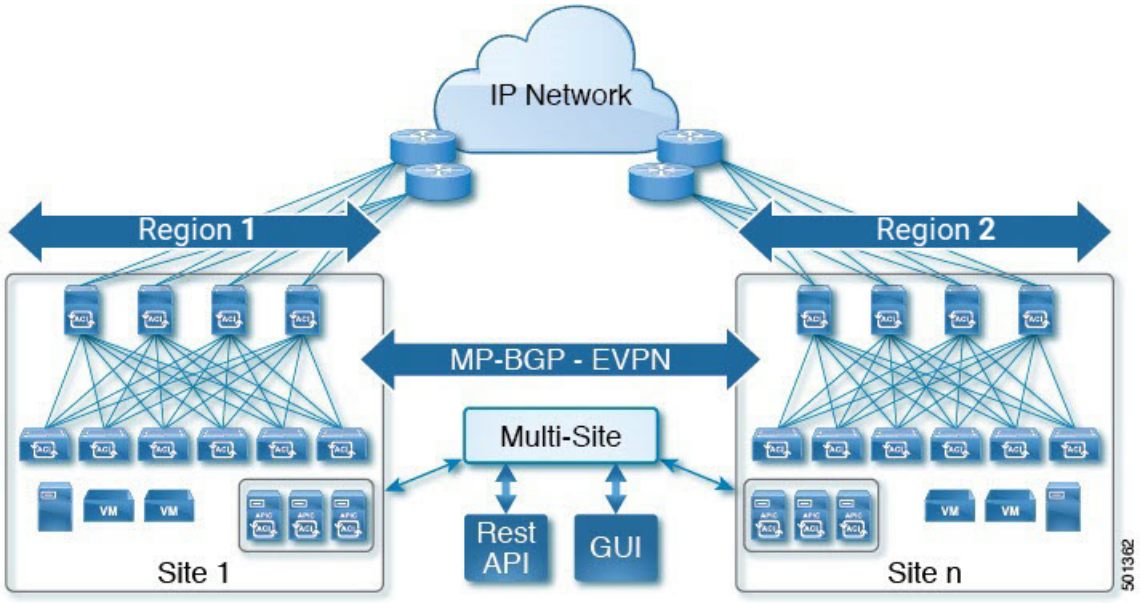
Cisco ACI マルチサイトについて

- About Cisco ACI マルチサイト, on page 1
- 用語 （2 ページ）
- ユーザ、ロールおよび権限 （3 ページ）
- Cisco ACI マルチサイト スキーマとテンプレート （5 ページ）

About Cisco ACI マルチサイト

Figure 1: Cisco ACI* マルチサイト *Architecture



As the newest advance on the Cisco ACI methods to interconnect networks, Cisco ACI マルチサイト is an architectural approach for interconnecting and managing multiple sites, each serving as a single fabric and region. As shown in the diagram, the マルチサイト architecture has three main functional components:

- Two or more ACI fabrics built with Nexus 9000 switches deployed as leaf and spine nodes.
- One APIC cluster domain in each fabric.

- An inter-site policy manager, named Cisco ACI マルチサイト, which is used to manage the different fabrics and to define inter-site policies.

マルチサイト has the following benefits:

- Complementary with Cisco APIC, in マルチサイト each site is a region (APIC cluster domain), which can be configured to be a shared or isolated change-control zone.
- MP-BGP EVPN is used as the control plane between sites, with data-plane VXLAN encapsulation across sites.
- The マルチサイト solution enables extending the policy domain end-to-end across fabrics. You can create policies in the マルチサイト GUI and push them to all sites or selected sites. Alternatively, you can import tenants and their policies from a single site and deploy them on other sites.
- マルチサイト enables a global view of site health.
- From the GUI of the マルチサイト Policy Manager, you can launch site APICs.
- Cross-site namespace normalization is performed by the connecting spine switches. This function requires Cisco Nexus 9000 Series switches with "EX" on the end of the name, or newer.
- Disaster recovery scenarios offering IP mobility across sites is one of the typical マルチサイト use cases.

For information about hardware requirements and compatibility, see *Cisco ACI Multi-Site Hardware Requirements Guide*.

For best practices for マルチサイト, see the *Deployment Best Practices* in **Cisco ACI マルチサイト Architecture White Paper**.

For the Cisco ACI マルチサイト documentation set, see http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

用語

Cisco ACI マルチサイト は、Cisco ACI を補完する製品であるため、その用語の多くが ACI および APIC の用語と共通しています（たとえば、ファブリック、テナント、コントラクト、アプリケーションプロファイル、*EPG*、ブリッジドメイン、*L3Out* などの用語が共通して使用されます）。ACIの用語の定義については、『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の基本』を参照してください。

マイクロサービスアーキテクチャ
最初の実装では、ESXi ホストで稼働している 3 つの仮想マシン（VM）のクラスタが、Cisco ACI マルチサイト（サイト間ポリシーマネージャ）になります。これらの ESXi ホストは、VM 間の IP 接続と、異なる APIC クラスタノードの OOB IP アドレスを確立するためだけに必要なので、ACI のリーフノードへの接続は不要です。

名前空間
各ファブリックでは、TEP プール、クラス ID（EPG 識別子）、VNID（異なるブリッジドメインと、定義された VRF を特定する）といった個別のデータを、名前空間で保持しま

す。サイト接続用スパイン スイッチ（EX 以降）であれば、必要に応じてサイト間で名前空間の変換（正規化）が実行されます。

スキーマ（Schema）
サイトにプッシュするサイト構成オブジェクトを含むプロファイルです。

Site
ACI リージョンとして扱われる APIC クラスタドメイン、または単一のファブリックです。その他のサイトと同じメトロ領域に配置することも、ワールドワイドに配置することもできます。

ストレッチ
複数のサイトに展開する場合、オブジェクト（テナント、VRF、EPG、ブリッジドメイン、サブネットまたはコントラクト）が拡張されます。

テンプレート
スキーマの子です。テンプレートには、サイト間で共有される、またはサイト固有の構成オブジェクトが含まれています。

テンプレートの適合性
サイトにまたがってテンプレートを拡張すると、その構成の詳細がサイト間でも共有され、標準化されます。テンプレートの適合性を維持する場合、ローカルサイトの APIC GUI ではなく、マルチサイト GUI のみを使用してテンプレートを変更することをお勧めします。

ユーザ、ロールおよび権限

Cisco ACI マルチサイト Orchestrator では、ロールベース アクセス コントロール (RBAC) を介して定義されたユーザのロールに従ってアクセスが提供されます。ロールは、ローカルと外部認証の両方に使用されます。Cisco ACI マルチサイト Orchestrator では、次のユーザ ロールを使用できます。

- パワー ユーザ—ユーザがすべての操作を実行できるロール。
- サイト マネージャ—ユーザがサイト、テナント、およびそれらの間の関連付けを管理できるようにするロール。
- スキーマ マネージャ—スキーマ マネージャは、テナントの関連付けに関係なくすべてのスキーマを管理できます。
- スキーマ エディタ: ユーザが明示的に関連付けられているテナントを1つ以上含むスキーマを管理するためのロール。
- ユーザおよびとロール マネージャ — ユーザおよびロール マネージャは、すべてのユーザ、そのロール、およびパスワードを管理できます。

上記の各ロールは一連の権限に関連付けられており、これを使用して、Orchestrator GUI のユーザのビューから関連性のない要素を表示し、無関係な要素を非表示にします。たとえば、ユーザ マネージャ ロールにはユーザ関連の権限のみが関連付けられているため、そのロールを持つユーザは GUI の **[ユーザ(User)]** および **[管理 (Admin)]** タブのみを表示できます。

ユーザ ロールおよび権限

次の表は、利用可能なユーザ ロールごとに許可されたCisco ACI マルチサイト の権限の一覧表示です。属性値 (AV) 列は、Multi-Site Orchestrator で使用する外部認証サーバを設定するときに必要なユーザ設定文字列を指定します。外部認証の詳細については、「管理操作」の章を参照してください。

表 *1:* ユーザ ロール

ユーザ ロール	権限	属性値（AV）のペア
パワー ユーザ	• ダッシュボード • サイト • スキーマ • テナント • ユーザ • トラブルシューティング レポート	`shell:msc-roles=powerUser`
サイト マネージャ	• ダッシュ ボード—サイト • サイト • テナント	`shell:msc-roles=siteManager`
スキーマ マネージャ	• ダッシュ ボード—サイト とスキーマの健全性 • スキーマ	`shell:msc-roles=schemaManager`
スキーマ エディタ	• ダッシュ ボード—サイト とスキーマの健全性 • スキーマ	`shell:msc-roles=schemaEditor`
ユーザ マネージャ	• ユーザ	`shell:msc-roles=userManager`

管理者ユーザ

初期の設定スクリプトで、デフォルト 管理者ユーザ アカウントが設定され、システムが起動したときにの唯一のユーザとなります。管理者ユーザの初期パスワードはシステムによって設定され、最初のログイン後に変更するように求められます。

- 管理者ユーザのデフォルトのパスワードは `We1come2msc!`
- 管理者ユーザは、電力ユーザのロールが割り当てられます。

- 管理者ユーザを使用して、ほかのユーザを作成しその他すべてのDay-0設定を実行します。
- 管理者 ユーザのアカウント ステータスは、**[非アクティブ]** に設定できません。

読み取り専用アクセス

上記の各ユーザロールを読み取り専用モードで割り当てることができます。読み取り専用権限が付与されている場合、ユーザは以前と同様に、そのロールで使用可能な任意のファブリックオブジェクトを表示できますが、それらのオブジェクトに変更を加えることはできません。

Cisco ACI マルチサイト スキーマとテンプレート

Cisco ACI オブジェクト モデル

最上位レベルでは、Cisco ACI オブジェクトモデルは 1 つ以上のテナントのグループに基づいて構築され、ネットワークインフラストラクチャの管理とデータフローを分離できるようにします。

ポリシー タイプ

さまざまなポリシータイプの用語と概念については、次のセクションを参照してください。

- スキーマ：スキーマは、ポリシーの定義に使用される単一または複数のテンプレートのコンテナです。テンプレートは、ポリシーを定義してサイトに展開するためのフレームワークです。
- テナント：テナントは、アプリケーションポリシーの論理コンテナで、管理者はドメインベースのアクセスコントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。

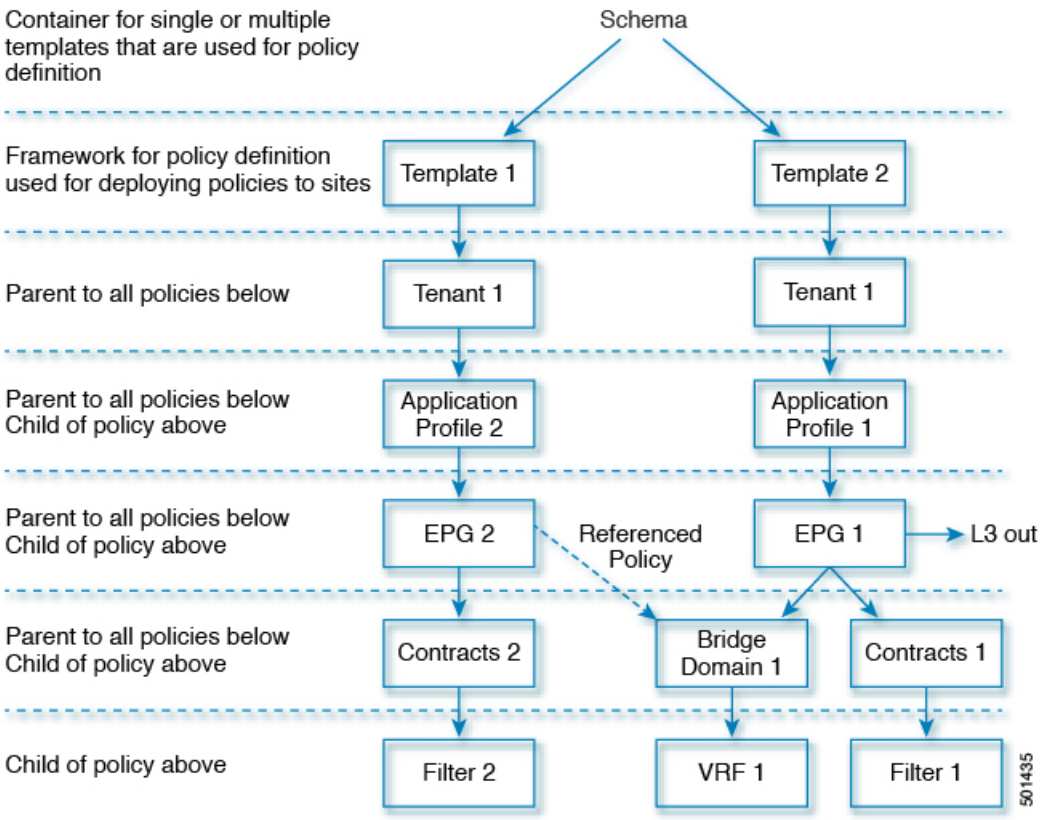
  テナントは、アプリケーションプロファイル、EPG、コントラクト、ブリッジドメイン、VRF、フィルタなど、すべてのポリシーの親ポリシーです。
- アプリケーションプロファイル：アプリケーションプロファイルとは、仮想化されたファブリックにおけるアプリケーション インスタンスの一連の要件です。ポリシーは、ポリシーの範囲に含まれるエンドポイント間の接続と可視性を規制します。
- EPG：EPGは、エンドポイントの集合を含む名前付き論理エンティティである、管理対象オブジェクトです。エンドポイントは、ネットワークに直接的または間接的に接続されるデバイスです。エンドポイントには、アドレス（ID）、ロケーション、属性（バージョンやパッチ レベルなど）があり、物理または仮想にできます。エンドポイントのアドレスを知ることで、他のすべての ID の詳細にアクセスすることもできます。EPG は、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ネットワーク接続ストレージ、またはクライアントが含まれます。EPG内のエンドポイントメンバシップは、ダイナミックまたはスタティックにできます。

- コントラクト：コントラクトは、インバウンドおよびアウトバウンドの許可、拒否、および QoS ルールとポリシー（リダイレクトなど）を定義します。コントラクトでは、環境の要件に応じて、EPG が他の EPG と通信する方法の単純な定義と複雑な定義の両方が可能です。コントラクトは EPG 間で適用されますが、プロバイダーとコンシューマの関係を使用して EPG に接続されます。基本的に、1 つの EPG がコントラクトを提供し、他の EPG がそのコントラクトを消費します。
- ブリッジ ドメイン：ブリッジ ドメイン（fvBD）は、ファブリック内のレイヤ 2 フォワーディングの構造を表します。次の図は、管理情報ツリー（MIT）内のブリッジドメインの場所とテナントの他のオブジェクトとの関係を示します。
- 仮想ルーティングおよび転送（VRF）：仮想ルーティングおよび転送（VRF）オブジェクト（fvCtx）またはコンテキストは、テナントのネットワークです（APIC GUI ではプライベートネットワークと呼ばれます）。テナントには、複数の VRF を含めることができます。VRF は、一意のレイヤ 3 フォワーディングおよびアプリケーション ポリシー ドメインです。次の図は、管理情報ツリー（MIT）内の VRF の場所とテナントの他のオブジェクトとの関係を示します。
- フィルタ：フィルタは、2 つの EPG 間のポリシーに固有のルールです。フィルタは、インバウンドルールとアウトバウンドルール（許可、拒否、リダイレクト、ログ、コピー、マーク）で構成されます。

スキーマとテンプレートのモデル

スキーマとテンプレートのオブジェクトモデルを簡潔に示す次の図をご覧ください。

図 *2 : Cisco ACI* マルチサイト スキーマとテンプレートのフレームワーク



各ポリシータイプ間の関係は次のようになっています。

- アプリケーションプロファイルは、EPG の親ポリシーです。
- EPG は、コントラクトとブリッジドメインの親ポリシーです。
- コントラクトは、フィルタの親ポリシーです。
- ブリッジドメインは、VRF の親ポリシーです。

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。