソースを持つことができますが、各リソースは1つのサブスクリプションにのみ属することができます。

次のセクションでは、これらのコンポーネントについて詳しく説明します。

- Azure と Cisco Cloud Network Controller コンポーネントのマッピング （7 ページ）
- Azureサブスクリプションについて （7 ページ）
- テナントとアイデンティティについて （7 ページ）

Azure と Cisco Cloud Network Controller コンポーネントのマッピング

Cisco Cloud Network Controller では、各 Azure リソース グループは 1 つの Cisco Cloud Network Controller テナントにマッピングされます。1 つの Cisco Cloud Network Controller テナントには複数の Azure リソース グループがあります。

特定の Cisco Cloud Network Controller コンポーネント間の関係は次の通りです。

テナントVRFリージョン ＞＞

Cisco Cloud Network Controller で VRF を作成すると、新しいリソース グループも Azure に作成されます。

Azureサブスクリプションについて

Azureサブスクリプションは、Azureクラウドサービスの支払いに使用されます。Azureサブスクリプションには、Azure Active Directory（Azure AD）との信頼関係があり、Azure ADを使用してユーザ、サービス、およびデバイスを認証します。複数のサブスクリプションは同じAzure ADを信頼できますが、各サブスクリプションは1つのAzure ADのみを信頼できます。

Azureでは、同じAzureサブスクリプションIDを複数のACIファブリックテナントに使用できます。これは、1つのAzureサブスクリプションを使用してインフラテナントを設定し、同じサブスクリプションで複数のユーザテナントを設定できることを意味します。ACIテナントはAzureサブスクリプションに関連付けられています。

テナントとアイデンティティについて

Azure および Cisco Cloud Network Controller で使用できるさまざまなタイプのテナントとアイデンティティを次に示します。

（注） マネージドアイデンティティとサービス プリンシパルの両方が、インフラ テナントとユーザ テナントのアクセス タイプとしてサポートされます。

マネージドアイデンティティ

マネージドアイデンティティは、Azure AD認証をサポートするリソースに接続するときに使用するアプリケーションのアイデンティティを提供します。アプリケーションは管理対象IDを使用してAzure ADトークンを取得できます。たとえば、開発者が安全な方法でクレデンシャルを保存したり、ストレージアカウントにアクセスしたりするために、アプリケーションでマネージドアイデンティティを使用してAzure KeyVaultなどのリソースにアクセスできます。
https://docs.microsoft.com/en-us/azure/key-vault/general/overview

管理対象IDを使用する利点は次のとおりです。

- クレデンシャルにはアクセスできないため、クレデンシャルを管理する必要はありません。
- マネージドIDを使用して、独自のアプリケーションを含むAzure AD認証をサポートする任意のリソースを認証できます。

- マネージドIDは追加コストなしで使用できます。

Azureの管理対象アイデンティティの詳細については、以下を参照してください。

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

[マネージド アイデンティティ（managed identity）]を使用して Cisco Cloud Network Controller のテナントを構成する場合、Azure ポータルおよび Cisco Cloud Network Contrller の次の構成を作成します。

1. Azureポータルで、仮想マシンのロール割り当てを追加します。このオプションは、Azure サブスクリプションが（同じ組織の）同じAzureディレクトリにある場合に使用します。

（注） Azureサブスクリプションが異なるディレクトリにあり、マネージドIDを使用してテナントを設定する場合は、Azureコンソールに移動し、各サブスクリプションをクリックして同じAzureディレクトリの下にサブスクリプションを移動できます。これは、（異なるサブスクリプションを含む）ディレクトリが同じ親組織の子である場合にのみ実行できます。

   仮想マシンのAzureにロール割り当てを追加する手順については、を参照してください。仮想マシンへのロール割り当ての追加

2. Cisco Cloud ネットワーク コントローラでは、Cisco Cloud ネットワーク コントローラでテナントを構成するとき **[独自のマネージド アイデンティティの作成（Create Your Own Managed Identity）]** オプションを選択します。このオプションは、テナントの設定 の手順に従って Cisco Cloud Network Controller GUI で構成します。

サービス プリンシパル（Service Principal）

Azureサービスプリンシパルは、Azureリソースにアクセスするためのアプリケーション、ホステッドサービス、および自動化ツールで使用するために作成されたIDです。異なるサブスクリプションでテナントを設定する場合は、サービスプリンシパルIDを使用します。サブスクリプションが同じ組織内の異なる Azure ディレクトリ（Azure テナント）にあるか、サブスクリプションが異なる組織にある可能性があります。

[サービス プリンシパル（service principal）]を使用して Cisco Cloud Network Controller でテナントを構成する場合は、Azure ポータルと Cisco Cloud Network Controller で次の構成を行います。

1. Azureポータルで、**アプリケーション**のロール割り当てを追加します。この場合、クラウドリソースは特定のアプリケーションを介して管理されます。

   アプリにAzureのロール割り当てを追加する手順については、を参照してください。ロール割り当ての追加

2. Cisco Cloud Network Controller では、Cisco Cloud Network Controller でテナントを構成するとき **[サービス プリンシパル（service principal）]** オプションを選択します。このページに入力するサブスクリプションは、同じ組織内の異なるAzureディレクトリ（Azureテナント）に配置することも、異なる組織に配置することもできます。このオプションは、テナントの設定 の手順に従って Cisco Cloud Network Controller GUI で構成します。

共有テナント

Azureサブスクリプションを上記の2つの方法のいずれかにすでに関連付けており、そのサブスクリプションにさらにテナントを作成する場合は、このオプションを選択します。

[共有テナント（shared tenant）]を使用して Cisco Cloud Network Controller でテナントを構成する場合は、Azure ポータルと Cisco Cloud Network Controller で次の構成を行います。

1. 上記の2つの方法のいずれかでAzureサブスクリプションをすでに関連付けているため、Azureで共有テナント専用の設定を行う必要はありません。共有テナントでは、既存のサブスクリプションにさらにテナントを作成します。
2. Cisco Cloud Network Controller では、Cisco Cloud Network Controller でテナントを構成するとき **[共有（Shared）]** オプションを選択します。このオプションは、テナントの設定 の手順に従って Cisco Cloud Network Controller GUI で構成します。

Cisco Cloud Network Controller のライセンシング

ここでは、Cisco Cloud Network Controller を使用するためのライセンシング要件を示します。

Cisco Catalyst 8000V

Cisco Cloud Network Controller 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

1. **所有ライセンス持ち込み（BYOL）**ライセンス モデル
2. **ペイアズユーゴー（PAYG）**ライセンス モデル

BYOL ライセンス モデル

Cisco Catalyst 8000V は、サブスクリプション ベースのライセンスをサポートしています。

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、Cisco Catalyst 8000V Edge ソフトウェアを参照してください。
- 層に基づくさまざまなスループットの詳細については、Azure パブリック クラウドの要件を参照してください。

Cisco Cloud Network Controller は、「Cisco DNA Advantage」サブスクリプションを利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、Cisco DNA ソフトウェア SD-WAN およびルーティング マトリックスを参照してください。

PAYGライセンス モデル

Cisco Cloud Network Controller は Cisco Catalyst 8000V でのペイアズユーゴー（PAYG）ライセンス モデルをサポートしています。これにより、ユーザーは VM サイズに基づいてクラウドに Catalyst 8000V インスタンスを展開し、時間単位で使用料を購入できます。

スループットを得るために VM サイズに完全に依存しているため、PAYG ライセンス モデルを有効にするには、まず現在の Cisco Catalyst 8000V の展開を解除してから、新しい VM サイ

ズでの初回セットアップを使用して再度展開します。詳細については、セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成を参照してください。

（注） 使用可能な 2 つのライセンス タイプを切り替える場合も、PAYG ライセンスを有効にする手順を使用できます。

（注） Azuru マーケットプレイスでライセンスを使用するには、**Catalyst 8000V Cisco DNA Essentials** と **Catalyst 8000V Cisco DNA Advantage** の 2 つの PAYG オプションがあります。Cisco Cloud Network Controller は、**Catalyst 8000V Cisco DNA Advantage** を利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、『Cisco DNA Software SD-WAN およびルーティング マトリックス』を参照してください。

Cisco Cloud Network Controller およびオンプレミス ACI ライセンスの概要

- オンプレミス Cisco ACI サイトのすべてのリーフスイッチのライセンス要件：
  - Cisco ACI オンプレミス サイトが単一サイトの場合、オンプレミス リーフスイッチには Essentials ライセンス階層（またはそれ以上）を使用します。
  - Cisco ACI オンプレミス サイトがマルチサイトの場合、オンプレミス リーフスイッチには Advantage ライセンス階層（またはそれ以上）を使用します。
- Cisco Cloud Network Controller インスタンスによって管理されるすべての VM インスタンスのライセンス要件：
  - クラウド上の Cisco ACI に Cisco Cloud Network Controller が 1 つしかない場合は、Cisco Cloud Network Controller に Essentials クラウド ライセンス階層（またはそれ以上）を使用します。
  - クラウド上の Cisco ACI に Cisco Cloud Network Controller が 1 つ以上ある場合は、Cisco Cloud Network Controller に Advantage クラウド ライセンス階層（またはそれ以上）を使用します。

Microsoft Azure

ライセンスのタイプに基づき、Microsoft Azure Marketplace を介して 登録する必要があります。

- **BYOL ライセンス モデル**の場合は、 **[Cisco Catalyst 8000V エッジ ソフトウェア - BYOL（Cisco Catalyst 8000V Edge Software- BYOL）]** に登録します。
- BYOL **ライセンス モデル**の場合は、 [Cisco Catalyst 8000V エッジ ソフトウェア - BYOL（**Cisco Catalyst 8000V Edge Software- BYOL）] に登録**します。

Microsoft Azure Marketplaceからサブスクライブするには、の手順に従ってください。Cisco Cloud Router 8000V への登録

Cisco Cloud Network Controller の関連ドキュメント

Cisco Cloud Network Controller、 Nexus Dashboard、および Microsoft Azure に関する情報は、さまざまなリソースから入手できます。

シスコのドキュメント

Cisco.com でシスコ製品のマニュアルを参照してください。

- Cisco Cloud Network Controller の関連ドキュメント

  ビデオ、リリース ノート、基礎、インストール、設定、およびユーザ ガイドが含まれています。

- Nexus Dashboard の関連ドキュメント

  ビデオ、リリース ノート、インストール、設定、およびユーザ ガイドが含まれています。

- Cisco Cloud Router の関連ドキュメント

  リリース ノート、コマンド リファレンス、データ シート、インストール、アップグレード、および設定ガイドが含まれています。

Microsoft Azure のマニュアル

Microsoft Azure Web サイトで、ユーザ ガイド、FAQ、ケース スタディ、ホワイト ペーパーなどのドキュメントを検索できます。

翻訳について
このドキュメントは、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。