Azure 向け Cisco Cloud APIC ユーザー ガイド、リリース 25.0(x)

初版：2021 年 9 月 20 日

最終更新：2021 年 12 月 17 日

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
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

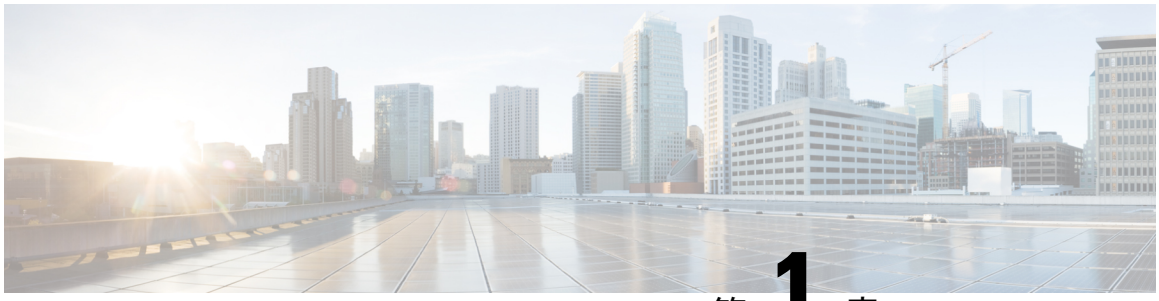
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks

目 次



第 1 章

新機能と変更情報

この章は、次の項で構成されています。

新機能と変更情報

次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco Cloud APIC* の リリース *25.0(3)* の新機能と変更された動作

機能または変更	説明	参照先
Azure network load balancer の複数のフロントエンド IP アドレスのサポート	このリリースでは、Cisco Cloud APIC における Azure network load balancer の複数のフロントエンド IP アドレスがサポートされています。	レイヤ 4 から レイヤ 7 サービスの展開 （209 ページ）
Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V への移行	Cisco Cloud APIC は、リリース 25.0(3) 以降、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。	

新機能と変更情報

機能または変更	説明	参照先
Cisco Cloud Services Router 1000v および Cisco Catalyst 8000V で使用される用語	上記の 2 種類のルータには、次の用語が使用されます。 • **CSR**：クラウド サービス ルータの省略語ですシスコ クラウド サービス ルータ 1000v を指し、リリース 25.0(3) より前のリリースで使用されました。 • **CCR**：Cisco Cloud ルータの略。リリース 25.0(3) 以降で使用される Cisco Catalyst 8000V を指します。 さらに、このドキュメント全体で、**CCR** は、リリースに応じて、上記のいずれかのルータの総称として使用されます。	
マルチサイト オーケストレータの名前の変更	Cisco ACI マルチサイト Orchestrator (MSO) は、2021 年 8 月 15 日の MSO リリース 3.4.1 から Cisco Nexus Dashboard Orchestrator (NDO) に変更されました。この Cisco Cloud APIC ドキュメントでは、MSO のすべてのインスタンスが NDO になりました。	

表 *2 : Cisco* クラウド *APIC* リリース *5.2(3)* の新機能と変更された動作

機能または変更	説明	参照先
Azure VPN ゲートウェイを使用したサイト外部 EPG のサポート	リリース 25.0(2) 以降、VPN ゲートウェイを使用して、Cisco Cloud APIC で管理されたクラウド サイトと非 ACI リモート サイト間の接続を提供するためのサポートが利用可能になりました。	Cisco Cloud APIC で管理されたクラウド サイトと非 ACI リモート サイト間の接続の設定（347 ページ）

機能または変更	説明	参照先
Azure および AWS でルーティングとセキュリティ ポリシーを個別に構成するためのサポート	リリース 25.0(2) 以降、ルーティング ポリシーに対して次の更新を利用できます。 • 内部 VRF ペア間のルートマップ ベースのルートリークのサポート • 内部 VRF ルート リーク ポリシーのサポート。これにより、内部 VRF のペア間で契約ベースのルーティングまたはマップ ベースのルーティングを使用するかどうかを選択できます。	• Cisco Cloud APIC の概要 （7 ページ） • Cisco Cloud APIC コンポーネントの設定 （67 ページ）
CCR IPsec トンネルは、外部ブランチ接続に使用可能な 3 つのデータ インターフェイスのいずれかを使用できるようになりました。	リリース 25.0(2) より前では、外部ネットワークへのすべてのトンネルは、CCR ルータの 1 つの特定のインターフェイス（GigabitEthernet3 インターフェイス、または cloudHostIfp-2）から発信されていました。 リリース 25.0(2) 以降、サポートが拡張され、同じ宛先へのトンネルを GigabitEthernet2、GigabitEthernet3、および GigabitEthernet4 インターフェイスから形成できるようになりました。これは、IKEv2 構成のトンネルでのみサポートされます。	• Cisco Cloud APIC の概要 （7 ページ） • Cisco Cloud APIC コンポーネントの設定 （67 ページ）
Azure NLB バックエンド プールの VM スケール セットのサポート	リリース 25.0(2) 以降、ロードバランサのバックエンド ターゲットとして Azure 仮想マシン スケール セットのサポートが追加されました。	レイヤ 4 から レイヤ 7 サービスの展開 （209 ページ）

新機能と変更情報

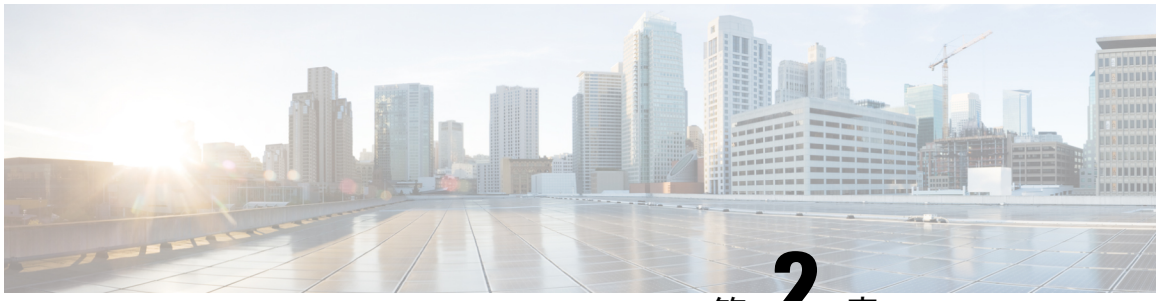
機能または変更	説明	参照先
ワークロード デプロイ用のクラウド リージョン数の増加のサポート	リリース 25.0(2) より前では、サイトごとに最大 4 つのリージョンを持つことができます。リリース 25.0(2) 以降、サイトごとに最大 16 のリージョンを持つことができます。	
overlay-2（セカンダリ）VRF での変更	リリース 25.0(2) 以前のリリースでは、セカンダリ VRF である overlay-2 VRF が Cisco Cloud APIC の起動時に暗黙的にインフラ テナントに作成されており、overlay-2（セカンダリ）VRF でのみ Azure のサービスを作成する必要がありました。 リリース 25.0(2) 以降、その制限が削除され、overlay-2 VRF が Cisco Cloud APIC 起動時にインフラ テナントで暗黙的に作成されることはありません。	overlay-2（セカンダリ）VRF の変更について （8 ページ）

表 *3 : Cisco* クラウド *APIC* リリース *25.0(1)* の新機能と変更された動作

機能または変更	説明	参照先
Cisco Cloud APIC のリリース番号の変更	リリース 25.0(1) 以降では、Cisco Cloud APIC のリリース番号が変更されています。Cisco Cloud APIC のリリース順序は次のとおりです。 • 4.1(x)（AWS のみのサポート） • 4.2(x) • 5.0(x) • 5.1(x) • 5.2(x) • 25.0(×)	

機能または変更	説明	参照先
Cisco Cloud APIC での Prometheus Node Exporter のサポート	Prometheus Node Exporter は、リリース 25.0(1) 以降から Cisco Cloud APIC でサポートされています。	VM ホスト メトリックのモニタリング （193 ページ）
インフラ VPC CCR から IPSec/BGP を使用した外部デバイスへの IPv4 接続のサポート。	インフラ VPC CCR から IPSec/BGP を使用する任意の外部デバイスへの IPv4 接続がサポートされるようになりました。	外部ネットワーク接続 （10 ページ）
外部接続の設定時に、セキュリティ ポリシーに関係なく、内部 VRF と外部 VRF の間でルーティング ポリシーを個別に設定するためのサポート。	外部接続の設定時に、セキュリティ ポリシーに関係なく、内部 VRF と外部 VRF の間でルーティング ポリシーを個別に設定するためのサポートが利用できるようになりました。	サポートされているルーティングとセキュリティ ポリシーの概要 （11 ページ）

新機能と変更情報



第 2 章

Cisco Cloud APIC の概要

概要

Cisco Application Policy Infrastructure Controller（APIC）リリース 4.1(1) では、クラウドベースの仮想マシン（VM）に展開する Cisco APIC のソフトウェア展開である Cisco Cloud APIC が導入されています。リリース 4.1(1) は Amazon Web サービスをサポートします。リリース 4.2(x) 以降、Azure のサポートが追加されました。

展開した場合の Cisco Cloud APIC：

- Azure パブリック クラウドと対話するための既存の Cisco APIC と同様のインターフェイスを提供します
- クラウド構成の展開と構成を自動化します
- 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 コンストラクトに変換します
- エンドポイントを検出します
- 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

（注）
- Cisco Multi-Site は、MP-BGP EVPN 構成をオンプレミスのスパイン スイッチにプッシュします
- オンプレミス VPN ルーターには、IPsec の手動構成が必要です

- 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。
- ポリシーは Cisco Nexus Dashboard Orchestrator によってオンプレミスおよびクラウド サイトにプッシュされ、Cisco Cloud APIC はポリシーをクラウド ネイティブ コンストラクトに変換して、ポリシーをオンプレミス サイトと一致させます。

パブリック クラウドに Cisco ACI を拡張することの詳細については、『*Cisco Cloud APIC Installation Guide*』を参照してください。

Cisco Cloud APIC が稼働している場合は、Cisco Cloud APIC コンポーネントの追加と構成を開始できます。このドキュメントでは、Cisco Cloud APIC ポリシー モデルについて説明し、GUI および REST API を使用して Cisco Cloud APIC コンポーネントを管理 (追加、構成、表示、および削除) する方法について説明します。

overlay-2（セカンダリ）VRF の変更について

リリース 25.0(2) より前では、セカンダリ VRF である overlay-2 VRF は、Cisco Cloud APIC の起動時にインフラ テナントで暗黙的に作成され、overlay-2（セカンダリ）VRF でのみ Azure のサービスを作成する必要がありました。リリース 25.0(2) 以降、その制限は削除され、overlay-2 VRF は Cisco Cloud APIC の起動中にインフラ テナントで暗黙的に作成されなくなりました。

Cloud APIC または Nexus Dashboard Orchestrator (NDO) のいずれかで、この overlay-2（セカンダリ）VRF の特別な処理はありません。任意の名前で任意のセカンダリ VRF を作成し、インフラ VPC で `RsSubnetToCtx` を関連付け、Azure のこれらの任意のセカンダリ VRF にサービスを展開できます。いつでもセカンダリ VRF を作成でき、overlay-2 はリリース 25.0(2) 以降では単なるセカンダリ VRF です。

リリース 25.0(2) へのアップグレード時に、overlay-2 VRF を使用していた場合、それは引き続き存在し、ユーザーが作成したセカンダリ VRF と同じように扱われます。引き続き、overlay-2 という名前のインフラまたはユーザー VPC でセカンダリ VRF を作成または削除することを選択できます。

このドキュメント全体で、「overlay-2 VRF」という用語のすべてのインスタンスは、より一般的な「セカンダリ VRF」という用語に変更されました。したがって、「セカンダリ VRF」という用語は、Cloud APIC が実行されているリリースに応じて、このドキュメントでは異なることを意味します。

- リリース 25.0(2) 以降 （9 ページ）

• リリース 25.0(1) 以前 （9 ページ）

リリース 25.0(2) 以降

Cloud APIC がリリース 25.0(2) 以降で実行されている場合、このドキュメントの「セカンダリ VRF」は、ユーザーが作成したセカンダリ VRF である VRF を指します。前述のように、リリース 25.0(2) 以降で自動的に作成される一意の overlay-2 VRF はなくなりましたが、overlay-2 という名前のインフラまたはユーザー VPC でセカンダリ VRF を作成または削除することを選択できます。

リリース 25.0(1) 以前

Cloud APIC がリリース 25.0(1) 以前で実行されている場合、このドキュメントの「セカンダリ VRF」は、特に Cisco Cloud APIC の起動中にインフラ テナントで暗黙的に作成された overlay-2 VRF を指します。次の情報は、リリース 25.0(1) 以前用に自動的に作成される overlay-2（セカンダリ）VRF に特に適用されます。

インフラ ハブ サービス VRF（インフラ VNet の overlay-2 VRF）について

リリース 25.0(1) 以前の場合、overlay-2 VRF は、Cisco Cloud APIC の起動中にインフラ テナントに暗黙的に作成されます。クラウド サイトで使用されるインフラ サブネット（CCR およびネットワーク ロード バランサ用）と共有サービス用に展開されたユーザー サブネットの間でネットワーク セグメンテーションをそのまま維持するために、インフラ サブネットとユーザーが展開したサブネットには異なる VRF が使用されます。

- **Overlay-1**：CCR、インフラ ネットワーク ロード バランサ、および Cisco Cloud APIC とともに、クラウド インフラのインフラ CIDR に使用されます。
- **Overlay-2**：ユーザー CIDR が共有サービスを展開するために使用され、インフラ VNet（Azure クラウドの overlay-1 VNet）のレイヤ 4 からレイヤ 7 サービス デバイスとともに使用されます。

CIDR が overlay-2（セカンダリ）VRF にマッピングされる方法は、リリースによって異なります。

- リリース 5.0(2) の場合、インフラ テナントでユーザーが作成したすべての EPG は、インフラ VNet の overlay-2 VRF にのみマッピングできます。追加の CIDR とサブネットを既存のインフラ VNet（既存のインフラ クラウド コンテキスト プロファイル）に追加できます。これらは、インフラ VNet の overlay-2 VRF に暗黙的にマッピングされ、Azure クラウドの overlay-1 VNet に展開されます。
- 5.0(2) 以降のリリースでは、これは当てはまりません。インフラ テナントで、overlay-2 VRF を含む任意のセカンダリ VRF でクラウド EPG を作成できます。インフラ VNet で新しい CIDR を作成すると、それらの CIDR は overlay-2 VRF に暗黙的にマッピングされないため、新しい CIDR をセカンダリ VRF にマッピングするのはユーザーの責任です。

リリース 5.0(2) より前では、特定のクラウド コンテキスト プロファイルは、特定の VNet のクラウド リソースにマップされていました。VNet のすべてのサブネットと関連するルート テーブルには、単一の VRF との 1 対 1 のマッピングがあります。リリース 5.0(2) 以降、インフラ

VNet のクラウド コンテキスト プロファイルは、複数の VRF（インフラ VNet の overlay-1 および overlay-2 VRF）にマッピングできます。

クラウドでは、サブネットのルートテーブルは、ネットワークの分離を実現するための最も詳細なエンティティです。したがって、overlay-1 VRF のすべてのシステム作成クラウドサブネットと、overlay-2 VRF のユーザー作成サブネットは、ネットワーク セグメンテーションを実現するためにクラウド内の個別のルート テーブルにマッピングされます。

（注） Azure クラウドでは、他の VNet とのアクティブなピアリングがある VNet で CIDR を追加または削除することはできません。したがって、インフラ VNet に CIDR を追加する必要がある場合は、最初にその中で VNet ピアリングを無効にする必要があります。これにより、インフラ VNet に関連付けられているすべての VNet ピアリングが削除されます。インフラ VNet に新しい CIDR を追加したら、インフラ VNet で VNet ピアリングを再度有効にする必要があります。

ハブ VNet の既存の CIDR に新しいサブネットを追加する場合は、VNet ピアリングを無効にする必要はありません。

外部ネットワーク接続

リリース 25.0(1) より前は、AWS と Cisco Cloud APIC の外部ネットワーク接続は、インフラ VNet の CCR からの EVPN 接続を使用することによってのみ利用可能でした。

リリース 25.0(1) 以降では、インフラ VNet CCR から IPSec/BGP を使用する任意の外部デバイスへの IPv4 接続もサポートされています。この IPSec/BGP 外部接続により、Cisco Cloud APIC をブランチ オフィスに接続できます。

次の項では、リリース 25.0(1) で提供される新しい外部ネットワーク接続を可能にするコンポーネントの詳細について説明します。

外部VRF

外部VRF は、クラウドに存在しない一意の VRF ですが、1 つ以上の外部ネットワークに関連付けられています。VNets をホストするために使用され、クラウド コンテキスト プロファイルに関連付けられている VRF である内部 VRF とは対照的に、外部VRF は、 で使用されるどのクラウド コンテキスト プロファイルでも参照されません。

外部VRF は、他のクラウドサイトまたはオンプレミスサイトに接続されている外部ネットワークを表します。複数のクラウド VRF は、外部VRF にルートをリークしたり、外部VRF からルートを取得したりできます。外部VRFで外部ネットワークが作成されると、VRF 間ルーティングが設定され、外部ネットワークで受信およびアドバタイズされたルートが 外部VRF で受信またはアドバタイズされます。

非 ACI 外部デバイスへの接続

リリース 25.0(1) では、既存の外部接続モデルが拡張され、AWS CCR から非 ACI 外部デバイスへの接続が提供されます。インフラ VNet CCR からこれらの非 ACI 外部デバイスへの IPv4 セッションが 外部VRF で作成され、外部VRF とサイト ローカル VRF の間で VRF 間ルーティングが設定されます。

このタイプの接続に関する注意事項と制限事項を次に示します。

- EVPN と IPv4 IPSec/BGP の両方を使用して、クラウドから同じリモート サイトに接続することはできません。

注意事項と制約事項

リリース 25.0(2) 以降、すべてのリージョンを手動で選択する代わりに、外部ネットワーク接続に対して `allRegion` を true に設定する必要があります。

サポートされているルーティングとセキュリティ ポリシーの概要

ルーティングとセキュリティ ポリシーは、Cisco Cloud APIC で実行しているリリースに応じて、異なる方法で処理されます。

ルーティングおよびセキュリティ ポリシー：リリース 25.0(1) 以前のリリース

リリース 25.0(1) より前のリリースでは、ルーティング ポリシーとセキュリティ ポリシーは緊密に結合されていました。EPG にまたがる 2 つのエンドポイント間の通信を許可するには、コントラクトを構成する必要があります。これらのコントラクトは、次の目的で使用されます。

- **ルーティング ポリシー**：トラフィック フローを確立するルートを定義するために使用されるポリシー
- **セキュリティ ポリシー**：セキュリティ グループ ルール、ネットワーク セキュリティ ルールなど、セキュリティ目的で使用されるルール

つまり、コントラクトは本質的に、セキュリティ ポリシーとルーティング ポリシーの両方を構成するという 2 つの目的を果たします。つまり、コントラクトを破棄すると、許可するトラフィックと拒否するトラフィックを管理するセキュリティポリシーが破棄されるだけでなく、そのトラフィックのルーティングに使用されるポリシーも破棄されます。リリース 25.0(1) より前では、セキュリティポリシーを設定せずにルーティングポリシーを設定する方法はなく、その逆も同様です。

ルーティングおよびセキュリティ ポリシー: リリース 25.0(1)

リリース 25.0(1) 以降、セキュリティ ポリシーから独立して、ルーティングを個別に構成するためのサポートが利用できるようになりました。

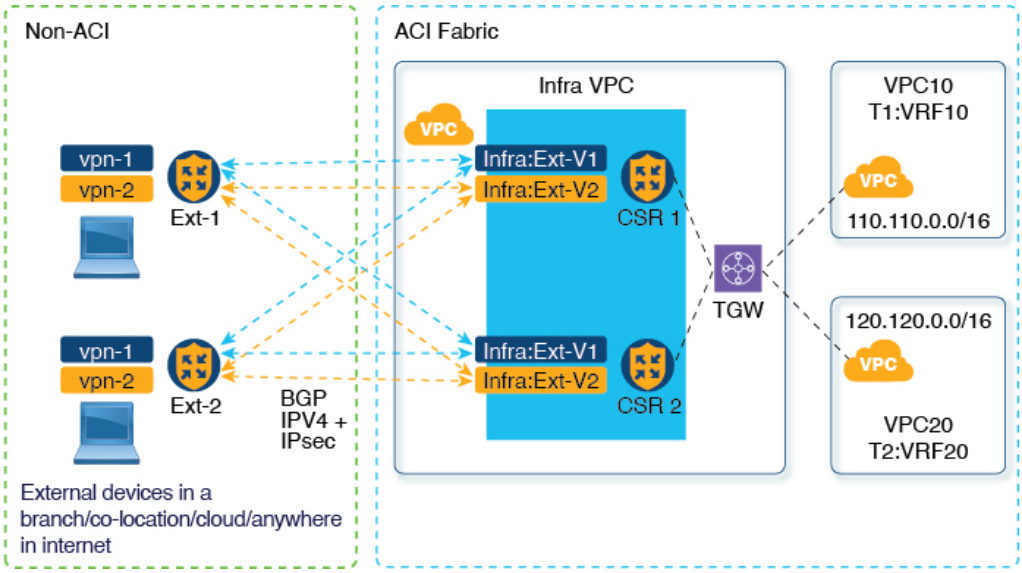
（注） このセクションで説明するルーティング ポリシーは、25.0(1) リリース専用であり、内部と外部VRF の間でのみ適用されます。 25.0(2) リリースでのルーティング ポリシーとセキュリティ ポリシーの変更については、ルーティング ポリシー: リリース 25.0(2) （14 ページ） を参照してください。

ルーティングおよびセキュリティ ポリシーを構成する手順は次のとおりです。

- **ルーティング ポリシー**: リリース 25.0(1) で導入された VRF 間ルーティング機能を使用して、ルーティング ポリシーを個別に設定します。これらの手順については、Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 （81 ページ） を参照してください。
- **セキュリティ ポリシー** : ルーティング ポリシーを構成した後、セキュリティ ポリシーを個別に構成するために以前に行ったように、引き続きコントラクトを使用します。
  - まず、外部 EPG を作成します。これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ） を参照してください。
  - 次に、外部 EPG とクラウド EPG の間のコントラクトを作成します。これらの手順については、Cisco Cloud APIC GUI を使用したコントラクトの作成 （121 ページ） を参照してください。

VRF 間ルーティングを使用すると、独立したルーティング ポリシーを構成して、次のタイプのサイト間のルーティングを設定するときに、内部のペアと外部VRF の間でリークするルートを指定できます。

次の図は、この種の構成のトポロジ例を示しています。このトポロジ例は、ACI以外のサイトにある可能性のある外部デバイス (Ext-1) の背後にあるリモート エンドポイント (vpn-1) に接続する方法を示しています。この非ACIサイトは、ブランチ オフィス、同じ場所にあるサイト、クラウド サイト、または BGP IPv4 および IPSec の機能を備えたインターネット上の任意の場所である可能性があります。



この例では、infra:Ext-V1 はインフラ VNet の CCR 上の 外部VRF にあり、リモート デバイスへの IPSec トンネルを介した BGP IPv4 セッションがあります。リモート エンドポイント ルートは、これらのセッションを介して infra:Ext-V1 VRF で受信され、図の右側に表示されている内部 VRF (たとえば、VNet10 の T1:VRF10) にリークされます。逆リーク ルートも設定されています。

ルート リークは、ルート マップを使用して内部 VRF と外部 VRF の間で発生します。Cisco Cloud APIC では、ルート マップを使用して、内部 VRF から 外部VRF へ、および 外部VRF から内部 VRF へのセキュリティ ポリシーとは独立したルーティング ポリシーを設定できます。内部 VRF のペア間のルーティングを設定するときに引き続きコントラクトを使用するため、内部 VRF 間のルーティング時に、ルーティング ポリシーとセキュリティ ポリシーが設定プロセスで結び付けられます。

次のリストは、**ルート マップ**を使用してセキュリティ ポリシーから独立してルーティング ポリシーを構成できる状況、およびルーティング ポリシーとセキュリティ ポリシーが結び付けられている**コントラクト**を使用する必要がある状況に関する詳細を示しています。

- コントラクトベースのルーティングを使用するルーティングの状況:
  - サイト内ルーティング（リージョン内およびリージョン間）
  - サイト間ルーティング（EVPN を使用したオンプレミスのクラウドから ACI）
  - クラウド間ルーティング
  - 内部 VRF 間のルート リーク
- ルート マップベースのルーティングを使用するルーティングの状況:
  - L3Out 外部VRF を使用したクラウドから非 ACI オンプレミス サイトへ (EVPN なし)
  - 内部 VRF から 外部VRF への特定のルートまたはすべてのルートをリークします。
  - 外部VRF から内部 VRF への特定のルートまたはすべてのルートをリークする

注意事項および制約事項

VRF 間ルーティングを使用してルートマップを使用して VRF ペア間のルートをリークする場合は、次の注意事項が適用されます。

- ルートは常に、内部 VRF と外部 VRF の間で双方向にリークされます。

  たとえば、内部 VRF (V1) と外部 VRF (Ext-V1) を持つユーザー テナント (t1) があるとします。ルート リークは、これらの VRF の両方に対して双方向に設定する必要があります。

- 「より大きな」プレフィックスがすでにリークされている間に、「より小さな」プレフィックスをリークするように設定することはできません。たとえば、10.10.0.0/16 プレフィックスがすでにリークされるように設定されている場合、10.10.10.0/24 プレフィックスの設定は拒否されます。同様に、0.0.0.0/0（すべてリーク）プレフィックスを設定した場合、他のプレフィックスは設定できません。
- クラウド外部 EPG (cloudExtEpgs) 間の契約は許可されていません。
- 外部VRF は、クラウド EPG の作成には使用できません。
- 外部VRF は常にインフラ テナントに属します。
- 外部VRF 間のリーク ルーティングはサポートされていません。

ルーティング ポリシー: リリース 25.0(2)

（注） このセクションで説明するルーティングおよびセキュリティ ポリシーは、25.0(2) リリース専用です。以前のリリースでのルーティング ポリシーとセキュリティ ポリシーの変更については、ルーティングおよびセキュリティ ポリシー: リリース 25.0(1) （12 ページ）を参照してください。

リリース 25.0(2) では、ルーティング ポリシーとセキュリティ ポリシーは、ルーティングおよびセキュリティ ポリシー: リリース 25.0(1) （12 ページ） で説明されているように引き続き分割されますが、特にルーティング ポリシーに次の変更が追加されています。

内部 VRF 間のルート リーク

以前の 25.0(1) リリースでは、内部 VRF と外部 VRF のペア間でリークするルートを指定する独立したルーティング ポリシーを設定できる、VRF 間ルート マップベースのルーティング機能が導入されました。このルート マップ ベースのルーティング機能は、特に内部 VRF と外部 VRF の間に適用されます。内部 VRF のペア間のルーティングを設定する場合、ルーティング

およびセキュリティ ポリシー: リリース 25.0(1) （12 ページ）で説明されているように、その状況ではコントラクトベースのルーティングのみを使用できます。

リリース 25.0(2) 以降、内部 VRF のペア間でのルート マップベースのルート リークがサポートされるようになりました。次のいずれかのオプションを使用して、ルートをリークする方法を指定します。

- 次を使用して、VRF に関連付けられているすべての CIDRS または特定のサブネット IP アドレスをリークします。
  - GUI を介した **Leak All** オプション
  - REST API を介した `leakInternalPrefix` フィールド
- 次を使用して、VRF のペア間でリークします。
  - GUI による **サブネット IP** オプション
  - REST API を介した `leakInternalSubnet` フィールド

グローバルな Inter-VRF ルート リーク ポリシー

内部 VRF のペア間でのルート マップ ベースのルート リークのサポートに加えて、内部 VRF ルート リーク ポリシーでは、コントラクト ベースのルーティングまたは内部 VRF のペア間のルートマップベースのルーティングを使用するかどうかを選択することもできます。これは、初回セットアップで利用可能なグローバル モード構成であり、コントラクトベースまたはルートマップ ベースのモデルを可能にします。このグローバル モードでコントラクト ベース ルーティングを有効にすると、ルートマップがない場合にのみ、コントラクトを使用して内部 VRF のペア間のルートがリークされる可能性があることに注意してください。

このポリシーには、次の特性があります。

- このポリシーは、すべての内部 VRF に関連付けられています。
- これは、Cisco Cloud APIC で作成されたポリシーです。
- 契約ベースのルーティングは、グリーンフィールド ケースに対してデフォルトで無効になっています（オフになっています）（Cisco Cloud APIC に初めて構成する場合）。アップグレードの場合、リリース 25.0(2) より前に設定された Cisco Cloud APIC がある場合、コントラクトベースのルーティングが有効になります (オンになります)。

内部 VRF ルート リーク ポリシーは、インフラ テナントの First Time Setup 画面で設定されるグローバル ポリシーです。ここでは、ブール フラグを使用して、ルート マップがない場合にコントラクトがルートを駆動できるかどうかを示します。

- **オフ**: デフォルト設定。ルートはコントラクトに基づいて漏洩するのではなく、ルートマップに基づいて漏洩します。
- **オン**: ルート マップが存在しない場合、コントラクトに基づいてルートが漏洩します。有効にすると、ルートマップが構成されていないときにコントラクトがルーティングを駆動します。ルートマップが存在する場合、ルートマップは常にルーティングを駆動します。

この Boolen フラグを前後に切り替えることができます。次に、このグローバル VRF ルート リーク ポリシーを切り替えるための一般的な推奨手順を示します。詳細な手順は、Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成 （84 ページ） で提供されています。

- EVPN を使用したマルチクラウドおよびハイブリッド クラウドの展開では、Cisco Cloud APIC で契約ベースのルーティングを有効にする必要があります。
- EVPN を使用しないマルチクラウドおよびハイブリッドクラウドの展開の場合、ルーティングは、コントラクトではなくルート マップのみを介して実行されます。
- コントラクト ベースのルーティングからルート マップ ベースのルーティングに切り替える (**オフ**設定に切り替える) ことによってコントラクト ベースのルーティングを無効にする場合、**オフ**に設定する前にルートマップベースのルーティングが構成されていないと、このアクションは混乱を招く可能性があります。

  ルートマップベースのルーティングに切り替える前に、次の設定変更を行う必要があります。

  1. 既存のコントラクトを持つ VRF のすべてのペア間でルート マップ ベースのルート リークを有効にします。
  2. グローバル ポリシーでコントラクトベースのルーティング ポリシーを無効にします。

  その時点で、ルーティング ポリシーをルート マップ ベースのルーティングに変更できます。その後、新しいルート マップ ベースのルーティングで必要な粒度を反映するようにルーティングを変更できます。
- ルートマップベースのルーティングからコントラクトベースのルーティングに切り替える (**オン**設定に切り替える) ことでコントラクトベースのルーティングを有効にする場合は、コントラクトベースのルーティングに切り替える前に構成を変更する必要はありません。これは、この設定が追加操作であるためです。つまり、コントラクトベースとルートマップベースの両方のルーティングを、VRF のペア間で有効にすることができます。ルーティングを有効にする場合、ルート マップはコントラクトよりも優先されます。ルート マップベースのルーティングを有効にすると、コントラクトベースのルーティングの追加は中断がないようにしなければなりません。

注意事項と制約事項

次の注意事項および制約事項は、リリース 25.0(2) に適用されます。

- 外部 VRF と内部 VRF 間のルーティングでは、引き続きルート マップ ベースのルーティングのみが使用されます。
- レイヤ 4 からレイヤ 7 へのサービス挿入は引き続き契約を介して行われるため、このような状況では、グローバル レベルでコントラクト ベースのルーティングを有効にする必要があります。
- Azure express route との外部接続では、引き続き契約ベースのルーティングが使用されます。

- leakExternalPrefix は、SSH を実行する外部 EPG 用に構成された外部エンドポイント セレクタと重複しないようにしてください。そうしないと、SSH が壊れます。この場合、プレフィックスは、Azure のインターネットへのデフォルトのルートではなく、ネットワーク ロード バランサを指します。
- インターネット トラフィックをリモート サイトにリダイレクトする必要がない限り、leakInternalPrefix（Leak All、または 0.0.0.0/0）は使用しないでください。そうしないと、SSH が破損します。この場合、インターネットへのデフォルト ルートは、ネットワーク ロード バランサを指す新しい UDR によって上書きされます。

トンネルのソース インターフェイスの選択

リリース 25.0(2) より前は、同じ宛先への IPsec トンネルは許可されていませんでした。リリース 25.0(2) 以降、異なる外部ネットワーク間で同じ宛先への複数のトンネルを持つことができます。これは、GUI でさまざまなソース インターフェイス (2、3、または 4) を使用するか、cloudtemplateIpseTunnlSourceInterface を使用して REST API を介して実行されます。

次の例は、インターフェイス 3 だけが発信元インターフェイスとして使用される状況を示しています。

```
<cloudtemplateIpSecTunnel peeraddr="173.36.19.2" preSharedKey="def" poolname="pool1">
    <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId=”3” />
 </cloudtemplateIpSecTunnel>
```

次の例は、インターフェイス 2 と 3 の両方が発信元インターフェイスとして使用されている状況を示しています。

```
<cloudtemplateIpSecTunnel peeraddr="173.36.19.2" preSharedKey="def" poolname="pool1">
    <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId=”2” />
    <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId=”3” />
</cloudtemplateIpSecTunnel>
```

注意事項と制約事項

- インターフェイスの数を増やすと、トンネルの内部ローカル IP アドレスの需要が増加します。
- IPsec トンネル ソース インターフェイスの機能は、IKEv2 構成でのみサポートされます。

注意事項と制約事項

ここでは、Cisco Cloud APIC の注意事項と制限事項について説明します。

- クラウド CCR（クラウド ルータ）で VRF 間ルート リークを使用しているときに、オンプレミスとクラウドの間で複数の VRF をストレッチすることはできません。たとえば、EPG1 を持つ VRF1 が拡張され、EPG2 を持つ VRF2 も拡張される状況では、EPG1 は EPG2 とコ

ントラクトできません。ただし、クラウド内に複数のVRFを設定して、1つのオンプレミス VRF と 1 つ以上のコントラクトを共有することができます。

- クラウド上の CSR にアドバタイズするために、外部でアドバタイズされたオンプレミス サイトのブリッジ ドメイン サブネットを設定します。
- テナントのオブジェクトを設定する前に、古いクラウド リソース オブジェクトを確認します。アカウントを管理していた以前の Cisco Cloud APIC 仮想マシンから適切に消去されなかった場合、古い設定が存在する可能性があります。Cisco Cloud APIC は古いクラウド オブジェクトを表示できますが、削除することはできません。クラウドアカウントにログインし、手動で削除する必要があります。

（注） テナント サブスクリプション ID を追加した後、Cisco Cloud APIC が古いクラウド リソースを検出するには時間がかかります。

Azure では、1 つのテナントが所有する Azure アカウントを複数のテナントが共有できます。アカウントが複数のテナントで共有されている場合、所有者テナントのみが他のテナントの古いオブジェクトを表示できます。

古いクラウド リソースを確認するには、次の手順を実行します。

1. Cisco Cloud APIC GUI から、**[ナビゲーション（Navigation）] メニュー > [アプリケーション管理（Application Management）] > [テナント（Tenants）]**の順にクリックします。**[テナント（Tenants）]** サマリー テーブルは、テナントのリストとともに、サマリー テーブルの行として作業ペインに表示されます。
2. オブジェクトを作成するテナントをダブルクリックします。[概要（Overview）]、[クラウド リソース（Cloud Resources）]、[アプリケーション管理（Application Management）]、[統計（Statistics）]、および[イベント分析（Event Analytics）] タブが表示されます。
3. **[クラウド リソース（Cloud Resources）] > [アクション（Actions）] > [古いクラウド リソース（View Stale Cloud Objects）]** の順にクリックします。**[古いクラウド オブジェクト（Stale Cloud Objects）]** ダイアログボックスが表示されます。

- Cisco Cloud APIC は、作成した Azure リソースの管理を試みます。既存のリソースをインベントリとしてリストするのではなく、他のアプリケーションによって作成されたリソースの管理を試みません。同時に、Azure インフラ テナント サブスクリプションの Azure IAM ユーザー、および他のテナント アカウントが、Cisco Cloud APIC が作成するリソースを妨害しないことも期待されます。このため、Cisco Cloud APIC が Azure 上で作成するすべてのリソースには、次の 2 つのタグの少なくとも 1 つがあります。
  - AciDnTag
  - AciOwnerTag

Cisco Cloud APIC は VM、またはその他のリソースを作成、削除、または更新する権限を持つ Azure IAM ユーザーが Cisco Cloud APIC によって作成および管理されるリソースへアクセスすることや変更することを防止する必要があります。このような制限は、インフラとその他のユーザーのテナント サブスクリプションの両方に適用する必要があります。Azure サブスクリプション管理者は、上記の 2 つのタグを使用して、意図しないアクセスや変更を防ぐ必要があります。たとえば、次のようなアクセス ポリシーがある場合、Cloud APIC によって管理されているリソースへのアクセスを防止することができます。

```
{
  "properties": {
    "level": "CanNotDelete",
    "notes": "Optional text notes."
  }
}
```

- 共有 L3Out を構成する場合:
  - オンプレミスの L3Out とクラウド EPG をテナント共通にすることはできません。
  - オンプレミスの L3Out とクラウド EPG が異なるテナントにある場合は、テナント共通でコントラクトを定義します。オンプレミス サイトまたはクラウド テナントでコントラクトすることはできません。
  - オンプレミスの L3Out 外部 EPG（l3extInstP）でクラウド EPG の CIDR を指定します。
  - オンプレミスの L3Out が別の VRF のクラウド EPG とコントラクトしている場合、クラウド EPG が存在する VRF をオンプレミス サイトに拡張することはできず、オンプレミス サイトの他の VRF とコントラクトすることはできません。 。
  - オンプレミスの外部 EPG で外部サブネットを構成する場合:
    - 外部サブネットをゼロ以外のサブネットとして指定します。
    - 外部サブネットは、別の外部サブネットと重複できません。
    - クラウド EPG とコントラクトするには、共有ルート制御フラグを使用して外部サブネットをマークします。
  - オンプレミスの外部 EPG でマークされている外部サブネットは、L3Out のルーティング プロトコルを介して学習されているか、静的ルートとして作成されている必要があります。
- サポートされているスケールの合計については、次のサポートされているスケールの表を参照してください。

（注） サポートされているスケール表で指定されているスケールにより、合計 4 つの管理リージョンのみ所持できます。

表 *4:* サポートされるスケール

コンポーネント	サポートされている数
テナント	20
アプリケーション プロファイル	500
EPG	500
クラウド エンドポイント	1000
VRF	20
クラウド コンテキスト プロファイル	40
コントラクト	1000
サービスグラフ	200
サービス デバイス	100

Cisco Cloud APIC GUI の概要

Cisco Cloud APIC GUI は、関連するウィンドウのグループに分類されます。各ウィンドウでは、特定のコンポーネントにアクセスして管理できます。GUIの左側にある **[ナビゲーション（Navigation）]** メニューを使用して、ウィンドウ間を移動します。メニューのいずれかの部分にマウスを移動すると、**[ダッシュボード（Dashboard）]**、**[アプリケーション管理（Application Management）]**、**[クラウド リソース（Cloud Resources）]**、**[操作（Operations）]**、**[インフラストラクチャ（Infrastructure）]**、および**[管理（Administrative）]** タブのリストが表示されます。

各タブには異なるサブタブのリストが含まれており、各サブタブから異なるコンポーネント固有のウィンドウにアクセスできます。たとえば、EPG固有のウィンドウを表示するには、マウスを**[ナビゲーション（Navigation）]** メニューに合わせ、**[アプリケーション管理（Application Management）]** > **[EPGs]** をクリックします。そこから、**[ナビゲーション（Navigation）]** メニューを使用して別のコンポーネントの詳細を表示できます。たとえば、**[運用（Operations）]**> **[アクティブ セッション（Active Sessions）]** をクリックして、**EPG**から**[アクティブ セッション（Active Sessions）]** ウィンドウに移動できます。

[インテント（Intent）] メニュー バー アイコンを使用すると、GUI の任意の場所からコンポーネントを作成できます。たとえば、**[ルータ（Routers）]** ウィンドウの表示中にテナントを作成するには、**[インテント（Intent）]** アイコンをクリックします。検索ボックスとドロップダウン リストを含むダイアログが表示されます。ドロップダウン リストをクリックして**[アプリケーション管理（Application Management）]** を選択すると、**[テナント（Tenant）]** オプションを含むオプションのリストが表示されます。**[テナント（Tenant）]** オプションをクリックすると、テナントの作成に必要なフィールドのグループを示す**[テナントの作成（Create Tenant）]** ダイアログが表示されます。

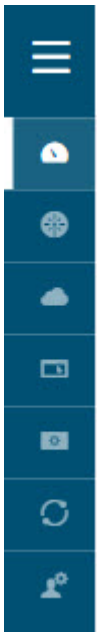
GUI アイコンの詳細については、Cisco Cloud APIC GUI アイコンについて （21 ページ） を参照してください。

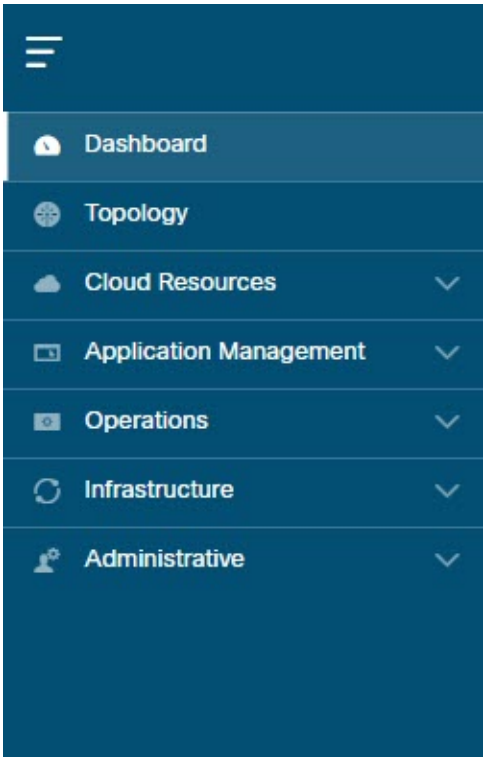
Cisco Cloud APIC コンポーネントの構成の詳細については、Cisco Cloud APIC コンポーネントの設定 （67 ページ） を参照してください。

Cisco Cloud APIC GUI アイコンについて

ここでは、Cisco Cloud APIC GUI で一般的に使用されるアイコンの概要について説明します。

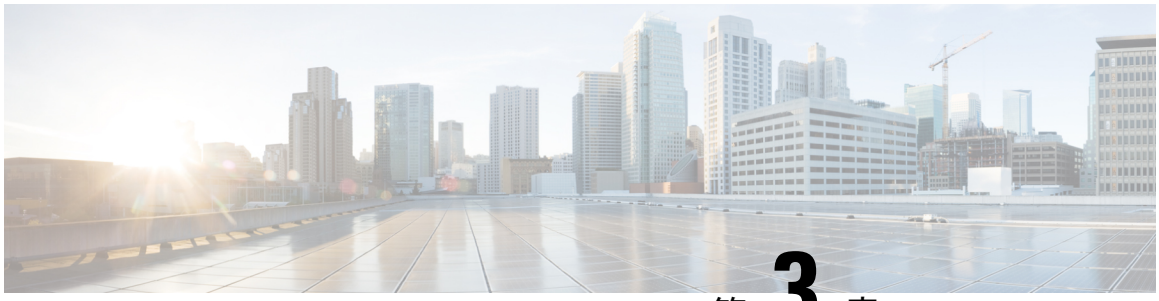
表 *5 : Cisco Cloud APIC GUI* アイコン

アイコン	説明
図 *1 :* ナビゲーション ペイン（折りたたみ） 	GUI の左側には **ナビゲーション** ウィンドウがあり、折りたたんだり展開したりします。ペインを展開するには、マウスアイコンをマウスオーバーするか、上部のメニューアイコンをクリックします。メニュー アイコンをクリックすると、**ナビゲーション** ペインが開いた位置でロックされます。折りたたむには、メニュー アイコンをもう一度クリックします。メニュー アイコンの上にマウスのアイコンを重ねて**ナビゲーション** ウィンドウを展開すると、**ナビゲーション** ウィンドウはマウス アイコンから移動して折りたたまれます。 展開すると、**ナビゲーション** ウィンドウにタブのリストが表示されます。各タブをクリックすると、Cisco Cloud APIC コンポーネント ウィンドウ間を移動できる一連のサブタブが表示されます。

アイコン	説明
図 *2:* ナビゲーション ウィンドウ（展開） 	Cisco Cloud APIC コンポーネント ウィンドウは、**ナビゲーション** ウィンドウで次のように構成されています。 • **[ダッシュボード（Dashboard）]** タブ：Cisco Cloud APIC コンポーネントに関する概要情報を表示します。 • **[トポロジ（Topology）]** タブ：Cisco Cloud APIC に関するトポロジ情報を表示します。 • **[クラウド リソース（Cloud Resources）]** タブ： リージョン、VNET、ルータ、セキュリティ グループ（アプリケーション セキュリティ グループ/ネットワーク グループ）、エンドポイント、インスタンス、クラウド サービス（およびターゲット グループ）に関する情報を表示します。 • **[アプリケーション管理（Application Management）]** タブ：テナント、アプリケーション プロファイル、EPG、コントラクト、フィルタ、VRF、サービス グラフ、デバイス、およびクラウド コンテキスト プロファイルに関する情報を表示します。 • **[操作（Operations）]** タブ：イベント分析、アクティブ セッション、バックアップおよび復元ポリシー、テクニカル サポート ポリシー、ファームウェア管理、スケジューラ、およびリモート ロケーションに関する情報が表示されます。 • **[インフラストラクチャ（Infrastructure）]** タブ： システム設定、リージョン間接続、およびオンプレミス接続に関する情報が表示されます。、 • **[管理（Administrative）]** タブ：認証、イベント分析、セキュリティ、ローカルおよびリモート ユーザー、およびスマート ライセンスに関する情報が表示されます。 （注） これらのタブの内容の詳細については、システムの詳細の表示（193ページ） を参照してください。
図 *3:* 検索メニュー バー アイコン 	**[検索（Search）]** メニュー バー アイコンは、検索フィールドを表示します。このフィールドを使用すると、名前またはその他の特徴的なフィールドでオブジェクトを検索できます。

アイコン	説明
図 *4 :* インテント メニュー バー アイコン 	メニュー アイコンの **検索** アイコンと**フィードバック**アイコンの間に、**[インテント（Intent）]**アイコンが表示されます。 クリックすると、**[インテント（Intent）]** ダイアログが表示されます（以下を参照）。**[インテント（Intent）]** ダイアログでは、Cisco Cloud APIC GUI の任意のウィンドウからコンポーネントを作成できます。コンポーネントを作成または表示すると、ダイアログボックスが開き、**[インテント（Intent）]** アイコンが非表示になります。**[インテント（Intent）]** アイコンに再度アクセスするには、ダイアログボックスを閉じます。 コンポーネントの作成の詳細については、Cisco Cloud APIC コンポーネントの設定 （67 ページ） を参照してください。
図 *5 : [インテント（Intent）]* ダイアログボックス 	**[インテント（Intent）]**（何をしたいか？）ダイアログ ボックスには、検索ボックスとドロップダウン リストがあります。ドロップダウン リストを使用すると、特定のオプションを表示するためのフィルタを適用できます。検索ボックスでは、フィルタリングされたリストを検索するためのテキストを入力できます。
図 *6 :* フィードバック アイコン 	**フィードバック** アイコンは、メニューバーの**インテント** アイコンと**ブックマーク** アイコンの間に表示されます。 クリックすると、**フィードバック**パネルが表示されます。
図 *7 :* ブックマーク アイコン 	**ブックマーク** アイコンは、**フィードバック**と**システム ツール** アイコンの間にあるメニュー バーに表示されます。 クリックすると、現在のページがシステム上でブックマークされます。
図 *8 :* システム ツール メニュー バー アイコン 	**システム ツール**のメニュー バー アイコンには、次のオプションがあります。 • **概要（About）** ：Cisco Cloud APIC のバージョンを表示します。 • **オブジェクト ストア ブラウザ**—管理対象オブジェクト ブラウザ (バイザー) を開きます。これは Cisco Cloud APIC に組み込まれているユーティリティで、管理対象オブジェクトを (MO) をブラウザによりグラフィカルに表示します。

アイコン	説明
図 *9 :* ヘルプ メニュー バー アイコン 	**[ヘルプ（Help）]** メニュー バー アイコンには、**[クラウド APIC について（About Cloud APIC）]** メニュー オプションが表示され、クラウド APIC のバージョン情報が提供されます。**[ヘルプ（Help）]** メニュー バー アイコンには、**[ヘルプ センター（Help Center）]**および **[ようこそ画面（Welcome Screen）]** メニュー オプションも表示されます。
図 *10 : [*ユーザー プロファイル（***User Profile***）*]*メニュー バー アイコン 	**ユーザー プロファイル** のメニュー バー アイコンには、次のオプションがあります。 • **[ユーザー設定（User Preferences）]** : 時刻形式（ローカルまたは UTC）を設定し、ログイン時にウェルカム画面を有効または無効にすることができます。 • **[パスワードの変更（Change Password）]** : パスワードを変更できます。 • **[SSH キーの変更（Change SSH Key）]** : SSH キーを変更できます。 • **[ユーザー証明書の変更（Change User Certificate）]** : ユーザー証明書を変更できます。 • **[ログアウト（Logout）]** : GUI からログアウトできます。



第 3 章

Cisco Cloud APIC ポリシー モデル

ACI ポリシー モデルの概要

ACI ポリシー モデルにより、アプリケーション要件のポリシーの指定を有効化します。Cisco Cloud APIC は、クラウド インフラストラクチャにポリシーを自動的にレンダリングします。ユーザーまたはプロセスがクラウドインフラストラクチャ内のオブジェクトへの管理上の変更を開始すると、Cisco Cloud APIC は最初にポリシー モデルにその変更を適用します。このポリシー モデルの変更により、実際の管理対象項目への変更がトリガーされます。この方法を、モデル方式フレームワークといいます。

ポリシー モデルの主な特性

ポリシー モデルの主な特性には次のものがあります。

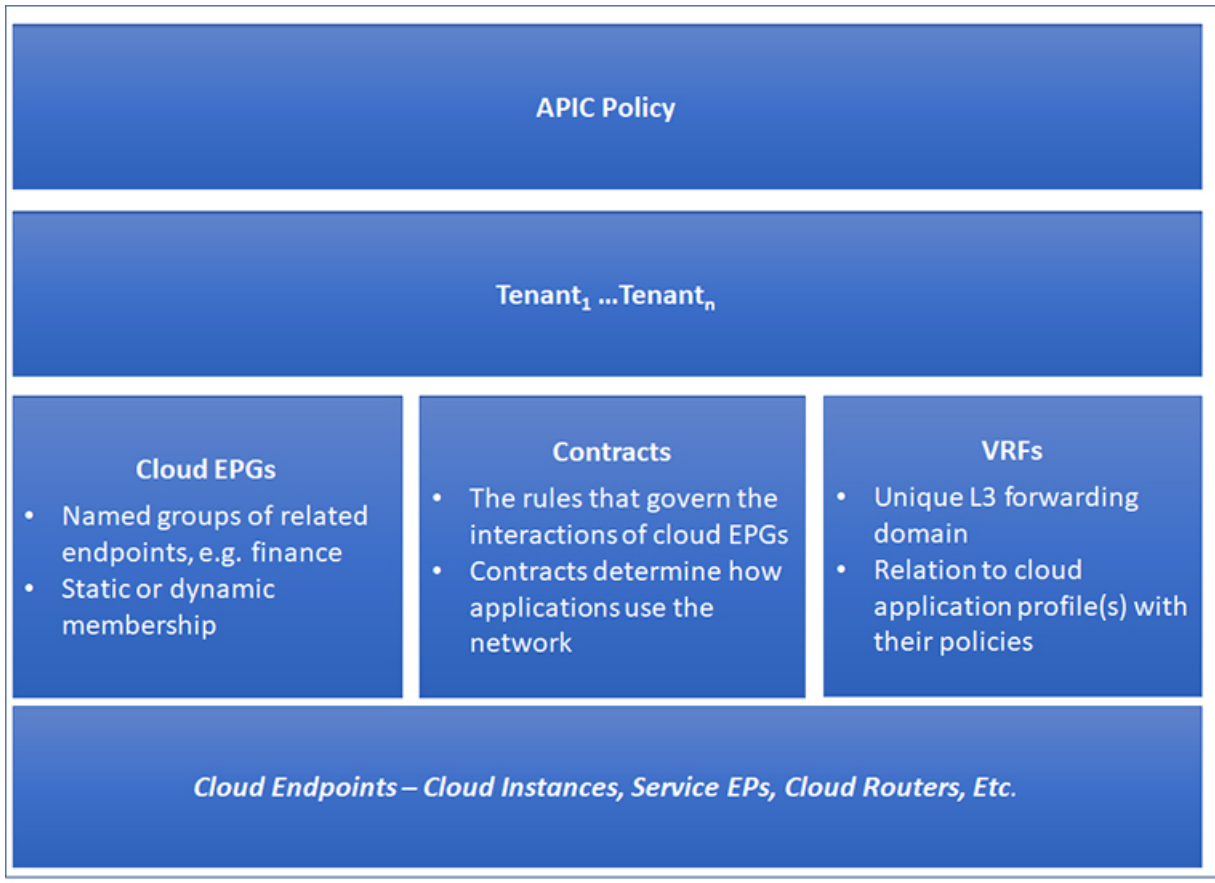
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシーモデルが更新されるまで、新たに接続されたエンドポイントとの通信を禁止します。
- ネットワーク管理者は、論理システムリソースを直接構成しません。代わりに、システム動作のさまざまな側面を制御する論理（ハードウェアに依存しない）構成とCisco Cloud APIC ポリシーを定義します。

モデル内の管理対象オブジェクトを操作することで、エンジニアは独立した個々のコンポーネントの構成を管理することから開放されます。これらの特性により、自動化と柔軟なワークロードのプロビジョニングが可能になり、インフラストラクチャ内のワークロードをどこでも検索できるようになります。ネットワーク接続されたサービスは簡単に展開でき、Cisco Cloud APIC により自動化フレームワークが提供され、それらのネットワーク接続されたサービスのライフサイクルを管理できます。

論理構造

ポリシーモデルは、インフラストラクチャ、認証、セキュリティ、サービス、アプリケーション、診断など、クラウドインフラストラクチャ全体を管理します。ポリシー モデルの論理構造は、クラウドインフラストラクチャの機能のニーズをクラウドインフラストラクチャがどのように満たすかを定義します。次の図は、ACI ポリシー モデルの論理構造の概要を示します。

図 *11 : ACI* ポリシー モデルの論理構造の概要



クラウドインフラストラクチャ全体またはテナントの管理者は、アプリケーションまたは共有リソースの要件を含む事前定義されたポリシーを作成します。これらのポリシーは、アプリケーション、ネットワーク接続サービス、セキュリティ ポリシー、およびテナント サブネットのプロビジョニングを自動化し、管理者をインフラストラクチャの構成要素ではなくアプリケーションの観点から、リソース プールにアプローチするポジションにします。アプリケーションは、ネットワーキングの動作を誘導する必要があり、その逆ではありません。

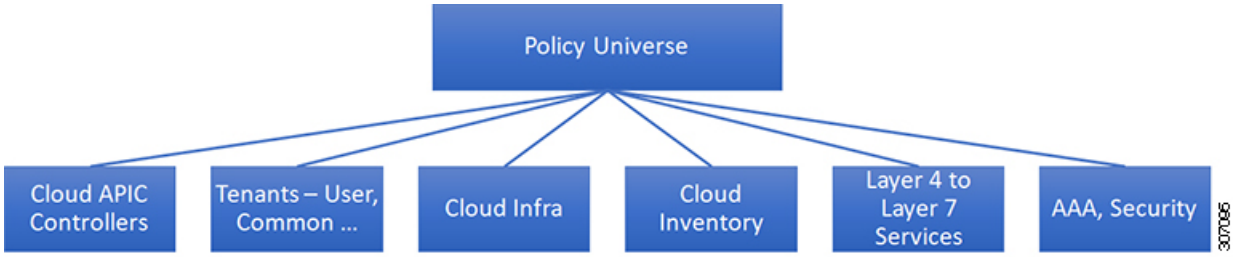
Cisco ACI ポリシー管理情報モデル

クラウドインフラストラクチャは、階層型管理情報ツリー（MIT）で表示できる管理情報モデル（MIM）に記録される論理コンポーネントから構成されます。Cisco Cloud APIC は、情報モデルを保存および管理するプロセスを実行します。OSI 共通管理情報プロトコル（CMIP）および他の X.500 バリアントと同様に、Cisco Cloud APIC によって、MIT の階層構造内のオブジェクトの場所に応じて継承できるオブジェクトのプロパティとして管理可能な特性を示すことにより、管理対象リソースの制御が可能になります。

ツリーの各ノードは、管理対象オブジェクト（MO）またはオブジェクトのグループを表します。MO は、クラウドインフラストラクチャ リソースの抽象化です。MO は、クラウド ルー

ター、アダプターなどの具象オブジェクト、またはアプリケーションプロファイル、エンドポイント グループ、クラウド エンドポイントまたは障害などの論理オブジェクトを表すことができます。次の図は、MIT の概要について説明します。

図 *12 : Cisco ACI* ポリシー管理情報モデルの概要



階層構造は、最上位（ルート）でポリシー ユニバースから始まり、親と子ノードが含まれます。ツリー内の各ノードはMOで、クラウドインフラストラクチャ内の各オブジェクトには、オブジェクトを説明しツリー内の場所を検索する一意な識別名（DN）があります。

次の管理対象オブジェクトには、システムの動作を管理するポリシーが含まれます。

- テナントは、ポリシーのコンテナで、管理者はロールベースのアクセス コントロールを実行できます。システムにより、次の 4 種類のテナントが提供されます。
  - 管理者は、ユーザーのニーズに応じてユーザテナントを定義します。アプリケーション、データベース、Web サーバ、ネットワークアタッチド ストレージ、仮想マシンなどのリソースの動作を管理するポリシーが含まれます。
  - システムは共通テナントを提供しますが、クラウドインフラストラクチャ管理者が設定できます。ファイアウォール、ロードバランサ、レイヤ4～レイヤ7サービス、侵入検知アプライアンスなど、すべてのテナントにアクセス可能なリソースの動作を管理するポリシーが含まれます。

（注） Cisco Application Policy Infrastructure Controller（APIC）リリース 4.1(1) の時点で、Cisco Cloud APIC は、レイヤ 4 からレイヤ 7 のサービスとしてロード バランサのみをサポートしています。

  - インフラストラクチャ テナントは、システムによって提供されますが、クラウド インフラストラクチャの管理者が設定できます。インフラストラクチャ リソースの動作を管理するポリシーが含まれます。また、ファブリック プロバイダーはリソースを 1 つ以上のユーザ テナントに選択的に展開できます。インフラストラクチャ テナント ポリシーは、クラウド インフラストラクチャ管理者によって構成可能です。

- クラウドインフラ ポリシーを使用すると、Cisco Cloud APIC を設定するときに、オンプレミスおよびリージョン間接続を管理できます。詳細については、『*Cisco Cloud APIC Installation Guide*』を参照してください。

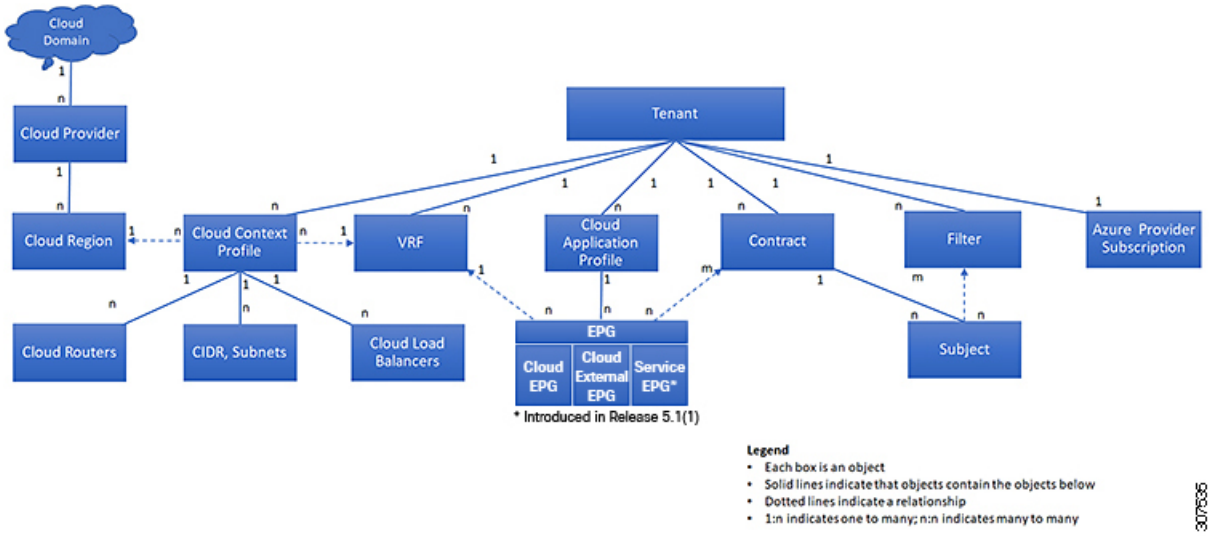
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ4～レイヤ7のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、レイヤ4からレイヤ7サービスの展開 （209ページ）を参照してください。
- アクセス、認証、およびアカウンティング（AAA）ポリシーは、Cisco Cloud ACI クラウド インフラストラクチャのユーザー権限、ロール、およびセキュリティ ドメインを管理します。詳細については、Cisco Cloud APIC セキュリティ （315ページ）を参照してください。

階層型ポリシー モデルは、REST API インターフェイスとうまく適合します。呼び出されると、API は MIT 内のオブジェクトで読み取りまたは書き込みを行います。URL は、MIT 内のオブジェクトを識別する識別名に直接マッピングします。MIT 内のデータは、XML または JSON でエンコードされた自己完結型の構造化ツリーテキスト ドキュメントとして説明できます。

テナント

テナント(`fvTenant`)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。次の図は、管理情報ツリー(MIT)のテナント部分の概要を示します。

図 *13 :* テナント



テナントは相互に分離することも、リソースを共有することもできます。テナントに、フィルタ、コントラクト、Virtual Routing and Forwarding（VRF）インスタンス、クラウド コンテキスト プロファイル、Azure プロバイダ構成、およびエンドポイント グループ（EPG）を含むクラウドアプリケーション プロファイルが含まれるプライマリ要素です。テナントのエンティティはそのポリシーを継承します。VRF はコンテキストとも呼ばれ、それぞれを複数のクラウド コンテキスト プロファイルに関連付けることができます。クラウド コンテキスト プロファイルは、VRF、テナント、およびリージョンとともに、Azure のリソース グループを表します。VNET は、VRF 名に基づいてリソース グループ内に作成されます。

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す。クラウド インフラストラクチャには、複数のテナントを含めることができます。レイヤ 4 ～ 7 のサービスを展開する前に、テナントを設定する必要があります。ACI クラウド インフラストラクチャは、テナント ネットワークに対して IPv4 およびデュアル スタック構成をサポートします。

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 および Cisco Cloud APIC コンポーネントのマッピング （31 ページ）
- Azureサブスクリプションについて （31 ページ）
- テナントとアイデンティティについて （31 ページ）

Azure および Cisco Cloud APIC コンポーネントのマッピング

Cisco Cloud APIC で、各 Azure リソース グループは 1 つの Cisco Cloud APIC テナントにマッピングされ、1 つの Cisco Cloud APIC 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 APIC 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 APIC 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 APIC 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） リリース5.2（1）より前のリリースでは、管理対象アイデンティティのみがインフラテナントのアクセスタイプとしてサポートされ、管理対象アイデンティティとサービスプリンシパルの両方がユーザテナントのアクセスタイプとしてサポートされていました。

リリース5.2（1）以降、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るようになりました。

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

管理対象アイデンティティを使用してCisco Cloud APICのテナントを構成する場合、Azureポータルおよび Cisco Cloud APIC 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。

2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するとき **[管理対象アイデンティティ（Managed Identity）]** オプションを選択します。

これらの設定の詳細については、Cisco Cloud APIC GUIを使用したテナントの作成 （67 ページ） を参照してください。

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 プリンシパルを使用して Cisco Cloud APIC でテナントを構成する場合は、Azure ポータルと Cisco Cloud APIC 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。
2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するときに、**サービス プリンシパル**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。

これらの設定の詳細については、Cisco Cloud APIC GUIを使用したテナントの作成 （67 ページ） を参照してください。

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。

共有テナントとして Cisco Cloud APIC でテナントを構成する場合は、Azure ポータルと Cisco Cloud APIC 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 APIC では、Cisco Cloud APIC でテナントを構成するときに **[共有]** オプションを選択します。

これらの設定の詳細については、Cisco Cloud APIC GUIを使用したテナントの作成 （67 ページ） を参照してください。

クラウド コンテキスト プロファイル

クラウド コンテキスト プロファイルには、以下の Cisco Cloud APIC コンポーネントに関する詳細が含まれます。

- CIDR
- VRF
- EPG
- [Regions]
- 仮想ネットワーク
- ルータ
- エンドポイント

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 APIC ソリューションには 2 つの CCR が必要です。

Cisco Cloud APIC で使用された CCR のタイプは、リリースによって異なります。

- リリース 25.2(3) よりも前のリリースでは、**Cisco Cloud Services Router 1000v** が Cisco Cloud APIC で使用されるCSRです。この CCR のタイプに関する詳細は、『Cisco Cloud Services Router 1000v マニュアル』を参照してください。
- リリース 25.0(3) 以降については、**Cisco Catalyst 8000V** が Cisco Cloud APIC で使用されます。この CCR のタイプに関する詳細は、『Cisco Catalyst 8000V Edge ソフトウェア マニュアル』を参照してください。

Cisco Catalyst 8000V について

リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。以下は、Cisco Catalyst 8000V に固有の更新です。

- ライセンス （34 ページ）
- スループット （34 ページ）

ライセンス

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、スループット （34 ページ） を参照してください。

Cisco Cloud APIC 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。

スループット

Cisco Catalyst 8000V は、ティアベース（T0/T1/T2/T3）のスループット オプションをサポートしています。次の表に、シスコ クラウド サービス ルータ 8000v のさまざまなルータ スループット設定に必要な Azure VM のサイズを示します。

CCR スループット	Azure VMサイズ
T0（最大 15M のスループット）	DS3_v2
T1（最大 100M のスループット）	DS3_v2

CCR スループット	Azure VMサイズ
T2（最大 1G のスループット）	DS3_v2
T3（最大 10G のスループット）	F16s_v2

Tier2（T2）は、Cisco Cloud APIC でサポートされるデフォルトのスループットです。

次の表は、アップグレード中の古い Cisco Cloud Services Router 1000v ルータから新しい Cisco Catalyst 8000V ルータへのスループットのマッピングを示しています。

Cisco クラウド サービス ルータ 1000v	Cisco Catalyst 8000V のスループット
10 M	T0 (最大 15M のスループット)
5,000 万人	T1（最大 100M のスループット）
1 億	T1 (最大 100M のスループット)
2 億 5000 万	T2 (最大 1G のスループット)
5 億	T2（最大 1G のスループット）
1G	T2 (最大 1G のスループット)
2.5G	T3 (最大 10G のスループット)
5G	T3 (最大 10G のスループット)
7.5G	T3（最大 10G のスループット）
10G	T3 (最大 10G のスループット)

CCR の数を変更する

リリース 5.1(2) 以降、リージョンごとにサポートされる CCR の最大数は 4 から 8 に増加しました。これらの手順では、CCR の数を 4 より増やすか、必要に応じて CCR の数を 4 に戻す手順を示します。

次のことに注意。

- 2 ～ 4 CCR の範囲で CCR の数を増減する場合は、これらの手順を使用する必要はありません。これらの手順は、CCR の数を 4 以上に増やす場合、または 5 ～ 8 の範囲から CCR の数を 減らす場合にのみ使用してください。
- CCR の数を変更すると、最大 30 分間、トラフィックに影響を与える可能性があります。

ステップ 1 すべてのインフラ クラウド コンテキスト プロファイルで、ローカル レベルで Azure VNet ピアリングを無効にします。

a) **[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ページに移動します。

[アプリケーション管理（Application Management）] > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**

b) インフラ クラウド コンテキスト プロファイルの **[名前（Name）]** 列の下にあるリンクをクリックします。

このクラウドコンテキストプロファイルの詳細を示すパネルが、ウィンドウの右側からスライドします。

c) [詳細（Details）] アイコンをクリックします（）。

このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。

d) ウィンドウの右上隅の鉛筆アイコンをクリックします。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

e) **[ハブ ネットワーク ピアリング（Hub Network Peering）]** フィールドのチェックを外します（無効にします）。

f) 設定が終わったら [Save] をクリックします。

これらの手順を繰り返して、すべてのインフラ クラウド コンテキスト プロファイルで Azure VNet ピアリングを無効にします。

ステップ 2 CCR の数を 4 より増やす場合は、必要に応じて、追加の CCR 用にサブネット プールを追加します。

CCR の数を 4 より大きくしようとするとエラー メッセージが表示され、システムは追加のサブネット プールが必要であると判断します。

a) Cloud APIC GUI で、インテント アイコン（）をクリックし、**[cAPIC Setup]** を選択します。

b) **[リージョン管理（Region Management）]** エリアで、**[設定の編集（Edit Configuration）]** をクリックします。

c) **[管理するリージョン（Regions to Manage）]** ウィンドウで **[次へ（Next）]** をクリックします。

[一般接続（General Connectivity）] ウィンドウが表示されます。

d) **[全般（General）]** 領域の **[クラウド ルータのサブネット プール（Subnet Pools for Cloud Routers）]** フィールドで、CCR のサブネットを追加する場合は、**[クラウド ルータのサブネット プールの追加（Add Subnet Pool for Cloud Routers）]** をクリックします。

このサブネットプールのアドレスは、クラウドAPICで管理する必要がある追加のリージョンのリージョン間接続に使用されます。これはマスク /24 の有効な Ipv4 サブネットである必要があります。

ステップ 3 CCR の数を 4 より増やすか、CCR の数を 5 ～ 8 の範囲から減らします。

a) クラウド APIC GUI で、[インターネット（Intent）]アイコン（）をクリックし、**[cAPIC セットアップ（cAPIC Setup）]** を選択します。

b) **[リージョン管理（Region Management）]** エリアで、**[設定の編集（Edit Configuration）]** をクリックします。

[管理するリージョン（Regions to Manage）] ウィンドウが表示されます。

c) **[次へ（Next）]** をクリックして、以前に選択したリージョンと CCR をそのままにします。

[一般接続（General Connectivity）] ウィンドウが表示されます。

d) General Connectivity ウィンドウで CCR 領域を見つけ、Number of Routers Per Region フィールドで、必要な変更を加えて CCR の数を増減します。

e) **[次へ（Next）]** をクリックし、次のページに必要な情報を入力して、**[保存して続行（Save and Continue）]** をクリックします。

CCR の追加または削除プロセスは、およそ 30 分ほどかかる場合があります。

ステップ 4 すべてのインフラ クラウド コンテキスト プロファイルで、ローカル レベルで Azure VNet ピアリングを再度有効にします。

a) **[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ページに移動します。

[アプリケーション管理（Application Management）] > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**

b) インフラ クラウド コンテキスト プロファイルの **[名前（Name）]** 列の下にあるリンクをクリックします。

このクラウド コンテキスト プロファイルの詳細を示すパネルが、ウィンドウの右側からスライドします。

c) [詳細（Details）] アイコンをクリックします（  ）。

このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。

d) ウィンドウの右上隅の鉛筆アイコンをクリックします。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

e) **[ハブ ネットワーク ピアリング（Hub Network Peering）]** フィールドをチェック（有効）します。

f) 設定が終わったら [Save] をクリックします。

これらの手順を繰り返して、すべてのインフラ クラウド コンテキスト プロファイルで Azure VNet ピアリングを有効にします。

Cisco Cloud APIC および CCR 向けプライベート IP アドレス サポート

リリース 5.1(2) 以前、Cisco Cloud Router (CCR) インターフェイスは、Cloud APIC によってパブリックおよびプライベート IP アドレス両方を割り当てられていました。リリース 5.1(2) 以降、CCR インターフェイスはプライベート IP アドレスのみが割り当てられ、パブリック IP アドレスを CCR インターフェイスに割り当てることはオプションとなりました。プライベート IP アドレスは、常に CCR のすべてのインターフェイスに割り当てられます。GigabitEthernet1 noプライベート IP CCR にプライベート IP アドレスが割り当てられている場合、エクスプレス ルートを介したオンプレミスの ACI サイトを持つ Hcloud がサポートされます。CCR のプライベー

トIPを有効にするには、Cisco Cloud APIC GUI を使用したリージョンの管理（クラウド テンプレートの設定） （169 ページ） の手順を参照してください。

リリース 5.1(2) 以前、クラウド APIC の管理インターフェイスは、パブリック IP アドレスおよびプライベート IP アドレスが割り当てられていました。リリース 5.1(2) 以降、プライベート IP アドレスは Cisco Cloud APIC の管理インターフェイスに割り当てられ、パブリック iP アドレスの割り当てはオプションです。Cloud APIC のプライベート IP を有効にするには、『*Azure* 内での *Cisco Cloud APIC* 展開インストール ガイド』の「*Azure* 内での *Cloud APIC* の展開」手順を参照してください。

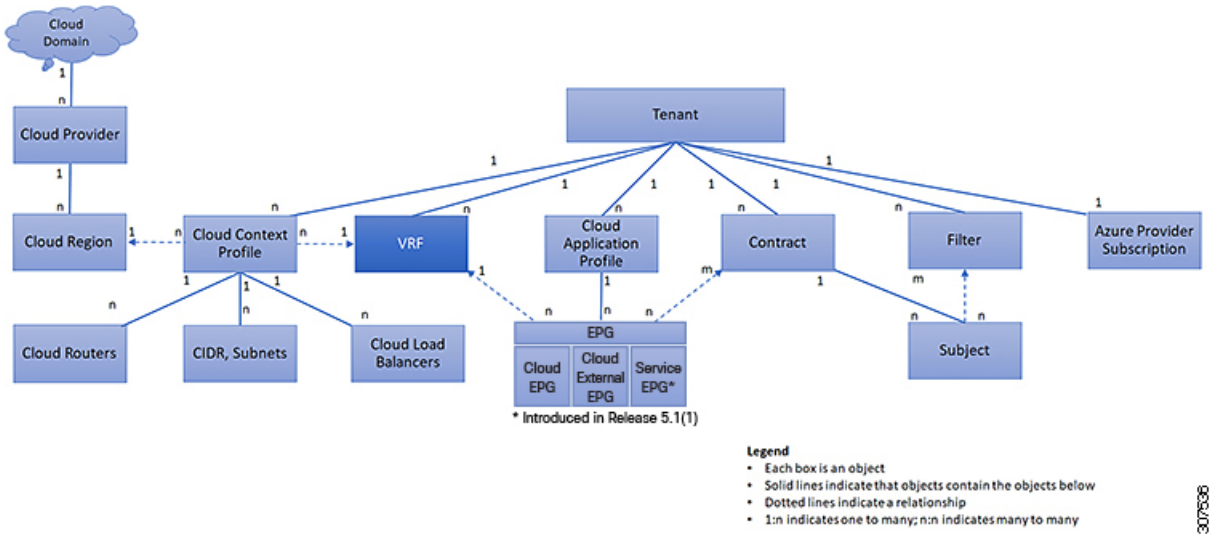
プライベート IP アドレスを使用した CCR の制限：

- サイト間通信には IPsec が必要なため、マルチクラウド展開はサポートされていません。

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 ネットワーク（Cisco Cloud APIC GUIではVRF）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。

図 *14 : VRF*



VRF は、レイヤ 3 のアドレス ドメインを定義します。1 つ以上のクラウド コンテキスト プロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウド コンテキスト プロファイルは 1 つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイス クラ

スタの選択基準ポリシーを提供する論理デバイスの VRF を作成できます。論理デバイスは、コントラクト名、グラフ名、またはグラフ内の関数ノード名に基づいて選択できます。

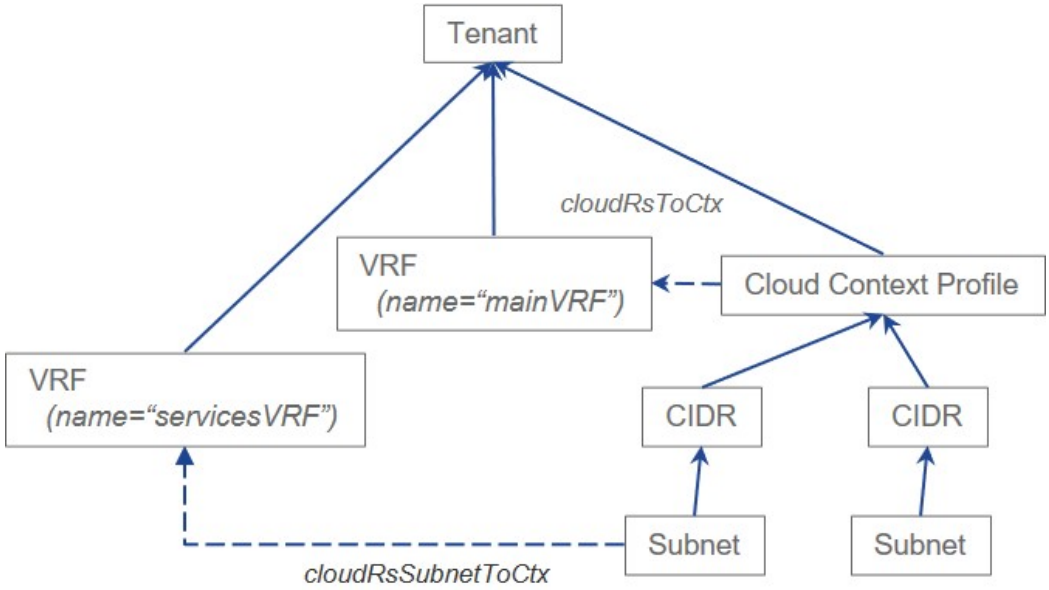
単一 VNet での複数の VRF のサポート

単一 VNet の下で複数の VRF がサポートされるようになりました。

複数の VRF に切り分けることができるインフラ（ハブ）VNet（インフラ テナントの `cloudCtxProfile`）を持つことができます。それぞれの VRF のすべてのサブネットは、VRF 分離のためにクラウド内に個別のルート テーブルを持ちます。

また、インフラ VNet を超えて複数の VRF を分割して、単一の VNet に複数の VRF が存在する場合、任意の VNet を同じテナントの下の複数の VRF に分割できるようにすることもできます。これは、クラウド サービス アクセスなど、特定の VNet 内に複数のネットワーク（VRF）を分割し、クラウドの VNet 内の各 VRF に固有のルート テーブルを用意することで個別のルーティングを行う必要がある場合に役立ちます。

次の図は、同じテナント（VNet）の下に複数の VRF がある管理対象オブジェクト（MO）関係ツリーの例を示しています。



この例では、同じテナント（VNet）の下に 2 つの VRF が存在します。

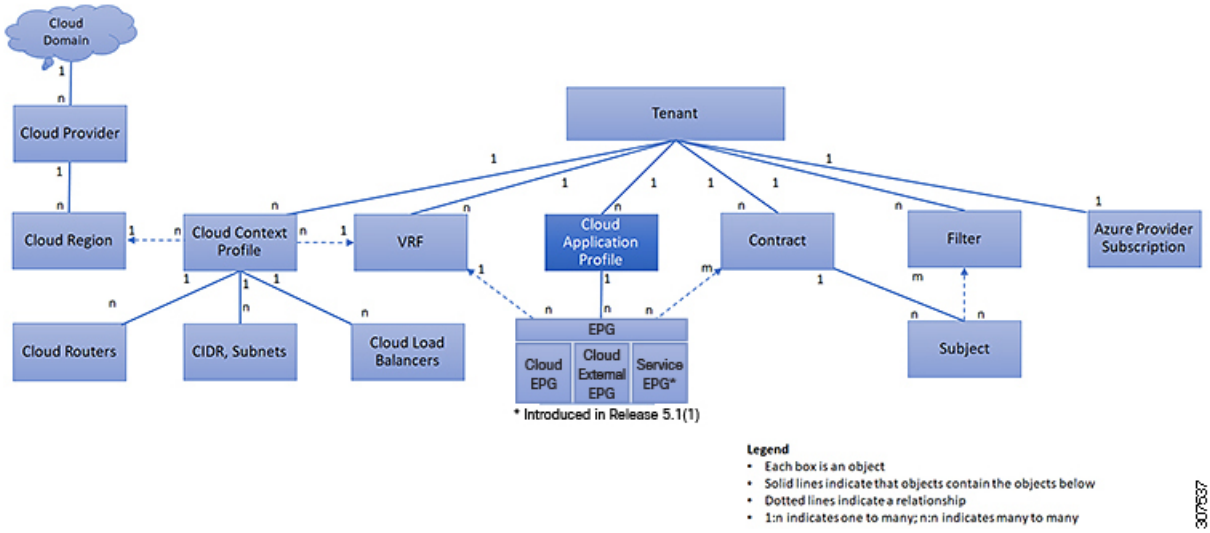
- `mainVRF` という名前のプライマリ VRF
- 名前が `servicesVRF` のセカンダリ VRF

2 番目の CIDR ブロックとサブネットは、同じテナント（VNet）の下の同じクラウド コンテキスト プロファイルに存在しますが、その 2 番目の CIDR ブロックとサブネットは、その同じ VNet 内のセカンダリ VRF に関連付けられています。

クラウド アプリケーション プロファイル

クラウド アプリケーション プロファイル (cloudAp) は、ポリシー、サービスおよび EPG 間の関係を定義します。次の図は、管理情報ツリー（MIT）内のクラウド アプリケーション プロファイルの場所と、テナント内の他のオブジェクトとの関係を示します。

図 *15*: クラウド アプリケーション プロファイル



クラウド アプリケーション プロファイルには、1 つ以上のクラウド EPG が含まれます。最新のアプリケーションには、複数のコンポーネントが含まれます。たとえば、e-コマース アプリケーションには、Web サーバ、データベース サーバ、ストレージ サービス内にあるデータ、および金融取引を可能にする外部リソースへのアクセスが必要となる場合があります。クラウド アプリケーション プロファイルには、アプリケーションの機能の提供に論理的に関連する必要な数の（またはそれ以下の）クラウド EPG が含まれます。

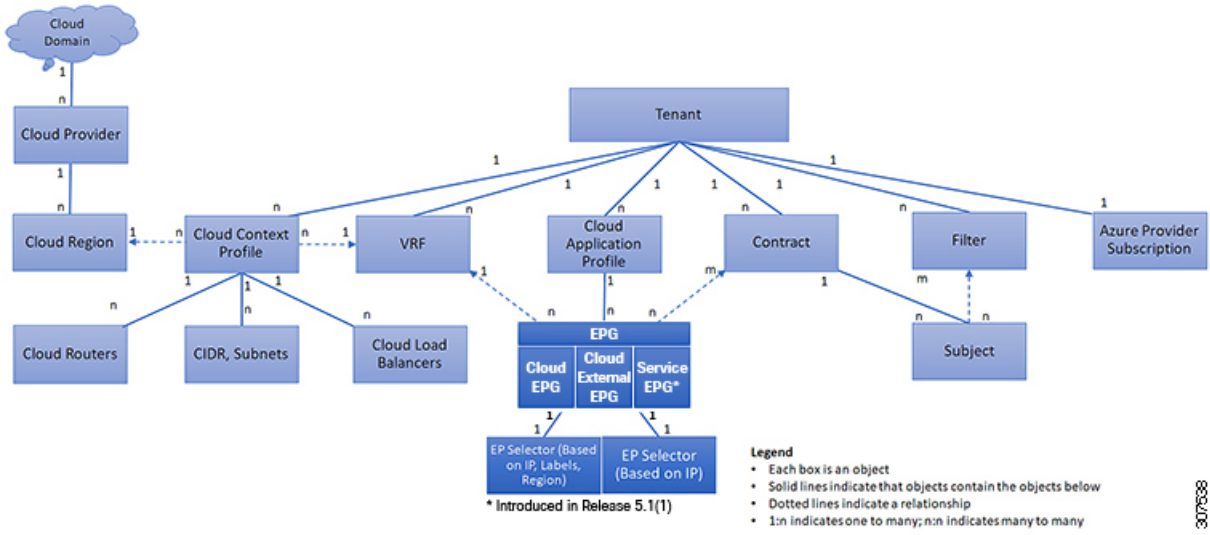
クラウド EPG は次のいずれかに従って組織化できます。

- 提供するアプリケーション（DNS サーバや SAP アプリケーションなど）（『*Cisco APIC REST API Configuration Guide*』の「*Tenant Policy Example*」を参照）。
- 提供する機能（インフラストラクチャなど）
- データセンターの構造内の場所（DMZ など）
- クラウドインフラストラクチャまたはテナントの管理者が使用することを選択した組織化の原則

クラウド エンドポイント グループ

クラウド エンドポイント グループ（クラウド EPG）は、ポリシー モデルの最も重要なオブジェクトです。次の図は、管理情報ツリー（MIT）内のアプリケーション クラウド EPG の場所とテナント内の他のオブジェクトとの関係を示します。

図 *16*：クラウド エンドポイント グループ



クラウド 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、ネットワークに接続されるデバイスです。エンドポイントは、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）を持ち、仮想です。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。クラウド 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、ストレージサービス、またはクライアントが含まれます。クラウド 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。

ACI クラウド インフラストラクチャには、次のタイプのクラウド EPG を含めることができます

- クラウド エンドポイント グループ（`cloudEPg`）
- クラウド外部エンドポイント グループ（`cloudExtEPg`）
- クラウド サービス エンドポイント グループ（`cloudSvcEPg`）：リリース 5.1(2) で導入されました。詳細については、「クラウド サービス エンドポイント グループ （42 ページ）」を参照してください。

クラウド EPG には、セキュリティまたはレイヤ 4 からレイヤ 7 サービスなどの共通のポリシー要件を持つエンドポイントが含まれます。エンドポイントは個別に設定および管理されるのではなく、クラウド EPG 内に配置され、グループとして管理されます。

ポリシーはクラウド EPG に適用されます。個々のエンドポイントに適用されることは絶対にありません。

クラウド EPG の設定内容にかかわらず、含まれるエンドポイントにクラウド EPG ポリシーが適用されます。

クラウド インフラストラクチャへの WAN ルータ接続は、スタティック クラウド EPG を使用する設定の 1 つの例です。クラウド インフラストラクチャへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む `cloudExtEPg` クラウド EPG を管理者が設定します。クラウド インフラストラクチャは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通してクラウド EPG のエンドポイントについて学習します。エンドポイントを学習すると、クラウドインフラストラクチャは、それに基づいて `cloudExtEPg` クラウド EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション（`cloudEPg`）クラウド EPG 内でサーバとの TCP セッションを開始すると、`cloudExtEPg` クラウドEPG は、`cloudEPg` クラウド EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアント サーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、その WAN エンドポイントはもうクラウド インフラストラクチャ内に存在しません。

Cisco Cloud APIC はエンドポイントセレクタを使用して、エンドポイントをクラウド EPG に割り当てます。エンドポイント セレクタは、基本的に言って、Cisco ACI によって管理される Azure VNET に割り当てられたクラウド インスタンスに対して実行される一連のルールです。エンドポイント インスタンスに一致するエンドポイント セレクタ ルールは、そのエンドポイントをクラウド EPG に割り当てます。エンドポイント セレクタは、 Cisco ACI で使用可能な属性ベースのマイクロ セグメンテーションに似ています。

クラウド サービス エンドポイント グループ

リリース 5.1(2) で導入されたクラウド サービス EPG は、クラウド ネイティブまたはサードパーティのサービス インスタンスまたはエンドポイントのコレクション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。この場合、エンドポイントは特定のサービス インスタンスを指します。たとえば、SQL サーバはエンドポイントと見なされ、SQL サーバのコレクションはサービス エンドポイント グループを形成します。サービス EPG の他の例としては、ストレージ アカウントのコレクション、Key Vault のコレクションなどがあります。

サービス EPG には、いくつかの固有の属性があります。

- **サービス タイプ**：この属性は、グループ化されているクラウド サービスのタイプを示します。利用可能なサービスの種類の例には、**Azure SQL**、**Azure Containter Registery**、**Azure ApiManagement Services** などがあります。サービス タイプ **カスタム**は、サードパーティ サービス EPG を構成するときに使用されます。
- **展開タイプ**：この属性は、サービスを展開する方法と場所を示します。 以下は使用可能な展開タイプです。
  - **クラウド ネイティブ**：このタイプの展開では、サービスはクラウドプロバイダのネットワークでインスタンス化され、サービスを使用するユーザーまたはアプリケーションはサービスを管理します。たとえば、Azure ストレージ アカウントが Azure 独自の

VNet 内に存在する場合があり、ストレージ コンテンツにアクセスするための URL があります。

- **クラウド ネイティブ管理対象**：このタイプの展開では、サービスは VNet またはサブネットでインスタンス化されます（Cisco Cloud APIC を介して作成されます）。たとえば、Azure Kubernetes cluster (AKS) は、Cisco Cloud APIC によって管理されるサブネットに展開できます。
- **サードパーティ**：これは、サードパーティ（Azure 以外）が市場を通じてサービスを提供している展開です。このサービスへのアクセスは、プライベートリンク機能を通じて提供されます。

- **アクセス タイプ**：サービスへのアクセス方法を示します。使用可能なアクセス タイプは次のとおりです。
  - **パブリック**：サービスには、割り当てられたパブリック IP アドレスを使用してアクセスできます。特定のサービスのパブリック IP アドレス範囲へのアクセスは、NSG ルールの Azure「サービスタグ」を使用して行います。
  - **プライベート**：割り当てられているプライベート IP アドレスを使用して、サービスにアクセスできます。この割り当ては、展開が**クラウド ネイティブ**およびサードパーティの場合、プライベート エンドポイントの作成を通して行われます。**[クラウド ネイティブ管理対象（Cloud Native Managed）]** 展開の場合、プライベート IP はサービスによってサブネット IP スペースから割り当てられます。

前の箇条書きで説明したように、特定の展開タイプ、および各展開タイプ内の特定のアクセス タイプのみが各サービスの種類でサポートされます。次の表は、各サービスの種類でサポートされている展開の種類とアクセスの種類の詳細を示しています。

サービス タイプ（Service Type）	プロバイダー	展開タイプ/アクセス タイプ		
		クラウドネイティブ	クラウドネイティブ管理対象	サードパーティ製の
Azure Storage Blob	Microsoft.Storage	プライベート	なし	なし
Azure SQL	Microsoft.Sql	• パブリック • プライベート	なし	なし
Azure Cosmos DB	Microsoft.DocumentDB	• パブリック • プライベート	なし	なし
Azure Databricks	Microsoft.Databricks	パブリック	• プライベート • パブリックとプライベート	N/A

サービス タイプ（**Service Type**）	プロバイダー	展開タイプ/アクセス タイプ		
		クラウドネイティブ	クラウドネイティブ管理対象	サードパーティ製の
Azure Storage	Microsoft.ストレージ	• パブリック • プライベート	なし	なし
Azure Storage File	Microsoft.ストレージ	プライベート	なし	なし
Azure Storage Queue	Microsoft.Storage	プライベート	なし	なし
Azure Storage Table	Microsoft.Storage	プライベート	なし	なし
Azure Kubernetes Services (AKS)	Microsoft.ContainerService	プライベート	• プライベート • パブリックとプライベート	N/A
Azure Active Directory ドメイン サービス	Microsoft.AAD	パブリック	• プライベート • パブリックとプライベート	N/A
Azure Container Registry	Microsoft.ContainerRegistry	• パブリック • プライベート	なし	なし
Azure ApiManagement Services	Microsoft.ApiManagement	パブリック	• プライベート • パブリックとプライベート	N/A
Azure Key Vault	Microsoft.KeyVault	• パブリック • プライベート	なし	なし
Redis キャッシュ	Microsoft.Cache	N/A	• プライベート • パブリックとプライベート	N/A
カスタムサービス		• パブリック • プライベート	N/A	プライベート

- **サービス エンドポイント セレクタ**：サービス エンドポイントは、既存のセレクタ（クラウド EPG 選択で使用される）と、以下にリストされている新しいタイプのセレクタを使用して選択できます。
  - **リソース名**：サービス リソースの名前
  - **リソース ID**：リソースのクラウド プロバイダの ID
  - **URL**：サービスを識別するエイリアスまたは FQDN（プライベート リンク エイリアスは Azure で使用されます）

次の表に、各展開の種類でサポートされているエンドポイント セレクタの詳細を示します。

（注） クラウド ネイティブ（パブリック）展開タイプに関する情報は、次の表に記載されていません。展開タイプがエンドポイント セレクタをサポートしていないためです。

展開タイプ	タグ	リージョン	IP	Resource Name	リソースID	URL
クラウドネイティブ（プライベート）	Y	Y	N	Y	Y	N
クラウド ネイティブ管理対象	N	N	Y	N	N	N
サードパーティ製の	N	N	N	N	N	Y（プライベート リンク接続にのみ適用）

クラウド サービス EPG の注意事項および制限事項

クラウド サービス EPG を構成している場合は、**サブネットごとの NSG** 構成を有効にする必要があります。詳細については、「セキュリティ グループ （50 ページ）」を参照してください。

サービス タイプについて

特定のサービス タイプに固有の追加情報を以下に示します。

- Azure Storage （46 ページ）
- Azure ApiManagement サービス （47 ページ）
- Azure Databricks サービス （47 ページ）
- Azure Active Directory ドメイン サービス （47 ページ）

- Azure Kubernetes サービス （47 ページ）
- Azure Redis キャッシュ （48 ページ）

Azure Storage

Azure Storage サービス タイプは、次の 4 つのサブタイプに分類できる一般的なサービス タイプです。

- BLOB
- ファイル
- テーブル
- キュー

一般的な Azure Storage サービス タイプを使用して、次の値でサービス EPG を構成する場合：

- **サービス タイプ**：`Azure Storage`
- **展開タイプ**：`Cloud Native`
- **アクセス タイプ**：`Private`

次に 4 つのプライベート エンドポイントが、上記の 4 つのサブタイプのそれぞれに対して 1 つ、このサービス EPG に対して自動的に構成されます。

ただし、より具体的な Azure Storage サービス タイプを使用して、次の値でサービス EPG を構成する場合は、次のようにします。

- **サービス タイプ**：これらのサービス タイプのうち 1 つ：
  - `Azure Storage Blob`
  - `Azure Storage File`
  - `Azure Storage Table`
  - `Azure Storage Queue`
- **展開タイプ**：`Cloud Native`
- **アクセス タイプ**：`Private`

次に、このサービス EPG のこの特定のサブタイプに対して、1 つのプライベート エンドポイントのみが自動的に構成されます。

展開タイプ `[クラウド ネイティブ（Cloud Native）]` でアクセス タイプ `[パブリック（Public）]` がある場合、特定の 4 つの Azure ストレージ サブタイプ（`Blob`、`File`、`Table`、`Queue`）は許可されないことに注意してください。これは、Azureサービスタグがストレージサブタイプ固有ではないためです。

Azure ApiManagement サービス

Azure ApiManagement (APIM) サービス インスタンスを VNet に展開するには、他の多くの Azure サービスにアクセスできる必要があります。これを行うには、このアクセスを許可するセキュリティ グループ ルールをプログラムする必要があります。

Cisco Cloud APIC はこれを自動化し、ここにリスト化されているルールを設定します。

https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet#-common-network-configuration-issues

Azure Databricks サービス

Azure Databricks には、次のものが必要です。

- 他のサービスへのアクセス
- サブネットが Microsoft に委任されている展開用の 2 つのサブネット

Azure Databricks の場合、次の構成を行います。

- サービス EPG を構成する前に、Azure Databricks サービス専用に 2 つのサブネットを構成する必要があります。
- サービス EPG を構成するときは、2 つのサービス サブネットを一致させるために使用される 2 つのサービス エンドポイント セレクタ作成する必要があります。

構成されたエンドポイント セレクタを介して Azure Databricks サービス EPG でサブネットが識別されると、Cisco Cloud APIC はサブネットを Azure に委任し、ここにリスト化されているルールを構成します。

https://docs.microsoft.com/en-us/azure/databricks/administration-guide/cloud-configurations/azure/vnet-inject

Azure Active Directory ドメイン サービス

Azure Active Directory Domain Services (ADDS) には、次のものが必要です。

- 他のサービスへのアクセス
- サブネットが展開されているときに、ルーティング テーブルがサブネットにアタッチされていません

サブネットからルーティング テーブルの関連付けを解除するアクションは、サービス EPG を構成した後、ADDS を展開する前に、Azure portal を介して実行する必要があります。展開が完了したら、ルーティング テーブルをサブネットに接続できます。

Cisco Cloud APIC は、ここにリストされているルールのプログラミングを自動化します。

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/network-considerations

Azure Kubernetes サービス

Azure Kubernetes Services (AKS) には、他のサービスへのアクセスが必要です。

Cisco Cloud APIC は、ここにリストされているルールのプログラミングを自動化します。

https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic#required-outbound-network-rules-and-fqdns-for-aks-clusters

AKS サービス EPG の構成例については、サービス EPG 構成例 （371 ページ） を参照してください。

Azure Redis キャッシュ

Azure Redis キャッシュには、他のサービスへのアクセスが必要です。

Cisco Cloud APIC は、ここにリストされているルールのプログラミングを自動化します。

https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-how-to-premium-vnet#outbound-port-requirements

展開タイプについて

特定の展開タイプに固有の追加情報を以下に示します。

- クラウドネイティブ （48 ページ）
- クラウド ネイティブ管理対象 （49 ページ）

クラウドネイティブ

このタイプの展開では、サービスはクラウド プロバイダのネットワークでインスタンス化され、サービスを使用するユーザーまたはアプリケーションはサービスを管理します。たとえば、Azure ストレージ アカウントが Azure 独自の VNet 内に存在する場合があり、ストレージ コンテンツにアクセスするための URL があります。

次に、クラウド ネイティブ展開タイプのサービス EPG の例を示します。

- **サービス タイプ**：Azure SQL
- **展開タイプ**：クラウド ネイティブ
- **アクセス タイプ**：プライベート

このサンプル シナリオでは、この順番で次の構成を行います。

1. Cisco Cloud APIC GUI で、Azure SQL サービス EPG によって使用されるクラウド コンテキスト プロファイルにプライベート リンク ラベルを作成します。

   Cisco Cloud Network Controller GUI を使用したクラウド コンテキスト プロファイルの作成（133 ページ）の手順を実行します。Azure SQL サービス EPG（`SQL-PLL` など）で使用されるプライベート リンク ラベルを構成します。

2. Cisco Cloud APIC GUI で、サービス タイプ Azure SQL のサービス EPG を作成します。

   次のパラメータを使用して、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） の手順に従います。

- **サービス タイプ**：Azure SQL
- **展開タイプ**：クラウド ネイティブ
- **アクセス タイプ**：プライベート

このタイプのサービス EPG を構成するプロセスの一部としてエンドポイント セレクタを構成する場合は、SQL サーバの適切な値と一致するようにエンドポイント セレクタを構成します。

たとえば、`ProdSqlServer` という名前の SQL サーバを選択する場合は、次のように選択します。

- **キー**：名前
- **演算子**：equals
- **値**：`ProdSqlServer`

別の例として、クラウド プロバイダのリソース ID `/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer` を使用して SQL サーバを選択する場合は、次のように選択します。

- **キー**：リソース ID
- **演算子**：equals
- **値**：`/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer`

3. Azure portal で、クラウド内の Azure SQL リソースを構成します。

クラウド ネイティブ管理対象

このタイプの展開では、サービスは VNet またはサブネットでインスタンス化されます（Cisco Cloud APIC を介して作成されます）。たとえば、Azure ApiManagement Services は、Cisco Cloud APIC によって管理されるサブネットに展開できます。

次に、クラウド ネイティブ管理対象展開タイプのサービス EPG の例を示します。

- **サービス タイプ**：Azure ApiManagement Services
- **展開タイプ**：クラウド ネイティブ管理対象
- **アクセス タイプ**：プライベート

このサンプル シナリオでは、この順番で次の構成を行います。

1. Cisco Cloud APIC GUI で、Azure ApiManagement Services service EPG によって使用されるクラウド コンテキスト プロファイルにサブネットを作成します。

   Cisco Cloud Network Controller GUI を使用したクラウド コンテキスト プロファイルの作成（133 ページ）の手順を実行します。Azure ApiManagement Services service EPG（たとえば、`10.50.0.0/16`）によって使用されるサブネットを構成します。

2. Cisco Cloud APIC GUI で、サービス タイプ Azure ApiManagement Services service EPG を作成します。

   次のパラメータを使用して、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） の手順に従います。

   - **サービス タイプ**：Azure ApiManagement Services
   - **展開タイプ**：クラウド ネイティブ マネージド
   - **アクセス タイプ**：プライベート

   このタイプのサービス EPG を構成するプロセスの一部としてエンドポイント セレクタを構成する場合は、最初の手順でクラウド コンテキスト プロファイルにサブネットを作成したときに使用した IP アドレスと一致するようにエンドポイント セレクタを構成します。

   たとえば、最初のステップで提供された例を使用して、このサービス EPG に対してこのエンドポイント セレクタを設定します。

   - **キー**：IP
   - **演算子**：equals
   - **値**：10.50.0.0/16

3. Azure portal で、クラウドの Azure ApiManagement Services リソースを構成します。

セキュリティ グループ

Azure では、2 種類のセキュリティ グループを使用して、仮想ネットワーク（VNet）内のネットワーク トラフィックを管理および制御します。

- **ネットワーク セキュリティ グループ**：ネットワーク セキュリティ グループ（NSG）は Azure で使用され、Azure リソースとの間のネットワーク トラフィックをフィルタ処理します。NSG は、受信および送信のセキュリティ ポリシーを定義するために使用され、いくつかの種類の Azure リソースへのインバウンド ネットワーク トラフィックまたはそこからのアウトバウンドネットワーク トラフィックを許可または拒否するセキュリティ ルールが含まれています。ルールごとに、送信元と送信先、ポート、およびプロトコルを指定できます。

  Cisco Cloud APIC では、NSG は契約に基づいて自動的に構成されます。

- **アプリケーション セキュリティ グループ**：アプリケーション セキュリティ グループ（ASG）は Azure で使用され、仮想マシン（VM）NIC で実行されるアプリケーションに従って仮想マシン（VM）NIC をグループ化し、それらのグループに基づいてネットワーク セキュリティ ポリシーを定義します。ASG は NSG 内でこれらのセキュリティ ポリシーを定義し、ネットワーク セキュリティ ルールを特定のワークロードまたは仮想マシンのグループに適用するために使用されます。

Cisco Cloud APIC では、ASG は各 EPG のエンドポイントの収集であり、NSG セキュリティ ポリシーの送信元または宛先として参照されます。

これらのセキュリティ グループの構成方法とマップ先は、リリースによって異なります。

- リリース 5.1(2) より前のリリース：EPG ごとの NSG 構成 （51 ページ）
- リリース 5.1(2) 以降：サブネットごとの NSG 構成 （51 ページ）
- リリース 5.1(2g) 以降：同じ VNet 内の VRF 間契約の IP ベースのルール （52 ページ）

リリース 5.1(2) より前のリリース：EPG ごとの NSG 構成

リリース 5.1(2) より前のリリースでは、Azure の NSG と Cisco Cloud APIC の EPG との間に 1 対 1 のマッピングがあります（これらの構成は、このドキュメント全体で **EPG ごとの NSG** 構成とも呼ばれます）。Cisco Cloud APIC EPG のこれらの NSG には、EPG に関連付けられた契約に基づいたセキュリティ ルールが設定されています。

リリース 5.1(2) より前のリリースでは、Cisco Cloud APIC で EPG を作成すると、次の Azure コンポーネントが作成されます。

- エンドポイント セレクタに基づいて各 EPG のすべてのエンドポイントまたは仮想マシン NIC をグループ化するために使用される ASG
- その ASG 内のすべての NIC に関連付けられ、その EPG のセキュリティ ポリシー定義を提供する NSG

リリース 5.1(2) 以降：サブネットごとの NSG 構成

リリース 5.1(2) 以降、以前に使用できた既存の EPG ごとの NSG 構成に加えて、Azure の NSG は Cisco Cloud APIC 上の EPG ではなくサブネットとの 1 対 1 のマッピングを持つこともできます（これらの構成は、このドキュメント全体で、**サブネットごとの NSG** 構成として呼ばれます）。デフォルトでは、NSG はリリース 5.1(2) 以降の EPG に対して作成されなくなり、NSG はその EPG の ASG 内のエンドポイントおよび VM NIC に関連付けられなくなりました。代わりに、各サブネットの NSG には、サブネットでエンドポイントが検出された ASG の契約に基づくすべてのルールが含まれます。

サブネットごとの NSG 構成の場合、Cisco Cloud APIC で EPG を作成すると、次の Azure コンポーネントが作成されます。

- エンドポイント セレクタに基づいて各 EPG のすべてのエンドポイントまたは仮想マシン NIC をグループ化するために使用される ASG [リリース 5.1(2) より前のリリースからの ASG の動作は基本的に変更されません]
- その EPG のセキュリティ ポリシー定義を提供し続けるが、Cisco Cloud APIC が管理する VNet のサブネットに関連付けられるようになった NSG

別の視点から見た場合：

- Cisco Cloud APIC で管理された VNet 内のすべての EPG には、それに関連付けられた ASG があり、EPG 用に構成されたエンドポイント セレクタに基づいてすべてのエンドポイントがグループ化されます。
- Cisco Cloud APIC で管理された VNet 内のすべてのサブネットには、NSG が関連付けられています。

グリーンフィールドまたは新しい Cisco Cloud APIC 展開のデフォルト設定は、**サブネットごとの NSG** です。この構成を手動で設定する場合、前述のように新しい**サブネットごとの NSG** 構成またはリリース 5.1(2) 以降の古い **EPG ごとの NSG** 構成を選択できます。ただし、いくつかの理由から、新しい**サブネットごとの NSG構成**を選択することをお勧めします。

- **サブネットごとの NSG** 構成を使用すると、VNet 内の NSG の数が減り、共通の共有サービスにアクセスする多数のサブネットがある展開のルール数も減ります。これにより、個々の EPG または ASG にマッピングされた各 NSG ではなく、サブネットの 1 つの NSG ですべてのルールをチェックできるため、管理が容易になります。
- サービス EPG を構成している場合は、**サブネットごとの NSG 構成**を使用する必要があります。詳細については、「クラウド サービス エンドポイント グループ （42 ページ）」を参照してください。

EPG ごとの NSG またはサブネットごとの NSG 構成を有効または無効にする手順については、Cloud APIC GUI を使用したネットワーク セキュリティ グループの構成 （126 ページ） を参照してください。

リリース 5.1(2g) 以降：同じ VNet 内の VRF 間契約の IP ベースのルール

リリース 5.1(2g) より前では、2 つの EPG に契約があり、同じ VNet にあるが異なる VRF に属している場合、ASG ベースのルールが使用され、その VNet でホストされている VRF 間の通信を有効にしていました。Azure ではすべての NSG のルールで 100 ASG の制限があり、状況によっては（たとえばすべての共有サービスに対して 1 つの VNet がある場合）、この制限にすぐに達する可能性があります。

リリース 5.1(2g) 以降、2 つの EPG に契約があり同じ VNet にあるが、異なる VRF に属している場合、IP ベースのルールが使用され、その VNet でホストされている VRF 間の通信を有効にするようになりました。ルールで 4000 個の IP アドレスをサポートできるため推奨されます。これらの IP ベースのルールは、検出されたエンドポイントまたは EPG で使用されるサブネット セレクタに基づいています。

ASG および NSG の注意事項と制限事項

以下は、ASG および NSG の注意事項と制限事項です。

- 5.1(2) より前のリリースの注意事項と制限事項 （53 ページ）
- リリース 5.1(2) 以降の注意事項と制限事項 （53 ページ）

5.1(2) より前のリリースの注意事項と制限事項

リリース 5.1(2) より前のリリースでは、Cisco Cloud APIC の NSG から EPG へのマッピングのみがサポートされています。

リリース 5.1(2) 以降の注意事項と制限事項

- リリース 5.1(2) 以降、Cisco Cloud APIC の NSG からサブネットへのマッピングもサポートされています。ただし、新しいサブネットごとの NSG 構成または EPG ごとの NSG 構成のいずれかを使用できますが、同じ Cisco Cloud APIC システムに両方を含めることはできません。
- Cisco Cloud APIC で管理される VNET では、サブネットごとに 1 つの NSG を構成できます。サブネットのグループごとに 1 つの NSG を持つことは、現時点では Cisco Cloud APIC ではサポートされていません。
- 透過ファイアウォールなどのパススルー デバイスでは、NIC に NSG が接続されません。サブネットを共有する複数のパススルー デバイスがある場合、各デバイスのパススルー ルールはサブネット内のすべてのエンドポイントに適用されます。

セキュリティ ルール

NSG のセキュリティ ルールは、それらが EPG ごとの NSG 構成のルールであるか、サブネットごとの NSG 構成のルールであるかによって異なります。2 種類の構成のセキュリティ ルールの処理に関する主な違いは、ルールのインストールと削除のトリガです。

- EPG ごとの NSG セキュリティ ルール （53 ページ）
- サブネットごとの NSG セキュリティ ルール （54 ページ）

EPG ごとの NSG セキュリティ ルール

- EPG と契約が Cisco Cloud APIC で定義されると、NSG セキュリティ ルールで参照される ASG のエンドポイントが検出されるかどうかに関係なく、ASG を送信元および宛先として使用する NSG セキュリティ ルールが常にプログラムされます 。
- VRF 間契約の場合：
  - コンシューマまたはプロバイダ EPG のいずれかがサブネットに基づくエンドポイント セレクタを使用する場合、エンドポイントの検出に関係なく、EPG セレクタからのサブネットとして送信元または宛先を持つ NSG セキュリティ ルールが常にプログラムされます。
  - コンシューマまたはプロバイダの EPG がサブネットに基づくエンドポイント セレクタを使用しない場合、エンドポイントの検出に応じて、エンドポイントの IP アドレスを送信元および宛先として使用する NSG セキュリティ ルールがプログラムされます。

- クラウド外部 EPG（cloudExtEPg）が関係するサイト間契約用に作成されたルールも、エンドポイントが検出されることなく事前にプログラムされます。

サブネットごとの NSG セキュリティ ルール

EPG の NSG セキュリティ ルールは、EPG がそのサブネットで少なくとも 1 つのエンドポイントを検出するまで、サブネット ベースの NSG でプログラムされません。

ソフトウェア アップグレードまたはダウングレードによる NGS 動作

リリース 5.1(2) より前のリリースでは NSG ごとの EPG マッピングのみがサポートされており、NSG ごとのサブネット マッピングのサポートがリリース 5.1(2) 以降で使用可能になったため、特定の状況でソフトウェアをアップグレードまたはダウングレードし他場合に、特定のシステム構成変更が行われる可能性があります。次のセクションでは、これらの状況と、これらのアップグレードまたはダウングレード操作中に発生する必要があることについて説明します。

- ソフトウェア アップグレードによる NSG の動作 （54 ページ）
- ソフトウェア ダウングレードによる NSG の動作 （55 ページ）

ソフトウェア アップグレードによる NSG の動作

リリース 5.1(2) より前のリリースからリリース 5.1(2) 以降への標準アップグレードを実行すると、リリース 5.1(2) より前のリリースでサポートされていた EPG ごとの NSG マッピングを使用して構成された NSG は、アップグレード後もそのまま残ります。これは、EPG ごとの NSG またはサブネットごとの NSG 構成のいずれかがリリース 5.1(2) 以降でサポートされているため、リリース 5.1(2) 以降への標準アップグレードを実行すると、古い EPG ごとの NSG 構成が自動的に保持されるためです。

ただし、サブネットごとの NSG 構成には利点があるため、これらの利点を利用するには、EPG ごとの NSG 構成をサブネットごとの NSG に変換することをお勧めします。さまざまな NSG 構成の詳細についてはセキュリティ グループ （50 ページ） を、EPG ごとの NSG またはサブネットごとの NSG 構成の有効化または無効化に関する指示についてはCloud APIC GUI を使用したネットワーク セキュリティ グループの構成 （126 ページ） を参照してください。

アップグレード後は、古い EPG ごとの NSG 構成または新しいサブネットごとの NSG 構成のいずれかを使用できますが、同じ Cisco Cloud APIC システムで両方を使用することはできないことに注意してください。詳細については、「ASG および NSG の注意事項と制限事項 （52 ページ）」を参照してください。

ただし、Cisco Cloud APIC GUI を使用したバックアップ構成の作成 （139 ページ） の手順を使用して既存の Cisco Cloud APIC 構成をバックアップし、アップグレードを実行し、アップグレード後にバックアップされた構成をインポートした場合、サブネットごとの NSG 構成は自動的にオンになり、古い EPG ごとの NSG 構成は新しいサブネットごとの NSG 構成に自動的に変換されます。

ソフトウェア ダウングレードによる NSG の動作

リリース 5.1(2) 以降からリリース 5.1(2) より前のリリースにダウングレードする場合は、サブネットごとの NSG 構成を、リリース 5.1(2) より前のリリースでサポートされていた EPG ごとの NSG 構成に手動で戻す必要があります。

ソフトウェアをダウングレードする前に、サブネットごとの NSG 構成から EPG ごとの NSG 構成に移行する一般的なプロセスを次に示します。

1. ソフトウェアをリリース 5.1(2) 以降から リリース 5.1(2) より前のリリースにダウングレードする前に、Cloud APIC GUI を使用したネットワーク セキュリティ グループの構成 （126 ページ） で説明されている手順を使用して、サブネットごとの NSG 構成を無効にします。Cisco Cloud APIC ソフトウェアは、サブネットごとの NSG マッピングから EPG ごとの NSG マッピングへの移行を開始します。
2. 移行が完了するまで待ちます。この場合、Cisco Cloud APIC ソフトウェアは、サブネットごとの NSG マッピング プロセスの一部として構成されたすべての NSG を削除し、EPG ごとの NSG マッピング構成用に新しい NSG を作成します。移行が完了する前にダウングレードを続行しようとすると、エラー メッセージが表示され、Cisco Cloud APIC ソフトウェアは、サブネット マッピングごとの NSG から EPG マッピングごとの NSG へのこの移行が完了するまで、ダウングレードを続行することを許可しません。

（注） GUI を使用してダウングレードするときに、移行が完了する前にソフトウェアのダウングレードを試みると、エラー メッセージが表示されます。ただし、REST API を使用してダウングレードするときに、ソフトウェアのダウングレードを早すぎてもエラーメッセージは表示されません。そのため、このような状況にある場合は、REST API を介してソフトウェアをダウングレードしないことをお勧めします。

REST API を使用してソフトウェアをダウングレードする場合は、次の MO を監視します。

`hcloudReconcileDone`

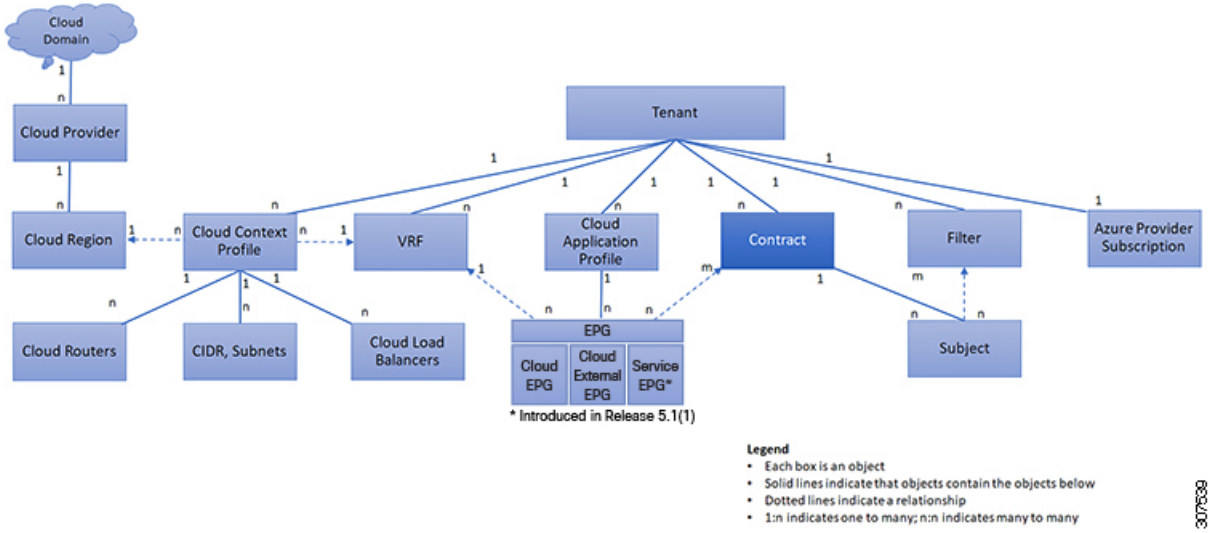
REST API を使用してダウングレードを続行する前に、プロパティ `sgForSubnetModeConverged` が `[yes]` に設定されていることを確認します。

3. システムが EPG ごとの NSG マッピングへの移行を正常に完了したことを確認したら、『*Cisco Cloud APIC for Azure* インストール ガイド』に記載されている手順を使用して、Cisco Cloud APIC ソフトウェアをダウングレードできます。

コントラクト

クラウド EPG に加えて、コントラクト（`vzBrCP`）はポリシー モデルのキー オブジェクトです。クラウド EPG が他のクラウド EPG と通信するには、コントラクトのルールに従う必要があります。次の図は、管理情報ツリー（MIT）内のコントラクト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。

図 *17:* コントラクト



管理者は、コントラクトを使用して許可されるプロトコルやポートを含む EPG 間を通過できるトラフィックの 1 つまたは複数のタイプを選択します。コントラクトがなければ、EPG 間通信はデフォルトでディセーブルになります。EPG 内の通信に必要なコントラクトはありません。EPG 内の通信は常に暗黙的に許可されています。

コントラクトは、次のタイプのクラウド EPG 通信を管理します。

- クラウド EPG （`cloudEPg`）間のテナント内およびテナント間の両方

（注） 共有サービス モードの場合、コントラクトはテナント間通信に必要です。テナント VRF がポリシーを適用していなくても、コントラクトが VRF 間でスタティック ルートを指定するために使用されます。

- クラウド EPGとクラウド外部 EPG 間（`cloudExtEPg`）

コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付されたクラウド EPG 間の通信を制御します。クラウド EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。クラウド EPG がコントラクトを提供すると、そのクラウド EPG 内のクラウドエンドポイントとの通信は、通信が提供されたコントラクトに準拠している限り、他のクラウド EPG 内のクラウドエンドポイントから開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウドエンドポイントは、コントラクトを指定したクラウド EPG のクラウドエンドポイントと通信を開始できます。

（注） 1 つのクラウド EPG で同じコントラクトを指定および使用できます。クラウド EPG は複数のコントラクトを同時に指定および使用することもできます。

契約ルール統合のためのコンマ区切りフィルタのサポート

契約が作成されると、契約で定義されたルールの一部が統合され、特定の基準に基づいてAzureに表示されます。複数のポートと複数のIPアドレスと範囲を1つのわかりやすいルールに組み合わせることができます。ルールの統合の基準は次のとおりです。

- ルールは、契約内でのみ統合されます。2つの異なる契約に起因する2つのルールは、Azureに統合されません。
- 送信元/宛先アドレス プレフィックスと宛先ポートが統合されます。
- 複数のルールをNSGに統合するための条件は次のとおりです。
  - 同一契約
  - 同じプロトコル（UDP、TCP、ICMP）
  - 同じ方向（インバウンド、アウトバウンド）
  - 同型（SG、IP）
- 同一契約内の同一プロトコル（TCP/UDP）の重複するポート範囲は1つに集約する。

  たとえば、TCPポート100 ～ 200、150 ～ 250は100 ～ 250に統合されます。
- 1.2.3.4/32（任意のアドレス プレフィックス）が許可され、0.0.0.0/0の拡張EPGが追加された場合、許可される送信元/宛先IPは[1.2.3.4/32, 0.0.0.0/0]ではなく任意になります。

以下の例は、契約C1およびC2に基づく、EPG1アウトバウンドルールと統合されたEPG1アウトバウンドルールを示しています。

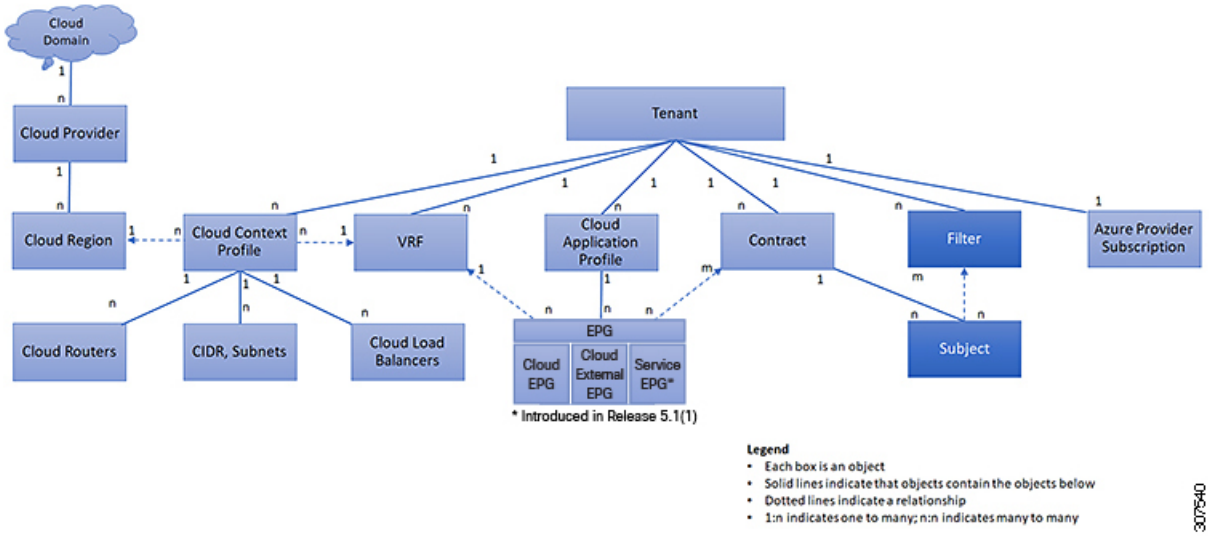
```
Contract C1:
Consumer: EPG1 , Provider: EPG2
Filter: TCP  (ports 53)
Filter: UDP (port 53, 5000)

Contract C2:
Consumer: EPG1 , Provider: EPG2
Filter: TCP (ports 80, 8080)

EPG1 outbound rules:
EPG1 -> EPG2   TCP  80
EPG1 -> EPG2   TCP  8080
EPG1 -> EPG2        TCP        53
EPG1 -> EPG2   UDP  53
EPG1 -> EPG2   UDP  5000
EPG1 -> 1.1.1.1/32  TCP  80
EPG1 -> 1.1.1.1/32  TCP  8080
EPG1 -> 1.1.1.1/32  TCP  53
EPG1 -> 1.1.1.1/32  UDP  53
EPG1 -> 1.1.1.1/32  UDP 5000
EPG1 -> 2.2.2.2/32  TCP  80
EPG1 -> 2.2.2.2/32  TCP  8080
EPG1 -> 2.2.2.2/32  TCP       53
EPG1 -> 2.2.2.2/32  UDP  53
EPG1 -> 2.2.2.2/32  UDP  5000
```

```
Rules are consolidated by comma-separated filters (consolidated based on C1 and C2):
EPG1 -> EPG2      TCP  80,8080
EPG1 -> EPG2      UDP  53,5000
EPG1 -> EPG2      TCP  53
EPG1 -> 1.1.1.1/32, 2.2.2.2/32   TCP  80,8080
EPG1 -> 1.1.1.1/32, 2.2.2.2/32   UDP  53,5000
EPG1 -> 1.1.1.1/32, 2.2.2.2/32   TCP  53
```

クラウド EPG 通信を制御するフィルタおよびサブジェクト

サブジェクトおよびフィルタの管理対象オブジェクトにより、さまざまなアプリケーションまたはサービスの提供要件を満たすためのクラウド EPG とコントラクト間の混合と照合が可能になります。次の図は、管理情報ツリー（MIT）内のアプリケーション サブジェクトおよびフィルタの場所と、テナント内の他のオブジェクトとの関係を示します。

図 *18 :* サブジェクトおよびフィルタ



コントラクトには、複数の通信ルールを含めることができ、複数のクラウド EPG は複数のコントラクトを消費および提供できます。ポリシーの設計者は、複雑な通信ポリシーを簡潔に表し、アプリケーションの複数のインスタンス間でこれらのポリシーを再利用できます。

（注） サブジェクトは Cisco Cloud APIC で非表示になり、設定できません。Azure にインストールされているルールの場合、フィルタ エントリで指定された送信元ポートは考慮されません。

サブジェクトおよびフィルタは次のオプションに従ってクラウド EPG 通信を定義します。

- フィルタは、レイヤ 3 ～ レイヤ 4 フィールド、レイヤ 3 プロトコル タイプなどの TCP/IP ヘッダー フィールド、レイヤ 4 ポートなどです。関連するコントラクトに従って、クラウド EPG プロバイダーは、IN および OUT 両方の方向でプロトコルおよびポートを決定しま

す。コントラクトのサブジェクトは、コントラクトを提供する側と消費する側のクラウドEPG の間に適用されるフィルタ（およびその方向）への関連付けが含まれています。

- サブジェクトはコントラクトに含まれています。コントラクト内のサブジェクトがフィルタを使用して、通信できるトラフィックのタイプと発生の仕方を指定します。たとえば、HTTPS メッセージの場合、サブジェクトはその方向と許可される IP アドレス タイプ（たとえば IPv4）、HTTP プロトコル、およびポートを指定するフィルタを指定します。サブジェクトは、フィルタを単方向にするか双方向にするかを決定します。単方向フィルタは 1 方向で使用されます。単方向フィルタは、IN または OUT の通信を定義しますが、両方に対して同じではありません。双方向フィルタは両方に対して同じで、IN および OUT の通信を定義します。
- Azure 構造体でレンダリングされる ACI 契約は常にステートフルであり、リターン トラフィックを許可します。

クラウド テンプレートの概要

クラウドテンプレートは、Cisco Cloud APICインフラ ネットワークを設定および管理するテンプレートを提供します。テンプレートには、設定に最も重要な要素のみが必要です。これらの要素から、クラウド テンプレートは Cisco Cloud APIC インフラ ネットワークのセットアップに必要な詳細設定を生成します。ただし、1 回限りの設定生成ではなく、テンプレート入力の要素を追加、変更、または削除できます。クラウドテンプレートは、それに応じて結果の設定を更新します。

Azureネットワーク構成の中央のうちいずれかは、仮想プライベートクラウド（VNET）です。Azure は世界中の多くのリージョンをサポートしており、1 つの VNET は 1 つのリージョンに固有です。

クラウドテンプレートは、1つ以上のリージョン名を承認し、それらのリージョンでインフラVNET の構成全体を生成します。それらはインフラ VNET です。Azure VNET に対応する Cisco Cloud APIC 管理対象オブジェクト（MO）は、`cloudCtxProfile` です。クラウド テンプレートで指定されたすべてのリージョンに対して、`cloudCtxProfile` 設定が生成されます。`cloudCtxProfile`は、リージョンに対応するすべての設定の最上位 MO です。その下には、特定の設定をキャプチャするためのツリーとして編成された他の多くのMOがあります。インフラ VNet の `cloudCtxProfile` MO は、クラウド テンプレートにより生成されます。これは `ctxProfileOwner == SYSTEM` を伝送します。これは、この MO がシステムによって生成されることを意味します。非インフラストラクチャ ネットワークの場合、`cloudCtxProfile`を直接設定できます。この場合、`cloudCtxProfile` は `ctxProfileOwner == USER` を伝送します。

Azure VNet の主要なプロパティは CIDR です。Cisco Cloud APIC では、ユーザー VNet で CIDR を選択して展開できます。インフラ VNet の CIDR は、クラウド サイトの最初のセットアップ時にユーザーによってクラウド テンプレートに提供され、クラウド テンプレートによって Azure クラウドに展開されます。

リリース 5.0(2) 以降、`createdBy` という新しいプロパティが CIDR に追加されています。この `createdBy` プロパティのデフォルト値は `USER` です。

- すべてのユーザー作成 CIDR について、`createdBy` プロパティの値は `USER` に設定されます。
- クラウド テンプレートで作成されたCIDRの場合、`createdBy` プロパティの値は `SYSTEM` に設定されます。

複数の CIDR ブロックとサブネット ブロックをインフラ VNet で構成できます。 CIDR を作成し、インフラストラクチャ VNet にサブネットを関連付けることができます。クラウド テンプレート サブネットは overlay-1 VRF にマッピングされますが、ユーザーが作成したサブネットの場合、同じインフラ VNet 内のセカンダリ VRF へのサブネットから VRF へのマッピングを手動で構成する必要があります。それぞれの VRF のすべてのサブネットは、VRF 分離のためにクラウド内に個別のルート テーブルを持ちます。

インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。すべてのクラウド EPG とクラウド外部 EPG は、インフラ テナントのセカンダリ VRF に関連付けられます。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外部 EPG と通信可能で、他のユーザー テナント VRF 内のクラウド EPG とも通信できます。既存の「クラウド インフラ」アプリケーション プロファイルを使用せず、代わりにインフラ テナントに新しいアプリケーション プロファイルを作成し、新しいアプリケーション プロファイルをセカンダリ VRF のクラウド EPG およびクラウド外部 EPG に関連付けることをお勧めします。

詳細については、Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成 （91 ページ）を参照してください。

クラウド テンプレートは、`cloudCtxProfile` サブツリーに次のような多数の MO を生成して管理します。

- サブネット
- クラウド ルータ
- クラウド ルータ インターフェイスの IP アドレス割り当て
- トンネルの IP アドレスの割り当てと設定
- ループバックの IP アドレスの割り当てと設定

クラウド テンプレートがない場合は、これらの設定と管理を担当します。

Cisco Cloud Template MO テーブルには、クラウド テンプレートへの入力（MO）の概要が含まれています。

表 *6 :* クラウド テンプレート *MO*

MO	目的
cloudtemplateInfraNetwork	クラウド テンプレート設定のルート。次の属性が含まれます。 numRoutersPerRegion：cloudtemplateIntNetwork で指定された各 cloudRegionName のクラウド ルータの数。
cloudtemplateProfile	すべてのクラウドルータの設定プロファイル。次の属性が含まれます。 • routerUsername （注） • ユーザ名を「admin」にすることはできません。 • Azure からのユーザー名の制限が適用されます。 • routerPassword • routerThroughput • routerLicenseToken • routeDataInterfacePublicIP • routerMgmtInterfacePublicIP
cloudtemplateIntNetwork	クラウドルータを展開する場所を指定するリージョンのリストが含まれます。各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateExtNetwork	クラウド外部のインフラ ネットワーク設定入力が含まれます。 クラウド ルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。 各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateVpnNetwork	ACI オンプレミス サイトまたは別の Cisco Cloud APIC サイトで VPN を設定するための情報が含まれています。

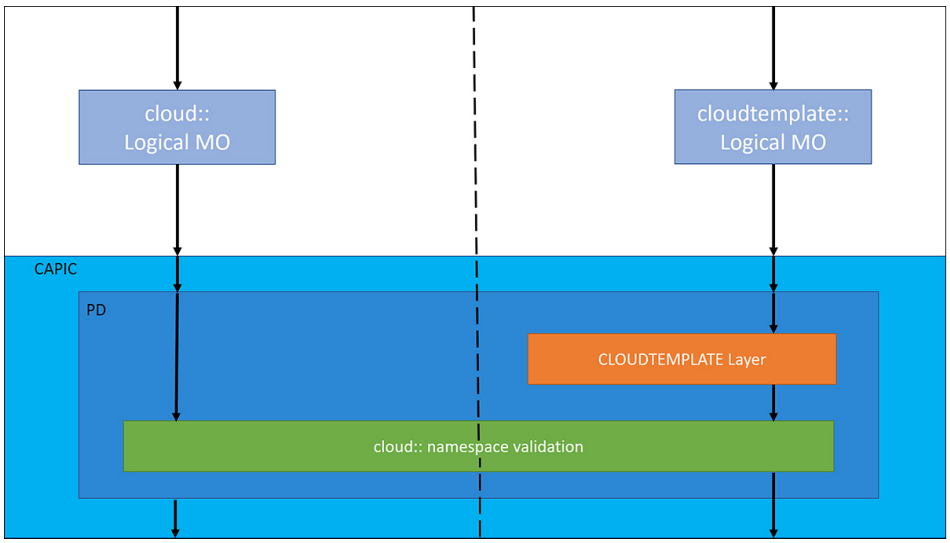
MO	目的
cloudtemplateIpSecTunnel	ACI オンプレミス サイトの IPSec ピアの IP アドレスをキャプチャします。
cloudtemplateOspf	VPN 接続に使用する OSPF エリアをキャプチャします。
cloudtemplateBgpEvpn	オンプレミス サイトとの BGP セッションを設定するために、ピア IP アドレス、ASN などをキャプチャします。

Cisco Cloud APIC では、クラウド テンプレートにより、MO の階層化は通常の Cisco APIC とは若干異なります。通常の Cisco APIC では、2 つの変換レイヤを通過する論理 MO をポストします。

1. 論理 MO から解決済み MO へ
2. 解決済みの MO から具体的な MO

Cisco Cloud APIC には、インフラ ネットワーク用の追加の変換レイヤがあります。この追加レイヤでは、クラウド テンプレートが `cloudtemplate` 名前空間の論理 MO をクラウド名前空間の論理 MO に変換します。インフラ ネットワーク外の設定では、クラウド名前空間に論理 MO をポストします。この場合、MO は通常の Cisco APIC と同様に通常の2層変換を実行します。

図 *19*: クラウドおよびクラウド テンプレート *MO* 変換



（注） クラウド テンプレートの設定については、Cisco Cloud APIC コンポーネントの設定 （67 ページ） を参照してください。

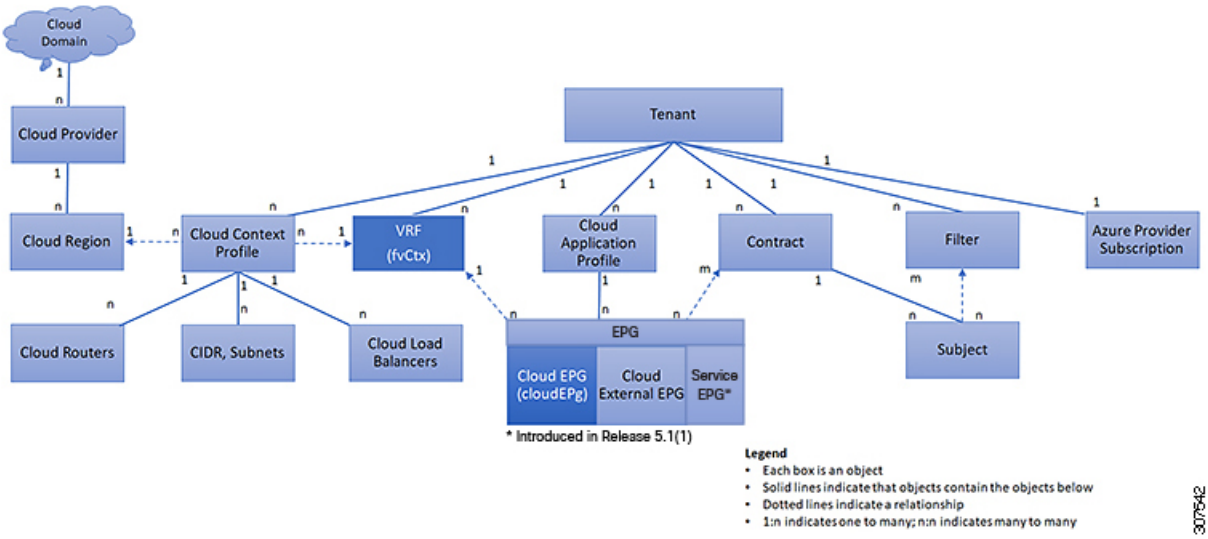
管理対象オブジェクトの関係とポリシー解決

関係管理対象オブジェクトは、抑制（親/子）の関係を共有しない管理対象オブジェクトのインスタンス間の関係を表します。MO の関係は、次の 2 つの方法のいずれかでソース MO とターゲット MO の間に確立されます。

- `cloudRsCloudEPgCtx` などの明示的な関係は、ターゲット MO 識別名（DN）に基づく関係を定義します。
- 名前付きの関係は、ターゲット MO の名前に基づいて関係を定義します。

次の図の点線は、いくつかの一般的な MO の関係を示します。

図 *20 : MO* の関係



たとえば、クラウド EPG と VRF 間の点線は、これら 2 つの MO 間の関係を定義します。この図では、EPG（`cloudEPg`）には、ターゲットの VRF MO（`fvCtx`）の名前が付いた関係 MO（`cloudRsCloudEPgCtx`）が含まれます。たとえば、実稼働が VRF 名（`fvCtx.name=production`）である場合、関係の名前は実稼働（`cloudRsCloudEPgCtx.tnFvCtxName=production`）になります。

名前付き関係に基づくポリシー解決の場合は、一致する名前を持つターゲット MO が現在のテナントに見つからない場合、ACI クラウドインフラストラクチャは共通のテナントで解決を試行します。たとえば、ユーザのテナント クラウド EPG がテナントに存在しない VRF を対象とした関係 MO を含んでいた場合、システムは共通のテナントでその関係の解決を試行します。名前付き関係が現在のテナントまたは共通のテナントで解決できない場合、ACI クラウドインフラストラクチャは、デフォルト ポリシーに解決を試行します。デフォルト ポリシーが現在のテナントに存在する場合、それが使用されます。存在しない場合、ACI クラウドインフラストラクチャは共通のテナントでデフォルト ポリシーを検索します。クラウド コンテキスト プロファイル、VRF およびコントラクト（セキュリティ ポリシー）の名前付き関係はデフォルトに解決されません。

デフォルト ポリシー

警告 デフォルト ポリシーは、変更または削除できません。デフォルト ポリシーを削除すると、ポリシー解決プロセスが異常終了する可能性があります。

ACI クラウドインフラストラクチャは、そのコア機能の多くにデフォルトのポリシーを含んでいます。デフォルト ポリシーの例には、次のものがあります。

- Cloud Azure プロバイダ（インフラ テナント用）
- モニタリングと統計情報

（注） デフォルト ポリシーを使用する構成を実装する際の混乱を避けるために、デフォルト ポリシーに加えられた変更を文書化します。デフォルト ポリシーを削除する前に、現在または将来の設定がデフォルト ポリシーに依存していないことを確認してください。たとえば、デフォルトのファームウェアの更新ポリシーを削除すると、将来のファームウェアの更新に問題が生じる可能性があります。

デフォルト ポリシーは、次の複数の目的に使用されます。

- クラウド インフラストラクチャの管理者がモデル内のデフォルト値を上書きできます。
- 管理者が明示的なポリシーを提供しない場合、Cisco Cloud APIC はデフォルトのポリシーを適用します。管理者はデフォルトのポリシーを作成でき、管理者が明示ポリシーを提供しない限り、Cisco Cloud APIC はそのポリシーを使用します。

次のシナリオでは、一般的なポリシー解決の動作について説明します。

- 構成は、デフォルト ポリシーを明示的に参照します。現在のテナントにデフォルト ポリシーが存在する場合は、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。
- 構成は、現在のテナントまたはテナント共通に存在しない名前付きポリシー (デフォルトではない) を参照します。現在のテナントにデフォルト ポリシーがある場合は、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。

（注） 上記のシナリオは、テナントの VRF には適用されません。

- 構成はポリシー名を参照しません。現在のテナントにデフォルト ポリシーが存在する場合、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。

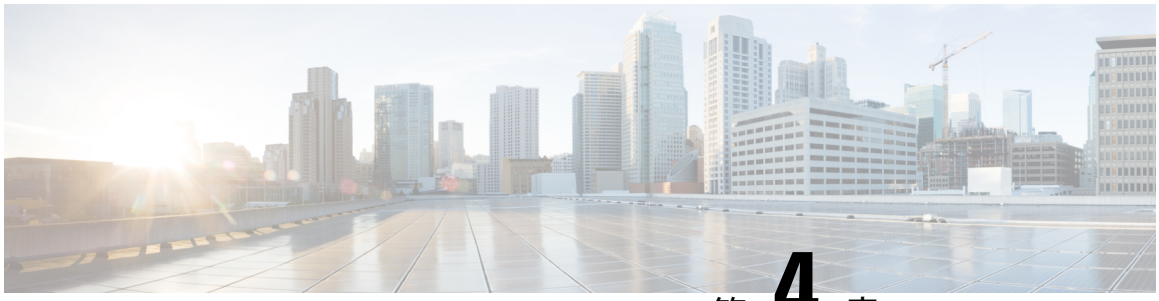
ポリシー モデルは、オブジェクトが自身の下に関係管理対象オブジェクト（MO）を持つことによって別のポリシーを使用していることや、関係 MO が名前によってターゲット ポリシーを参照することを指定します。この関係が、名前による明示的なポリシー参照を行わない場合には、システムは、デフォルトと呼ばれるポリシーを解決しようとします。クラウドコンテキスト プロファイルと VRF は、このルールの例外です。

共有サービス

あるテナントのクラウド EPG は、共有テナントに含まれるコントラクト インターフェイスを介して他のテナントのクラウド EPG を伝達できます。同じテナント内で、ある VRF のクラウド EPG は、テナントで定義された契約を通じて、別の VRF の別のクラウド EPG と通信できます。コントラクト インターフェイスは、異なるテナントに含まれるクラウド EPG によってコントラクト消費インターフェイスとして使用できる MO です。インターフェイスへの関連付けによって、クラウド EPG は共有テナントに含まれるコントラクトへのインターフェイスによって表される情報カテゴリを消費します。テナントは第 3 位で定義された単一のコントラクトに参加できます。より厳しいセキュリティ要件は、テナントが互いに完全に独立したままになるようにテナント、コントラクト、情報カテゴリおよびフィルタの方向を定義することで満たすことができます。

共有サービス コントラクトの設定時は、次のガイドラインに従ってください。

- 共有サービスは、重複しない CIDR サブネットのみでサポートされます。共有サービスの CIDR サブネットを構成するときは、次のガイドラインに従ってください。
  - ある VRF から漏れた CIDR サブネットは、切り離されている必要があり、重複してはなりません。
  - 複数のコンシューマー ネットワークから VRF に、またはその逆にアドバタイズされる CIDR サブネットは、切り離されている必要があり、重複してはなりません。
  - テナント間契約にはグローバル範囲が必要です。



第 4 章

Cisco Cloud APIC コンポーネントの設定

Cisco クラウド APIC の設定について

Cisco Cloud APIC GUI または REST API を使用して Cisco Cloud APIC コンポーネントを作成します。ここでは、設定、アプリケーション管理、運用、および管理コンポーネントの作成方法について説明します。

（注）

- ロードバランサとサービス グラフの設定については、レイヤ 4 から レイヤ 7 サービスの展開 （209 ページ） を参照してください。
- ナビゲーションや構成可能なコンポーネントのリストなどの GUI については、Cisco Cloud APIC GUI の概要 （20 ページ） を参照してください。

GUI を使用した Cisco Cloud Cisco APIC の設定

Cisco Cloud APIC GUIを使用したテナントの作成

このセクションでは、Cisco Cloud APIC GUI を使用したテナントの作成方法について説明します。

始める前に

- Cisco Cloud APIC によって管理されるテナント、または管理されていないテナントを作成できます。管理対象テナントを確立するには、最初に Azure portal から Azure サブスクリプション ID を取得する必要があります。テナントの作成時に、Cisco Cloud APIC の適切

なフィールドにサブスクリプションIDを入力します。管理対象テナントを使用する前に、サブスクリプションを管理するためのアクセス許可をCisco Cloud APICに明示的に付与する必要があります。これを行うための手順は、テナントの作成中にCisco Cloud APIC GUIに表示されます。ただし、インフラ テナントの手順は、インフラ テナントの詳細ビューに表示されます。

1. **[ナビゲーション（Navigation）]** メニュー > **[アプリケーション管理（Application Management）]** サブタブをクリックします。
2. インフラ テナントをダブルクリックします。
3. **[Azure ロールの割り当てコマンドの表示（View Azure Role Assignment Command）]** をクリックします。サブスクリプションを管理するためのアクセス許可をCisco Cloud APICに付与する手順が表示されます。

（注） Azure サブスクリプション ID の取得については、Microsoft Azure のドキュメントを参照してください。

- 非管理対象テナントを作成するには、エンタープライズアプリケーションからディレクトリ（Azureテナント）ID、Azureエンタープライズ アプリケーションID、およびクライアント シークレットを取得する必要があります。詳細については、Microsoft Azureのマニュアルを参照してください。

（注） Cloud APICは、他のアプリケーションまたはユーザーによって作成されたAzureリソースを妨害しません。自身で作成したAzureリソースのみを管理します。

- 特定のサブスクリプションを管理するための許可をCisco Cloud APICに明示的に付与するために必要な手順は、Cisco Cloud APIC GUIにあります。テナントを作成する場合、クライアント シークレットを入力した後に手順が表示されます。
- Cloud APICは所有権チェックを適用して、意図的にまたは誤って行われた同じテナントとリージョンの組み合わせでポリシーが展開されないようにします。たとえば、リージョンR1のAzureサブスクリプションIA1にCloud APICが展開されているとします。ここで、リージョンR2にテナントTA1を展開します。このテナント展開（TA1-R2のアカウントとリージョンの組み合わせ）は、IA1-R1によって所有されています。別のCloud APICが将来のある時点で同じテナントとリージョンの組み合わせを管理しようとした場合（たとえば、CAPIC2がリージョンR3のAzureサブスクリプションIA2に導入されている場合）、これは展開TA1-R2の所有者が現在、IA1-R1であるため許可されません。つまり、1つのCloud APICで管理できるのは1つのリージョン内の1つのアカウントのみです。以下の例は、いくつかの有効な展開の組み合わせと間違った展開の組み合わせを示しています。

```
Capic1:
IA1-R1: TA1-R1 - ok
```

```
        TA1-R2 - ok

Capic2:
IA1-R2: TA1-R1 - not allowed
        TA1-R3 - ok

Capic3:
IA2-R1: TA1-R1 - not allowed
        TA1-R4 - ok
        TA2-R4 - ok
```

- 所有権の強制は、Azure リソース グループを使用して行われます。リージョン R2 のサブスクリプション TA1 の新しいテナントが Cloud APIC によって管理される場合、リソース グループ CAPIC_TA1_R2（例：CAPIC_123456789012__eastus2）がサブスクリプションに作成されます。このリソース グループには、値が IA1_R1_TA1_R2 のリソース タグ AciOwnerTag があります（サブスクリプション IA1 の Cloud APIC によって管理され、リージョン R1 に展開されていると想定）。AciOwnerTag の不一致が発生した場合、テナントとリージョンの管理は中止されます。

  AciOwnerTag の不一致ケースの概要は次のとおりです。

  - 最初に Cloud APIC がサブスクリプションにインストールされ、次に削除され、Cloud APIC が別のサブスクリプションにインストールされます。既存のすべてのテナント リージョンの展開が失敗します。
  - 別の TA1-R2 が同じテナント リージョンを管理しています。

  所有権が一致しない場合、**再試行** (テナント リージョンの再セットアップ) は現在サポートされていません。回避策として、他の CloudAPIC が同じテナントとリージョンの組み合わせを管理していないことが確実な場合は、テナントの Azure サブスクリプションにログオンし、影響を受けるリソース グループ（例：CAPIC_123456789012__eastus2 など）を手動で削除します。次に、Cloud APIC をリロードするか、テナントを再度削除して追加します。

- リリース 5.2(1) より前は、テナントのタイプに応じて、Azure リソースへのアクセスに使用できる方法のサポートが異なりました。
  - **インフラ テナント**：リリース 5.2(1) より前では、認証または資格情報を処理するときに、管理対象 ID のみがサポートされていました。
  - **ユーザー テナント**：認証または資格情報を処理するときに、管理対象 ID と非管理対象 ID/サービス プリンシパルの両方をサポートできます。

  リリース 5.2(1) 以降、インフラ テナントおよびユーザー テナント両方で、認証または資格情報を処理するとき、管理対象 ID と非管理対象 ID/サービス プリンシパルの両方をサポートできるようになりました。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[テナントの作成（Create Tenant）]** をクリックします。**[テナントの作成（Create Tenant）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[テナント ダイアログボックス フィールドの作成（Create Tenant Dialog Box Field）]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *7:* テナント ダイアログボックス フィールドの作成

[プロパティ（Properties）]	**説明**
名前（Name）	テナント名を入力します。
説明	テナントの説明を入力します。
設定	
セキュリティ ドメインの追加	テナントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。
Azure サブスクリプション	
[モード（Mode）]	アカウント タイプを選択します。 • **固有作成**：新しいテナントを作成するには、このオプションを選択します。 • **共有を選択**：このオプションを選択して、既存のテナントから管理対象または非管理対象の設定を継承します。
Azure サブスクリプション ID	Azure サブスクリプション ID を入力します。

[プロパティ（Properties）]	説明
アクセスタイプ	アクセス タイプを選択します。 • **サービス プリンシパル**または**非管理対象 ID**：テナント サブスクリプションが Cisco Cloud APIC によって管理されていない場合は、このオプションを選択します。 • **管理対象 ID**：テナント サブスクリプションが Cisco Cloud APIC によって管理されている場合は、このオプションを選択します。 （注） リリース 5.2(1) より前は、インフラストラクチャ テナントにのみ**管理対象 ID** を割り当てることができました。リリース 5.2(1) 以降では、インフラ テナントに**サービス プリンシパル**または**管理対象 ID** を割り当てることができるようになりました。 詳細については、テナント、ID、およびサブスクリプションについて （30 ページ）を参照してください。
アプリケーションID	（注） このフィールドは、**サービス プリンシパル**または**非管理対象 ID** アクセス タイプに対してのみ有効です。 アプリケーション ID を入力します。 （注） アプリケーション ID の取得については、Azure のドキュメントまたはサポートを参照してください。

[プロパティ（Properties）]	説明
クライアントのシークレット（Client Secret）	（注） このフィールドは、**サービス プリンシパル**または**非管理対象 ID** アクセス タイプに対してのみ有効です。 クライアント シークレットを入力します。 （注） • クライアント シークレットの作成については、Azure のドキュメントまたはサポートを参照してください。 • 特定のサブスクリプションを管理するには、Cloud APIC のアクセス許可を明示的に付与する必要があります。Azure portal に移動して、次の手順に従います。 1. クラウド シェルをオープンします。 2. 「バッシュ」を選択 3. Cisco Cloud APIC GUI に表示されるコマンドをコピーして貼り付けます。
Active Directory ID	（注） このフィールドは、**サービス プリンシパル**または**非管理対象 ID** アクセス タイプに対してのみ有効です。 ディレクトリ ID を入力します。 （注） Active Directory ID の取得については、Azure のドキュメントまたはサポートを参照してください。

[プロパティ（Properties）]	説明
セキュリティドメインの追加	アカウントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したアプリケーション プロファイルの作成

このセクションでは、Cisco Cloud APIC GUI を使用したアプリケーション プロファイルの作成方法を説明します。

始める前に

テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[アプリケーション プロファイルの作成（Create Application Profile）]** をクリックします。**[アプリケーション プロファイルの作成（Create Application Profile）]** ダイアログ ボックスが表示されます。

ステップ 4 [Name] フィールドに名前を入力します。

ステップ 5 テナントを選択します。

a) **[テナントの選択（Select Tenant）]** をクリックします。

[テナントの選択（Select Tenant）] ダイアログボックスが表示されます。

b) **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。

[アプリケーションプロファイルの作成（Create Application Profile）] ダイアログボックスで、次の手順を実行します。

ステップ 6 **[説明（Description）]** フィールドに説明を入力します。

ステップ 7 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した VRF の作成

このセクションでは、Cisco Cloud APIC GUI を使用した VRF の作成方法について説明します。

始める前に

テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[VRF の作成（Create VRF）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[VRF* ダイアログボックスの作成（*Create VRF*）*]* ダイアログボックスのフィールドの表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *8 : [VRF* の作成（*Create VRF*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	**[Name]** フィールドに、VRF の表示名を入力します。 すべての VRF に *vrfEncoded* 値が割り当てられます。テナントと VRF 名の組み合わせが 32 文字を超える場合、VRF 名（テナント名も含む）は *vrfEncoded* 値を使用してクラウド ルータで識別されます。*vrfEncoded* 値を表示するには、**[Application Management]** > **[VRFs]** サブタブに移動します。右側のペインで VRF をクリックし、クラウド ルータで *[Encoded VRF Name]* を探します。

[プロパティ（Properties）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログボックスに戻ります。
説明	VRF の説明を入力します。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。

Cisco Cloud APIC GUI を使用した外部ネットワークの作成

この手順は、外部ポリシーの作成方法を示しています。オンプレミス サイトの複数のルータに接続できる単一の外部ネットワーク、または CCR への接続に使用できる複数の VRF を持つ複数の外部ネットワークを設定できます。

始める前に

外部ネットワークを作成する前に、ハブ ネットワークを作成しておく必要があります。

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[外部ネットワーク（External Networks）]**に移動します。
構成された外部ネットワークが表示されます。

ステップ 2 **[アクション（Actions）]** をクリックし、**[外部ネットワークの作成（Create External Network）]** を選択します。
[外部ネットワークの作成（Create External Network）] ウィンドウが表示されます。

ステップ 3 次の *[*外部ネットワークの作成ダイアログボックスのフィールド（*Create External Network Dialog Box Fields*）*]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *9 : [*外部ネットワークの作成（*Create External Network*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	外部ネットワーク名を入力します。

[プロパティ（Properties）]	説明
VRF	この外部VRFは、外部の非ACIデバイスとの外部接続に使用されます。この目的で複数の外部VRFを作成できます。 この VRF は、VRF が次の 3 つの特性をすべて備えている場合に 外部VRF として識別されます。 • インフラ テナントの下で構成された • 外部ネットワークに関連付けられている • クラウド コンテキスト プロファイルに関連付けられていない 外部ネットワークに関連付けられているVRFはすべて 外部VRF になります。外部VRF をクラウド コンテキスト プロファイルまたはサブネットに関連付けることはできません。 外部VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成（+ Create VRF）] オプションを使用してVRFを作成することもできます。 3. [選択（Select）] をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。
ホスト ルーター名	このフィールドは編集できません。デフォルトのホスト ルータが自動的に選択されます。
設定	
地域	リージョンを選択するには: 1. **[地域の追加（Add Region）]** をクリックします。 **[地域の選択（Select Regions）]** ダイアログボックスが表示されます。 初回セットアップの一部として選択した地域がここに表示されます。 2. **[地域の選択（Select Regions）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

[プロパティ（**Properties**）]	説明
VPN ネットワーク	

[プロパティ（Properties）]	説明
	VPN ネットワーク エントリは、外部接続に使用されます。設定されたすべてのVPNネットワークが、選択したすべてのリージョンに適用されます。 VPN ネットワークを追加するには、次の手順を実行します。 1. **[VPNネットワークの追加（Add VPN Network）]** をタップします。 **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスが表示されます。 2. **[名前（Name）]** フィールドに VPN ネットワークの名前を入力します。 3. **[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。 IPSec ピア エントリごとにトンネルが作成されます。 4. 追加する IPSec トンネルの次の次のフィールドに値を入力します。 • **IPSec トンネル ピアの パブリック IP** • **事前共有キー** • **IKE Version**：IPSec トンネル接続用に **ikev1** または **ikev2** を選択します。 • **BGP ピア ASN** • **Subnet Pool Name**：**[サブネット プール名の選択（Select Subnet Pool Name）]** をクリックします。 **[サブネット プール名の選択（Select Subnet Pool Name）]** ダイアログボックスが表示されます。リストされている使用可能なサブネット プールのいずれかを選択し、**[選択（Select）]** をクリックします。 • **IPsec トンネル ソース インターフェイス**: このフィールドのエントリを使用して、Cisco Cloud APIC は、選択された各ソース インターフェイスから接続先 IP アドレスへの 1 つの IPsec トンネルを作成します。 （注） **ikev2** は、このフィールドのデフォルト オプションです。IPsec トンネル ソース インターフェイス機能は、IKEv2 構成でのみサポートされます。 **gig3**は、デフォルトで選択されます。次の中から1つまたは複数のインターフェイスを選択します • **gig2**: GigabitEthernet2 インターフェイス • **gig3**: GigabitEthernet3 インターフェイス • **gig4**: GigabitEthernet4 インターフェイス （注） この外部ネットワークで IPsec トンネル ソース インターフェイスを構成した後、ルーティング ポリシー: リリース 25.0(2) （14 ページ） で説明されているように、同じ接続先へのトンネルを形成できる追加のネットワークで IPsec トンネル ソース インターフェイスを構成できます。

[プロパティ（Properties）]	説明
	5. この IPSec トンネルを追加するには、チェックマークをクリックします。 別の IPSec トンネルを追加する場合は、**[+ IPSec トンネルの追加（+ Add IPSec Tunnel）]** をクリックします。 6. **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスで **[追加（Add）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

ステップ 4 外部ネットワークの作成が完了したら、**[保存（Save）]** をクリックします。
[外部ネットワークの作成（Create External Network）] ウィンドウで **[保存（Save）]** をクリックすると、クラウド ルータが AWS で構成されます。

グローバル VRF 間ルート リーク ポリシーの構成

グローバル VRF 間ルート リーク ポリシー機能は、リリース 25.0(2) で導入されました。

始める前に

[クラウド APIC セットアップ（Cloud APIC Setup）] ウィンドウの **[コントラクト ベース ルーティング（Contract Based Routing）]** 領域で変更を行う前に、内部 VRF 間のルート リーク（14 ページ）で提供された情報を確認してください。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[クラウド APIC セットアップ（Cloud APIC Setup）]** をクリックします。
[セットアップ - 概要] ダイアログ ボックスが表示されます。

ステップ 4 **[コントラクト ベースのルーティング]** 領域で、**[コントラクト ベースのルーティング]** フィールドの現在の設定を書き留めます。

[コントラクト ベースのルーティング]設定は、現在の内部 VRF ルート リーク ポリシーを反映しています。これは、インフラ テナントの下のグローバル ポリシーであり、ブール フラグを使用して、コントラクトがルート マップがない場合にルートを駆動できるかどうかを示します。

- **オフ**: デフォルト設定。ルートがコントラクトに基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。

- **オン（On）**：ルート マップが存在しない場合に、契約に基づいてルートが漏洩していることを示します。有効にすると、ルート マップが構成されていないときにコントラクトがルーティングを駆動します。ルート マップが存在する場合、ルート マップは常にルーティングを駆動します。

ステップ 5 **[コントラクト ベースのルーティング]** フィールドの現在の設定を変更するかどうかを決定します。

ある設定から別の設定に切り替える場合は、次の手順に従います。

- **オン設定からオフへの切り替え (コントラクト ベースのルーティングを無効にする)**：この状況では、現在、コントラクトベースのルーティングが構成されており、ルートマップベースのルーティングに切り替えることが想定されています。コントラクトベースのルーティングからルート マップベースのルーティングに切り替える前にマップ ベースのルーティングが設定されていない場合、これは混乱を招く可能性があります。

  この状況で**オン**設定から**オフ**設定に切り替える前に、次の変更を行います。

  1. 既存の契約を持つ VRF のすべてのペア間で、ルート マップ ベースのルート リークを有効にします。

     Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 （81 ページ） の手順を実行します。

  2. グローバル ポリシーでコントラクト ベースのルート ポリシーを無効にします。

     [コントラクト ベースのルーティング] フィールドのスイッチを **[オン]** 設定から **[オフ]** 設定に切り替えて、契約ベースのルーティングからルート マップ ベースのルーティングに切り替えます。

  3. 有効にした新しいルート マップ ベースのルーティングに基づいて必要な粒度を反映するようにルーティングを変更します。

- **オフ設定からオンへの切り替え（契約ベースのルーティングを有効にする）**：この状況では、現在マップ ベースのルーティングが構成されており、契約ベースのルーティングに切り替えることが想定されています。コントラクトとルート マップの両方を VRF のペア間で有効にできるため、これは中断を伴う操作ではなく、付加的な操作です。このような状況では、ルーティングを有効にするときに、コントラクトよりもルートマップが優先されます。マップ ベースのルーティングが有効になっている場合、コントラクト ベースのルーティングを追加しても中断は発生しません。

  そのため、この状況では、**オフ**設定から**オン**設定に切り替える前に変更を行う必要はありません。ただし、VRF のペア間でコントラクトとルート マップの両方を有効にせず、完全にコントラクト ベース ルーティングに移行する場合は、VRF 間のコントラクトを完全に設定し、**[コントラクト ベースのルーティング]** フィールドで **[オン]** 設定に切り替える前に VRF 間のルート マップを削除する必要があります。

ステップ 6 **[コントラクト ベースのルーティング]** 領域の現在の設定を変更する場合は、必要なルーティングのタイプに基づいて設定を切り替えます。

ステップ 7 **Cloud APIC セットアップ**の構成が完了したら、**[完了]** をクリックします。

Cisco Cloud APIC GUI を使用したリーク ルートの構成

Cisco Cloud APIC GUI を使用してリーク ルートを設定する手順は、リリースによって若干異なります。

- 25.0(2) より前のリリースでは、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先の間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。これらの手順については、Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 （81 ページ） を参照してください。
- リリース 25.0(2) 以降では、内部 VRF のペア間のルート マップベースのルート リークがサポートされています。これらの手順については、Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成 （84 ページ） を参照してください。

Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定

リーク ルートの設定は、ルーティング ポリシーとセキュリティ ポリシーが別々に設定されるリリース 25.0(1) アップデートの一部です。VRF 間ルーティングを使用すると、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先との間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。詳細については、「サポートされているルーティングとセキュリティ ポリシーの概要（11 ページ）」を参照してください。

外部宛先は、Azure サイトから外部デバイスへの接続を有効にする （87 ページ） 手順を使用して手動で構成する必要があります。外部の接続先は、別のクラウドサイト、ACIオンプレミス サイト、または分散拠点である可能性があります。

（注）
- これら手順を使用して、セキュリティ ポリシーとは無関係に、内部と 外部VRF の間でのみルーティング ポリシーを構成します。
- これらの手順を使用して、内部 VRF のペア間のルーティングを設定しないでください。その場合、リリース 25.0(1) より前の通常どおりにコントラクトを使用します。

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。
設定された VRF が表示されます。

ステップ 2 **[リーク ルート（Leak Routes）]** タブをクリックします。
すでに構成されているリーク ルートが表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[リーク ルートの作成（Create Leak Route）]** を選択します。
[リーク ルートの作成（Create a Leak Route）] ウィンドウが表示されます。

ステップ 4 次の *[*リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *10* : リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）

[プロパティ（Properties）]	説明
Source VRF	送信元 VRF を選択するには： 1. **[送信元 VRF の選択（Select Source VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。 送信元 VRF は、内部または 外部VRF であることに注意してください。 3. **[選択（Select）]** をクリックして、この送信元 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。
宛先 VRF	宛先 VRF を選択するには、次の手順を実行します。 1. **[宛先の選択（Select destination）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択してます。 送信元 VRF も内部 VRF である場合、接続先 VRF を内部 VRF にすることはできないことに注意してください。 3. **[選択（Select）]** をクリックして、この宛先 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。
Type	構成するリーク ルートのタイプを選択します。 • **すべてをリーク**: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを構成することを選択します。 この場合、デフォルトでは、エントリ `0.0.0.0/0` がサブネット IP エリアに自動的に入力されます。 • **サブネット IP** : 接続元 VRF から 接続先 VRF までのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。**[サブネット IP（Subnet IP）]** ダイアログボックスが表示されます。 **[サブネット IP（Subnet IP）]** ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。
[成功（Success）] ウィンドウが表示されます。

ステップ 6 追加の VRF 間ルート リークを設定するかどうかを決定します。

- VRF のペア間でリークする別のルートを追加する場合は、**[成功（Success）]** ウィンドウで **[別のリーク ルートの追加（Add Another Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （81 ページ）ーステップ 5 （82 ページ） を繰り返します。

- リバース ルートを追加する場合は、次のようにします。

  - 以前の設定の宛先 VRF が送信元 VRF になり、
  - 以前の設定の送信元 VRF が宛先 VRF になります。

  次に、**[成功（Success）]** ウィンドウで **[リバース リーク ルートの追加（Add Reverse Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。ステップ 4 （81 ページ）ーステップ 5 （82 ページ） を繰り返して別のルートを設定しますが、今度は次のようになります。

  - **[送信元 VRF（Source VRF）]** フィールドで、前の設定で宛先 VRF として選択したVRF を選択します。
  - **[宛先 VRF（Destination VRF）]** フィールドで、前の設定で送信元 VRF として選択した VRF を選択します。

ステップ 7 リーク ルートの設定が完了したら、**[完了（Done）]** をクリックします。

メイン **VRF** ページの **[リーク ルート（Leak Routes）]**タブが再び表示され、新しく設定されたリーク ルートが表示されます。

ステップ 8 送信元または宛先VRFの詳細情報を取得したり、構成済みのリーク ルートを変更したりするには、メイン **[VRF]** ページの**[リーク ルート（Leak Routes）]** タブで [VRF] をダブルクリックします。
そのルート テーブルの **[概要（Overview）]** ページが表示されます。

ステップ 9 [VRF] ページの上部にある **[アプリケーション管理（Application Management）]** タブをクリックし、左側のナビゲーションバーで**[リーク ルート（Leak Routes）]**タブをクリックします。
この特定の VRF に関連付けられているリーク ルートが表示されます。

ステップ 10 必要に応じて、この VRF に関連付けられた追加のリーク ルートを設定します。

- この VRF からリーク ルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> からリーク ルートを追加（Add Leak Route from <VRF_name>）]**を選択します。

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （81 ページ） の情報を使用して、必要な情報を入力します。**送信元 VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

- この VRF にリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> にリーク ルートを追加（Add Leak Route to <VRF_name>）]**を選択します。

[リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （81 ページ）の情報を使用して、必要な情報を入力します。**宛先 VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

次のタスク

これでルーティング ポリシーが構成されました。ルーティング ポリシーとセキュリティ ポリシーは別であるため、セキュリティ ポリシーを別個に構成する必要があります。

- Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ）: 次の手順を使用して、外部 EPG を作成します。
- Cisco Cloud APIC GUI を使用したコントラクトの作成 （121 ページ）: これらの手順を使用して、外部 EPG とクラウド EPG 間のコントラクトを作成します。

Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成

リリース 25.0(2) 以降、内部 VRF 間のルート リーク （14 ページ） で説明されているように、内部 VRF のペア間のルート マップベースのルート リークがサポートされます。この機能は、リリース 25.0(1) で提供されたルーティングとセキュリティの分割更新を拡張したもので、ルーティングとセキュリティ ポリシーが別々に設定されています。

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。
設定された VRF が表示されます。

ステップ 2 **[リーク ルート（Leak Routes）]** タブをクリックします。
すでに構成されているリーク ルートが表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[リーク ルートの作成（Create Leak Route）]** を選択します。
[リーク ルートの作成（Create a Leak Route）] ウィンドウが表示されます。

ステップ 4 次の *[*リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *11 :* リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）

[プロパティ（Properties）]	説明
Source VRF	送信元 VRF を選択するには： 1. **[送信元 VRF の選択（Select Source VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続元 VRF には内部 VRF を選択します。 3. **[選択（Select）]** をクリックして、この送信元 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。
宛先 VRF	宛先 VRF を選択するには、次の手順を実行します。 1. **[宛先の選択（Select destination）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択してます。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続先 VRF には内部 VRF を選択します。 3. **[選択（Select）]** をクリックして、この宛先 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。
Type	構成するリーク ルートのタイプを選択します。 • **すべてをリーク**: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを構成することを選択します。 この場合、デフォルトでは、エントリ `0.0.0.0/0` がサブネット IP エリアに自動的に入力されます。 • **サブネット IP**：接続元 VRF から 接続先 VRF までのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。**[サブネット IP（Subnet IP）]** ダイアログボックスが表示されます。 **[サブネット IP（Subnet IP）]** ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。

ステップ 5　作業が完了したら、[保存（Save）] をクリックします。

[成功（Success）] ウィンドウが表示されます。

ステップ 6 追加の VRF 間ルート リークを設定するかどうかを決定します。

- VRF のペア間でリークする別のルートを追加する場合は、**[成功（Success）]** ウィンドウで **[別のリーク ルートの追加（Add Another Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （84 ページ）ーステップ 5 （85 ページ） を繰り返します。

- リバース ルートを追加する場合は、次のようにします。

  - 以前の設定の宛先 VRF が送信元 VRF になり、
  - 以前の設定の送信元 VRF が宛先 VRF になります。

  次に、**[成功（Success）]** ウィンドウで **[リバース リーク ルートの追加（Add Reverse Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。ステップ 4 （84 ページ）ーステップ 5 （85 ページ） を繰り返して別のルートを設定しますが、今度は次のようになります。

  - **[送信元 VRF（Source VRF）]** フィールドで、前の設定で宛先 VRF として選択したVRF を選択します。
  - **[宛先 VRF（Destination VRF）]** フィールドで、前の設定で送信元 VRF として選択した VRF を選択します。

ステップ 7 リーク ルートの設定が完了したら、**[完了（Done）]** をクリックします。

メイン **VRF** ページの **[リーク ルート（Leak Routes）]**タブが再び表示され、新しく設定されたリークルートが表示されます。

ステップ 8 送信元または宛先VRFの詳細情報を取得したり、構成済みのリークルートを変更したりするには、メイン **[VRF]** ページの**[リーク ルート（Leak Routes）]** タブで [VRF] をダブルクリックします。
そのルート テーブルの **[概要（Overview）]** ページが表示されます。

ステップ 9 [VRF] ページの上部にある **[アプリケーション管理（Application Management）]** タブをクリックし、左側のナビゲーションバーで**[リーク ルート（Leak Routes）]**タブをクリックします。
この特定の VRF に関連付けられているリーク ルートが表示されます。

ステップ 10 必要に応じて、この VRF に関連付けられた追加のリーク ルートを設定します。

- このVRFからリーク ルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> からリーク ルートを追加（Add Leak Route from <VRF_name>）]**を選択します。

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （84 ページ） の情報を使用して、必要な情報を入力します。**送信元VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

- この VRF にリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> にリーク ルートを追加（Add Leak Route to <VRF_name>）]**を選択します。

[リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （84 ページ）の情報を使用して、必要な情報を入力します。**宛先 VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

Azure サイトから外部デバイスへの接続を有効にする

次の手順に従って、インフラ VNet CCR から IPSec/BGP を使用して任意の外部デバイスへの IPv4 接続を手動で有効にします。

外部デバイス構成ファイルのダウンロード

ステップ 1 Cisco Cloud APIC GUI で、**[ダッシュボード（Dashboard）]** をクリックします。
Cisco Cloud APIC の **[ダッシュボード（Dashboard）]** ビューを表示します。

ステップ 2 **[インフラストラクチャ]** > **[外部接続]**に移動します。
[外部接続（External Connectivity）] ウィンドウが表示されます。

ステップ 3 **[アクション（Actions）]** > **[外部デバイス構成ファイルのダウンロード（Download External Device Configuration Files）]** をクリックします。
[外部デバイス構成ファイルのダウンロード（Download External Device Configuration Files）] ポップアップが表示されます。

ステップ 4 ダウンロードする外部デバイス構成ファイルを選択し、**[ダウンロード（Download）]** をクリックします。
このアクションにより、CCR への IPv4 接続のための外部デバイスの手動構成に使用する構成情報を含む zip ファイルがダウンロードされます。

Azure サイトから外部デバイスへの接続を有効にする

ステップ 1 インフラ VNet CCR から EVPN を使用しない外部デバイスへの IPv4 接続を手動で有効にするために必要な情報を収集します。

ステップ 2 外部デバイスにログインします。

ステップ 3 外部ネットワーキング デバイスを接続するための構成情報を入力します。

外部デバイス構成ファイルのダウンロード （87 ページ） の手順を使用して外部デバイス構成ファイルをダウンロードした場合、最初のトンネルの構成情報を見つけて、その構成情報を入力します。

最初のトンネルの外部デバイス設定ファイルの例を示します。

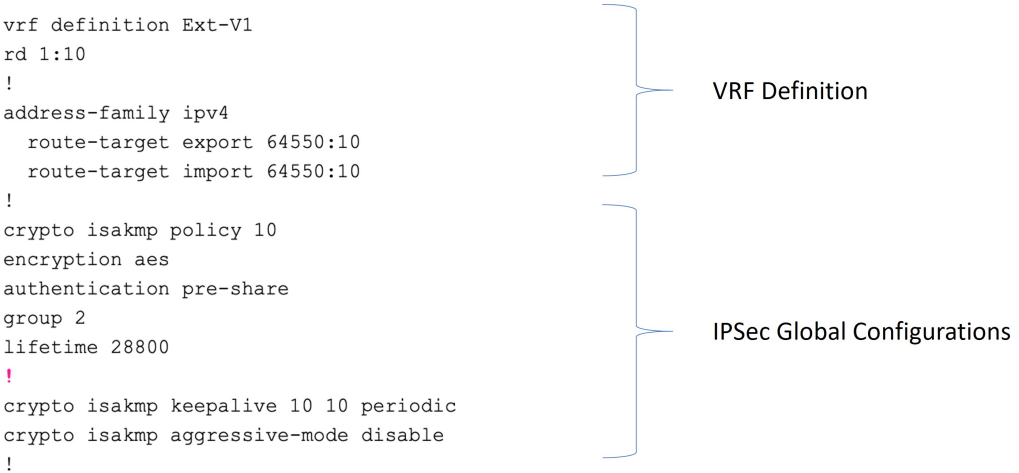
```
! The following file contains configuration recommendation to connect an external networking device
 with the cloud ACI Fabric
! The configurations here are provided for an IOS-XE based device. The user is expected to understand
 the configs and make any necessary amends before using them
! on the external device. Cisco does not assume any responsibility for the correctness of the config.
```

```
! Tunnel to 128.107.72.122 1.100 [ikev2] for
hctunnIf.acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! USER-DEFINED: please define GigabitEthernet2 if required
! USER-DEFINED: please define tunnel-id: 100 if required
! USER-DEFINED: please define vrf-name: infra:externalvrf1 if required
! USER-DEFINED: please define gig3-public-ip: 13.88.168.176 if 0.0.0.0 ip still not provided by AWS.
! Device:            128.107.72.122
! Tunnel ID:         100
! Tunnel counter:    1
! Tunnel address:    5.16.1.9
! Tunnel Dn:
acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! VRF name:          infra:externalvrf1
! ikev:              ikev2
! Bgp Peer addr:     5.16.1.10
! Bgp Peer asn:      65015
! Gig3 Public ip:    13.88.168.176
! PreShared key:     device1azure
! ikev profile name: ikev2-100

vrf definition infra:externalvrf1
    rd 1:1

    address-family ipv4
        route-target export 64550:1
        route-target import 64550:1
    exit-address-family
exit

crypto ikev2 proposal ikev2-infra:externalvrf1
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-infra:externalvrf1
    proposal ikev2-infra:externalvrf1
exit

crypto ikev2 keyring keyring-ikev2-100
    peer peer-ikev2-keyring
        address 13.88.168.176
        pre-shared-key device1azure
    exit
exit

crypto ikev2 profile ikev2-100
    match address local interface GigabitEthernet2
    match identity remote address 13.88.168.176 255.255.255.255
    identity local address 128.107.72.122
    authentication remote pre-share
    authentication local pre-share
    keyring local keyring-ikev2-100
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set ikev2-100 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile ikev2-100
    set transform-set ikev2-100
```

```
    set pfs group14
    set ikev2-profile ikev2-100
exit

interface Tunnel100
    vrf forwarding infra:externalvrf1
    ip address 5.16.1.10 255.255.255.252
    ip mtu 1400
    ip tcp adjust-mss 1400
    tunnel source GigabitEthernet2
    tunnel mode ipsec ipv4
    tunnel destination 13.88.168.176
    tunnel protection ipsec profile ikev2-100
exit

ip route 13.88.168.176 255.255.255.255 GigabitEthernet2 GIG-GATEWAY

router bgp 65015

address-family ipv4 vrf infra:externalvrf1
    redistribute connected
    maximum-paths eibgp 32

    neighbor 5.16.1.9 remote-as 65008
    neighbor 5.16.1.9 ebgp-multihop 255
    neighbor 5.16.1.9 activate
    neighbor 5.16.1.9 send-community both

    distance bgp 20 200 20
exit-address-family
```

次の図に、外部デバイス構成ファイルで使用される各フィールド セットの詳細を示します。

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - vrf definition
  - IPSec global configurations



- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - トンネルごとの IPSec および ikev1 構成

- VRF ネイバーの BGP 設定

```
!
crypto keyring Ext-V1-1000-ike
  pre-shared-key address <50.18.55.126>[cAPIC CSR Gig3 public IP] key <abcdefg12345>
!
crypto isakmp profile Ext-V1-1000-ike
   keyring Ext-V1-1000-ike
   match identity address <50.18.55.126>[cAPIC CSR1 gig3 Public IP] 255.255.255.255
!
crypto ipsec transform-set Ext-V1-1000-ike esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile Ext-V1-1000-ike
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set Ext-V1-1000-ike
set pfs group14
!
interface Tunnel1000
vrf forwarding Ext-V1
ip address 50.50.0.2[cAPIC CSR BGP Peer Addr] 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1400
tunnel source GigabitEthernet2
tunnel mode ipsec ipv4
tunnel destination <50.18.55.126>[cAPIC CSR1 gig3 Public IP]
tunnel protection ipsec profile Ext-V1-1000-ike
!
router bgp 64550
!
address-family ipv4 vrf Ext-V1
  redistribute connected
  neighbor <50.50.0.1>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.1 ebgp-multihop 255
  neighbor 50.50.0.1 activate
  neighbor 50.50.0.1 send-community both
  neighbor <50.50.0.5>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.5 ebgp-multihop 255
  neighbor 50.50.0.5 activate
  neighbor 50.50.0.5 send-community both
  distance bgp 20 200 20
!
ip route 50.18.55.126[cAPIC CSR1 gig3 Public IP] 255.255.255.255 GigabitEthernet2 10.10.0.103
```

IPSec and Ikev1
Per Tunnel Configurations

BGP Configurations for VRF Neighbor

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - グローバル構成
  - トンネルごとの IPSec および ikev2 の構成

```
crypto ikev2 proposal ikev2-1
 encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
 integrity sha512 sha384 sha256 sha1
 group 24 21 20 19 16 15 14 2
!
crypto ikev2 policy ikev2-1
 proposal ikev2-1
!
crypto ikev2 keyring keyring-ikev2-2000
 peer peer-ikev2-keyring
  address 35.81.94.248 [cAPIC CSR1 gig3 Public IP]
  pre-shared-key abcdefg12345
!
crypto ikev2 profile ikev2-2000
 match address local interface GigabitEthernet3
 match identity remote address 35.81.94.248[cAPIC CSR1 gig3 Public IP] 255.255.255.255
 identity local address 52.53.49.193 [Local Device tunnel source interface Public IP (Gig3 public IP)]
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-ikev2-2000
 lifetime 3600
 dpd 10 5 on-demand
!
crypto ipsec transform-set ikev2-2000 esp-gcm 256
 mode tunnel
!
crypto ipsec profile ikev2-2000
 set transform-set ikev2-2000
 set pfs group14
 set ikev2-profile ikev2-2000
!
interface Tunnel2000
 vrf forwarding Ext-V1
 ip address 50.50.0.14 [cAPIC CSR1 BGP Peer Addr] 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet3
 tunnel mode ipsec ipv4
 tunnel destination 35.81.94.248[cAPIC CSR1 gig3 Public IP]
 tunnel protection ipsec profile ikev2-2000
```

Ikev2 Global Configurations

IPSec and Ikev2
Per Tunnel Configurations

ステップ 4 前の手順を繰り返して、追加のトンネルを構成します。

Cisco Cloud APIC GUI を使用した EPG の作成

このセクションの手順を使用して、アプリケーション EPG、外部 EPG、サービス EPG を作成します。使用可能な構成オプションは、作成する EPG のタイプによって異なります。

Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成

このセクションでは、Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成方法を説明します。各サービスは、少なくとも 1 つのコンシューマー EPG と 1 つのプロバイダー EPG を必要とします。

（注） インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。すべてのクラウド EPG とクラウド外部 EPG は、インフラ テナントのセカンダリ VRF に関連付けられます。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外部 EPG と通信可能で、他のユーザー テナント VRF 内のクラウド EPG とも通信できます。既存の「クラウド インフラ」アプリケーション プロファイルを使用せず、代わりにインフラ テナントに新しいアプリケーション プロファイルを作成し、新しいアプリケーション プロファイルをセカンダリ VRF のクラウド EPG およびクラウド外部 EPG に関連付けることをお勧めします。

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。

[EPG の作成（Create EPG）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[EPG* 作成ダイアログボックスのフィールド（*Create EPG Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *12 : [EPG* の作成（*Create EPG*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	EPG の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 リリース 5.0(2) 以降では、このセクションで前述したように、インフラ テナントを選択し、インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
アプリケーション プロファイル	アプリケーション プロファイルを選択します。 1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。 2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーション プロファイルをクリックして選択します。 （注） インフラ テナントで EPG を作成する場合、アプリケーション プロファイルはオーバーレイ-1 VRF の EPG で使用されるため、クラウド インフラ アプリケーション プロファイルを選択しないことを推奨します。異なるアプリケーション プロファイルを選択するか、**[アプリケーション プロファイルの作成（Create Application Profile）]** を選択して、新しいプロファイルを作成します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定（Settings）]	
タイプ（Type）	これはアプリケーション EPG であるため、EPG タイプとして **[アプリケーション（Application）]** を選択します。

[プロパティ（Properties）]	説明
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 インフラ テナントで EPG を作成している場合は、この手順でセカンダリ VRF を選択します。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外部 EPG と通信可能で、他のユーザー テナント VRF 内のクラウド EPG とも通信できます。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
エンドポイントセレクタ	

[プロパティ（Properties）]	説明
	（注） エンドポイントセレクタ設定プロセスの一部として Azure で仮想マシンを設定する手順については、Azure での仮想マシンの構成 （138 ページ） を参照してください。 エンドポイント セレクタを追加するには： 1. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックして、**[エンドポイント セレクタの追加]** ダイアログを開きます。 2. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ダイアログの **[Name（名前）]** フィールドに名前を入力します。 3. **[セレクタ式（Selector Expression）]** をクリックします。**[キー（Key）]**、**[演算子（Operator）]**、および **[値（Value）]** フィールドが有効になります。 4. **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。次のオプションがあります。 • エンドポイント セレクタに IP アドレスまたはサブネットを使用する場合は、**[IP]** を選択します。 （注） IPv6 は Azure では Cisco Cloud APIC に対してサポートされていません。このフィールドには有効なIPv4アドレスを使用する必要があります。 • エンドポイント セレクタに Azure リージョンを使用する場合は、**[リージョン（Region）]** を選択します。 • エンドポイント セレクタのカスタム キーを作成する場合は、**[カスタム（Custom）]** を選択します。 （注） **[カスタム（Custom）]** オプションを選択すると、ドロップダウン リストがテキスト ボックスになります。**custom:** の後にスペースのキーの名前を入力する必要があります（例：**custom: Location**）。 5. **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。次のオプションがあります。 • **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。 • **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。 • **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。 • **[の中にない（Not In）]**:値フィールドに複数のカンマ区切り値がある場合に使用されます。 • **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。 • **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用され

[プロパティ（Properties）]	説明
	ます。 **6.** **[値（Value）]** フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。入力する値は、**[キー（Key）]** フィールドと **[演算子（Operator）]** フィールドで選択した内容によって異なります。たとえば、**[キー（Key）]** フィールドが **[IP]** に設定され、**[演算子（Operator）]** フィールドが **[等しい（equals）]** に設定されている場合、**[値（Value）]** フィールドは IP アドレスまたはサブネットでなければなりません。ただし、**[演算子（Operator）]** フィールドが **[キー（keys）]** に設定されている場合、**[値（Value）]** フィールドは無効になります。 **7.** 完了したら、チェックマークをクリックしてセレクタ式を検証します。 **8.** エンドポイント セレクタに追加のエンドポイント セレクタ式を作成するかどうかを決定します。単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。 たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。 • エンドポイント セレクタ 1、式 1: • **[キー (Key):]** Region • **演算子（Operator）** : equals • 値：westus • エンドポイント セレクタ1、式 2: • **[キー (Key):]** IP • **演算子 (Operator）** : equals • **[値 (Value):]** 192.0.2.1/24 この場合、これらの式の両方が真になる場合（リージョンが westus で、IP アドレスがサブネット 192.0.2.1/24 に属している場合）に、そのエンドポイントはクラウド EPG に割り当てられます。

[プロパティ（Properties）]	説明
	9. このエンドポイント セレクタで作成するすべての式を追加した後で、 チェックマークをクリックし、終了したら、**[追加（Add）]** をクリックします。 EPG の下で複数のエンドポイント セレクタを作成した場合は、それらのエンドポイント セレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイント セレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイント セレクタを作成したとします。 • エンドポイント セレクタ 2、式 1: • **[キー (Key):]** Region • **演算子**： in • **値**： eastus、centralus その場合、次のようになります。 • リージョンが westus で、IP アドレスが 192.0.2.1/24 サブネットに属している (エンドポイント セレクタ 1 の式) または • リージョンが eastus または centralus のどちらかである場合（エンドポイント セレクタ 2 式） その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した外部 EPG の作成

このセクションでは、Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成方法を説明します。各サービスには、少なくとも 1 つのコンシューマ EPG と 1 つのプロバイダー EPG が必要です。

（注） インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。すべてのクラウド EPG とクラウド外部 EPG は、インフラ テナントのセカンダリ VRF に関連付けられます。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外部 EPG と通信可能で、他のユーザー テナント VRF 内のクラウド EPG とも通信できます。既存の「クラウド インフラ」アプリケーション プロファイルを使用せず、代わりにインフラ テナントに新しいアプリケーション プロファイルを作成し、新しいアプリケーション プロファイルをセカンダリ VRF のクラウド EPG およびクラウド外部 EPG に関連付けることをお勧めします。

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。

[EPG の作成（Create EPG）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[EPG* 作成ダイアログボックスのフィールド（*Create EPG Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *13 : [EPG* の作成（*Create EPG*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	EPG の名前を入力します。

[プロパティ（Properties）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 リリース 5.0(2) 以降では、このセクションで前述したように、インフラ テナントを選択し、インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
アプリケーション プロファイル	アプリケーション プロファイルを選択します。 1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。 2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーション プロファイルをクリックして選択します。 （注） インフラ テナントで EPG を作成する場合、アプリケーション プロファイルはオーバーレイ-1 VRF の EPG で使用されるため、クラウド インフラ アプリケーション プロファイルを選択しないことを推奨します。異なるアプリケーション プロファイルを選択するか、**[アプリケーション プロファイルの作成（Create Application Profile）]** を選択して、新しいプロファイルを作成します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定（Settings）]	
タイプ（Type）	これは外部 EPG であるため、EPG タイプとして **[外部（External）]** を選択します。

[プロパティ（Properties）]	説明
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 インフラ テナントで EPG を作成している場合は、この手順でセカンダリ VRF を選択します。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外部 EPG と通信可能で、他のユーザー テナント VRF 内のクラウド EPG とも通信できます。 3. **[選択（Select）]** をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
ルート到達可能性	外部 EPG のルート到達可能性のタイプを選択します。次のオプションがあります。 • **インターネット** • **外部サイト**

[プロパティ（Properties）]	説明
エンドポイントセレクタ	（注） エンドポイントセレクタ設定プロセスの一部として Azure で仮想マシンを設定する手順については、Azure での仮想マシンの構成 （138 ページ） を参照してください。 エンドポイント セレクタを追加するには： 1. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックして、エンドポイント セレクタを追加します。 2. [名前（Name）] フィールドに名前を入力します。 3. **サブネット**にサブネットを入力します。 （注） IPv6 は Azure では Cisco Cloud APIC に対してサポートされていません。このフィールドには有効なIPv4アドレスを使用する必要があります。 4. 終了したら、チェックマークをクリックしてエンドポイント セレクタを検証します。 5. 追加のエンドポイント セレクタを作成するかどうかを決定します。 EPG の下で複数のエンドポイント セレクタを作成した場合は、それらのエンドポイント セレクタの間には論理 OR があるものとみなされます。たとえば、2 つのエンドポイント セレクタを作成したとします。 • エンドポイントセレクタ 1： • **名前**：EP_Sel_1 • **サブネット**：192.1.1.1/24 • エンドポイント セレクタ 2： • **名前**：EP_Sel_2 • **サブネット**：192.2.2.2/24 その場合、次のようになります。 • IP アドレスが 192.1.1.1/24 サブネット（エンドポイント セレクタ 1）に属する場合 または • IPアドレスが 192.2.2.2/24 サブネット（エンドポイント セレクタ 2）に属する場合 その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 5 設定が終わったら [Save] をクリックします。

サービス EPG の作成

次のセクションの手順を使用して、サービス EPG を作成します。

サービス EPG を構成する前に実行するタスク

サービス EPG を構成する前に、事前に実行する必要がある特定のタスクがあります。サービス EPG でサブネットまたはプライベート リンク ラベルを使用している場合は、最初にサービス EPG の外部にサブネットまたはプライベート リンク ラベルを構成する必要があります。

ステップ 1 必要に応じて VRF を作成します。

a) **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

b) **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

c) **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[VRF の作成（Create VRF）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログ ボックスが表示されます。

d) 次のように選択します。

- **名前**：VRF の名前を入力します。
- **テナント**：テナントを選択します。

e) [保存（Save）] をクリックします。

ステップ 2 クラウド コンテキスト プロファイルを構成します。

a) **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

b) **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

c) **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[クラウド コントラクト プロファイルの作成（Create Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログ ボックスが表示されます。

ステップ 3 次の *[クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド（Create Cloud Context Profile Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *14:* クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（**Name**）	クラウド コンテキスト プロファイルの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
説明	クラウド コンテキスト プロファイルの説明を入力します。
Settings	
リージョン（**Region**）	リージョンを選択するには: 1. **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。 2. **[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
CIDR の追加（Add CIDR）	

[プロパティ（Properties）]	説明
	（注） VNet ピアリングが有効なとき、CIDR を追加、削除、または編集できません。CIDR を追加、削除、または編集する前に、VNet ピアリングを無効にする必要があります。VNet ピアリングを無効にするには： • インフラ テナントの場合は、クラウド コンテキスト プロファイルの **[ハブ ネットワーク ピアリング（Hub Network Peering）]** オプションを無効にします。 • ユーザー（非インフラ）テナントの場合、クラウド コンテキスト プロファイルの **[VNet ピアリング（VNet Peering）]** オプションを無効にします。 CIDR 構成を変更した後、VNet ピアリングを再度有効にします。 次の機能はリリースによってサポートされます。 • インフラ VNet の追加のセカンダリ CIDR およびサブネットを追加することもできます（クラウド テンプレートで作成された `cloudCtxProfiles`）。クラウド テンプレートで作成されたプライマリ CIDR を追加したり、既存の CIDR を変更できません。サブネットがユーザー作成の CIDR で作成された後、サブネットが暗黙的にセカンダリ VRF にマッピングされます。 • インフラ VNet 以外の追加のセカンダリ CIDR および VNet のサブネットを追加することもできます。 詳細については、「単一 VNet での複数の VRF のサポート （39 ページ）」を参照してください。 CIDR を追加するには、次の手順を実行します。 1. **[CIDR の追加（Add CIDR）]** をクリックします。**[CIDR の追加（Add CIDR）]** ダイアログボックスが表示されます。 2. **[CIDR ブロック範囲（CIDR Block Range）]** フィールドにアドレスを入力します。 3. **[プライマリ（Primary）]** チェックボックスをオン（有効）またはオフ（無効）にします。 追加のセカンダリ CIDR および VNet のサブネットを追加している場合、**[プライマリ（Primary）]** ボックスのチェックを外します。 4. **[サブネットの追加（Add Subnet）]** をクリックして、次の情報を入力します。 • **[アドレス（Address）]** フィールドに、サブネット アドレスを入力します。 • **[名前（Name）]** フィールドに、このサブネットの名前を入力します。 • **[プライベート リンク ラベル（Private Link Label）]** フィールドで、**[新規作成（Create New）]** を選択し、プライベート リンク ラベルの固有の名前を入力し、このサブネットに関連付けます。 5. **[VRF]** フィールドで、必要に応じて選択します。

[プロパティ（Properties）]	説明
	• **[プライマリ（Primary）]** フィールドの横にあるボックスをオンにすると、この CIDR は自動的にプライマリ VRF に関連付けられます。 • **[プライマリ（Primary）]** フィールドの横にあるチェックボックスをオンにしなかった場合は、この CIDR をセカンダリ VRF に関連付けることができます。VRFの横にある **[X]** をクリックし、**[VRF の選択（Select VRF）]** をクリックして、この CIDR に関連付けるセカンダリ VRF を選択します。 **6.** 完了したら、**[追加（Add）]** をクリックします。
VNet ゲートウェイ ルータ	クリックして **[VNet ゲートウェイ ルータ（VNet Gateway Router）]** チェック ボックスをチェック（有効）またはチェックを外します（無効）。
VNET ピアリング	クリックしてAzure VNet ピアリング機能をチェック（有効）またはチェックを外します（無効）。 VNetピアリング機能の詳細については、Cisco Cloud APICドキュメンテーションページの「Configuring VNet Peering for Cloud APIC for Azure」を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/series.html#Configuration

ステップ 4 [保存（Save）] をクリックします。

Cisco Cloud APIC GUI を使用したサービス EPG の作成

このセクションでは、Cisco Cloud APIC GUI を使用したサービス EPG の作成方法を説明します。各サービスには、少なくとも 1 つのコンシューマ EPG と 1 つのプロバイダー EPG が必要です。

始める前に

- クラウド サービス エンドポイント グループ （42 ページ）の情報を確認してください。
- **サブネットごとの NSG** 構成が有効になっていることを確認します。

  クラウドサービス EPG を構成している場合は、**サブネットごとの NSG** 構成を有効にする必要があります。詳細については、「セキュリティ グループ （50 ページ）」を参照してください。
- アプリケーション プロファイルと VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが**[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。

[EPG の作成（Create EPG）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[EPG* 作成ダイアログボックスのフィールド（*Create EPG Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *15 : [EPG* の作成（*Create EPG*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	EPG の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
アプリケーション プロファイル	アプリケーション プロファイルを選択します。 1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。 2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーション プロファイルをクリックして選択します。 （注） インフラテナントでサービス EPG を作成する場合、アプリケーションプロファイルはオーバーレイ-1 VRF の EPG で使用されるため、クラウド インフラ アプリケーション プロファイルを選択しないことを推奨します。異なるアプリケーション プロファイルを選択するか、**[アプリケーション プロファイルの作成（Create Application Profile）]** を選択して、新しいプロファイルを作成します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
説明	EPG の説明を入力します。
[設定（Settings）]	
タイプ（Type）	これはサービス EPG であるため、EPG タイプとして [サービス（Service）] を選択します。
VRF	VRF を選択するには、次の手順を実行します。 1. [VRF の選択（Select VRF）] をクリックします。[VRF の選択（Select VRF）] ダイアログボックスが表示されます。 2. [VRFの選択（Select VRF）] ダイアログで、左側の列の VRF をクリックして選択します。 3. [選択（Select）]をクリックします。[EPG の作成（Create EPG）] ダイアログボックスに戻ります。
導入タイプ	EPG 展開タイプを選択します。 サービスは展開モードによって異なります。 • クラウド ネイティブ：プロバイダ ネットワークに展開されたクラウド ネイティブ サービス • クラウド ネイティブ管理対象：ネットワークに展開されたクラウド ネイティブ サービス • サードパーティ：市場からのサードパーティ サービス

[プロパティ（Properties）]	説明
アクセスタイプ	EPG 展開のアクセス タイプを選択します。アクセス タイプは、他のサービスまたは VM がサービスに接続する方法を示します。 選択肢は、**[展開タイプ（Deployment Type）]** フィールドで行った選択によって異なります。 • **クラウド ネイティブ**展開タイプ： • **パブリック**：サービスのパブリック IP にアクセスします。 • **プライベート**：プライベート リンクとプライベート エンドポイントを使用してサービスにアクセスします。 • **クラウド ネイティブ管理対象**展開タイプ： • **プライベート**：管理対象サブネットに展開されたサービスにプライベート IP アドレスのみがある場合は、このタイプを選択します。 • **パブリックおよびプライベート**：パブリック エンドポイントとプライベート エンドポイントを使用してサービスにアクセスします。これは、Cisco Cloud APIC で管理されたサブネットに展開されたときにパブリック IP アドレスも公開するサービスに使用されます。 • **サードパーティ**展開タイプ：**プライベート**は、アクセス タイプとして使用できる唯一のオプションです。これは、サービスが提供する場合、サービスへのプライベート エンドポイントのみを使用することを意味します。

[プロパティ（Properties）]	説明
サービスの種類	Azure サービス タイプを選択します。 特定のサービス タイプは、特定の特定の展開タイプでのみサポートされます。特定の展開タイプでサポートされるサービス タイプの詳細については、クラウド サービス エンドポイント グループ （42 ページ） を参照してください。 次のオプションがあります。 • **Azure Storage Blob**（Azure Storage （46 ページ） を参照） • **Azure SQL** • **Azure Cosmos DB** • **Azure Databricks**（Azure Databricks サービス （47 ページ） を参照） • **Azure Storage**（Azure Storage （46 ページ） を参照） • **Azure Storage File**（Azure Storage （46 ページ） を参照） • **Azure Storage Queue**（Azure Storage （46 ページ） を参照） • **Azure Storage Table**（Azure Storage （46 ページ） を参照） • **Azure Kubernetes Services (AKS)**（Azure Kubernetes サービス （47 ページ） を参照） • **Azure Active Directory Domain Services**（Azure Active Directory ドメイン サービス （47 ページ） を参照） • **Azure Container Registry** • Azure ApiManagement サービス (を参照)Azure ApiManagement サービス （47 ページ） • **Azure Key Vault** • **Redis Cache**（Azure Redis キャッシュ （48 ページ） を参照） • **カスタム サービス**（**展開タイプ**として**サードパーティ**を選択した場合に使用）

ステップ 5 **[展開タイプ（Deployment Type）]** フィールドで選択した内容に応じて、**[エンドポイント セレクタ（Endpoint Selector）]** 領域に必要な情報を入力します。

- 展開タイプとして**クラウド ネイティブ**を選択した場合は、展開タイプとしてクラウド ネイティブを構成する （111 ページ） に進みます。
- 展開タイプとして**クラウド ネイティブ管理対象**を選択した場合は、展開タイプとしてクラウド ネイティブ管理対象を構成する （114 ページ） に進みます。

- 展開タイプとして**サードパーティ**を選択した場合は、展開の種類としてサードパーティを構成する（116 ページ） に進みます。

展開タイプとしてクラウド ネイティブを構成する

このセクションの手順を使用して、サービス EPG の展開タイプとして**クラウド ネイティブ**を構成します。

始める前に

クラウドネイティブ（48 ページ） に記載されている情報を確認して、これらの手順を使用する前に実行する必要があるタスクを理解してください。

ステップ 1 これらの手順を開始する前に、Cisco Cloud APIC GUI を使用したサービス EPG の作成（106 ページ） の手順を完了していることを確認します。

これらの手順は、これらのの手順で展開タイプを構成する前に、`Azure SQL` などのサービス タイプを設定する Cisco Cloud APIC GUI を使用したサービス EPG の作成（106 ページ） で提供される手順の続きです。

ステップ 2 アクセス タイプとして **[プライベート（Private）]** を選択した場合、**[プライベート リンク ラベルの選択（Select Private Link Label）]** オプションが使用可能になります。

プライベート リンク ラベルは、サブネットをサービス EPG に関連付けるために使用されます。

ステップ 3 **[プライベート リンク ラベルの選択（Select Private Link Label）]** をクリックします。

[プライベート リンク ラベルの選択（Select Private Link Label）] ウィンドウが表示されます。

ステップ 4 適切なプライベート リンク ラベルを検索します。

サービス EPG を構成する前に実行するタスク（102 ページ） で提供されている手順を使用して作成したプライベート リンク ラベルを検索します。

ステップ 5 **[プライベート リンク ラベルの選択（Select Private Link Label）]** ウィンドウで、適切なプライベート リンク ラベルを選択します。

[EPG の作成（Create EPG）] ウィンドウに戻ります。

次に、**[エンドポイント セレクタ（Endpoint Selectors）]** フィールドにエンドポイント セレクタを追加します。

ステップ 6 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックします。

[エンドポイント セレクタの追加（Add Endpoint Selector）] ウィンドウが表示されます。

ステップ 7 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ウィンドウの **[Name（名前）]** フィールドに名前を入力します。

ステップ 8 **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。

次のオプションがあります。

- カスタム エンドポイント セレクタを作成する場合は、**[カスタム（Custom）]** を選択します。
- エンドポイント セレクタに Azure リージョンを使用する場合は、**[リージョン（Region）]** を選択します。
- エンドポイント セレクタにサービス リソースの名前を使用する場合、**[名前（Name）]** を選択します。

  たとえば、`ProdSqlServer` という名前の SQL サーバを選択するには、これらの手順の後半で、**[キー（Key）]** フィールドで **[名前（Name）]** を選択し、`[値（Value）]` フィールドに **ProdSqlServer** と入力します。
- エンドポイントセレクタにクラウドプロバイダの ID を使用する場合、**[リソース ID（Resource ID）]** を選択します。

  たとえば、クラウド プロバイダのリソース ID を使用して SQL サーバを選択するには、これらの手順の後に **[キー]** フィールドで **[リソース ID]** を選択し、セレクタの値（`/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer` など）を **[値]** フィールド入力します。

ステップ 9 **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。

次のオプションがあります。

- **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。
- **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 10 **[値（Value）]** フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。

入力する値は、**[キー（Key）]** フィールドと **[演算子（Operator）]** フィールドで選択した内容によって異なります。

たとえば、**[キー（Key）]** フィールドが **[IP]** に設定され、**[演算子（Operator）]** フィールドが **[等しい（equals）]** に設定されている場合、**[値（Value）]** フィールドは IP アドレスまたはサブネットでなければなりません。ただし、**[演算子（Operator）]** フィールドが **[キー（keys）]** に設定されている場合、**[値（Value）]** フィールドは無効になります。

ステップ 11 完了したら、チェックマークをクリックしてセレクタ式を検証します。

ステップ 12 エンドポイント セレクタに追加のエンドポイント セレクタ式を作成するかどうかを決定します。

単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。

たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイント セレクタ 1、式 1:
  - **[キー (Key):]** Region
  - **演算子（Operator）** : equals
  - **値**：`westus`
- エンドポイント セレクタ1、式 2:
  - **キー**： Name
  - **演算子 (Operator）** : equals
  - **値**：`ProdSqlServer`

このケースでは、これらの式の両方が *true* の場合（リージョンが `westus` であり、リソースに関連付けられた名前が `ProdSqlServer` である場合）、そのエンドポイントはサービス EPG に割り当てられます。

ステップ 13 このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックし、終了したら、**[追加（Add）]** をクリックします。

[EPG の作成（Create EPG）] 画面に戻り、新しいエンドポイントセレクタと構成された式が表示されます。

ステップ 14 追加のエンドポイント セレクタを作成する場合は、**[エンドポイント セレクタの追加（Add Endpoint Selector）]** を再度クリックし、これらの手順を繰り返して追加のエンドポイント セレクタを作成します。

EPGの下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイント セレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイント セレクタを作成したとします。

- エンドポイント セレクタ 2、式 1:
  - **[キー (Key):]** Region
  - **演算子**： in
  - **値**： `eastus`、`centralus`

その場合、次のようになります。

- リージョンが `westus` であり、リソースに付けられた名前が `ProdSqlServer` である場合（エンドポイント セレクタ 1 式）

  または

- リージョンが `eastus` または `centralus` のどちらかである場合（エンドポイント セレクタ 2 式）

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 15 設定が終わったら [Save] をクリックします。

展開タイプとしてクラウド ネイティブ管理対象を構成する

このセクションの手順を使用して、サービス EPG の展開タイプとして**クラウド ネイティブ管理**を構成します。

始める前に

クラウド ネイティブ管理対象 （49 ページ） に記載されている情報を確認して、これらの手順を使用する前に実行する必要があるタスクを理解してください。

ステップ 1 これらの手順を開始する前に、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） の手順を完了していることを確認します。

これらの手順は、これらのの手順で展開タイプを構成する前に、`Azure ApiManagement Services` などのサービス タイプを設定する Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） で提供される手順の続きです。

ステップ 2 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックします。

[エンドポイント セレクタの追加（Add Endpoint Selector）] ウィンドウが表示されます。

ステップ 3 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ウィンドウの **[Name（名前）]** フィールドに名前を入力します。

ステップ 4 **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。

現時点では、このアクセス タイプのキーとして使用できるオプションは **IP** のみです。

（注） IPv6 は Azure では Cisco Cloud APIC に対してサポートされていません。このフィールドには有効なIPv4アドレスを使用する必要があります。

ステップ 5 **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。

次のオプションがあります。

- **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。
- **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 6 **[値（Value）]** フィールドに適切な IP アドレスまたはサブネットを入力し、チェックマークをオンにしてエントリを検証します。

サービス EPG を構成する前に実行するタスク （102 ページ） で提供されている手順を使用して作成した IP アドレスまたはサブネットを入力します。

ステップ 7 完了したら、チェックマークをクリックしてセレクタ式を検証します。

ステップ 8 エンドポイント セレクタに追加のエンドポイント セレクタ式を作成するかどうかを決定します。

単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。

たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイント セレクタ 1、式 1:
  - **[キー (Key):]** IP
  - **演算子 (Operator）** ： equals
  - **値** ：192.1.1.1/24
- エンドポイント セレクタ1、式 2:
  - **[キー (Key):]** IP
  - **演算子** ： not equals
  - **値** ：192.1.1.2

この場合、これらの式の両方が true の場合（IP アドレスがサブネット 192.1.1.1/24 に属し、IP アドレスが 192.1.1.2 でない場合）、そのエンドポイントはサービス EPG に割り当てられます。

ステップ 9 このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックし、終了したら、**[追加（Add）]** をクリックします。

[EPG の作成（Create EPG）] 画面に戻り、新しいエンドポイント セレクタと構成された式が表示されます。

ステップ 10 追加のエンドポイント セレクタを作成する場合は、**[エンドポイント セレクタの追加（Add Endpoint Selector）]** を再度クリックし、これらの手順を繰り返して追加のエンドポイント セレクタを作成します。

EPG の下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイント セレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイント セレクタを作成したとします。

- エンドポイント セレクタ 2、式 1:
  - **[キー (Key):]** IP
  - **演算子 (Operator）** ： equals
  - **値** ：192.2.2.2/24

その場合、次のようになります。

- IP アドレスがサブネット 192.1.1.1/24 に属し、IP アドレスが 192.1.1.2 でない場合（エンドポイントセレクタ 1 式）

  または

- IPアドレスがサブネット 192.2.2.2/24 に属する場合

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 11 設定が終わったら [Save] をクリックします。

展開の種類としてサードパーティを構成する

このセクションの手順を使用して、サービス EPG の展開タイプとして**サードパーティ**を構成します。

（注） **[展開タイプ（Deployment Type）]**として**[サードパーティ（Third-Party）]**を選択した場合は、**[サービス タイプ（Service Type）]**として**[カスタム（Custom）]**を選択する必要があります。

ステップ 1 これらの手順を開始する前に、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） の手順を完了していることを確認します。

これらの手順は、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） で提供されている手順の続きであり、これらの手順で展開タイプを構成する前にサービス タイプを`[カスタム サービス（Custom Service）]`として設定します。

ステップ 2 **サードパーティ**の展開タイプのアクセス タイプに必要な選択を行います。

プライベートは、アクセス タイプとして使用できる唯一のオプションです。これは、サービスが提供する場合、サービスへのプライベート エンドポイントのみを使用することを意味します。

[プライベート リンク ラベルの選択（Select Private Link Label）] オプションは、このアクセス タイプで使用できるようになります。プライベート リンク ラベルは、サブネットをサービス EPG に関連付けるために使用されます。

ステップ 3 適切なプライベート リンク ラベルを検索します。

サービス EPG を構成する前に実行するタスク （102 ページ） で提供されている手順を使用して作成したプライベート リンク ラベルを検索します。

ステップ 4 **[プライベート リンク ラベルの選択（Select Private Link Label）]** ウィンドウで、適切なプライベート リンク ラベルを選択します。

[EPG の作成（Create EPG）] ウィンドウに戻ります。

次に、**[エンドポイント セレクタ（Endpoint Selectors）]** フィールドにエンドポイント セレクタを追加します。

ステップ 5 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックします。

[エンドポイント セレクタの追加（Add Endpoint Selector）] ウィンドウが表示されます。

ステップ 6 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ウィンドウの **[Name（名前）]** フィールドに名前を入力します。

ステップ 7 **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。

現時点では、このアクセス タイプのキーとして使用できるオプションは **URL** のみであり、エンドポイント セレクタのサービスを識別するエイリアスまたは完全修飾ドメイン名（FQDN）を使用します。

ステップ 8 **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。

次のオプションがあります。

- **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。
- **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 9 **[値（Value）]** フィールドに有効な URL を入力し、チェックマークをクリックしてエントリを検証します。

ステップ 10 完了したら、チェックマークをクリックしてセレクタ式を検証し、**[追加（Add）]** をクリックします。

[EPG の作成（Create EPG）] 画面に戻り、新しいエンドポイント セレクタと構成された式が表示されます。

ステップ 11 追加のエンドポイント セレクタを作成する場合、**[エンドポイント セレクタ（Add Endpoint Selector）]** を再度クリックし、これらの手順を繰り返して追加のエンドポイント セレクタを作成します。

EPG の下で複数のエンドポイント セレクタを作成した場合は、それらのエンドポイント セレクタの間には論理 OR があるものとみなされます。

たとえば、下で説明しているように 2 つのエンドポイント セレクタを作成したとします。

- エンドポイントセレクタ 1：
  - **キー**： URL
  - **演算子 (Operator）**： equals
  - **値**： `www.acme1.com`
- エンドポイント セレクタ 2：
  - **キー**： URL
  - **演算子 (Operator）**： equals

- 値： `www.acme2.com`

その場合、次のようになります。

- URL が `www.acme1.com` の場合

  または

- URL が `www.acme2.com` の場合

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 12 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したフィルタの作成

このセクションでは、クラウド APIC GUI を使用したフィルタの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[フィルタの作成（Create Fileter）]** をクリックします。**[フィルタの作成（Create Filter）]** ダイアログボックスが表示されます。

ステップ 4 次の *[フィルタの作成ダイアログボックスのフィールド（Create Filter Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *16 :* フィルタの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	**[名前（Name）]** フィールドにハードウェア フィルタの名前を入力します。

[プロパティ（Properties）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[フィルタの作成（Create ）]** ダイアログボックスに戻ります。
説明	フィルタの説明を入力します。

[プロパティ（Properties）]	説明
Add Filter	フィルタを追加するには、次の手順を実行します。 1. **[フィルタ エントリの追加（Add Filter Entry）]** をクリックします。**[フィルタの追加（Add Filter）]** ダイアログボックスが表示されます。 2. **[名前（Name）]** フィールドにフィルタエントリの名前を入力します。 3. **[イーサネット タイプ（Ethernet Type）]** ドロップダウン リストをクリックして、イーサネットタイプを選択します。次のオプションがあります。 • **IP** • **[Unspecified]** （注） **[指定なし（Unspecified）]** を選択すると、IP を含むすべてのトラフィックタイプが許可され、残りのフィールドは無効になります。 4. **[IP プロトコル（IP Protocol）]** ドロップダウンメニューをクリックして、プロトコルを選択します。次のオプションがあります。 • **tcp** • **udp** • **[Unspecified]** （注） 残りのフィールドは、**tcp** または **udp** が選択されている場合にのみ有効になります。 5. **[宛て先ポート（Destination Port）]** フィールドに適切なポート範囲情報を入力します。 6. フィルタエントリ情報の入力が完了したら、**[追加（Add）]** をクリックします。**[フィルタの作成（Create Filter）]** ダイアログボックスに戻り、別のフィルタエントリを追加する手順を繰り返すことができます。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。

Cisco Cloud APIC GUI を使用したコントラクトの作成

このセクションでは、Cisco Cloud APIC GUI を使用したコントラクトの作成方法について説明します。

始める前に

フィルタを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが**[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[コントラクトの作成（Create Contract）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*コントラクト ダイアログ ボックス フィールドの作成（*Create Contract Dialog Box Fields*）*]* テーブルにリストされているように、各フィールドに適切な値を入力して続行します。

表 *17 : [*コントラクトの作成（*Create Contract*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	契約の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 （注） リリース 5.0(2) 以降、インフラテナントでコントラクトを作成できます。共有サービスの使用例では、インフラテナントからコントラクトをエクスポートしたり、インフラテナントにコントラクトをインポートしたりすることもできます。 3. **[選択（Select）]**をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。
説明	コントラクトの説明を入力してください。
[設定（Settings）]	

[プロパティ（Properties）]	説明
スコープ	このスコープは、同じアプリケーション プロファイル内、同じ VRF インスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイント グループにコントラクトを制限します。 （注） 共有サービスにより、異なるテナントの EPG 間および異なる VRF の EPG 間の通信が可能になります。 1 つのテナントの EPG が別のテナントの EPG と通信できるようにするには、**[グローバル（Global）]** スコープを選択します。 1 つの VRF の EPG が別の VRF の別の EPG と通信できるようにするには、**[グローバル（Global）]** または **[テナント（Tenant）]** スコープを選択します。 共有サービスの詳細については、共有サービス （65 ページ） を参照してください。 ドロップダウン矢印をクリックして、次のスコープ オプションから選択します。 • **アプリケーション プロファイル** • **VRF** • **Global** • **テナント**
フィルタの追加	フィルタを選択します。 1. [フィルタの追加（Add Filter）] をクリックします。フィルタ行が表示され、**[フィルタの選択（Select Filter）]** オプションが表示されます。 2. **[フィルタの選択（Select Filter）]** をクリックします。**[フィルタの選択（Select Filter）]** ダイアログボックスが表示されます。 3. **[フィルタの選択（Select Filter）]** ダイアログで、左側の列のフィルタをクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したテナント間契約の作成

このセクションでは、Cisco Cloud Network Controller GUI を使用したテナント間契約の作成方法について説明します。テナント間契約の作成が必要になる状況の詳細については、共有サービス （65 ページ） を参照してください。

始める前に

フィルタを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが**[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[コントラクトの作成（Create Contract）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*コントラクト ダイアログ ボックス フィールドの作成（*Create Contract Dialog Box Fields*）*]* テーブルにリストされているように、各フィールドに適切な値を入力して続行します。

表 *18 : [*コントラクトの作成（*Create Contract*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	契約の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 （注） リリース 5.0(2) 以降、インフラテナントでコントラクトを作成できます。共有サービスの使用例では、インフラテナントからコントラクトをエクスポートしたり、インフラテナントにコントラクトをインポートしたりすることもできます。 3. **[選択（Select）]**をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。
説明	コントラクトの説明を入力してください。
[設定（Settings）]	

[プロパティ（Properties）]	説明
スコープ	このスコープは、同じアプリケーション プロファイル内、同じ VRF インスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイント グループにコントラクトを制限します。 テナント間通信の場合は、まずテナントの1つ（**tenant1** など）の**グローバル**スコープとの契約を作成します。このテナントのEPGは、常にこの契約のプロバイダーになります。 このコントラクトは、他のテナント（**tenant2**など）にエクスポートされます。この契約をインポートする他のテナントでは、そのEPGがインポートされた契約のコンシューマになります。**tenant2** の EPG をプロバイダー、tenant1 の EPG をコンシューマにするには、tenant2 でコントラクトを作成し、**tenant1** にエクスポートします。
フィルタの追加	フィルタを選択します。 **1.** [フィルタの追加（Add Filter）] をクリックします。フィルタ行が表示され、**[フィルタの選択（Select Filter）]** オプションが表示されます。 **2.** **[フィルタの選択（Select Filter）]** をクリックします。**[フィルタの選択（Select Filter）]** ダイアログボックスが表示されます。 **3.** **[フィルタの選択（Select Filter）]** ダイアログで、左側の列のフィルタをクリックして選択し、**[選択（Select）]**をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。

ステップ 5 設定が終わったら [Save] をクリックします。

ステップ 6 作成したコントラクトを別のテナントにエクスポートします。

たとえば、次のようなケースがあるとします。

- 上記の手順で作成したコントラクトの名前は、tenant **tenant1** の **contract1** です。
- エクスポートするコントラクトは、**exported_contract1** という名前で、テナント **tenant2** にエクスポートします。

a) [コントラクト（Contracts）] ページ（**[あプリケーション管理（Application Management）]** > **[コントラクト（Contracts）]**）に移動します。

設定されたコントラクトがリストされます。

b) 作成したばかりのコントラクトを選択します。

たとえば、コントラクト **contract1** が表示されるまでリストをスクロールし、その横にあるボックスをクリックして選択します。

c) **[アクション（Actions）]** > **[コントラクトのエクスポート（Export Contract）]**に移動します。

[[コントラクトのエクスポート（Export Contract）] ウィンドウが表示されます。

d) **[テナントの選択（Select Tenant）]** をクリックします。

[テナントの選択（Select Tenant）] ウィンドウが表示されます。

e) 契約をエクスポートするテナントを選択し、**[保存（Save）]** をクリックします。

たとえば、**tenant2** です。**[コントラクトのエクスポート（Export Contract）]** ウィンドウに戻ります。

f) **[名前（Name）]** フィールドに、エクスポートされたコントラクトの名前を入力します。

たとえば、**exported_contract1** です。

g) **[説明（Description）]** フィールドに、コントラクトの説明を入力します。

h) [**保存（Save**）] をクリックします。

コントラクトのリストが再び表示されます。

ステップ 7 最初のテナントの EPG をプロバイダー EPG として設定し、EPG 通信設定の最初の部分として元のコントラクトを設定します。

a) **[インテント（Intent）]** ボタンをクリックし、**[EPG 通信（EPG Communication）]** を選択します。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

b) **[では始めましょう（Let's Get Started）]** をクリックします。

c) **[コントラクト（Contract）]** 領域で、**[コントラクトの選択（Select Contract）]** をクリックします。

[選択（Select）] ウィンドウが表示されます。

d) これらの手順の最初に作成したコントラクトを見つけて選択します。

この例では、**contract1** を見つけて選択します。

e) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

f) **[プロバイダー EPG（Provider EPGs）]** 領域で、**[プロバイダー EPG の追加（Add Provider EPGs）]** をクリックします。

[プロバイダー EPG の選択（Select Provider EPGs）] ウィンドウが表示されます。

g) **[選択した項目を保持（Keep selected Items）]**チェックボックスをオンのままにして、最初のテナント（**tenant1**）の EPG を選択します。

h) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

i) [**保存（Save**）] をクリックします。

ステップ 8 2 番目のテナントの EPG をコンシューマ EPG として構成し、エクスポートされたコントラクトを EPG 通信構成の 2 番目の部分として設定します。

a) **[インテント（Intent）]** ボタンをクリックし、**[EPG 通信（EPG Communication）]** を選択します。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

b) **[では始めましょう（Let's Get Started）]** をクリックします。

c) **[コントラクト（Contract）]** 領域で、**[コントラクトの選択（Select Contract）]** をクリックします。

[選択（Select）] ウィンドウが表示されます。

d) これらの手順の最初に作成したコントラクトを見つけて選択します。

この例では、**exported_contract1** を見つけて選択します。

e) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

f) **[コンシューマー EPG（Consumer EPGs）]** 領域で、**[コンシューマー EPG の追加（Add Consumer EPGs）]** をクリックします。

[コンシューマー EPG の選択（Select Consumer EPGs）] ウィンドウが表示されます。

g) **[選択した項目を保持（Keep selected Items）]** チェックボックスをオンのままにして、2 番目のテナント（**tenant2**）の EPG を選択します。

h) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

i) [保存（Save）] をクリックします。

Cloud APIC GUI を使用したネットワーク セキュリティ グループの構成

セキュリティ グループ （50 ページ） で説明されているように、ネットワーク セキュリティ グループの構成方法は、リリースによって異なります。

- リリース 5.1(2) より前のリリースでは、Azure の NSG と Cisco Cloud APIC の EPG との間に 1 対 1 のマッピングがあります（これらの構成は、このドキュメント全体で **EPG ごとの NSG** 構成とも呼ばれます）。
- リリース 5.1(2) 以降、以前に使用できた既存の EPG ごとの NSG 構成に加えて、Azure の NSG は Cisco Cloud APIC 上の EPG ではなくサブネットとの 1 対 1 のマッピングを持つこともできます（これらの構成は、このドキュメント全体で、**サブネットごとの NSG** 構成として呼ばれます）。

（注） Cisco Cloud APIC では、新しい**サブネットごとの NSG** 構成または古い **EPG ごとの NSG** 構成を使用できます。同じ Cisco Cloud APIC システムに両方の構成を含めることはできません。

これらの手順では、リリース 5.1(2) 以降の Cisco Cloud APIC に対して、新しい**サブネットごとの NSG** 構成または古い **EPG ごとの NSG** 構成のいずれかを選択する方法について説明します。

始める前に

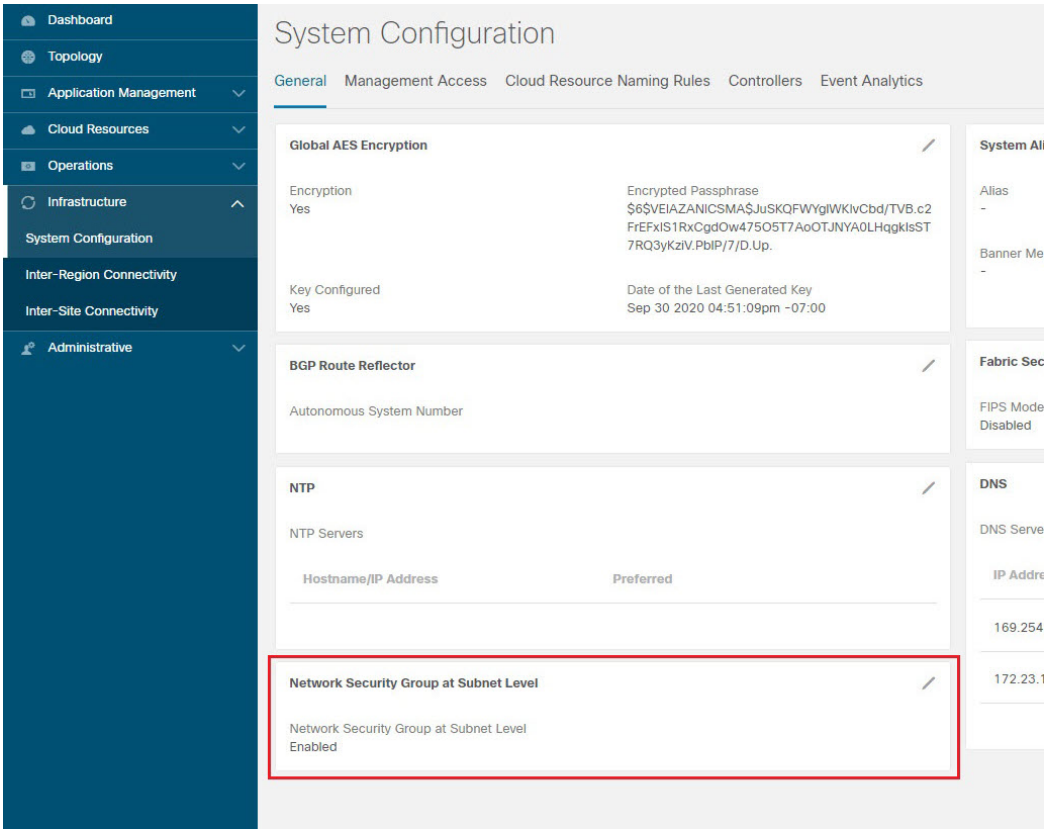
セキュリティ グループ （50 ページ） で提供されている情報を確認して、リリースに応じてセキュリティ グループがどのように構成されているかを理解し、セキュリティ グループのガイドラインと制限を理解してください。

ステップ 1 まだログインしていない場合は、Cloud APIC にログインします。

ステップ 2 左のナビゲーション バーで、**[インフラストラクチャ（Infrastructure）]** > **[システム構成（System Configuration）]**に移動します。

デフォルトでは **[全般（General）]** タブが表示されます。

ステップ 3 **[システム構成（System Configuration）]** ウィンドウの **[全般（General）]** 領域で、**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドを見つけます。



ステップ 4 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの現在の構成を確認します。

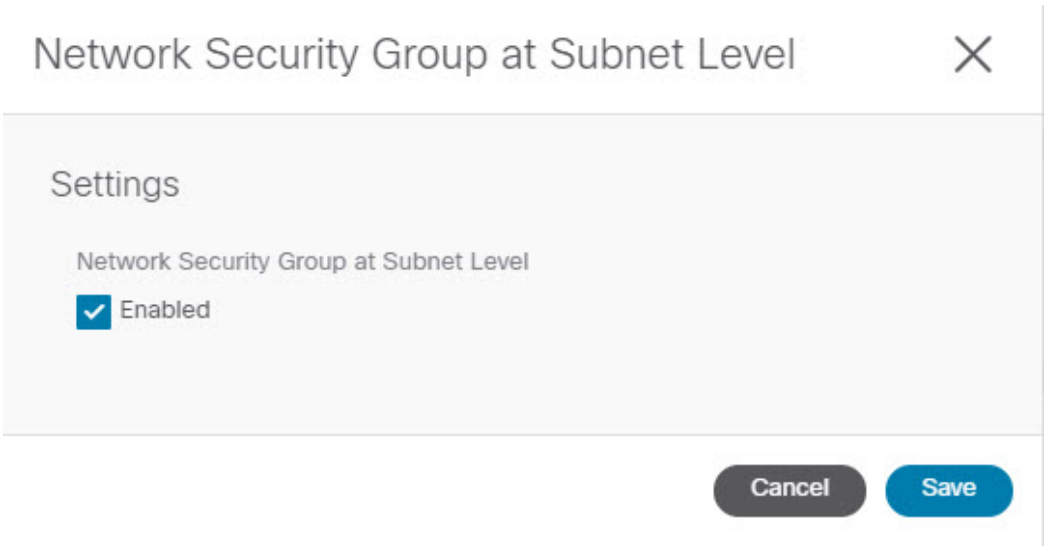
- このフィールドの値として **[有効（Enabled）]** が表示されている場合は、Cisco Cloud APIC の新しい**サブネットごとの NSG** 構成があることを意味します。
- このフィールドの値として **[無効（Disabled）]** が表示されている場合は、Cisco Cloud APIC に古い **EPG ごとの NSG** 構成があることを意味します。

ステップ 5 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更するか、そのままにするかを決定します。

希望の構成	既存の構成	アクション
Cisco Cloud APIC の新しい**サブネットごとの NSG** 構成が必要な場合、および：	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの値として **[有効（Enabled）]** が表示されている場合は、次のようにします。	Cisco Cloud APIC は、必要な**サブネットごとの NSG** 構成ですでにセットアップされています。変更を加える必要はありません。
	[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）] フィールドの値として **[無効（Disabled）]** が表示されている場合は、次のようにします。	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更する必要があります。ステップ 6 （128 ページ） に進みます。
Cisco Cloud APIC に古い **EPG ごとの NSG** 構成を使用する場合、および：	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの値として **[有効（Enabled）]** が表示されている場合は、次のようにします。	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更する必要があります。ステップ 6 （128 ページ） に進みます。
	[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）] フィールドの値として **[無効（Disabled）]** が表示されている場合は、次のようにします。	Cisco Cloud APIC は、必要な **EPG ごとの NSG** 構成ですでにセットアップされています。変更を加える必要はありません。

ステップ 6 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更する必要がある場合は、フィールドの右上隅にある鉛筆アイコンをクリックします。

[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）] の **[設定（Settings）]**ウィンドウが表示されます。



ステップ 7 ウィンドウで必要な変更を行います。

（注） ネットワーク セキュリティ グループの設定を変更すると、トラフィックが失われます。ネットワーク セキュリティ グループの設定を変更する必要がある場合は、メンテナンス期間中に変更を行うことをお勧めします。

- Cisco Cloud APIC の新しい**サブネットごとの NSG** 構成が必要で、このウィンドウの **[有効（Enabled）]** フィールドの横にあるボックスにチェックが入っていない場合は、ボックスをクリックしてチェックマークを追加します。これにより、Cisco Cloud APIC の新しい**サブネットごとの NSG** 構成を有効にすることができます。
- Cisco Cloud APIC に古い **EPG ごとの NSG** 構成を使用する必要があり、このウィンドウの **[有効（Enabled）]** フィールドの横にあるボックスにチェックが入っている場合は、ボックスをクリックしてチェック マークを外します。これにより、Cisco Cloud APIC に対して、新しい**サブネットごとの NSG** 構成を無効にし、古い **EPG ごとの NSG** 構成を有効にすることができます。

  次のことに注意。

  - 新しい**サブネットごとの NSG** から古い **EPG ごとの NSG** 構成に設定を変更することはお勧めしません。**[サブネットごとの NSG（NSG-per-subnet）]** 設定を無効にすると、サービス EPG 構成のサポートが失われ、トラフィックが失われます。
  - サービス EPG またはプライベート リンク ラベルが構成されている場合、**サブネットごとの NSG** 構成を無効にすることはできません。**サブネットごとの NSG** 構成を無効にする前に、構成されたサービス EPG またはプライベート リンク ラベルを無効にする必要があります。
    - 設定されたサービス EPG を無効にするには：
      1. **[アプリケーション管理]** > **[EPG ｓ]** の順に移動します。
      2. **[タイプ（Type）]** 列に表示されている **[サービス（Service）]** を含む EPG を見つけます。
      3. 削除するサービス EPG を選択し、**[アクション（Actions）]** > **[EPG の削除（Delete EPG）]** をクリックします。

- 構成されたプライベート リンク ラベルを無効にするには:

1. **[アプリケーション管理（Application Management）]** > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**に移動します。
2. 必要なクラウド コンテキスト プロファイルを見つけて、そのプロファイルをクリックします。

   このクラウド コンテキスト プロファイルの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。
3. [詳細（Details）] アイコンをクリックします（）。

   このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。**[CIDR]** 領域の **[サブネット（Subnets）]** 列に、テキスト **プライベート リンク ラベル**が表示されます。
4. ウィンドウの右上隅の鉛筆アイコンをクリックします。

   [クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。
5. **[設定（Settings）]** 領域で、もう一度 **[CIDR]** 領域を見つけて、その行の鉛筆アイコンをクリックします。

   [CIDR の編集（Edit CIDR）] ウィンドウが表示されます。
6. **[サブネット（Subnets）]** 領域で、**[プライベート リンク ラベル（Private Link Label）]** 列にエントリがある行を見つけ、そのサブネットの行の鉛筆アイコンをクリックします。

   このサブネット行のエントリが編集可能になります。
7. そのサブネット行の **[プライベート リンク ラベル（Private Link Label）]** 列のエントリの横にある **[X]** をクリックします。

   これにより、プライベート リンク ラベルが削除されます。

ステップ 8 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** ウィンドウで必要な変更を行った後、**[保存（Save）]** をクリックします。

[システム構成（System Configuration）] ウィンドウの **[全般（General）]** 領域が再び表示され、**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定に、前の手順で行った変更が反映されます。

セキュリティ グループの詳細の表示

ステップ 1 まだログインしていない場合は、Cisco Cloud APIC GUI にログインします。

ステップ 2 **[クラウド リソース（Cloud Resources）]** > **[セキュリティ グループ（Security Groups）]**に移動します。

[セキュリティ グループ（Security Groups）] ウィンドウが表示されます。

ステップ 3 詳細を取得するセキュリティ グループのタイプに応じて、**[ネットワーク セキュリティ グループ（Network Security Groups）]**（NSG）タブまたは **[アプリケーション セキュリティ グループ（Application Security Groups）]** ASG タブをクリックします。

各タブには、次の情報が表示されます。

- **[ネットワーク セキュリティ グループ（Network Security Groups）]** タブ：
  - **名前**：ネットワーク セキュリティ グループの名前。
  - **クラウド プロバイダ ID**：ネットワーク セキュリティ グループに関連付けられているクラウド プロバイダ ID。

    [名前（Name）] および **[クラウド プロバイダ ID（Cloud Provider ID）]** フィールドに入力されている値は、NSG が新しいサブネットごとの NSG 構成（**[クラウド プロバイダ ID（Cloud Provider ID）]** の**サブネット**として表示）で構成されているか、古い EPG ごとの NSG 構成（**[クラウド プロバイダ ID（Cloud Provider ID）]** 列の **epg**）で構成されているかを示しますソフトウェア リリースに応じて使用できるさまざまなタイプの NSG 構成の詳細については、セキュリティ グループ（50 ページ） を参照してください。
  - **EPG**：以前の EPG ごとの NSG 構成を使用している場合、ネットワーク セキュリティ グループに関連付けられている EPG。
  - **仮想マシン**：ネットワーク セキュリティ グループに関連付けられている仮想マシン。
  - **エンドポイント**：ネットワーク セキュリティ グループに関連付けられているエンドポイント。
  - **サブネット**：新しいサブネットごとの NSG 構成を使用している場合、ネットワーク セキュリティ グループに関連付けられているサブネット。
- **[アプリケーション セキュリティ グループ（Application Security Groups）]** タブ：
  - **ヘルス**：アプリケーション セキュリティ グループのヘルス ステータス。
  - **名前**：アプリケーション セキュリティ グループの名前。
  - **クラウド プロバイダ ID**：アプリケーション セキュリティ グループに関連付けられているクラウド プロバイダ ID。
  - **EPG**：アプリケーション セキュリティ グループに関連付けられている EPG。
  - **仮想マシン**：アプリケーション セキュリティ グループに関連付けられている仮想マシン。
  - **エンドポイント**：アプリケーション セキュリティ グループに関連付けられているエンドポイント。

ステップ 4 いずれかの列の値をクリックして、詳細情報を取得します。

たとえば、**[ネットワーク セキュリティ グループ（Network Security Groups）]** タブの **[名前（Name）]** 列の値をクリックすると、その特定のネットワーク セキュリティ グループに関する詳細情報が表示されます。

このウィンドウで [詳細（Details）] アイコン（）をクリックすると、別のウィンドウが表示され、入力ルールと出力ルールを含むクラウドリソース情報など、このセキュリティ グループの詳細情報が表示されます。

Cisco Cloud APIC を使用したコンシューマおよびプロバイダー EPG の指定

ここでは、EPG をコンシューマまたはプロバイダーとして指定する方法について説明します。

始める前に

- コントラクトを設定できます。
- EPG が設定済みです。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウンをクリックし、**[構成（Configuration）]** を選択します。

[インテント（Intent）] の [構成（Configuration）] オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[EPG Communication]** をクリックします。**[EPG通信（EPG Communication）]** ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

ステップ 4 コントラクトを選択します。

a) **[コントラクトの選択（Select Contract）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが表示されます。

b) **[コントラクトの選択（Select Contract）]** ダイアログの左側のペインで、契約をクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが閉じます。

ステップ 5 コンシューマ EPG を追加するには、次の手順を実行します。

a) **[コンシューマ EPG の追加（Add Consumer EPGs）]** をクリックします。**[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログが表示されます。

（注） テナント内（契約が作成される）の EPG が表示されます。

b) **[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにして EPG を選択します。

ステップ 6 プロバイダー EPG を追加するには、次の手順を実行します。

a) **[プロバイダー EPG の追加（Add Provider EPGs）]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログが表示されます。

（注） テナント内（契約が作成される）の EPG が表示されます。

b) **[プロバイダーEPGの選択（Select Provider EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダー EPG を選択します。

（注） 選択したコントラクトがインポート済みコントラクトの場合、プロバイダー EPG の選択は無効になります。

c) 完了したら、**[選択（Select）]** をクリックします。**[プロバイダーEPGの選択（Select Provider EPGs）]** ダイアログボックスが閉じ、**[EPS コミュニケーション構成（EPG Communication Configuration）]** ウィンドウに戻ります。

d) [保存（Save）] をクリックします。

Cisco Cloud Network Controller GUI を使用したクラウドコンテキスト プロファイルの作成

このセクションでは、Cisco Cloud Network Controller GUI を使用したロールの作成方法について説明します。

始める前に

VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[クラウド コントラクト プロファイルの作成（Create Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド（Create Cloud Context Profile Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *19* : クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	クラウド コンテキスト プロファイルの名前を入力します。
テナント	テナントを選択します。 1. [テナントの選択（Select Tenant）] をクリックします。[テナントの選択（Select Tenant）] ダイアログボックスが表示されます。 2. [テナントの選択（Select Tenant）] ダイアログで、左側の列のテナントをクリックして選択し、[選択（Select）] をクリックします。[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）] ダイアログボックスで、次の手順を実行します。
説明	クラウド コンテキスト プロファイルの説明を入力します。
Settings	
リージョン（Region）	リージョンを選択するには: 1. [リージョンの選択（Select Region）] をクリックします。[リージョンの選択（Select Region）] ダイアログボックスが表示されます。 2. [リージョンの選択（Select Region）] ダイアログで、左側の列のテナントをクリックして選択し、[選択（Select）] をクリックします。[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）] ダイアログボックスで、次の手順を実行します。
VRF	VRF を選択するには、次の手順を実行します。 1. [VRF の選択（Select VRF）] をクリックします。[VRF の選択（Select VRF）] ダイアログボックスが表示されます。 2. [VRF の選択（Select VRF）] ダイアログで、左側の列の VRF をクリックして選択し、[選択（Select）] をクリックします。[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）] ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
CIDR の追加（Add CIDR）	

[プロパティ（Properties）]	説明
	（注） 次のサブネットは予約されているため、この **[CIDR の追加（Add CIDR）]** フィールドでは使用しないでください。 192.168.100.0/24（ブリッジ ドメイン インターフェイス用に CCR によって予約済み） （注） VNet ピアリングが有効になっている場合、CIDR を追加、削除、または編集することはできません。CIDR を追加、削除、または編集する前に、VNet ピアリングを無効にする必要があります。VNet ピアリングを無効にするには： • インフラ テナントの場合は、クラウド コンテキスト プロファイルの **[ハブ ネットワーク ピアリング（Hub Network Peering）]** オプションを無効にします。 • ユーザー（非インフラ）テナントの場合、クラウド コンテキスト プロファイルの **[VNet ピアリング（VNet Peering）]** オプションを無効にします。 CIDR 構成を変更したら、VNet ピアリングを再度有効にします。 次の機能はリリースによってサポートされます。 • インフラ VNet の追加のセカンダリ CIDR およびサブネットを追加することもできます（クラウド テンプレートで作成された `cloudCtxProfiles`）。プライマリ CIDR を追加したり、クラウド テンプレートによって作成された既存の CIDR を変更したりすることはできません。ユーザーが作成した CIDR の下にサブネットが作成されると、サブネットは暗黙的にセカンダリ VRF にマッピングされます。 • インフラ VNet 以外の VNet のセカンダリ CIDR とサブネットを追加することもできます。 詳細については、「単一 VNet での複数の VRF のサポート （39 ページ）」を参照してください。 CIDR を追加するには、次の手順を実行します。 1. **[CIDR の追加（Add CIDR）]** をクリックします。**[CIDR の追加（Add CIDR）]** ダイアログボックスが表示されます。 2. **[CIDR ブロック範囲（CIDR Block Range）]** フィールドにアドレスを入力します。 3. **[プライマリ（Primary）]** チェックボックスをオン（有効）またはオフ（無効）にします。 追加のセカンダリ CIDR および VNet のサブネットを追加している場合、**[プラ**

[プロパティ（Properties）]	説明
	イマリ（Primary）] ボックスのチェックを外します。 4. **[サブネットの追加（Add Subnet）]** をクリックして、次の情報を入力します。 • **[アドレス（Address）]** フィールドに、サブネットアドレスを入力します。 • [**名前（Name）**] フィールドに、このサブネットの名前を入力します。 • **[プライベート リンク ラベル（Private Link Label）]** フィールドで、次のいずれかを選択します。 • **既存のものを選択（Select Existing）**：**[プライベート リンク ラベルの選択（Select Private Link Label）]** をクリックし、このサブネットに関連付ける既存のプライベート リンク ラベルを選択します。 • **新規作成（Create New）**：このサブネットに関連付けるプライベート リンク ラベルの一意の名前を入力します。 5. **[VRF]** フィールドで、必要に応じて選択します。 • **[プライマリ（Primary）]** フィールドの横にあるボックスをオンにすると、この CIDR は自動的にプライマリ VRF に関連付けられます。 • **[プライマリ（Primary）]** フィールドの横にあるチェックボックスをオンにしなかった場合は、この CIDR をセカンダリ VRF に関連付けることができます。VRFの横にある **[X]** をクリックし、**[VRF の選択（Select VRF）]** をクリックして、この CIDR に関連付けるセカンダリ VRF を選択します。 6. 完了したら、**[追加（Add）]** をクリックします。
VNet ゲートウェイ ルータ	クリックして **[VNet ゲートウェイ ルータ（VNet Gateway Router）]** チェック ボックスをチェック（有効）またはチェックを外します（無効）。
VNET ピアリング	クリックして、Azure VNet ピアリング機能をオン（有効）またはオフ（無効）にします。 VNetピアリング機能の詳細については、*Azure* 向け *Cisco Cloud APIC* の *Vnet* ピアリング構成ページの「Azure 向け Cloud APIC のVNet ピアリングの構成」を参照してください。

ステップ 5 設定が終わったら [Save] をクリックします。

Azure での仮想マシンの構成

Cisco Cloud APIC のためのエンドポイント セレクタを設定するとき Cisco Cloud APIC を構成するエンドポイントセレクタに対応する Azure で必要なインスタンスについても構成することが必要になります。

このトピックでは、Azure で仮想マシンを設定するための要件について説明します。Cisco Cloud APIC のエンドポイントセレクタを設定する前に、または後で、これらの要件を使用して Azure のインスタンスを設定することができます。たとえば、先に Azure のアカウントに移動し、Azure のカスタム タグまたはラベルを作成してから、Cisco Cloud APIC のカスタム タグまたはラベルを使用して、エンドポイント セレクタを作成することができます。先に Cisco Cloud APIC のカスタム タグまたはラベルを使用してエンドポイント セレクタを作成し、Azure のアカウントに移動して、その穂カスタム タグまたはラベルを作成することができます。

始める前に

Azure仮想マシンの設定プロセスの一環として、クラウドコンテキストプロファイルを設定する必要があります。GUI を使用してクラウド コンテキスト プロファイルを設定すると、VRF やリージョンの設定などの設定情報は、Azure にプッシュされます。

ステップ 1 クラウド コンテキスト プロファイル設定を確認して、次の情報を取得します。

- VRF 名
- サブネット情報
- サブスクリプション ID
- クラウド コンテキスト プロファイルが展開されている場所に対応するリソース グループ。

（注） 上記の情報に加えて、タグベースのEPGを使用している場合は、タグ名も知っている必要があります。タグ名は、クラウド コンテキスト プロファイル設定では使用できません。

クラウド コンテキスト プロファイル設定情報を取得するには、次の手順を実行します。

a) **[ナビゲーション (Navigation)]** メニューで、**[アプリケーション管理 (Application Management)]** タブを選択します。

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。

b) **[クラウド コンテキスト プロファイル (Cloud Context Profiles)]** サブタブ オプションを選択します。

Cisco Cloud APIC 用に作成したクラウド コンテキスト プロファイルのリストが表示されます。

c) この Azure インスタンス設定プロセスの一部として使用するクラウド コンテキスト プロファイルを選択します。

リージョン、VRF、IP アドレス、サブネットなど、このクラウドコンテキストプロファイルのさまざまな設定パラメータが表示されます。Azure 仮想マシンを設定するときに、このウィンドウに表示される情報を使用します。

ステップ 2 Azure ユーザー テナントの Cisco Cloud APIC ポータル アカウントにログインし、クラウド コンテキスト プロファイル設定から収集した情報を使用して Azure VM の作成を開始します。

（注） Azure ポータルで VM を作成する方法の詳細については、Microsoft Azure のマニュアルを参照してください。

Cisco Cloud APIC GUI を使用したバックアップ構成の作成

ここでは、バックアップ構成を作成する方法を説明します。

始める前に

必要に応じて、リモート ロケーションとスケジューラを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[バックアップ構成の作成（Create Backup Configuration）]** をクリックします。**[バックアップ構成の作成（Create Backup Configuration）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[バックアップ構成の作成ダイアログボックスのフィールド（Create Backup Configuration Dialog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *20* : バックアップ構成の作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
全般	
名前	バックアップ構成の名前を入力します。
説明	バックアップ構成の説明を入力します。
Settings	
Backup Destination	バックアップ接続先を選択します。 • **Local** • **[リモート（Remote）]**

[プロパティ（**Properties**）]	説明
バックアップ オブジェクト	

[プロパティ（Properties）]	説明
	バックアップで考慮するルート階層コンテンツを選択します • ポリシー ユニバース • セレクタオブジェクト（Selector Object）：これを選択すると、[オブジェクトタイプ（Object Type）] ドロップダウンリストと [オブジェクト DN（Object DN）] フィールドが追加されます。 1. オブジェクトタイプ（Object Type）ドロップダウン リストで、次のオプションから選択します。 • テナント（Tenant）：選択すると、[テナントの選択（Select Tenant）] オプションが表示されます。 • アプリケーション プロファイル（Application Profile）：選択すると、[アプリケーション プロファイルの選択（Select Application Profile）] オプションが表示されます。 • EPG：これを選択すると [EPG の選択（Select EPG）] オプションが表示されます。 • コントラクト（Contract）：これを選択すると、[コントラクトの選択（Select Contract）] オプションが表示されます。 • フィルタ（Filter）：これを選択すると、[フィルタの選択（Select Filter）] オプションが表示されます。 • VRF：これを選択すると、[VRFの選択（Select VRF）] オプションが表示されます。 • デバイス：[SelectfvcloudLBCtx] プションが表示されます。 • サービス グラフ：選択すると、[Select Service Graph] オプションが表示されます。 • [クラウド コンテキスト プロファイル（Cloud Context Profile）]：これを選

[プロパティ（Properties）]	説明
	択すると、**[クラウド コンテキスト プロファイルの選択**（Select Cloud Context Profile）]オプションが表示されます。 2. **Select <object_name>** をクリックjします。**Select <object_name>** ダイアログが表示されます。 3. **Select <object_name>** ダイアログから左側の列のオプションからクリックして選んで、**[選択（Select）]** をクリックします。**[バックアップ構成の作成（Create Backup Configuration）]** ダイアログ ボックスに戻ります。 （注） **[オブジェクトDN（Object DN）]** フィールドには、バックアップするオブジェクトツリーのルートとして使用するオブジェクトの DN が自動的に入力されます。 • **DN の入力（Enter DN）**：このオプションを選択すると、**[オブジェクト DN（Object DN）]** フィールドが表示されます。 1. **[オブジェクトDN（Object DN）]** フィールドに、バックアップするオブジェクト ツリーのルートとして使用する特定のオブジェクトの DN を入力します。
スケジューラ	1. **[スケジューラの選択（Select Scheduler）]** をクリックして **[スケジューラの選択（Select Scheduler）]** ダイアログを開き、左側の列からスケジューラを選択します。 2. 終了したら、右下隅にある **[選択（Select）]** ボタンをクリックします。
作成後のバックアップのトリガー	次のいずれかを選択します。 • **はい（Yes）**：（デフォルト）バックアップ設定の作成後にバックアップをトリガーします。 • **いいえ（No）**：バックアップ設定の作成後にバックアップをトリガーしません。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したテクニカル サポート ポリシーの作成

このセクションでは、テクニカル サポート ポリシーを作成する方法について説明します。

始める前に

リモート ロケーションのテクニカル サポート ポリシーを作成する場合は、まずリモート ロケーションを作成する必要があります。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[テクニカル サポートの作成（Create Tech Support）]** をクリックします。**[テクニカル サポートの作成（Create Tech Support）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[テクニカル サポートの作成ダイアログボックスのフィールド（Create Tech Support Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

表 *21* : テクニカル サポートの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
全般	
名前	テクニカル サポート ポリシーの名前を入力します。
説明	テクニカル サポートの説明を入力します。
Settings	

[プロパティ（Properties）]	説明
エクスポート先	エクスポート先を選択します。 • コントローラ • [リモート ロケーション（Remote Location）]：選択すると、[リモート ロケーションの選択（Select Remote Location）] オプションが表示されます。 1. [リモート ロケーションの選択（Select Remote Location）] をクリックします。[リモート ロケーションの選択（Select Remote Location）] ダイアログボックスが表示されます。 2. [[リモート ロケーションの選択（Select Remote Location）] ダイアログで、左側の列のリモート ロケーションをクリックして選択し、[選択（Select）] をクリックします。[テクニカル サポートの作成（Create Tech Support）] ダイアログボックスに戻ります。
アップグレード前のログを含める	テクニカル サポート ポリシーにアップグレード前のログを含める場合は、[有効（Enabled）] チェックボックスをオンにします。
作成後のトリガー	ポリシーの作成後にテクニカル サポート ポリシーを作成する場合は、[有効] (デフォルト) チェックボックスをクリックしてオンにします。無効にするには、チェックボックスをオフにします。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したスケジューラの作成

このセクションでは、ユーザー ラップトップブ ラウザのローカル時間で、Cisco Cloud APIC のデフォルト UTC 時間に変換されるスケジューラを作成する方法について説明します。

ステップ 1 インテント アイコンをクリックします。[インテント（Intent）] メニューが表示されます。

ステップ 2 [インテント（Intent）] 検索ボックスの下のドロップダウン□をクリックし、[操作（Operations）] を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[スケジューラの作成（Create Scheduler）]** をクリックします。**[スケジューラの作成（Create Scheduler）]** ダイアログボックスが表示されます。

ステップ 4 次の *[*スケジューラの作成ダイアログボックスのフィールド（*Create Scheduler Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *22 :* スケジューラの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	トリガー スケジューラ ポリシーの名前を入力します。
説明	トリガーの説明を入力します。
Settings	

[プロパティ（Properties）]	説明
繰り返しウィンドウ	**[繰り返しウィンドウの追加（Add Recurring Window）]** をクリックします。**[繰り返しウィンドウの追加（Add Recurring Window）]** ダイアログウィンドウが表示されます。 1. **[スケジュール（Schedule）]** ドロップダウンリストから、次のいずれかを選択します。 • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日 2. **[開始時間（Start Time）]** フィールドに、時間を入力します。 3. **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドから数値を入力するか、フィールドを空白のままにして無制限を指定します。 4. **[最大実行時間（Maximum Running Time）]** で、**[無制限（Unlimited）]** または **[カスタム（Custom）]** をクリックして選択します。 5. 終了したら、[Add] をクリックします。

[プロパティ（Properties）]	説明
ワンタイム ウィンドウの追加	**[ワンタイムウィンドウの追加（Add One Time Window）]** をクリックします。**[ワンタイムウィンドウの追加（Add One Time Window）]** ダイアログが表示されます。 1. **[開始時間（Start Time）]** フィールドに、時間を入力します。 2. **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドに数値を入力するか、フィールドを空白のままにして無制限を指定します。 3. **[最大実行時間（Maximum Running Time）]** で、**[無制限（Unlimited）]** または **[カスタム（Custom）]** をクリックして選択します。 4. 終了したら、[Add] をクリックします。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したリモート ロケーションの作成

このセクションでは、Cisco Cloud APIC を使用したリモート ロケーションの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[操作（Operations）]** リストで、**[リモート ロケーションの作成（Create Remote Location）]** をクリックします。**[リモート ロケーションの作成（Create Remote Location）]** ダイアログボックスが表示されます。

ステップ 4 次の *[リモート ロケーションの作成ダイアログボックスのフィールド（Create Remote Location Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *23 :* リモート ロケーションの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	

[プロパティ（Properties）]	説明
名前	リモート ロケーション ポリシーの名前を入力します。
説明	リモート ロケーション ポリシーの説明を入力します。
Settings	
Hostname/IP Address	リモート ロケーションのホスト名または IP アドレスを入力します
Protocol	プロトコルを選択します。 • **FTP** • **SFTP** • **SCP**
Path	リモート ロケーションのパスを入力します。
Port	リモート ロケーションのポートを入力します。
Username	リモートロケーションのユーザー名を入力します。
認証タイプ	SFTP または SCP を使用する場合は、認証タイプを選択します。 • **[Password]** • **SSH キー（SSH Key）**
SSH キー コンテンツ	SSH キーのコンテンツを入力します。
SSH キー パスフレーズ	SSH キー パスフレーズ
Password	リモート ロケーションにアクセスするためのパスワードを入力します。
Confirm Password	リモート ロケーションにアクセスするためのパスワードを再入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したローカル ドメインの作成

このセクションでは、クラウドAPIC GUIを使用したログイン ドメインの作成方法について説明します。

始める前に

非ローカルドメインを作成する前に、プロバイダーを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ログイン ドメインの作成（Create Login Domain）]** をクリックします。**[ログイン ドメインの作成（Create Login Domains）]** ダイアログボックスが表示されます。

ステップ 4 次の *[ログイン ドメインダイアログボックスのフィールド（Login Domains Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

表 *24 :* ログイン ドメインダイアログボックスの作成のフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	ログイン ドメインの名前を入力します。
説明	ログイン ドメインの説明を入力します。
レルム	レルムを選択します。 • **Local** • **LDAP**：プロバイダーを追加し、認証タイプを選択する必要があります。 • **RADIUS**：プロバイダーを追加する必要があります。 • **TACACS+**：プロバイダーの追加が必要です。 • **SAML**：プロバイダーの追加が必要です。

[プロパティ（Properties）]	説明
プロバイダ	プロバイダーを追加するには、次の手順を実行します。 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. クリックしてプロバイダーを選択します。 3. **[選択 (Select)]** をクリックして、プロバイダを追加します。
詳細設定	**[認証タイプ（Authentication Type）]** および **[LDAP グループ マップ ルール（LDAP Group Map Rules）]** フィールドを表示します。
認証タイプ	レルム オプションにLDAPを選択した場合は、次のいずれかの認証タイプを選択します。 • **Cisco AV ペア**：（デフォルト） • **LDAP グループ マップ ルール**：LDAP グループ マップ ルールを追加する必要があります。

[プロパティ（Properties）]	説明
LDAP グループ マップ ルール	

[プロパティ（Properties）]	説明
	LDAP グループ マップ ルールを追加するには、次の手順を実行します。 1. **[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. **[名前（Name）]** フィールドに、ルールの名前を入力します。 3. **[説明（Description）]** フィールドに、ルールの説明を入力します。 4. **[グループ DN（Group DN）]** フィールドにルールのグループ DN を入力します。 5. セキュリティ ドメインの追加： 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。 2. **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。 3. セキュリティ ドメインをクリックして選択します。 4. **[選択（Select）]** をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）] ダイアログボックスに戻ります。** 5. ユーザー ロールを追加する: 1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログボックスが表示され、左側のペインにロールのリストが表

[プロパティ（Properties）]	説明
	示されます。 2. クリックしてロールを選択します。 3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。 4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスから、**[権限タイプ（Privilege Type）]** ドロップダウンリストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。 5. **[権限タイプ（Privilege Type）]** ドロップダウン リストの右側のチェックマークをクリックして、確認します。 6. 終了したら、[Add] をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログボックスに戻り、別のセキュリティドメインを追加できます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成

セキュリティドメインは、追加するセキュリティドメインにテナントを制限します。セキュリティドメインを追加しない場合、すべてのセキュリティドメインがこのテナントにアクセスできます。このセクションでは、GUI を使用してセキュリティ ドメインを作成する方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの**[管理（Administrative）]** リストで、**[セキュリティ（Security）]** > **[セキュリティ ドメイン（Security Domains）]** > **[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。**[セキュリティ ドメインの作成（Create Security Domain）]** ダイアログ ボックスが表示されます。

ステップ 4 **[名前（Name）]** フィールドに、セキュリティ ドメインの名前を入力します。

ステップ 5 **[説明（Description）]** フィールドに、セキュリティ ドメインの説明を入力します。

ステップ 6 **制限付きドメイン**制御を **[はい（Yes）]** または **[いいえ（No）]** に設定します。

セキュリティ ドメインが制限付きドメインとして構成されている場合（**[はい（Yes）]**）、このドメインに割り当てられているユーザーは、他のセキュリティ ドメインで構成されたポリシー、プロファイル、またはユーザーを表示できません。

ステップ 7 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したロールの作成

このセクションでは、クラウド APIC GUI を使用したロールの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[Intent]** メニューの **[Administrative]** リストで、**[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。**[ロールの作成（Create Role）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*ロールの作成ダイアログボックスのフィールド（*Create Role Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *25 :* ロールの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
全般	
名前	**[Name]** フィールドにロール名を入力します。
説明	ロールの説明を入力します。
Settings	

[プロパティ（**Properties**）]	説明
特権	

[プロパティ（Properties）]	説明
	クリックして、ユーザに割り当てる権限のチェックボックスをオンにします。権限は次のとおりです。 • **aaa**：認証、許可、アカウンティング、インポート/エクスポート ポリシーの設定に使用されます。 • **access-connectivity-l1** インフラの下のレイヤ 1 設定に使用されます。例：セレクタとポート レイヤ 1 のポリシー設定。 • **access-connectivity-l2** ：インフラの下のレイヤ 2 設定に使用されます。例：セレクタおよび接続可能なエンティティ設定をカプセル化します。 • **access-connectivity**：インフラでのレイヤ 3 の設定、テナントの L3Out でのスタティック ルート設定に使用されます。 • **access-connectivity-mgmt** ：管理インフラ ポリシーに使用されます。 • **access-connectivity-util** ：テナント ERSPAN ポリシーに使用されます。 • **access-equipment**：アクセスポートの設定に使用されます。 • **access-protocol-l1** ：インフラのレイヤ 1 プロトコル設定に使用されます。 • **access-protocol-l2** ：インフラのレイヤ 2 プロトコル設定に使用されます。 • **access-protocol-l3** ：インフラでのレイヤ 3 プロトコル設定に使用されます。 • **access-protocol-mgmt** ：NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • **access-protocol-ops** ：クラスタ ポリシーやファームウェア ポリシーなどの操作関連のアクセス ポリシーに使用されます。 • **access-protocol-util** ：テナント ERSPAN ポリシーに使用されます。 • **access-qos**：CoPP および QoS に関連するポリシーの変更に使用されます。

[プロパティ（Properties）]	説明
	• **admin**：すべてへのアクセス（すべてのロールの組み合わせ） • **fabric-connectivity-l1** ：ファブリックの下のレイヤ 1 設定に使用されます。例: セレクタとポート レイヤ 1 ポリシーと VNET 保護。 • **fabric-connectivity-l2** ：ポリシー展開の影響を推定するための警告を生成するために、ファームウェアおよび展開ポリシーで使用されます。 • **fabric-connectivity-l3** ：ファブリックの下のレイヤ 3 設定に使用されます。例: ファブリック IPv4 および MAC 保護グループ。 • **fabric-connectivity-mgmt**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、および診断ポリシーに使用されます。 • **fabric-connectivity-util**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • **fabric-equipment**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • **fabric-protocol-l1** ：ファブリックの下のレイヤ 1 プロトコル設定に使用されます。 • **fabric-protocol-l2** ：ファブリックの下のレイヤ 2 プロトコル設定に使用されます。 • **fabric-protocol-l3** ：ファブリックの下のレイヤ 3 プロトコル設定に使用されます。 • **fabric-protocol-mgmt** ：NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • **fabric-protocol-ops** ：ERSPAN およびヘルス スコア ポリシーに使用されます。 • **fabric-protocol-util** ：ファームウェア管理の traceroute およびエンドポイント トラッキング ポリシーに使用されます。 • **none**：特権なし。

[プロパティ（Properties）]	説明
	• **nw-svc-device** ：レイヤ 4 からレイヤ 7 のサービス デバイスを管理するために使用されます。 • **nw-svc-devshare** ：共有レイヤ 4 ～ レイヤ 7 サービス デバイスの管理に使用されます。 • **nw-svc-params**：レイヤ 4 ～ レイヤ 7 のサービス ポリシーの管理に使用されます。 • **nw-svc-policy**：レイヤ 4 ～ レイヤ 7 のネットワーク サービス オーケストレーションの管理に使用されます。 • **ops**：アトミック カウンタ、SPAN、TSW、技術サポート、トレースルート、分析、コア ポリシーなど、ポリシーのモニタリングとトラブルシューティングを含む動作ポリシーに使用されます。 • **tenant-connectivity-l1** ：ブリッジ ドメインやサブネットなど、レイヤ 1 接続の変更に使用されます。 • **tenant-connectivity-l2** ：ブリッジ ドメインやサブネットなど、レイヤ 2 接続の変更に使用されます。 • **tenant-connectivity-l3** ：VRF を含むレイヤ 3 接続の変更に使用されます。 • **tenant-connectivity-mgmt** ：テナントのインバンドおよびアウトオブバンドの管理接続構成、およびアトミック カウンターやヘルス スコアなどのポリシーのデバッグ/監視に使用されます。 • **tenant-connectivity-util**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • **tenant-epg**：エンドポイント グループ、VRF、ブリッジ ドメインの削除/作成など、テナント設定の管理に使用されます。 • **tenant-ext-connectivity-l2**：テナントの L2Out 構成を管理するために使用されます。 • **tenant-ext-connectivity-l3**：テナント L3Out 構成の管理に使用されます。

[プロパティ（Properties）]	説明
	• **tenant-ext-connectivity-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。 • **tenant-ext-connectivity-util** ： traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-ext-protocol-l1**：テナントの外部レイヤ 1 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。 • **tenant-ext-protocol-l2** ：テナントの外部レイヤ 2 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。 • **tenant-ext-protocol-l3** ：BGP、OSPF、PIM、IGMP などのテナントの外部レイヤ 3 プロトコルを管理するために使用されます。 • **tenant-ext-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。 • **tenant-ext-protocol-util**：traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-network-profile**：ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。 • **tenant-protocol-l1** ：テナントの下でレイヤ 1 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-l2** ：テナントの下でレイヤ 2 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-l3** ：テナントの下でレイヤ 3 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。

[プロパティ（Properties）]	説明
	• **tenant-protocol-ops** ：テナント traceroute ポリシーに使用されます。 • **tenant-protocol-util** — traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-qos**：ファームウェア ポリシーの書き込みアクセスとしてのみ使用されます。 • **tenant-security**：テナントの契約関連の設定に使用されます。 • **vmm-connectivity**：VM 接続に必要な APIC の VMM インベントリ内のすべてのオブジェクトを読み取るために使用されます。 • **vmm-ep**：APIC の VMM インベントリ内の VM およびハイパーバイザーエンドポイントを読み取るために使用されます。 • **vmm-policy**：VM ネットワーキングのポリシーの管理に使用されます。 • **vmm-protocol-ops**：VMM ポリシーでは使用されません。 • **vmm-security**：テナントの契約関連の設定に使用されます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した認証局の作成

ここでは、GUI を使用して認証局を作成する方法について説明します。

始める前に

- 証明書チェーン（certificate chain）を設定します。
- 認証局がテナント用の場合は、テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。
ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[インテント（Intent）] メニューに**管理**オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[証明書認証局の作成（Create Certificate Authority）]** をクリックします。**[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスが表示されます。

ステップ 4 *[*証明書認証局の作成ダイアログボックスのフィールド（*Create Certificate Authority Dialog Box Fields*）*]* のテーブルにリストされた各フィールドに適切な値を入力して、続行します。

表 *26 :* 証明書認証局の作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	証明書認証局の名前を入力してください。
説明	証明書認証局の説明を入力してください。
用途	次のオプションから選択します。 • **テナント（Tenant）**：認証局が特定のテナント用かどうかを選択します。選択すると、**[テナントの選択（Select Tenant）]** オプションがGUIに表示されます。 • **システム（System）**：認証局がシステム用である場合に選択します。
テナントの選択	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスが表示されます。
Certificate Chain	**[証明書チェーン (Certificate Chain)]** フィールドに、証明書チェーンを入力します。 （注） チェーンの証明書を次の順序で追加します。 1. CA 2. Sub-CA 3. サブサブCA 4. サーバー

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したキー リングの作成

このセクションでは、Cisco Cloud APIC GUI を使用したキー リングの作成方法について説明します。

始める前に

- 認証局を作成します。
- 証明書を持っています。
- キー リングが特定のテナント用である場合は、テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[キー リングの作成（Create Key Ring）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[キー リングの作成ダイアログボックスのフィールド（Create Key Ring Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *27*：キー リングの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	キー リングの名前を入力します。
説明	キー リングの説明を入力します。
用途	• **System**：キー リングはシステム用です。 • **Tenant**：キー リングは特定のテナント用です。テナントを指定する **[テナント（Tenant）]** フィールドを表示します。

[プロパティ（Properties）]	説明
テナントの選択	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。
Settings	
認証局	認証局を選択するには： 1. **[認証局の選択（Select Certificate Authority）]** をクリックします。**[認証局の選択（Select Certificate Authority）]** ダイアログが表示されます。 2. 左側の列で認証局をクリックして選択します。 3. **[選択（Select）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。
秘密キー（Private Key）	次のいずれかを選択します。 • **[新しいキーの生成（Generate New Key）]**：新しいキーを生成します。 • **[既存のキーのインポート（Import Existing Key）]**：**[秘密キー（Private Key）]** テキストボックスが表示され、既存のキーを使用できます。
秘密キー（Private Key）	**[秘密キー（Private Key）]** テキストボックスに既存のキーを入力します（**[既存のキーのインポート（Import Existing Key）]** オプションの場合）。

[プロパティ（Properties）]	説明
Modulus	**[モジュール（Modulus）]** ドロップダウン リストをクリックし、次の項目の中から選択します。 • **MOD 512** • **MOD 1024** • **MOD 1536** • **MOD 2048**：デフォルト
証明書	**[証明書（Certificate）]** テキスト ボックスに証明書情報を入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したローカル ユーザーの作成

このセクションでは、クラウド APIC GUI を使用したローカル ユーザーの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ローカル ユーザーの作成（Create Local User）]** をクリックします。**[ローカル ユーザーの作成（Create New User）]** ダイアログボックスが表示されます。

ステップ 4 次の *[ローカル ユーザーの作成ダイアログボックスのフィールド（Create Local User Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *28 :* ローカル ユーザーの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	ローカル ユーザーのユーザー名を入力します。
Password	ローカル ユーザーのパスワードを入力します。
Confirm Password	ローカル ユーザーのパスワードを再入力します。
説明	ローカル ユーザーの説明を入力します。
Settings	

[プロパティ（Properties）]	説明
アカウント ステータス	アカウント ステータスを選択するには、次の手順を実行します。 • **Active**：ローカル ユーザー アカウントをアクティブにします。 • **Inactive**：ローカル ユーザー アカウントを非アクティブにします。
[名（First Name）]	ローカル ユーザーの名を入力します。
姓（**Last Name**）	ローカル ユーザーの姓を入力します。
電子メール アドレス（**Email Address**）	ローカル ユーザーの E メール アドレスを入力します。
Phone Number	ローカル ユーザーの 電話番号を入力します。

[プロパティ（**Properties**）]	説明
セキュリティ ドメイン	

[プロパティ（Properties）]	説明
	セキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。 2. **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。 3. セキュリティ ドメインをクリックして選択します。 4. **[選択（Select）]** をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）] ダイアログボックスに戻ります。** 5. ユーザー ロールを追加する: 1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログ ボックスが表示され、左側のペインにロールのリストが表示されます。 2. クリックしてロールを選択します。 3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。 4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスから、**[権限タイプ（Privilege Type）]** ドロップダウン リストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。 5. **[権限タイプ（Privilege Type）]** ドロップダウンリストの右側のチェックマークをクリッ

[プロパティ（Properties）]	説明
	クして、確認します。 6. 終了したら、[Add] をクリックします。**[ローカル ユーザーの作成（Create Local User）]** ダイアログボックスに戻り、別のセキュリティ ドメインを追加できます。

ステップ 5 **[高度な設定（Advanced Settings）]** をクリックして、*[ローカルユーザーの作成ダイアログボックスのフィールド：高度な設定（Create Local User Dailog Box Fields: Advanced Settings）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *29 :* ローカル ユーザーの作成ダイアログボックスのフィールド：高度な設定

プロパティ	説明
Account Expires	**[はい（Yes）]** を選択すると、アカウントは選択した時点で期限切れになるように設定されます。
パスワードの更新が必要です	**[はい（Yes）]** を選択した場合、ユーザーは次回ログイン時にパスワードを変更する必要があります。
OTP	ユーザーのワンタイム パスワード機能を有効にするには、チェックボックスをオンにします。
ユーザー証明書	ユーザー証明書を追加するには、次の手順を実行します。 1. **[X509 証明書の追加（Add X509 Certificate）]** をクリックします。**[X509 証明書の追加（Add X509 Certificate）]** ダイアログボックスが表示されます。 2. [Name] フィールドに名前を入力します。 3. **[ユーザー X509 証明書（User X509 Certificate）]** テキストボックスにX509証明書を入力します。 4. [Add] をクリックします。**[ユーザー X509 証明書の X509 証明書]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。

プロパティ	説明
SSH キー	SSH キーを追加するには、次の手順を実行します。 1. **[SSH キーを追加（Add SSG Key）]** をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが表示されます。 2. [Name] フィールドに名前を入力します。 3. **[キー（Key）]** テキストボックスに SSH キーを入力します。 4. [Add] をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。

ステップ 6 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したリージョンの管理（クラウド テンプレートの設定）

リージョンは、初回セットアップ時に構成されます。構成時に、Cisco Cloud APIC によって管理されるリージョンと、そのリージョンのサイト間およびリージョン間の接続を指定します。このセクションでは、初期インストール後に Cisco Cloud APIC GUI を使用してクラウド テンプレートでリージョンを管理する方法について説明します。

クラウド テンプレートの詳細については、クラウド テンプレートの概要 （59 ページ） を参照してください。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[構成（Configuration）]** リストから、**[cAPIC Setup]** をクリックします。
[設定-概要（Set up-Overview）] ダイアログボックスが表示され、**[DNS と NTPサーバ]**、**[リージョン管理]**、**[スマート ライセンシング]** のオプションが示されます。

ステップ 4 **[リージョン管理（Region Management）]** で、**[構成の編集（Edit Configuration）]** をクリックします。

[セットアップ - リージョン管理] ダイアログ ボックスが表示されます。**セットアップ - リージョン管理**の一連のステップの最初のステップ、**管理するリージョン**が表示され、管理対象リージョンのリストが表示されます。

ステップ 5 サイト間接続が必要な場合は、[サイト間接続（Inter-Site Connectivity）] 領域の [有効（Enabled）] ボックスをクリックしてオンにします。
このオプションを選択すると、ページ上部の**[セットアップ-リージョン管理（Setup-Region Management）]**の手順に**サイト間接続**の手順が追加されます。

ステップ 6 Cisco Cloud APIC で管理するリージョンを選択するには、そのリージョンのチェック ボックスをクリックしてチェック マークを付けます。

ステップ 7 クラウド ルータをこのリージョンにローカルに展開するには、そのリージョンの [Cloud Routers] チェック ボックスをオンにします。

ステップ 8 クラウド サイトのファブリック インフラ接続を構成するには、**[次へ]** をクリックします。
セットアップ - リージョン管理の一連の手順の次の手順である、**一般的な接続**が表示されます。

ステップ 9 CCR のサブネット プールを追加するには、**[クラウド ルータのサブネット プールを追加する（Add Subnet Pool for Cloud Router）]** をクリックし、テキスト ボックスにサブネットを入力します。

（注） クラウド APIC の導入時に提供される /24 サブネットは、最大 2 つのクラウド サイトに十分です。3 つ以上のクラウド サイトを管理する必要がある場合は、さらにサブネットを追加する必要があります。

ステップ 10 **[CCR 用 BGP自律システム番号（BGP Autonomous System Number for CCRs）]** フィールドに値を入力します。

BGP ASN の範囲は 1 ー 65534 です。

ステップ 11 **[Assign Public IP to CCR Interface（パブリック IP を CCR インターフェイスに割り当てる）]** フィールドで、CCR インターフェイスにパブリック IP アドレスまたはプライベート IP アドレスを割り当てるかどうかを決定します。

CCR では、サイト間通信のためにパブリック IP アドレスが必要であることに注意してください。

- パブリック IP アドレスを CCR インターフェイスに割り当てるには、**[有効（Enabled）]** チェック ボックスをオンのままにします。デフォルトでは、この **[有効]** チェック ボックスはオンになっています。
- プライベート IP アドレスを CCR インターフェイスに割り当てるには、**[有効（Enabled）]** チェック ボックスのチェックを外します。この場合、接続にはプライベート IP アドレスが使用されます。

（注） CCR アドレスをパブリック IP アドレスからプライベート IP アドレスに（またはその逆に）変更すると、中断が発生し、トラフィックが失われる可能性があります。

リリース 5.1(2) 以降では、CCRに割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、[クラウド リソース（Cloud Resources）] 領域にルータの他の詳細とともに表示されます。パブリック IP が CSR に割り当てられていない場合は、プライベート IP だけが表示されます。

ステップ 12 リージョンごとのルータ数を選択するには、**[リージョンごとのルータ数]** ドロップダウン リストをクリックし、**[2]**、**[3]**、または **[4]**、**[6]**、 または **[8]** をクリックします。

ステップ 13 **[ユーザー名（Username）]** テキストボックスにユーザー名を入力します。

（注） Azure クラウド サイトに接続する場合は、CCR のユーザー名として admin を使用しないでください。

ステップ 14 **[パスワード（Password）]** テキスト ボックスと **[パスワードの確認（Confirm Password）]** テキスト ボックスに新しいパスワードを入力します。

ステップ 15 スループット値を選択するには、**[ルーターのスループット]** ドロップダウン リストをクリックします。

（注）
- クラウド ルータは、ルータのスループットまたはログイン情報を変更する前に、すべてのリージョンから展開解除する必要があります。
- リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。Cisco Catalyst 8000V のスループット値については、Cisco Catalyst 8000V について （34 ページ） を参照してください。

ステップ 16 必要に応じて、**[TCP MSS]** フィールドに必要な情報を入力します。

リリース 4.2(4q) 以降では、TCP 最大セグメントサイズ（MSS）を設定するために **TCP MSS** オプションを使用できます。この値は、クラウドへの VPN トンネルとオンプレミス サイトまたは他のクラウド サイトへの外部トンネルを含む、すべてのクラウドルータ トンネルインターフェイスに適用されます。クラウドへのVPNトンネルの場合、クラウドプロバイダーのMSS値がこのフィールドに入力した値よりも小さい場合は、低い方の値が使用されます。それ以外の場合は、このフィールドに入力した値が使用されます。

MSS値はTCPトラフィックにのみ影響し、pingトラフィックなどの他のタイプのトラフィックには影響しません。

ステップ 17 (オプション) ライセンス トークンを指定するには、**[ライセンス トークン]** テキスト ボックスに製品インスタンスの登録トークンを入力します。

（注）
- リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。Cisco Catalyst 8000V のライセンス情報については、Cisco Catalyst 8000V について （34 ページ） を参照してください。
- トークンが入力されていない場合、CCR は EVAL モードになります。
- プライベート IP アドレスを ステップ 11 （170 ページ） の CCR に割り当てた場合、プライベート IP アドレスを使用して CCR のスマート ライセンスを登録するときに、**Cisco Smart Software Manager（CSSM）**に直接接続できます（**[管理（Administrative）]** > **[スマート ライセンス（Smart Licensing）]**）に移動して使用可能。この場合、エクスプレスルート経由でCSSMに到達可能性を提供する必要があります。

ステップ 18 [次へ（Next）] をクリックします。

- これらの手順の前半で **[サイト間接続]** 領域の **[有効]** ボックスにチェック マークを付けた場合、**サイト間接続**は、**セットアップ - リージョン管理**の一連のステップの次のステップとして表示されます。ステップ 19 （172 ページ） に進みます。

- これらの手順の前半で **[サイト間接続（Inter-Site Connectivity）]** 領域の **[有効（Enabled）]** ボックスにチェック マークを付けなかった場合、**クラウド リソース命名ルール**は、**セットアップ - リージョン管理**の一連の手順の次の手順として表示されます。ステップ 23 （172 ページ） に進みます。

ステップ 19 テキスト ボックスにオンプレミスの IPsec トンネル ピアのピア パブリック IP アドレスを入力するには、**[IPSec トンネル ピアのパブリック IP を追加]** をクリックします。

ステップ 20 **[エリア ID]** フィールドに OSPF エリア ID を入力します。

ステップ 21 外部サブネット プールを追加するには、**[外部サブネットの追加]** をクリックし、テキスト ボックスにサブネット プールを入力します。

ステップ 22 すべての接続オプションを設定したら、ページの下部にある[次へ（Next）]をクリックします。

[クラウド リソース 命名規則（Cloud Resource Naming Rules）] ページが表示されます。

ステップ 23 **[クラウド リソースの命名ルール（Cloud Resource Naming Rules）]** ページで、必要に応じてクラウド リソースの命名ルールを構成します。

クラウド リソースの命名ルールについては、クラウドリソースの命名 （173 ページ） セクションで詳しく説明します。命名ルールを変更する必要がない場合は、このページをスキップできます。

ステップ 24 終了したら **[Save and Continue（保存して続行）]** ボタンをクリックします。

スマート ライセンスの設定

このタスクでは、Cisco Cloud APIC でスマート ライセンスを設定する方法を示します。

始める前に

製品インスタンス登録トークンが必要です。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[構成（Configuration）]** リストから、**[cAPIC のセットアップ（Set Up cAPIC）]** をクリックします。**[設定-概要（Set up-Overview）]** ダイアログボックスが表示され、**[DNS サーバ（DNS Servers）]**、**[リージョン管理（Region Management）]**、**[スマート ライセンス（Smart Licensing）]** のオプションが示されます。

ステップ 4 Cloud APIC をシスコの統合ライセンス管理システムに登録するには、**[スマート ライセンス（Smart Licensing）]** から、**[登録（Register）]** をクリックします。**[スマート ライセンス（Smart Licensing）]** ダイアログが表示されます。

ステップ 5 トランスポート設定を選択してください。

- **Cisco Smart Software Manager (CSSM)に直接接続する**

- トランスポートゲートウェイ/Smart Software Managerサテライト
- **HTTP/HTTPS プロキシ（HTTP/HTTPS Proxy）**

（注） **HTTP/HTTPS プロキシ**を選択するときは、IP アドレスが必要です。

ステップ 6 指定されたテキスト ボックスで製品インスタンス登録トークンを入力します。

ステップ 7 完了したら **[登録（Register）]** をクリックします。

クラウドリソースの命名

クラウドAPICリリース5.0（2）より前では、Azureのクラウドapicによって作成されたクラウドリソースには、ACIオブジェクトの名前から派生した名前が割り当てられていました。

- リソースグループは、テナント、VRF、およびリージョンに基づいて作成されました。たとえば、`CAPIC_<tenant>_<vrf>_<region>`。
- VNET名は、クラウドAPIC VRFの名前と一致しました。
- サブネット名はCIDRアドレス空間から取得されました。たとえば、10.10.10.0 / 24クラウドサブネットの場合はsubnet-10.10.10.0_24です。
- クラウドアプリケーション名は、EPG名とアプリケーションプロファイル名から取得されました。たとえば、`<epg-name>_cloudapp_<app-profile-name>`

このアプローチは、クラウドリソースの命名規則が厳格な導入には適していません。また、クラウドリソースの命名とタグ付けに関するAzureのベストプラクティスに従っていません。

クラウド APIC リリース 5.0（2）以降、クラウド APIC でグローバル ネーミング ポリシーを作成できます。これにより、クラウド APIC から Azure クラウドに展開されたすべてのオブジェクトのカスタム クラウド リソース命名規則を定義できます。クラウド APIC ARM テンプレートの導入に使用される**リソース グループ**名を除き、クラウド APIC の初回セットアップ ウィザードで、すべてのクラウドリソースのカスタム命名ルールを定義できます。テンプレートのリソース グループ名は、最初に展開したときに定義され、その後は変更できません。グローバル ポリシーに加えて、REST API を使用して各クラウド APIC オブジェクトから作成されたクラウド リソースの名前を明示的に定義することもできます。

クラウド APIC リリース 5.1（2）以降、レイヤ 4ーレイヤ 7 サービスの導入では、ネットワーク ロード バランサ、アプリケーション ロード バランサ、デバイス アプリケーション セキュリティグループなどのクラウドリソースにカスタム名を指定できます。

（注） カスタム ネーミング ポリシーを使用しても、クラウドリソースが作成されると、名前を変更できないことに注意してください。既存のクラウド リソースの名前を変更する場合は、構成したすべてのクラウド リソースを削除して再作成する必要があります。削除されるクラウド リソースには、セカンダリ CIDR とサブネット、Cloud APIC によって展開された CCR が含まれ、したがって、CCR からすべてのリモート サイトへの IPSec トンネルが含まれます。

命名ルールに使用できる変数

クラウドリソースの命名ポリシーを作成する場合、次の変数を使用して、Cisco Cloud APIC オブジェクトに基づいてクラウドリソースの名前を動的に定義できます。

- $ {tenant} –リソースにはテナントの名前が含まれます
- $ {ctx} –リソースにはVRFの名前が含まれます。
- $ {ctxprofile}：リソースにはクラウドコンテキストプロファイルが含まれます。これは、特定のクラウド領域に導入されたVRFです。
- $ {subnet}：リソースには文字列subnetの後にサブネットIPアドレスが含まれます。
- $ {app}：リソースにはアプリケーションプロファイルの名前が含まれます。
- $ {epg}：リソースにはEPGの名前が含まれます。
- $ {contract} –リソースには契約の名前が含まれます
- $ {region} –リソースにはクラウドリージョンの名前が含まれます。
- $ {priority}：リソースにはネットワークセキュリティグループ（NSG）ルールの優先度が含まれます。この番号は、各NSGルール名が一意になるように自動的に割り当てられます。
- $ {serviceType}：リソースにはサービスタイプの省略形が含まれます（プライベートエンドポイントリソースにのみ有効）。
- $ {resourceName}：リソースにはターゲットリソースの名前が含まれます（プライベートエンドポイントリソースにのみ有効）。
- $ {device}：リソースにはレイヤ4ーレイヤ7デバイスの名前が含まれます。
- $ {interface}：リソースには、レイヤ4ーレイヤ7のデバイスインターフェイスの名前が含まれます。
- $ {deviceInterfaceDn}：リソースには、レイヤ7デバイスインターフェイスのDNが含まれます。

プライベートエンドポイントの場合、$ {app}-$ {svcepg}-$ {subnet}-$ {serviceType}-$ {resourceName}の組み合わせにより、プライベートエンドポイント名が一意になります。これ

らの変数のいずれかを削除すると、すでに存在するプライベートエンドポイントの名前になる場合があります。これにより、Cisco Cloud APIC によって障害が発生します。また、最大長の要件はAzureサービスによって異なります。

1つ以上の上記の変数を使用してグローバル名前付けポリシーを定義すると、Cisco Cloud APIC はすべての必須変数が存在し、無効な文字列が指定されていないことを確認するために文字列を検証します。

Azureには名前の最大長の制限があります。名前の長さがクラウドプロバイダーでサポートされている長さを超えると、構成が拒否され、Cisco Cloud APIC リソースの作成に失敗したというエラーが発生します。その後、障害の詳細を確認し、命名規則を修正できます。Cisco Cloud APIC リリース5.0（2）の時点での最大長の制限を以下に示します。最新の最新情報および長さ制限の変更については、Azure のドキュメントを参照してください。

次の表に、上記の各命名変数をサポートするクラウドリソースの概要を示します。アスタリスク（*）で示されたセルは、そのタイプのクラウドリソースに必須の変数を示します。プラス記号（+）で示されるセルは、これらの変数の少なくとも1つがそのタイプのクラウドリソースに必須であることを示します。たとえば、VNETリソースの場合、${ctx}、${ctxprofile}、またはその両方を指定できます。

表 *30 :* クラウドリソースでサポートされる変数

Azure のリソース	`${tenant}`	`${ctx}`	`${ctxprofile}`	`${subnet}`	`${app}`	`${epg}`	`${contract}`	`${region}`	`${priority}`
リソースグループ 最長：90	対応*	対応*						対応*	
仮想ネットワーク (VNET) 最長：64	対応	はい+	Yes+					対応	
Subnet 最長：80	はい	はい	はい	対応*				○	
アプリケーションセキュリティグループ（ASG） 最長：80	はい				対応*	対応*		○	

Azure のリソース	${tenant}	${ctx}	${ctxprofile}	${subnet}	${app}	${epg}	${contract}	${region}	${priority}
ネットワーク セキュリティ グループ（NSG） 最長：80	はい				対応*	対応*		○	
ネットワーク セキュリティ グループ ルール 最長：80	はい						はい		Yes *（自動）

表 *31 :* クラウドリソースでサポートされる変数（レイヤ*4*～レイヤ*7*デバイスサービス）

Azure のリソース	${tenant}	${region}	${ctxprofile}	${device}	${interface}	${deviceInterfaceDN}
インターネット ネットワーク ロード バランサ 最長：80	はい	はい	はい	対応*		
インターネット側のネットワークロードバランサ 最長：80	はい	はい	はい	対応*		
インターネット アプリケーション ロード バランサ 最長：80	はい	はい	はい	対応*		

Azure のリソース	${tenant}	${region}	${ctxprofile}	${device}	${interface}	${deviceInterfaceDN}
インターネット向けApplication Load Balancer 最長：80	はい	はい	はい	対応*		
デバイスASG 最長：80	はい	はい		対応*	対応*	対応*

命名ルールのガイドラインと制限事項

クラウドリソースの命名にカスタムルールを設定する場合、次の制限が適用されます。

- クラウドAPICの初回セットアップ時に、次の2つの命名ルールセットを使用して、グローバル命名ポリシーを定義します。
  - **ハブ リソース名前付けルール**は、インフラ テナントのハブ リソース グループ、ハブ VNET、オーバーレイ 1 CIDR、セカンダリ 2 CIDR サブネットの名前、およびインフラ テナントのシステムによって自動的に作成されるサブネットのサブネット プレフィックスを定義します。
  - クラウドリソース名前付けルールは、ネットワークセキュリティグループ（NSG）、アプリケーションセキュリティグループ（ASG）、ネットワークロードバランサ、アプリケーションロードバランサ、デバイスアプリケーションセキュリティグループ、およびインフラテナントで作成するサブネットの名前と名前を定義します。ユーザテナント内のすべてのリソース（リソースグループ、仮想ネットワーク、サブネット、NSG、ASG、ネットワークロードバランサ、アプリケーションロードバランサ）。

  命名規則を定義したら、それらを確認して確認する必要があります。クラウドリソースを展開する前に、命名規則を確認する必要があることに注意してください。
- クラウドリソースが作成されると、その名前は変更できず、GUIで命名ポリシーを更新できません。クラウドAPICをリリース5.0（2）にアップグレードし、一部のリソースがすでにAzureに導入されている場合は、グローバルカスタム命名ルールを変更することもできません。

  既存のクラウドリソースまたはポリシーの名前を変更する場合は、GUIでグローバル名前付けポリシーを更新する前に、展開されたリソースを削除する必要があります。

  このような場合、REST APIを使用して、作成する新しいリソースにカスタム名を明示的に割り当てることができます。
- REST APIを使用してクラウドリソースの命名を更新する場合は、同時に設定をインポートしないことを推奨します。

最初に命名規則を定義することをお勧めします。それからテナント設定も行ってください。

テナント設定の展開後は、命名ポリシーを変更しないことをお勧めします。

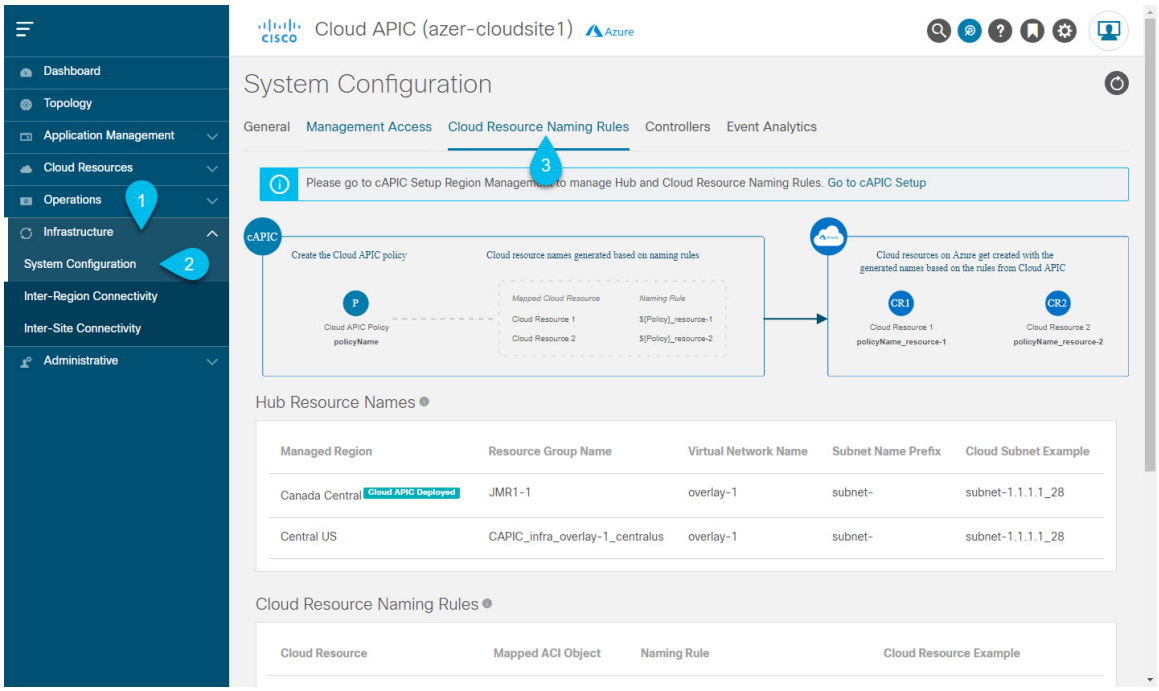
クラウド リソースの命名ルールの表示

最初に、Cloud APIC を展開するときに、初回セットアップ ウィザードのリージョン管理部分でクラウド リソースの命名ルールを定義します。これについては、『*Cisco Cloud APIC* インストール ガイド』で説明されています。初期セットアップの後、このセクションで説明されているように、Cloud APIC GUI の **[システム構成（System Configuration）]** 画面で構成したルールを表示できます。

この画面の情報は読み取り専用ビューで表示されます。最初の展開後にルールを変更する場合は、最初のセットアップ ウィザードを再実行する必要があります。

ステップ 1 Cloud APIC GUI にログインします。

ステップ 2 **[クラウド リソースの命名ルール（Cloud Resource Naming Rules）]** 画面に移動します。



a) **[ナビゲーション（Navigation）]** サイドバーで、**[インフラストラクチャ（Infrastructure）]** カテゴリを展開します。

b) **インフラストラクチャ** カテゴリから、**[システム構成（System Configuration）]** を選択します。

c) **[システム構成（System Configuration）]** 画面で、**[クラウド リソースの命名ルール（Cloud Resource Naming Rules）]** タブを選択します。

[クラウド リソースの命名規則（Cloud Resource Naming Rules）] タブでは、Cloud APIC からクラウド サイトに展開するリソースの名前に対して現在構成されている規則の概要を確認できます。

以前にカスタム命名規則を構成していない場合は、クラウドリソースの Cloud APIC オブジェクト名を使用するデフォルトの規則がここにリストされます。

最初のセットアップ時に定義した命名規則を受け入れなかった場合は、画面の上部に警告バナーが表示されます。

（注） クラウドリソースを展開する前に、命名規則を確認する必要があることに注意してください。

REST API を使用した Cisco Cloud APIC の構成

REST API を使用したテナントの作成

サブスクリプションには次の 2 つのタイプがあります：独自および共有。各サブスクリプション タイプにはプライマリ テナントがあります。新しい管理対象テナントまたは非管理対象テナントを作成するときに、独自のサブスクリプションを選択します。既存のプライマリテナントの管理対象または管理対象外の設定を継承するテナントを作成するときに、共有サブスクリプションを選択します。このセクションでは、独自のタイプのサブスクリプションを使用して管理対象テナントと非管理対象テナントを作成する方法と、共有サブスクリプションを作成する方法を示します。

このセクションでは、Postman の本文からのサンプル POST 要求を使用して、REST API を使用してテナントを作成する方法を示します。

ステップ 1 独自サブスクリプションの作成。

a) クライアント シークレットを使用して非管理対象テナントを作成するには：

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="{{primary-tenant-name}}">
    <cloudAccount id="{{user-tenant-subscription-id}}" vendor="azure" accessType="credentials"
 status="">
       <cloudRsCredentials tDn="uni/tn-{{primary-tenant-name }}/credentials-{{ primary-tenant-name
 }}"/>
    </cloudAccount>
    <cloudCredentials name="{{ primary-tenant-name }}" keyId="{{application_key_id}}"
key="{{client_secret_key}}">
        <cloudRsAD tDn="uni/tn-{{ primary-tenant-name }}/ad-{{active_directory_id}}"/>
    </cloudCredentials>
    <cloudAD name="{{active_directory_name}}" id="{{active_directory_id}}" />
    <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
 }}]-vendor-azure" status=""/>
</fvTenant>
```

b) 管理対象テナントを作成するには：

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml
```

```
    <fvTenant name="{{ primary-tenant-name }}">
        <cloudAccount id="{{ user-tenant-subscription-id }}" vendor="azure" accessType="managed"
    status="" />
        <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
     }}]-vendor-azure" status=""/>
    </fvTenant>
```

ステップ 2 共有サブスクリプションの作成：

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="{{ primary-tenant-name }}">
    <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
}}]-vendor-azure" status=""/>
</fvTenant>
```

REST API を使用したコントラクトの作成

この例では、REST API を使用して Cisco Cloud APIC のコントラクトを作成する方法を示します。

始める前に

フィルタを作成します。

コントラクトを作成するには：

例：

```
<polUni>
  <fvTenant name="t2" status="">
    <vzFilter descr="" name="http-family-destination" ownerKey="" ownerTag="">
      <vzEntry name="http" prot="tcp" etherT="ip" dFromPort="http" dToPort="http"/>
      <vzEntry name="https" prot="tcp" etherT="ip" dFromPort="https" dToPort="https"/>
    </vzFilter>
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjFiltAtt action="permit" directives="" tnVzFilterName="http-family-destination"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

REST API を使用したクラウド コンテキスト プロファイルの作成

このセクションでは、クラウド コンテキスト プロファイルを作成する方法を示します。

始める前に

VRF を作成します。

ステップ 1 基本的なクラウド コンテキスト プロファイルを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
    <cloudCtxProfile name="cProfilewestus151">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
      <cloudRsToCtx tnFvCtxName="ctx151"/>
    <cloudCidr addr="15.151.0.0/16" primary="true" status="">
          <cloudSubnet ip="15.151.1.0/24" name="GatewaySubnet" usage="gateway">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
          <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
    </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>
```

ステップ 2 VNet のセカンダリ VRF、CIDR、およびサブネットを追加するクラウド コンテキスト プロファイルを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tenant1" status="">
        <fvCtx name="VRF1" />
        <fvCtx name="VRF2" />
        <cloudCtxProfile name="vpc1" status="">
           <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-centralus" status=""/>

            <cloudRsToCtx tnFvCtxName="VRF1" />
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
            <cloudCidr name="cidr1" addr="192.0.2.0/16" primary="yes" status="">
                <cloudSubnet ip="192.0.3.0/24" usage="gateway" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-centralus/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr name="cidr1" addr="193.0.2.0/16" primary="no" status="">
                <cloudSubnet ip="193.0.3.0/24" usage="" status="">
                    <cloudRsSubnetToCtx tnFvCtxName="VRF2"/>
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-centralus/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
```

```
</polUni>
```

REST API を使用したクラウド リージョンの管理

このセクションでは、REST API を使用してクラウド リージョンを管理する方法を示します。

クラウド リージョンを作成するには:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <cloudDomP name="default">
       <cloudProvP vendor="azure">
          <cloudRegion adminSt="managed" name="eastus"><cloudZone name="default"/></cloudRegion>
          <cloudRegion adminSt="managed" name="eastus2"><cloudZone name="default"/></cloudRegion>
          <cloudRegion adminSt="managed" name="westus"><cloudZone name="default"/></cloudRegion>
        </cloudProvP>
    </cloudDomP>
</polUni>
```

REST API を使用したフィルタの作成

このセクションでは、REST API を使用してフィルタを作成する方法を示します。

フィルタを作成するには、次の手順を実行します。

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="t15">
    <vzFilter name="rule1">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
      <vzEntry etherT="ip" prot="unspecified" name="any"/>
    </vzFilter>
    <vzFilter name="rule2">
      <vzEntry etherT="ip" dToPort="http" prot="tcp" dFromPort="http" name="http"/>
    </vzFilter>
    <vzFilter name="rule3">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
    </vzFilter>
    <vzFilter name='all_rule'>
        <vzEntry etherT="ip" prot="unspecified" name="any"/>
  </vzFilter>

    <vzBrCP name="c1">
        <vzSubj name="c1">
            <vzRsSubjFiltAtt tnVzFilterName="rule2"/>
            <vzRsSubjGraphAtt tnVnsAbsGraphName="c13_g1"/>
```

```
            <vzRsSubjFiltAtt tnVzFilterName="rule3"/>
            <vzRsSubjFiltAtt tnVzFilterName="all_rule"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

REST API を使用したアプリケーション プロファイルの作成

このセクションでは、REST API を使用してアプリケーション プロファイルを作成する方法を示します。

始める前に

テナントを作成します。

アプリケーション プロファイルを作成する方法：

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">

    </cloudApp>

  </fvTenant>
</polUni>
```

REST API を使用したネットワーク セキュリティ グループの構成

この例は、REST API を使用して、Cisco Cloud APIC の新しい**サブネットごとの NSG** 構成を設定する方法を示しています。

始める前に

セキュリティ グループ （50 ページ）に記載の情報について、確認してください。

Cisco Cloud APIC のサブネットごとの NSG 構成を設定するには、次の手順を実行します。

例：

```
<polUni>
    <cloudDomP status="">
        <cloudProvP vendor="azure">
            <cloudProvResPolCont><cloudProvSGForSubnetP enableSGForSubnet="true"
status=""/></cloudProvResPolCont>
        </cloudProvP>
    </cloudDomP>
</polUni>
```

REST API を使用した EPG の作成

このセクションの手順を使用して、REST API を使用したアプリケーション EPG、外部 EPG、サービス EPG を作成します。

REST API を使用したクラウド EPG の作成

この例では、REST API を使用してクラウド EPG を作成する方法を示します。

始める前に

アプリケーション プロファイルと VRF を作成します。

クラウド EPG を作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">


        <cloudEPg name="epg1">
            <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
            <cloudEPSelector matchExpression="custom:tag1=='value1'" name="selector-1"/>
        </cloudEPg>


    </cloudApp>
```

```
  </fvTenant>
</polUni>
```

REST API を使用した外部クラウド EPG の作成

この例では、REST API を使用して外部クラウド EPG を作成する方法を示します。

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 外部クラウド EPG を作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
        <fvCtx name="ctx151"/>
        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="internet" name="extEpg-1">
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
            <cloudExtEPSelector name="extSelector1" subnet="0.0.0.0/0"/>
       </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

ステップ 2 タイプ **site-external** で外部クラウド EPG を作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="infra">
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="site-ext" name="extEpg-1">
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="overlay-2"/>
            <cloudExtEPSelector name="extSelector1" subnet="10.100.0.0/16"/>
       </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

REST API を使用したサービス EPG の作成

この例では、REST API を使用してサービス EPG を作成する方法を示します。

始める前に

- クラウド サービス エンドポイント グループ （42 ページ）の情報を確認してください。
- アプリケーション プロファイルと VRF を作成します。

ステップ 1 クラウド ネイティブの展開タイプでサービス EPG を作成するには、次の手順を実行します。

例：

```
<cloudSvcEPg name="Storage" type="Azure-Storage" accessType="Private" deploymentType="CloudNative">

    <cloudPrivateLinkLabel name="ProductionSubnets"/>
    <cloudRsCloudEPgCtx tnFvCtxName="HUB-SERVICES-VRF"/>
    <cloudSvcEPSelector matchExpression="ResourceName=='StorageAcct1'" name="selector-1"/>
    <cloudSvcEPSelector matchExpression="custom:Tag=='ProdStorage'" name="selector-2"/>
</cloudSvcEPg>
```

ステップ 2 クラウド ネイティブ管理対象の展開タイプでサービス EPG を作成するには、次の手順を実行します。

例：

```
<cloudSvcEPg name="APIM" type="Azure-ApiManagement" accessType="Private"
deploymentType="CloudNativeManaged" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="infra-SvcCtx" />
    <fvRsCons tnVzBrCPName="infra-APIM-Mock"/>
    <fvRsProv tnVzBrCPName="infra-managedAPIM" status=""/>
    <cloudSvcEPSelector matchExpression="IP=='10.21.52.0/28'" name="sel1" status=""/>
</cloudSvcEPg>
```

ステップ 3 サードパーティの展開タイプでサービス EPG を作成するには：

例：

```
<cloudSvcEPg name="SaaS-Hub" type="Custom"  accessType="Private" deploymentType="Third-party"
status="">
    <cloudRsCloudEPgCtx tnFvCtxName="infra-SvcCtx" status=""/>
    <cloudSvcEPSelector
matchExpression="URL=='saassvcepg.286b0377-a9b7-40d7-a94f-67abe03ce5f4.centralus.azure.privatelinkservice'"
 name="s1" status=""/>
    <cloudPrivateLinkLabel name="saas-hub" status=""/>
    <fvRsProv tnVzBrCPName="SaaS-Hub" status=""/>
</cloudSvcEPg>
```

REST API を使用したクラウド テンプレートの作成

このセクションでは、REST API を使用してクラウド テンプレートを作成する方法を示します。クラウド テンプレートの詳細については、クラウド テンプレートの概要 （59 ページ）を参照してください。

始める前に

クラウドテンプレートを作成するには:

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2" numRoutersPerRegion="2"
status="" vrfName="overlay-1">
         <cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="250M" routerLicenseToken="thisismycsrtoken" />
             </cloudtemplateProfile>
      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="westus"/>
        <cloudRegionName provider="azure" region="westus2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="azure" region="westus2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

REST API を使用して VRF リーク ルートの構成

始める前に

このセクションの手順を実行する前に、内部 VRF 間のルート リーク （14 ページ） と グローバルな Inter-VRF ルート リーク ポリシー （15 ページ） に記載されている情報を確認してください。

ステップ 1 次のような投稿を入力して、契約ベースのルーティングを有効または無効にします。

```
<fvTenant name=”infra”>
    <cloudVrfRouteLeakPol name="default" allowContractBasedRouting=”true”/>
</fvTenant>
```

`allowContractBasedRouting` フィールドには、次のいずれかの設定があります。

- **true** : ルート マップがない場合、契約に基づいてルートが漏洩していることを示します。有効にすると、ルートマップが構成されていないときにコントラクトがルーティングを駆動します。ルートマップが存在する場合、ルート マップは常にルーティングを駆動します。
- **false**: デフォルト設定です。ルートが契約に基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。

ステップ 2 次のような投稿を入力して、leakInternalPrefix フィールドを使用して、VRF に関連付けられたすべてのクラウド CIDR のルート リークを設定します。

```
<fvTenant name=”t1”>
  <fvCtx name="v1">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t2" ctxName="v2" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>

<fvTenant name=”t2”>
  <fvCtx name="v2">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t1" ctxName="v1" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>
```

ステップ 3 次のような投稿を入力して、leakInternalSubnet フィールドを使用して、VRF のペア間の特定のルートをリークします。

```
<fvTenant name=”anyTenant" status="">
    <fvCtx name="VRF1" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.1.0/24" >
                <leakTo ctxName=”VRF2" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
    <fvCtx name="VRF2" status="" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.2.0/24" >
                <leakTo ctxName=”VRF1" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
</fvTenant>
```

REST API を使用したトンネルのソース インターフェイス選択の構成

始める前に

このセクションの手順を実行する前に、トンネルのソース インターフェイスの選択 （17 ページ） に記載されている情報を確認してください。

次のような投稿を入力して、トンネルの送信元インターフェイスの選択を構成します。

```
<cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
  <cloudtemplateProfile name="defaultxyz" routerUsername="james" routerPassword="bond@@7" />

  <cloudtemplateIpSecTunnelSubnetPool subnetpool="10.20.0.0/16" poolname="pool1" />

  <cloudtemplateIntNetwork name="default">
    <cloudRegionName provider="aws" region="us-west-1"/>
    <cloudRegionName provider="aws" region="us-west-2"/>
  </cloudtemplateIntNetwork>

  <cloudtemplateExtNetwork name="something” vrfName=”xyz” >
    <cloudRegionName provider="aws" region="us-west-2"/>
    <cloudtemplateVpnNetwork name="default">
      <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" poolname="" presharedkey=”abcd”
ikeVersion=”v1|v2”>
          <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId="2" />
      </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
```

グローバルクラウドリソースの命名規則の定義または特定のオブジェクトの名前のオーバーライド

このセクションでは、クラウド リソースに名前を付けるためのグローバル ポリシーを構成したり、特定のクラウド リソースの名前をオーバーライドしたりするために使用できる REST API POST の例を示します。

（注） カスタム命名規則を確実にサポートできるようにするために、クラウド リソース名をオブジェクトごとに定義できます。これらの明示的な名前のオーバーライドは Cloud APIC GUI では使用できず、REST API を使用してのみ実行できます。名前を定義するには、グローバル クラウド リソースの名前付けポリシーを使用することをお勧めします。明示的な名前のオーバーライドは、グローバルな名前付けポリシーを使用して名前付け要件を満たすことができない場合にのみ使用する必要があります。

ステップ 1 ハブ リソースの命名規則を作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2"
    numRoutersPerRegion="2" status="" vrfName="overlay-1">
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="‟west’s” status="">
          <cloudtemplateRegionNameCustomization ctxProfileName="infra-vnet"
          resourceGroupName="infra-rh" subnetNamePrefix="snet-" />
        </cloudRegionName>
      </cloudtemplateIntNetwork>
    </cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

ステップ 2 クラウド リソースの命名規則を作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <cloudDomP name="default">
    <cloudNaming
    azResourceGroup="${tenant}-network-${ctx}-${region}-rg"
    azVirtualNetwork="${tenant}-${ctxprofile}-vnet"
    azSubnet="${tenant}-${ctxprofile}-snet-${subnet}"
    azNetworkSecurityGroup="${app}-${epg}-nsg"
    azApplicationSecurityGroup="${app}-${epg}-asg"
    azNetworkSecurityGroupRule="${contract}--${priority}"
    internetApplicationBalancer="agw-e-${device}"
    internalApplicationBalancer="agw-i-${device}"
    internetNetworkBalancer="lbe-${device}"
    internalNetworkBalancer="lbi-${device}"
    l4L7DeviceApplicationSecurityGroup="${deviceInterfaceDn}"
   reviewed="yes" />
  </cloudDomP>
</polUni>
```

ステップ 3 特定の Cloud APIC オブジェクトに対応する Azure クラウド リソース名をオーバーライドするには:

API を使用してカスタム名を指定するときに、同じ変数 (たとえば、 `${tenant}`) を使用できます。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<fvTenant name="ExampleCorp" status="">
  <fvRsCloudAccount status="" tDn="uni/tn-infra/act-[<infra-subscription>]-vendor-azure"/>
  <fvCtx name="VRF1"/>
  <cloudApp name="App1">
    <cloudEPg name="Db" azNetworkSecurityGroup="db-nsg" azApplicationSecurityGroup="db-asg-${region}">

      <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
      <cloudEPSelector matchExpression="custom:EPG=='db'" name="100"/>
    </cloudEPg>
  </cloudApp>
  <cloudCtxProfile name="c02" azResourceGroup="custom-tc-rg1" azVirtualNetwork="vnet1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
    <cloudRsToCtx tnFvCtxName="VRF1"/>
    <cloudCidr addr="10.20.20.0/24" name="cidr1" primary="yes" status="">
      <cloudSubnet ip="10.20.20.0/24" name="subnet1" azSubnet="s1" status="">
        <cloudRsZoneAttach status="" tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
```

```
      </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>
</fvTenant>
```

ステップ 4 特定の Cloud APIC オブジェクトに対応するレイヤ 4 からレイヤ 7 の Azure クラウド リソース名をオーバーライドするには：

API を使用してカスタム名を指定するときに、同じ変数 (たとえば、`${tenant}`) を使用できます。

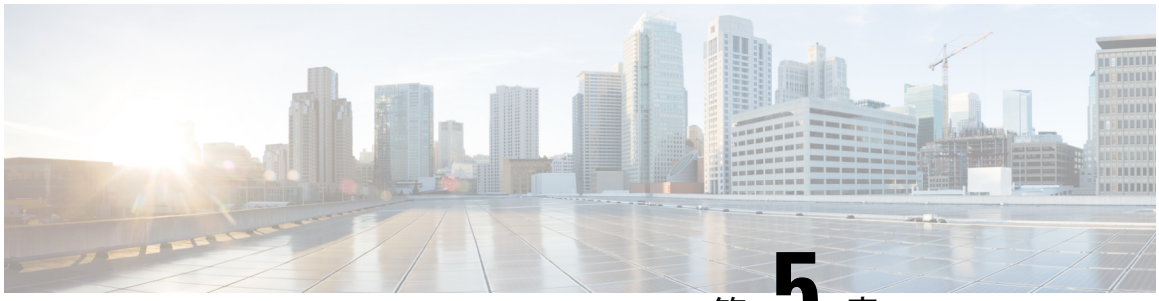
ロード バランサのポリシーを上書きします。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
 <fvTenant>
 <cloudLB name="ALB" type="application" scheme="internet" size="small" instanceCount="2" status=""
 nativeLBName=”ALB” >
                <cloudRsLDevToCloudSubnet
tDn="uni/tn-{{tenantName}}/ctxprofile-c1/cidr-[31.10.0.0/16]/subnet-[31.10.80.0/24]" status="" />
        </cloudLB>
 </fvTenant>
```

デバイス ASG のオーバーライド ポリシー：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
 <fvTenant>
 <cloudLDev name="{{FWName}}" status="" l4L7DeviceApplicationSecurityGroup="Group1" >
            <cloudRsLDevToCtx tDn="uni/tn-{{tenantName}}/ctx-VRF1" status=""/>
            </cloudLIf>
        </cloudLDev>
 <fvTenant>
```

グローバル クラウド リソースの命名規則の定義または特定のオブジェクトの名前のオーバーライド



第 5 章

システムの詳細の表示

VM ホスト メトリックのモニタリング

リリース 25.0(1) 以降では、Prometheus Node Exporter を使用して Cisco Cloud ネットワーク コントローラが展開されている VM ホストのメトリックのモニタリングがサポートされます。Prometheus Node Exporter は、さまざまなハードウェアおよびカーネル関連のメトリックを可視化し、Linux ノードから CPU、ディスク、メモリの統計情報などの技術情報を収集します。Prometheus ノード エクスポータの概要については、以下を参照してください。

https://prometheus.io/docs/introduction/overview/

Cisco Cloud ネットワーク コントローラがリリース 25.0(1) 以降で実行されている場合、Prometheus Node Exporter はデフォルトで自動的に使用可能になります。

注意事項と制約事項

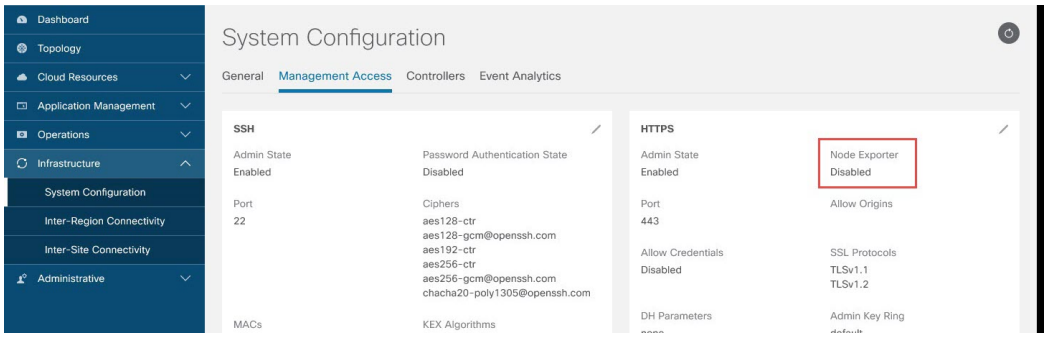
HTTP は、Prometheus Node Exporter を使用したモニタリング メトリックではサポートされていません。Prometheus Node Exporter を使用したメトリックのモニタリングでは、HTTPS のみがサポートされます。

GUI を使用した VM ホストメトリックのモニタリング

次の手順では、GUI を使用して Prometheus Node Exporter で VM ホスト メトリックをモニタできるようにする方法について説明します。

ステップ 1 Cisco Cloud Network Controller GUI で、**[インフラストラクチャ（Infrastructure）]** > **[システム構成（System Configuration）]** に移動し、**[管理アクセス（Management Access）]** タブをクリックします。

ステップ 2 ウィンドウの右側の **[HTTPS]** 領域で、**[ノード エクスポータ（Node Exporter）]** フィールドのエントリを確認します。

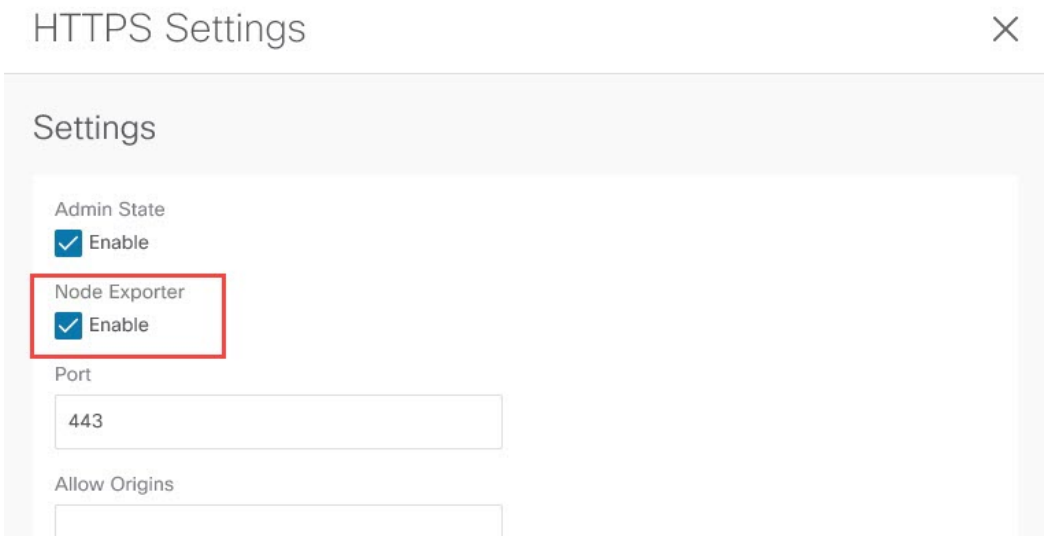


- **有効化（Enabled）**：Prometheus Node Exporter はすでに有効になっています。この場合、これらの手順を続行する必要はありません。
- **無効化（Disabled）**：Prometheus Node Exporter はまだ有効になっていません。Prometheus Node Exporter を有効にするには、次の手順に従います。

ステップ 3 **[HTTPS]** 領域の鉛筆アイコンをクリックして、HTTPS 設定を編集します。

[HTTPS 設定（HTTPS Settings）] ウィンドウが表示されます。

ステップ 4 **[ノード エクスポータ（Node Exporter）]** フィールドを見つけ、**[有効化（Enable）]** をクリックします。



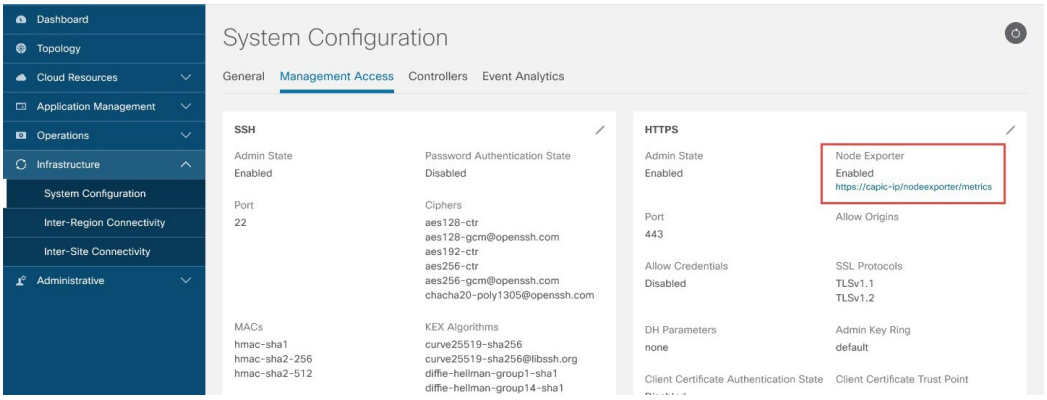
これらの設定を保存すると Web サービスが再起動され、要求への応答が再開されるまで少し時間がかかることを示す警告メッセージが表示されます。**[OK]** をクリックして、変更内容を確定します。

ステップ 5 ウィンドウの左下の **[保存（Save）]** をクリックします。

[システム構成/管理アクセス（System Configuration/Management Access）] ウィンドウに戻ります。Web サービスが再起動し、数秒後にオンラインに戻ります。

ステップ 6 ウィンドウの右側の **[HTTPS]** 領域で、**[ノード エクスポータ（Node Exporter）]** フィールドのエントリが **[有効化（Enabled）]** に設定されていることを確認します。

これにより、Prometheus Node Exporter が有効になっていることが確認されます。



ステップ 7 **[ノード エクスポータ（Node Exporter）]** 領域の **[有効化（Enabled）]** テキストの下にあるリンクをクリックします。

ブラウザに別のタブが表示され、Cisco Cloud Network Controller が展開されている VM ホストのメトリックが示されます。

REST API を使用した VM ホスト メトリックスの監視

これらの手順では、REST API を使用して VM ホスト メトリックを監視するようにPrometheus Node Exporter を有効にする方法について説明します。

ステップ 1 Prometheus Node Exporter が有効になっているかどうかを確認するには、次の GET コールを送信します。

```
GET https://<cloud-network-controller-ip-address>/api/mo/uni/fabric/comm-default/https.xml
```

`nodeExporter` フィールドを見つけて、`有効`または `無効` に設定されているかどうかを確認します。

ステップ 2 VM ホスト メトリックを監視するには、次の投稿を送信して、Prometheus ノード エクスポータを有効にします。

```
POST https://<cloud-network-controller-ip-address>/api/mo/uni/fabric/comm-default/https.xml

<commHttps nodeExporter="enabled" />
```

メトリックスは、Cisco Cloud Network Controller が展開されている VM ホストに表示されます。

ステップ 3 REST API を使用してメトリックを表示するには、次の GET コールを送信します。

```
GET https://<cloud-network-controller-ip-address>/nodeexporter/metrics
```

ステップ 4 Prometheus ノード エクスポータを無効にするには、次の投稿を送信します。

```
POST https://<cloud-network-controller-ip-address>/api/mo/uni/fabric/comm-default/https.xml

<commHttps nodeExporter="disabled" />
```

アプリケーション管理詳細の表示

ここでは、Cisco Cloud APIC GUI を使用してアプリケーション管理の詳細を表示する方法について説明します。アプリケーション管理の詳細には、特定のテナント、アプリケーションプロファイル、EPG、コントラクト、フィルタ、VRF、サービス、またはクラウド コンテキスト プロファイルの情報が含まれます。

ステップ 1 **[ナビゲーション (Navigation)]** メニューで、**[アプリケーション管理 (Application Management)]** タブを選択します。

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。詳細については、「アプリケーション管理オプション」のテーブルを参照してください。

表 *32:* アプリケーション管理サブタブ

サブタブ名	説明
テナント	テナントをサマリー テーブルの行として表示します。
アプリケーション プロファイル	サマリー テーブルの行としてアプリケーション プロファイルを表示します。
EPG	EPG をサマリー テーブルの行として表示します。
契約	コントラクトをサマリーテーブルの行として表示します。
フィルタ（**Filters**）	サマリー テーブルの行としてフィルタを表示します。
VRF	サマリー テーブルの行として VRF を表示します。

サブタブ名	説明
Services	次の 2 つのサブタブと情報が含まれています。 • **デバイス**：サマリーテーブルの行としてデバイスを表示します。 • **サービス グラフ**：サービス グラフをサマリーテーブルの行として表示します。
クラウド コンテキスト プロファイル	クラウドコンテキストプロファイルをサマリーテーブルの行として表示します。

ステップ 2 表示する詳細のコンポーネントを表すタブをクリックします。

サマリーテーブルは、テーブルの行として表示されます。たとえば、**[テナント（Tenants）]**サブタブを選択した場合、テナントのリストがサマリー テーブルの行として表示されます。

属性によるフィルタ処理バーをクリックすることにより、行をフィルタ処理できます。属性、演算子、およびフィルタ値を選択します。たとえば、テナントに基づくフィルタリングの場合は、[Name] == T1（T1 はテナントの名前）を選択します。

ステップ 3 サマリー ペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。

ステップ 4 詳細については、表示する特定のコンポーネントを表すサマリーテーブルの行をダブルクリックします。

新しいダイアログ ボックスが、次のタブのいずれかと共に**作業**ペインの上に表示されます。

（注） 表示されるタブは、コンポーネントと構成が異なるように見えます。

- **概要（Overview）**：クラウドリソース、設定関係、およびコンポーネントの設定の概要を示します。
- **トポロジ**：オブジェクトと他の関連オブジェクトとの視覚的な関係を提供します。選択したオブジェクトが中央に表示されます。
- **クラウドリソース**：このコンポーネントに関連するクラウドリソース情報を表示するサブタブのリストを含みます。
- **アプリケーション管理**：コンポーネントに関係する ACI 関連情報を表示するサブタブのリストを含みます。
- **統計**：選択したサンプリング間隔と統計タイプに基づいて統計を表示できるようにします。**[統計]** タブは表示しているコンポーネントに応じたサブタブを含みます。
- **イベント分析**：障害、イベント、監査ログを表示するサブタブのリストを含みます。

（注） **作業**ウィンドウの上部に表示されるダイアログボックスの右上隅には、**更新**ボタンと**[アクション（Actions）]**ボタンの間に**編集**ボタンがあります。**[編集（Edit）]**ボタンをクリックすると、選択したコンポーネントを編集できます。

クラウド リソースの詳細の表示

ここでは、Cisco Cloud APIC GUI を使用してクラウド リソースの詳細を表示する方法について説明します。クラウド リソースの詳細には、特定のリージョン、VNET、ルータ、セキュリティ グループ（アプリケーション セキュリティ グループ/ネットワーク セキュリティ グループ）、エンドポイント、VM、およびクラウド サービスに関する情報が含まれます。

リリース 5.0(2) 以降、**[エンドポイント（Endpoints）]** サブタブでは、*[クラウド タグ（Cloud Tag）]* 属性に基づく検索がサポートされています。

ステップ 1 **[ナビゲーション（Navigation）]** メニューから、**[クラウド リソース（Cloud Resources）]** タブを選択します。

[クラウド リソース（Cloud Resources）] タブが展開すると、サブオプション オプションのリストが表示されます。詳細については、「*Cloud Resource Options*」の表を参照してください。

表 *33* : クラウド リソース サブタブ

サブタブ名	説明
[Regions]	リージョンをサマリー テーブルの行として表示します。
仮想ネットワーク	サマリー テーブルの行として VNET を表示します。
Routers	ルータをサマリー テーブルの行として表示します。
セキュリティ グループ	サマリー テーブルの行としてセキュリティを表示します。
エンドポイント	エンドポイントをサマリー テーブルの行として表示します。
仮想マシン	VM をサマリー テーブルの行として表示します。
クラウド サービス（**Cloud Services**）	次のサブタブを含みます。 • **[クラウド サービス（Cloud Service）]** タブ：クラウド サービスをサマリー テーブルの行として表示します。 • **[ターゲット グループ]** タブ：ターゲット グループをサマリー テーブルの行として表示します。

ステップ 2 表示する詳細のコンポーネントを表すタブをクリックします。

サマリー テーブルは、テーブルの行として表示されます。たとえば、**[エンドポイント（Endpoints）]** サブタブを選択した場合、エンドポイントのリストがサマリー テーブルの行として表示されます。

*[*属性によるフィルタ（*Filter by attributes*）*]* バーをクリックすると、ドロップダウン メニューから属性を選択して行をフィルタリングできます。ドロップダウン メニューに表示される属性は、選択したサブタブによって異なります。

[エンドポイント（Endpoints）]サブタブでは、**キー**または**値**の用語を入力して、クラウドタグに基づいて検索を絞り込むことができます。両方の用語に基づいて検索する場合は、**キー**または**値**の用語の上に表示される（+）をクリックします（最初に入力された用語に応じて）。クラウド タグ フィルタは編集できません。検索を変更するには、最初にフィルタを削除してから、目的の**キー**または**値**の用語を再度入力します。複数のクラウド タグ フィルタに基づく検索がサポートされています。

ステップ 3 サマリー ペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。

ステップ 4 詳細については、表示する特定のコンポーネントを表すサマリー テーブルの行をダブルクリックします。

新しいダイアログ ボックスが、次のタブのいずれかと共に**作業**ペインの上に表示されます。

（注） 表示されるタブは、コンポーネントと構成が異なるように見えます。

- **概要（Overview）**：クラウドリソース、設定関係、およびコンポーネントの設定の概要を示します。リリース 5.0(2) 以降、エンドポイントに関連付けられたクラウド タグが表示されます。
- **クラウドリソース**：このコンポーネントに関連するクラウドリソース情報を表示するサブタブのリストを含みます。
- **アプリケーション管理**：コンポーネントに関係する ACI 関連情報を表示するサブタブのリストを含みます。
- **統計**：選択したサンプリング間隔と統計タイプに基づいて統計を表示できるようにします。**[統計]** タブは表示しているコンポーネントに応じたサブタブを含みます。
- **イベント分析**：障害、イベント、監査ログを表示するサブタブのリストを含みます。

操作の詳細の表示

ここでは、Cisco Cloud APIC GUI を使用して操作の詳細を表示する方法について説明します。操作の詳細には、特定の障害、イベント、監査ログ、アクティブ セッション、バックアップおよび復元ポリシー、テクニカル サポート ポリシー、ファームウェア管理、スケジューラ ポリシー、およびリモート ロケーションの情報が含まれます。

ステップ 1 **[ナビゲーション（Navigation）]** メニューから **[操作（Operations）]** タブを選択します。

[操作（Operations）] タブが展開すると、サブタブ オプションのリストが表示されます。詳細については「操作オプション」の表を参照してください。

表 *34 : [*操作（*Operations*）*]* サブタブ

サブタブ名	説明
イベント分析	次のサブタブを含みます。 • **[障害（Faults）]** タブ：障害をサマリ テーブルの行として表示します。 • **[障害レコード（Fault Records）]** タブ：障害レコードをサマリーテーブルの行として表示します。 • **[イベント（Events）]** タブ：イベントをサマリーテーブルの行として表示します。 • **[監査ログ（Audit Logs）]** タブ：監査ログをサマリー テーブルの行として表示します。
アクティブセッション	Cloud APIC にログインしているアクティブ ユーザーのリストを表示します。

バックアップと復元	次のサブタブを含みます。
	• **[バックアップ（Backups）]** タブ：バックアップをサマリーテーブルの行として表示します。
	• **[バックアップ ポリシー（Backup Policies）]** タブ：バックアップ ポリシーをサマリー テーブルの行として表示します。
	• **[ジョブ ステータス（Job Status）]** タブ：ジョブのステータスをサマリーテーブルの行として表示します。
	• **[イベント分析（Event Analytics）]** タブ：次のサブタブが含まれます。
	  • **[障害（Faults）]** タブ：サマリー テーブルの行として障害を表示します。
	  • **[イベント（Events）]** タブ：イベントをサマリー テーブルの行として表示します。
	  • **[監査ログ（Audit Logs）]** タブ：監査ログをサマリー テーブルの行として表示します。

サブタブ名	説明
[Tech Support]	次のサブタブを含みます。 • **[Tech Support]** タブ：テクニカル サポート ポリシーをサマリー テーブルの行として表示します。 • **[コア ログ（Core Logs）]**タブ：コア ログをサマリー テーブルの行として表示します。
Firmware Management	次のサブタブを含みます。 • **[全般（General）]** タブ：現在のファームウェア バージョン、アップグレード ステータスなどの一般的なファームウェア管理情報が表示されます。 • **[イメージ（Images）]** タブ：イメージのリストを表示します。 • **[イベント分析（Event Analytics）]** タブ：次のサブタブが含まれます。 • **[障害（Faults）]** タブ：サマリー テーブルの行として障害を表示します。 • **[イベント（Events）]** タブ：イベントをサマリー テーブルの行として表示します。 • **[監査ログ（Audit Logs）]** タブ：監査ログをサマリー テーブルの行として表示します。
スケジューラ	スケジューラ ポリシーをサマリー テーブルの行として表示します。
リモート ロケーション	リモート ロケーションをサマリー テーブルの行として表示します。

ステップ 2 表示するコンポーネントを表すタブをクリックします。

サマリー テーブルは、テーブルの行として表示されます。たとえば、**[アクティブ セッション（Active Sessions）]**サブタブを選択した場合、アクティブ セッションのリストがサマリーテーブルの行として表示されます。

属性によるフィルタ処理バーをクリックすることにより、行をフィルタ処理できます。属性、演算子、およびフィルタ値を選択します。たとえば、ユーザー名に基づいてフィルタリングするには、username == user1 を選択します（user1は Cloud APIC にログインしているユーザーです）。

ステップ 3 サマリー ペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。

ステップ 4 詳細については、表示する特定の項目を表すサマリーテーブルの行をダブルクリックします。

新しいダイアログボックスがサマリー テーブルから選択する項目の追加情報を表示する **作業** ペインの上に表示されます。

インフラストラクチャの詳細の表示

ここでは、Cisco Cloud APIC GUI を使用してインフラストラクチャの詳細を表示する方法について説明します。インフラストラクチャの詳細には、システム設定、リージョン間接続、および外部接続に関する情報が含まれます。

ステップ 1 **[ナビゲーション（Navigation）]** メニューから **[インフラストラクチャ（Infrastructure）]** タブを選択します。

[インフラストラクチャ（Infrastructure）] タブが展開すると、サブタブ オプションのリストが表示されます。詳細については、「インフラストラクチャ オプション」の表を参照してください。

表 *35* : インフラストラクチャ サブタブ

サブタブ名	説明
システム設定	**[全般（General）]** システム構成情報、**[管理アクセス（Management Access）]** 情報、**[コントローラ（Controllers）]**、**[クラウド リソース名前付けルール（Cloud Resource Naming Rules）]**、**[イベント分析（Event Analytics）]** を表示します。
リージョン間接続	リージョン間接続ビューおよび各リージョンの追加ペインを含むマップを 1 つのペインに表示します。
サイト間接続	サイト間接続ビューおよび各サイトの追加ペインを含むマップを 1 つのペインに表示します。

ステップ 2 表示する詳細を含むコンポーネントを表すタブをクリックします。

管理の詳細の表示

ここでは、Cisco Cloud APIC GUI を使用して管理の詳細を表示する方法について説明します。管理の詳細には、認証、セキュリティ、ユーザ、およびスマート ライセンスに関する情報が含まれます。

ステップ 1 **[ナビゲーション（Navigation）]** メニューから **[管理（Administrative）]** タブを選択します。

[管理（Administrative）] タブが展開すると、サブタブ オプションのリストが表示されます。詳細については「*Administrative Options*」の表を参照してください。

表 *36* : 管理サブタブ

サブタブ名	説明
Authentication	**[認証デフォルト設定（Authentication Default Settings）]**、**[ログイン ドメイン（Login Domains）]**、**[プロバイダー（Providers）]**、および **[イベント分析（Event Analytics）]** サブタブが表示されます。 • **[認証デフォルト設定（Authentication Default Settings）]** タブ：設定情報が表示されます。 • **[ログイン ドメイン（Login Domains）]** タブ：ログイン ドメインをサマリー テーブルの行として表示します。 • **[プロバイダー（Providers）]** タブ：プロバイダーをサマリー テーブルの行として表示します。 • **[イベント分析（Event Analytics）]** タブ：**[障害（Faults）]**、**[イベント（Events）]**、および **[監査ログ（Audit Logs）]** サブタブを表示します。各サブタブには、対応する情報が行としてサマリー テーブルに表示されます。

サブタブ名	説明
セキュリティ	次のサブタブのリストが含まれます。 • **[セキュリティ デフォルト設定（Security Default Settings）]** タブ：デフォルトのセキュリティ設定情報を表示できます。 • **[セキュリティ ドメイン（Security Domains）]** タブ：サマリー テーブルにセキュリティ ドメイン情報を表示できます。 • **[ロール（Roles）]** タブ：ロール情報をサマリー テーブルに表示できます。 • **[RBAC ルール（RBAC Rules）]** タブ：サマリー テーブルにRBACルール情報を表示できます。 • **[証明書権限（Certificate Authorities）]** タブ：サマリー テーブルの認証局情報を表示できます。 • **[キー リング（Key Rings）]** タブ：キー リング情報をサマリー テーブルに表示できます。 • **[ユーザー アクティビティ（User Activity）]** タブ：ユーザー アクティビティを表示できます。
Users	次のサブタブを含みます。 • **[ローカル（Local）]** タブ：ローカル ユーザーをサマリー テーブルの行として表示します。 • **[リモート（Remote）]** タブ：リモートユーザーをサマリー テーブルの行として表示します。
スマート ライセンス	次のサブタブを含みます。 • **[一般（General）]** タブ：ライセンスをサマリー テーブルの行として表示します。 • **[CCR]** タブ：CCR をサマリー テーブルの行として表示します。 • **[障害（Faults）]** タブ：障害をサマリー テーブルの行として表示します。

ステップ 2 表示するコンポーネントを表すタブをクリックします。

一部のオプションでは、サマリーテーブルに項目がテーブル内の行として表示されます（たとえば、**[ユーザー（Users）]** タブを選択した場合、ユーザーのリストはサマリー テーブルに行として表示されます）。

サマリー ペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。詳細を表示するには、表示する特定の項目を表すサマリー テーブルの行をダブルクリックします。**作業**ウィンドウに新しいダイアログボックスが表示され、サマリー テーブルから選択した項目に関する追加情報が表示されます。

属性によるフィルタ処理バーをクリックすることにより、行をフィルタ処理できます。属性、演算子、およびフィルタ値を選択します。たとえば、ユーザーに基づいてフィルタリングする場合は、[User ID == admin] を選択します（admin はユーザー ID です。

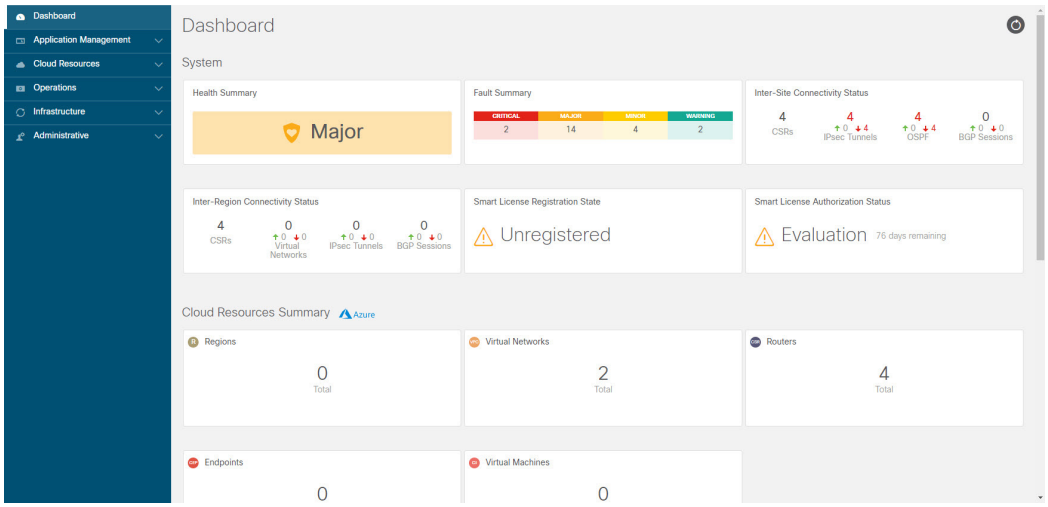
Cisco Cloud APIC GUI を使用したヘルスの詳細の表示

ここでは、Cisco Cloud APIC GUI を使用して正常性の詳細を表示する方法について説明します。Cisco Cloud APIC GUI の [クラウド リソース（Cloud Resources）] 領域で確認できるオブジェクトのヘルス詳細は、次のように表示できます。

- [Regions]
- アベイラビリティー ゾーン (AWS クラウド サイトの場合)
- VPC (AWS クラウド サイト用)
- VNET (Azure クラウド サイト用)
- ルータ
- セキュリティ グループ
- エンドポイント
- Instances
- クラウド サービス

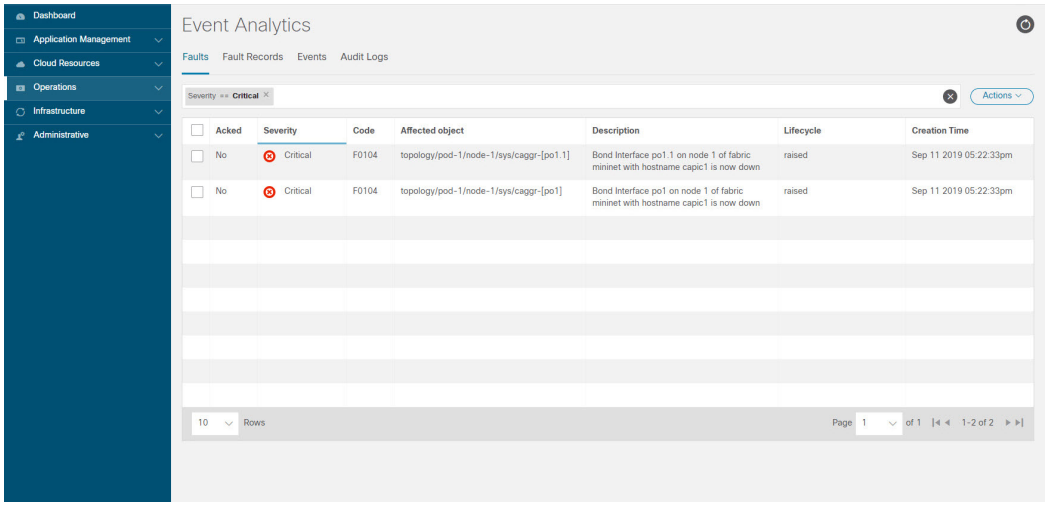
ステップ 1 **[ナビゲーション（Navigation）]** メニューから **[ダッシュボード（Dashboard）]** タブを選択します。

Cisco Cloud APIC システムの **[ダッシュボード（Dashboard）]** ウィンドウが表示されます。このウィンドウから、システムの全体的なヘルス ステータスを表示できます。



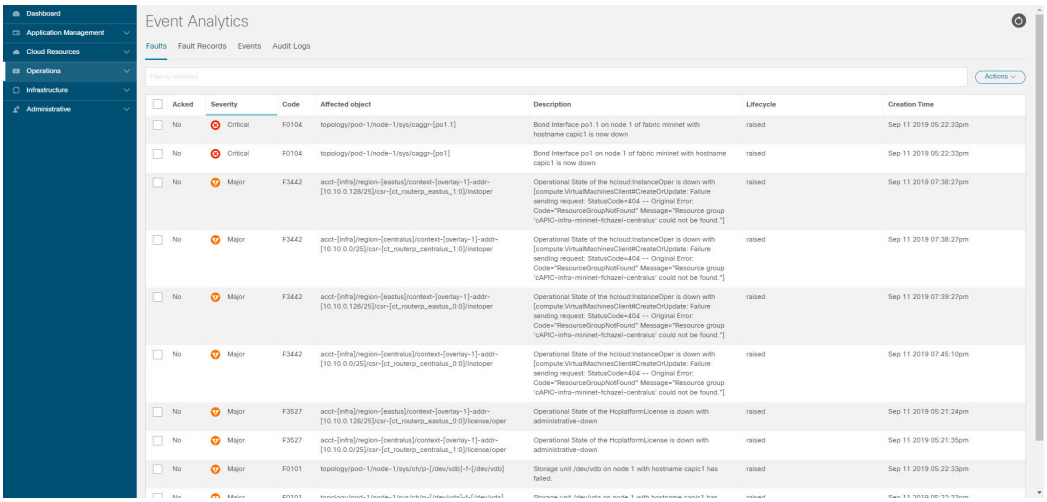
ステップ 2 **[ダッシュボード（Dashboard）]** ウィンドウの [障害サマリー] 領域内をクリックします。

[イベント分析（Event Analytics）] ウィンドウが表示され、クリックした特定の障害レベルの詳細情報が表示されます。次の画面は、重大度がクリティカルでリストされている障害の **[イベント分析（Event Analytics）]** ウィンドウの例を示しています。



ステップ 3 重大度レベルの横にある **[X]** をクリックして、すべての障害のイベント分析情報を表示します。

[イベント分析（Event Analytics）] ウィンドウに表示される情報が変更され、重大度がクリティカル、メジャー、および警告レベルのイベントが表示されます。

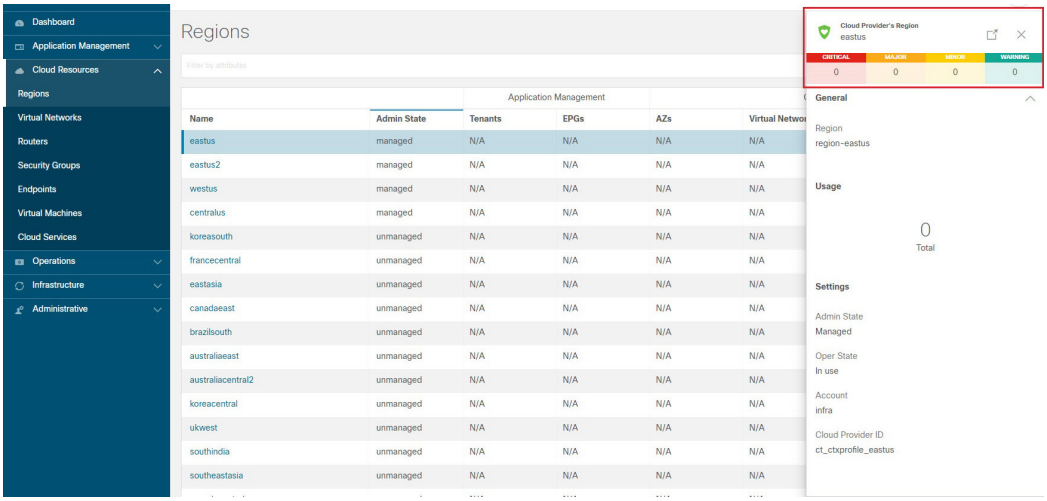


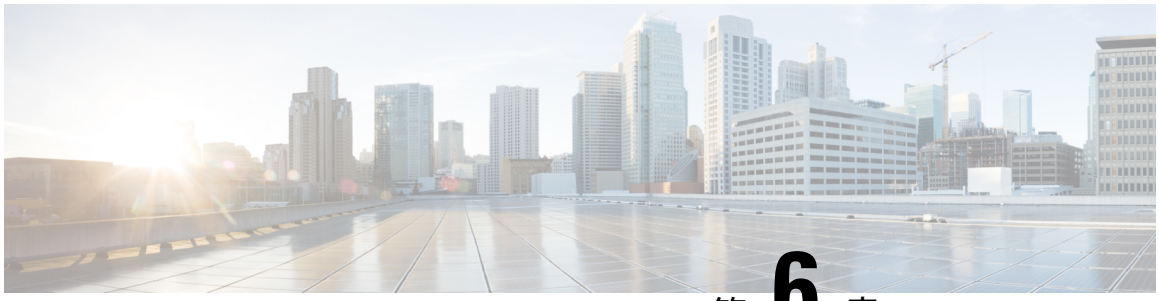
ステップ 4 **[ナビゲーション（Navigation）]** メニューから、**[クラウド リソース（Cloud Resources）]** タブを選択します。

[クラウドリソース（Cloud Resources）] タブが展開すると、サブオプション オプションのリストが表示されます。詳細については「*Administrative Options*」の表を参照してください。

ステップ 5 **[クラウド リソース（Cloud Resources）]** タブで任意の項目を選択すると、そのコンポーネントのヘルス情報が表示されます。

たとえば、次の図は、**[クラウド リソース（Cloud Resources）]** > **[リージョン（Regions）]**をクリックしたときに表示される可能性のあるヘルス情報を示しているので、特定のリージョンを選択します。





第 6 章

レイヤ 4 から レイヤ 7 サービスの展開

概要

Cisco Cloud APIC を使用すると、レイヤ 4 からレイヤ 7 のサービス デバイスをパブリック クラウドに展開できます。初期リリース (4.2(x)) では、Azure での Azure Application Gateway（アプリケーション ロード バランサ）の展開がサポートされています。リリース 5.0(2) 以降、Azure での Azure Load Balancer（ネットワーク ロード バランサ）およびサード パーティ ファイアウォールの展開がサポートされています。リリース 5.1(2) 以降、Azure でのサード パーティ ロード バランサの展開がサポートされています。

Azure での展開では、次の 4 種類のレイヤ 4 からレイヤ 7 サービスがサポートされています。

- ALB は、Azure アプリケーション ゲートウェイまたはアプリケーション ロード バランサを指します。
- NLB は Azure ロード バランサまたはネットワーク ロード バランサを指します。
- サードパーティ ファイアウォール
- サードパーティ ロード バランサ

サービス グラフについて

サービス グラフは、2 つ以上の EPG ペア間に挿入された一連のレイヤ 4 ～ レイヤ 7 サービス デバイスを表すために使用されます。EPG は、クラウド（Cloud EPG など）またはインターネット（cloudExtEPG）内で実行されているアプリケーション、または他のサイト（オンプレ

ミスまたはリモート クラウド サイトなど）から実行されているアプリケーションを表すことができます。レイヤ 4 からレイヤ 7 のサービス デバイスは、NLB、ALB、サード パーティのファイアウォールのクラスタ、またはサード パーティのロード バランサにすることができます。

サービス グラフと契約（およびフィルタ）は、2 つの EPG 間の通信を指定するために使用されます。Cisco Cloud Network Controller は、契約およびサービス グラフで指定されたポリシーに基づいて、セキュリティ ルール（ネットワーク セキュリティ グループ/NSG および ASG）と転送ルート（UDR）を自動的に導出します。

複数のサービス グラフを指定して、さまざまなトラフィック フローまたはトポロジを表すことができます。

サービス グラフでは、次の組み合わせが可能です。

- 同じデバイスを複数のサービス グラフで使用できます。
- 複数のコンシューマ EPG とプロバイダ EPG の間で同じサービス グラフを使用できます。

サービス グラフを使用することで、ユーザーはポリシーを一度指定するだけで、リージョン内またはリージョン間でサービス チェーンを展開できます。グラフを展開するたびに、Cisco ACI は新しい論理トポロジでの転送を行えるように、ネットワーク構成の変更を行います。

サードパーティのファイアウォールの場合、デバイス内の構成は Cisco Cloud Network Controller によって管理されません。

サービス グラフは、次の要素を使ってネットワークを表します。

- サービス グラフ ノード：ロードバランサなどのトラフィックに適用される機能を示すノード。サービス グラフ内の 1 つの機能は 1 つ以上のパラメータを必要とし、1 つまたは複数のコネクタを持っている場合があります。
- コネクタ：コネクタはノードからの入出力を有効にします。

グラフが設定されると、Cisco APIC はサービス グラフに明記されたサービス機能の要件に従って、サービスを自動的に設定します。Cisco APIC もまた、サービス グラフで指定されるサービス機能のニーズに応じてネットワークを自動的に設定します。これにより、サービス デバイスを変更する必要がなくなります。

クラウド ネイティブおよびサードパーティ サービスでのサービス グラフの使用

リリース 5.1(2) 以降、クラウド ネイティブおよびサードパーティのサービスでサービス グラフを使用できるようになりました。これらの状況では、リダイレクトの有無にかかわらずサービス グラフを使用できます。リダイレクトの有無にかかわらず使用例については クラウド ネイティブおよびサードパーティ サービスによるサービス グラフの使用例 （242 ページ） を参照してください。

このタイプのサービス グラフでは、同じくリリース 5.1(2) で導入されたクラウド サービス エンドポイント グループ（サービス EPG）を使用します。サービス EPG、およびサービス EPG で使用できる展開タイプとアクセス タイプの詳細については、クラウド サービス エンドポイント グループ （42 ページ） を参照してください。

この目的でサービス EPG で使用されるサービス グラフでは、次の展開タイプとアクセス タイプがサポートされています。

表 *37* : プロバイダ サービスの *EPG* タイプ

導入タイプ	アクセス タイプ
クラウドネイティブ	プライベート
クラウド ネイティブ管理対象	パブリックとプライベート
サードパーティ製の	プライベート

表 *38* : コンシューマ サービス *EPG* タイプ

導入タイプ	アクセス タイプ
クラウド ネイティブ管理対象	パブリックとプライベート

注意事項と制約事項

- サービス EPG を使用して、クラウド ネイティブおよびサードパーティ サービスでサービス グラフを使用するには、新しいサブネットごとの NSG 構成を有効にする必要があります。サブネットごとの NSG 構成の詳細については、セキュリティ グループ （50 ページ）を参照してください。
- クラウド EPG とサービス グラフの組み合わせに適用される制限は、サービス EPG とサービス グラフの組み合わせにも適用されます。たとえば、タグベースのコンシューマとプロバイダが同じリージョンの同じ VRF に存在できないというクラウド EPG/サービス グラフの制限は、サービス EPG とサービス グラフにも適用されます。
- リダイレクトを実行しない 2 つのノード グラフでは、SNAT と DNAT が有効になっています。DNATed アドレスはロードバランサと同等のデバイスであると想定されており、異なるサブネットにある可能性のある異なるターゲット間でトラフィックを分散させることができます。

  これらのターゲットが異なるサブネットにある場合、サービス グラフはそれらのターゲットのルート到達可能性ルールを提供しないことに注意してください。この場合、サービス EPG が到達可能性を処理すると想定されます。
- AKS とサービス グラフが関係する場合、サービス グラフは、AKS クラスタのロードバランサのサブネットへのルートの到達可能性のみを確立します。

アプリケーション ロード バランサの概要

アプリケーション ロード バランサ（Azure Application Gateway または ALB とも呼ばれます）は、HTTP リクエスト、URL フィルタリングなどの属性に基づいて Web トラフィックを分散

するレイヤ 7 ロード バランサです。 詳細については、『Microsoft マニュアル』を参照してください。

Cisco ACI では、2 つのアプリケーション ロード バランサを展開する方法があります。

- インターネット向け：アプリケーション ロード バランサを、コンシューマ外部 EPG とプロバイダ クラウド EPG の間のサービスとして挿入します。
- 内部向け：アプリケーションロードバランサを、コンシューマ クラウド EPG とプロバイダ クラウド EPG 間のサービスとして挿入します。

サービス グラフを使用してアプリケーション ロード バランサを使用できます。一般的な構成には次のものが含まれます。

- アプリケーション ロード バランサとしてのレイヤ 4 からレイヤ 7 サービス デバイスの作成
- サービス グラフのノードとして ALB を使用する
- サービス グラフが契約に関連付けられている場合、EPG 通信での 1 つ以上のリスナーの作成。

リスナーを使用すると、アプリケーション ロード バランサ がトラフィックを受け入れるポートとプロトコル（HTTP または HTTPS）を指定できます。HTTPS を指定する場合は、セキュリティ ポリシーと SSL 証明書も選択します。

（注） リスナーは複数の証明書をもつことができます。

すべてのリスナーで、少なくとも 1 つのルール (条件のないデフォルトのルール) を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。たとえば、指定されたホスト名またはパスへの要求が行われたときに、トラフィックを指定された URL にリダイレクトするルールを作成できます。

アプリケーション ロード バランサ（ALB）は、他のアプリケーションの展開に使用しない別のサブネットに配置する必要があります。Cloud APIC は、ALB の NSG を作成し、ALB に関連付けられたサブネットに接続します。Cloud APIC は Azure アプリケーション ゲートウェイの標準および Standard_v2 SKUs をサポートします。

ネットワーク ロード バランサについて

ネットワーク ロード バランサ（Azure ロード バランサまたは NLB）は、レイヤ 4 ポートに基づいてインバウンド フロー パケットを分散するレイヤ 4 デバイスです。詳細については、『Microsoft マニュアル』を参照してください。

ALB と同様に、NLB はサービス グラフを使用して展開できます。1 以上のリスナーを構成することで、これらのアクションを指定できます。

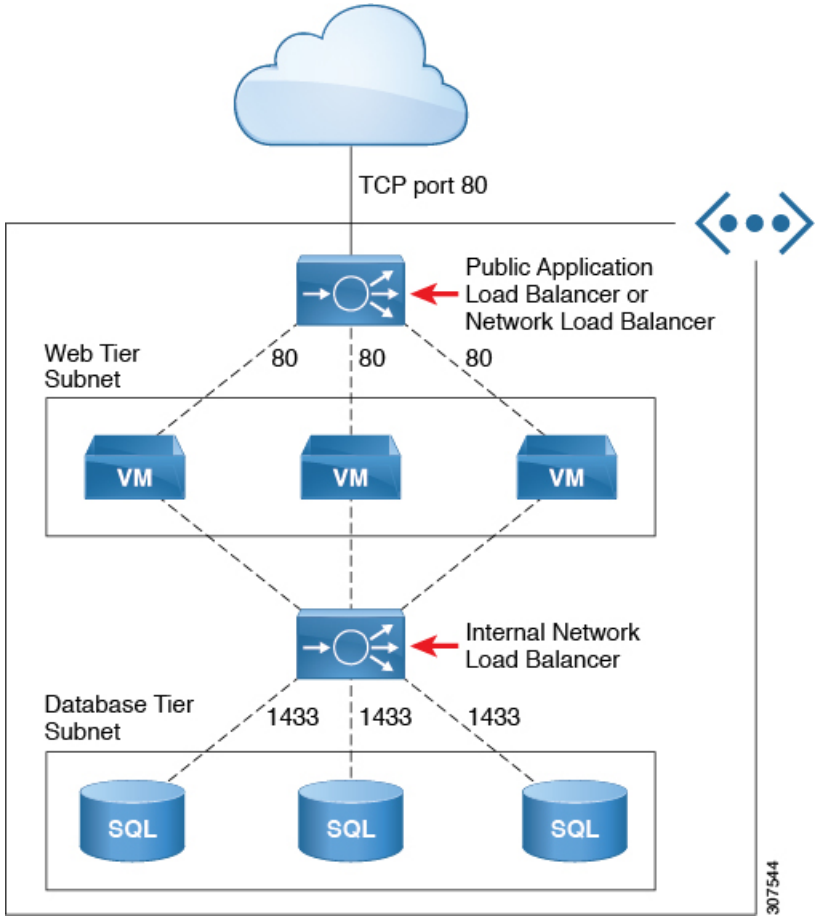
リスナーでは、ロードバランサがトラフィックを受け入れて転送するポートおよびプロトコル（TCP または UDP）を指定できます。すべてのリスナーで、少なくとも 1 つのルール (条件のないデフォルトのルール) を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。アプリケーション ゲートウェイとは異なり、ここではルールはバックエンドプールの特定のポートにのみトラフィックを転送できます。NLB は ALB と同様に別のサブネットにある必要があります。ネットワーク ロード バランサには、次の 2 つの動作モードがあります。

- 転送モード：トラフィックは、特定のリスナー ポートから指定されたバックエンド ポートに転送されます。
- HA ポート モード：ネットワーク ロード バランサは、すべてのポートで TCP フローと UDP フローを同時に負荷分散します。

Cloud APIC は、標準 SKU ネットワーク ロード バランサのみをサポートしています。

図 1 では、フロントエンド ロード バランサ（ALB/NLB）- VM またはファイアウォール - バックエンド ロード（ALB/NLB）バランサがサービスとして、コンシューマの外部 EPG とプロバイダのクラウド EPG の間に挿入されます。

図 *21* : インターネットおよび内部向け展開



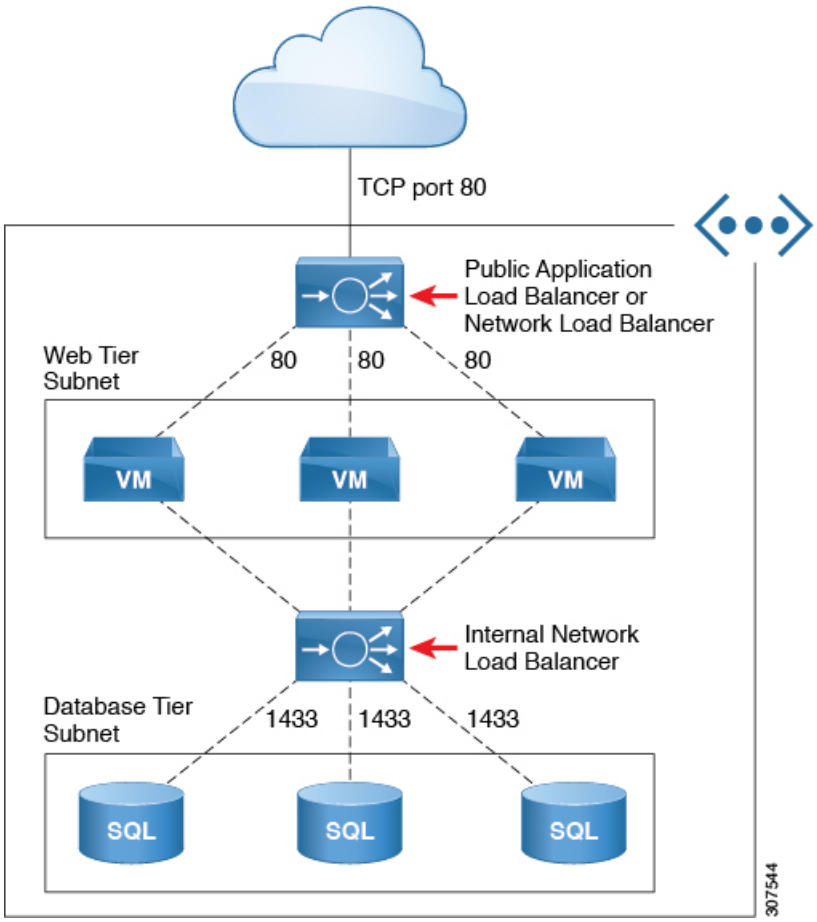
Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について

次のセクションでは、Cisco Cloud APIC リリース 25.0(3) 以降で使用できる Azure Network Load Balancer での複数のフロントエンド IP アドレスのサポートに関する情報を提供します。

Azure Network Load Balancer の複数のフロントエンド IP アドレスについて

インターネット向けのネットワーク ロード バランサを構成する場合、インターネット トラフィックのフロントエンドに割り当てることができるパブリック IP アドレスの数は、リリースによって異なります。

- Cisco Cloud APIC リリース 25.0(3) より前では、インターネット向けのネットワーク ロード バランサには、インターネット トラフィックのフロントエンドに割り当てられた単一のパブリック IP アドレスがあります。次の図は、マルチノード サービス グラフ構成の例を示しています。インターネット向けのネットワーク ロード バランサがグラフィックの上部に表示され、その後に VM またはファイアウォールが表示され、次に内部向けのネットワーク ロード バランサがこのマルチノード サービス グラフの一部として表示されます。

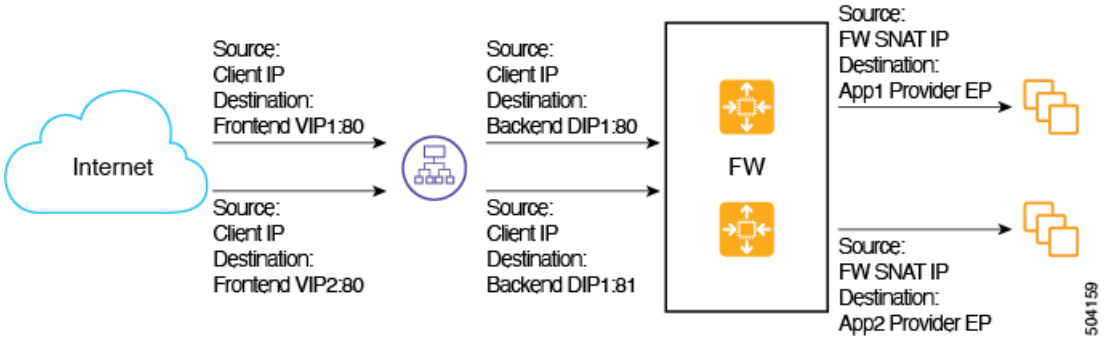


この例では、インターネット向けのネットワーク ロード バランサには、インターネット トラフィックのフロントエンドに割り当てられた単一のパブリック IP アドレスがあります。

ただし、この構成では、サービス グラフがあり、複数の HTTPS サービスを公開する必要がある場合に問題が発生する可能性があります。インターネット向けネットワーク ロード バランサのインターネット トラフィックのフロントエンドに割り当てられる単一のパブリック IP アドレスに制限があるということは、そのネットワーク ロード バランサにフロントエンド IP アドレスを追加できないことを意味します。さらに、Azure の制限により、複数のネットワーク ロード バランサが同じバックエンド デバイス（この例ではファイアウォール）を共有できないため、この状況ではネットワーク ロード バランサを追加できません。

- Cisco Cloud APIC リリース 25.0(3) 以降、インターネットに接続するネットワーク ロード バランサの複数のフロントエンド IP アドレスを構成するためのサポートが利用できるようになりました。この更新により、各フロントエンド IP アドレスは、特定のバックエンド プールに対する 1 つ以上のルールにアタッチされます。

  次の図は、インターネットに接続するネットワーク ロード バランサに対して複数のフロントエンド IP アドレスが構成されている構成例を示しています。



この構成例は、次のリスナー ルールのパケット フローを示しています。

	リスナー ルール（フロントエンド構成）	ルール アクション（バックエンド構成）
Rule1	• **IP**: VIP1 • **Port**: 80	**Port**: 80
Rule2	• **IP**: VIP2 • **Port**: 80	**Port**: 81

サービス グラフでは、サービス デバイスでのリスナー ルールとルール アクションの設定を構成できます。ネットワーク ロード バランサで定義されている場合、リスナー ルールとルール アクションの設定は、ロードバランサのフロントエンド構成からバックエンドプールへのマッピングを構築します。Cisco Cloud APIC リリース 25.0(3) より前は、インターネット向けのネットワーク ロード バランサは、単一のフロントエンド IP アドレスを使用してリスナーを構成する機能を提供していましたが、ポートとプロトコルの組み合わせは異なりました。Cisco Cloud APIC リリース 25.0(3) 以降では、インターネットに接続するネットワーク ロード バランサの複数のフロントエンド IP アドレス構成がサポートされ、その機能が拡張されて、各フロントエンドがフロントエンド IP アドレス、ポート、およびプロトコルのタプルの組み合わせとして示される複数のフロントエンドでリスナー ルールが構成可能です。

注意事項と制約事項

インターネット向けのネットワーク ロード バランサに複数のフロントエンド IP アドレスを構成するためのサポートに関するガイドラインと制限を次に示します。

- 複数のフロントエンド IP アドレスのサポートは、インターネット向けのネットワーク ロード バランサでのみ使用できます。
- 複数のリスナー ルールでのバックエンド ポートの再利用はサポートされていません。

サードパーティのロードバランサについて

サードパーティ ロード バランサは、非クラウド ネイティブのレイヤ 4 からレイヤ 7 のロード バランサです。Cloud APIC は、サードパーティのロード バランサの構成を管理しません。ただし、Cloud APIC は、サードパーティのロード バランサへの接続のためのネットワーク スティッチングを自動化します。

外部インターフェイス サブネットからサード パーティのロード バランサの VIP を構成できます。サード パーティのロード バランサ用の追加の VIP を、外部インターフェイスのセカンダリ IP アドレスとして構成することもできます。

Cloud APIC は、ソース NAT が有効になっている 2 アーム モード（外部インターフェースと内部インターフェース）で展開されたサードパーティのロードバランサをサポートしています。

サードパーティ ロード バランサの制限事項：

- Cloud APIC は、サードパーティのロード バランサでの Direct Server Return（DSR）構成をサポートしていません。
- サードパーティのロードバランサは、active/standby の高可用性構成ではサポートされていません。

  active/active モードのサードパーティ ロード バランサ VM の詳細については、ユースケースの例 （224 ページ） を参照してください。
- エイリアン VIP 範囲は、サードパーティのロードバランサではサポートされていません。

すべてのトラフィックを許可について

リリース 5.1(2g) 以降、**[すべてのトラフィックを許可（Allow All Traffic）]** オプションは、リダイレクト対応のサービス グラフでパススルー デバイスとして展開されたサード パーティ ファイアウォールおよび Azure network load balancers で使用できます。

（注） このオプションは、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。このオプションを有効にする前に、これがセキュリティ リスクとならないことを確認します。

次のセクションでは、**[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にする手順について説明します。

- サードパーティ ファイアウォール （217 ページ）
- Azure Network Load Balancer （219 ページ）

サードパーティ ファイアウォール

- 新しいサービス グラフ タイプを作成するときにこのオプションを有効にするには：

1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]**>**[デバイス（Devices）]**>**[デバイスの作成（Create Device）]**をクリックします。
2. **[サービス タイプ（Service Type）]** として **[サード パーティ ファイアウォール（Third party firewall）]** を選択します。
3. **[インターフェイスの追加（Add Interface）]** をクリックし、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域を見つけます。
4. **[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[許可（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。
5. 設定が終わったら [Save] をクリックします。

- 既存のサービス グラフ タイプを編集するときにこのオプションを有効にするには:

1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]** をクリックし、**[デバイス タイプ（Device Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** が表示されている既存のサービス デバイスをクリックします。

   このサービス デバイス タイプの詳細を示すパネルがウィンドウの右側からスライドします。
2. [詳細（Details）] アイコンをクリックします（  ）。

   このサービスデバイスタイプの詳細情報を提供する別のウィンドウが表示されます。
3. ウィンドウの **[インターフェイス（Interfaces）]** 領域を見つけ、**[インターフェイス セレクタ（Interface Selectors）]** 列で必要なインターフェイス セレクタをクリックします。

   このインターフェースの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。
4. [詳細（Details）] アイコンをクリックします（  ）。

   このインターフェイスの詳細情報を提供する別のウィンドウが表示されます。
5. 鉛筆アイコンをクリックして、このインターフェイスの構成設定を編集します。
6. **[すべてのトラフィックを許可（Allow All Traffic）]** 領域を見つけ、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[許可（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。
7. 設定が終わったら [Save] をクリックします。

Azure Network Load Balancer

- 新しいサービス グラフ タイプを作成するときにこのオプションを有効にするには:

1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]**>**[デバイス（Devices）]**>**[デバイスの作成（Create Device）]**をクリックします。
2. **[サービス タイプ（Service Type）]**として **[Network Load Balancer]** を選択します。
3. **[設定（Settings）]** 領域で、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[有効（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスを許可します。
4. 設定が終わったら [Save] をクリックします。

- 既存のサービス グラフ タイプを編集するときにこのオプションを有効にするには:

1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]** をクリックし、**[デバイス タイプ（Device Type）]** として **[Network Load Balancer]** が表示されている既存のサービス デバイスをクリックします。

   このサービス デバイス タイプの詳細を示すパネルがウィンドウの右側からスライドします。

2. [詳細（Details）] アイコンをクリックします（  ）。

   このサービスデバイス タイプの詳細情報を提供する別のウィンドウが表示されます。
3. 鉛筆アイコンをクリックして、このサービス デバイスの構成設定を編集します。
4. **[設定（Settings）]** 領域で、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域を見つけ、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[有効（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。
5. 設定が終わったら [Save] をクリックします。

サーバー プールへのダイナミック サーバーのアタッチ

プロバイダ EPG 内のサーバ、または ALB/NLB の背後にあるサードパーティ ファイアウォールなどのサービスデバイスは、ターゲット グループに動的に追加されます。Azure では、ターゲット グループはバックエンド プールとして参照されます。フロントエンドとバックエンドのプロトコルとポート番号、および負荷分散アクションを定義するリスナーとルール構成は、ユーザーによって提供されます。サービス グラフ構成の一部として最後のノードである ALB/NLB でリスナー ルールを構成する場合、特定のルールに対してプロバイダ EPG を選択できます。その EPG からのエンドポイントは、ロード バランサのターゲット グループに動的に追加され

ます。サードパーティ ファイアウォールなどの別のノードが ALB/NLB とプロバイダ EPG の間に存在する場合、ファイアウォール エンドポイントはロード バランサのターゲット グループに動的に追加されます。ターゲットのエンドポイントまたはFQDN を指定する必要はありません。

Azure リリース 25.0(2) の Cisco Cloud APIC より前は、VM スケール セットはロード バランサのバックエンド ターゲットとしてサポートされていませんでした。Azure リリース 25.0(2) の Cisco Cloud APIC は、バックエンド ターゲットとして VM スケール セットを追加します。

（注） ファイアウォールに VM スケール セットを使用する場合は、ファイアウォール インターフェイスにサブネット ベースの EP セレクタのみを使用します。Azure は、複数のインターフェイスを持つ VM スケール セットの NIC ごとのタグ付けをサポートしていません。

VNet 間サービスについて

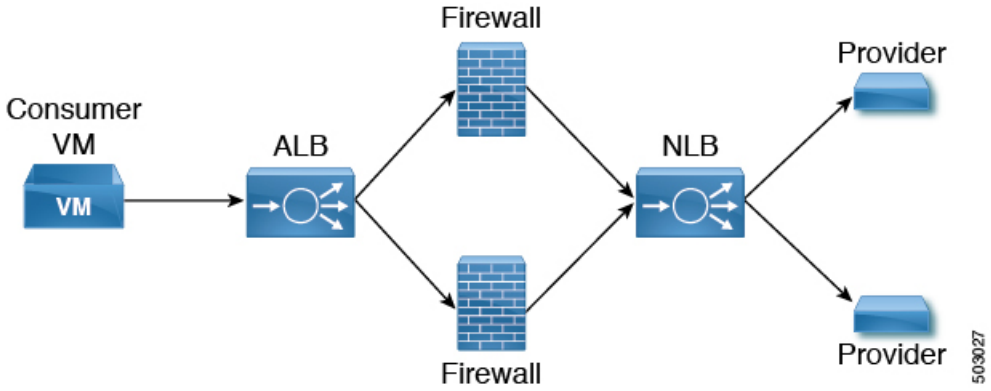
リリース 5.0(2) 以降、VNet 間サービスの展開と自動化がサポートされています。これは、クラウド内の East-West と North-South の両方のユース ケースに当てはまります。

このサポートについては、以下の点に注意してください。

- VNet ピアリングは、ハブスポーク トポロジ用に構成する必要があります。詳細については、「Azure 向け Cloud APIC の VNet ピアリングを構成する」を参照してください。
  - リダイレクトを使用したマルチノード サービスの場合: サービス デバイスがインフラ VNet に存在する必要があります。プロバイダの前にある ALB などのサービス デバイスは、プロバイダ VNet に存在できます。
  - リダイレクトのないマルチノード サービスの場合：サービス デバイスは、プロバイダ VNet 内にあるか、ハブ VNet とプロバイダ VNet にまたがって分散することができます。
- VNet 間トラフィックは、インフラ VNet のアプリケーション ロード バランサまたはネットワーク ロード バランサ、および非インフラ VNet のプロバイダでサポートされます。VNet は相互にピアリングする必要があり、ロード バランサとプロバイダは同じリージョンからのものである必要があります。

マルチノードについて

リリース 5.0(2) 以降、マルチノード サービス グラフがサポートされています。マルチノードにより、サービス グラフを使用した複数の展開シナリオが可能になります。



展開可能なサービス デバイスは、アプリケーション ロード バランサ、ネットワーク ロード バランサ、およびサードパーティ ファイアウォールです。

グラフには 2 種類のノードが許可されます。

- 非リダイレクト: トラフィックはサービス デバイスに向けられます（ロード バランサ、DNAT と SNAT を備えたサードパーティ ファイアウォール、ネットワーク ロード バランサ）。
- リダイレクト：サービス デバイスはパススルー デバイス（ネットワーク ロード バランサまたはファイアウォール）です。

レイヤ 4 ～レイヤ 7 サービス リダイレクト

リリース 5.0(2) 以降、レイヤ 4 からレイヤ 7 へのサービス リダイレクト機能は、Cisco Cloud APIC で使用できます。これは、Cisco APIC で使用可能なポリシーベースのリダイレクト（PBR）機能と同様です。レイヤ 4 からレイヤ 7 へのサービス リダイレクト機能は、Cisco Cloud APIC の **[リダイレクト（Redirect）]** オプションを使用して設定されます。

（注） このセクション全体で、「コンシューマからプロバイダへ」という用語は、ポイント A からポイント B に向かうトラフィックを表す包括的な用語として使用されることがあり、これらの 2 つのポイントの間にリダイレクト サービス デバイスが挿入される場合があります。ただし、これは、コンシューマからプロバイダへのトラフィックのみがリダイレクトでサポートされるという意味ではありません。トラフィックは、スポークツースポーク （227 ページ） で説明されているユース ケースのように、プロバイダからコンシューマへの場合もあります。

リダイレクトでは、ポリシーを使用して特定のサービス デバイス経由でトラフィックをリダイレクトします。サービス デバイスは、ネットワーク ロード バランサまたはサードパーティのファイアウォールとして展開できます。このトラフィックは、標準のコンシューマからプロバイダへの構成の一部として、必ずしもサービス デバイスを宛先とするものではありません。むしろ、通常どおりにコンシューマからプロバイダへのトラフィックを構成し、そのコンシュー

マからプロバイダへのトラフィックを特定のサービスデバイスにリダイレクトするようにサービス グラフを構成します。

Cisco Cloud APIC のリダイレクトのサポートは、VNet ピアリングで使用されるハブ アンド スポーク トポロジを利用して、VNet ピアリング機能と組み合わせてのみ利用できます。VNet ピアリング機能の詳細については、『Configuring VNet Peering for Cloud APIC for Azure』ドキュメントを参照してください。

パススルー ルール

リダイレクトを有効にすると、サービス デバイスにアタッチされている NSG（ネットワーク セキュリティ グループ）のルールが更新され、コンシューマからプロバイダへのトラフィックが許可されます。これらのルールは「パススルー ルール」と呼ばれます。一般に、パススルー ルールは、コンシューマ IP からプロバイダ IP へのトラフィックを許可することです。宛先 IP がアプリケーション ロード バランサ（ALB）VIP の場合、ルールはコンシューマ IP から ALB VIP へのトラフィックを許可することです。

リダイレクト プログラミング

リダイレクト プログラミングは、宛先 EPG の分類（タグベースまたはサブネットベース）によって異なります。

- サブネット ベースの EPG の場合、宛先 EPG のサブネットを使用してリダイレクトをプログラムします。
- タグベースの EPG の場合、宛先 VNet の CIDR を使用してリダイレクトをプログラムします。

この結果、リダイレクトは、EPG がリダイレクトのサービス グラフの一部でない場合でも、リダイレクトで同じ宛先に向かう他の EPG からのトラフィックに影響を与えます。リダイレクトの一部ではない EPG からのトラフィックも、サービス デバイスにリダイレクトされます。

次の表は、さまざまなシナリオでリダイレクトがどのようにプログラムされるかを示しています。

コンシューマ	プロバイダー	コンシューマ VNet でのリダイレクト	プロバイダ VNet でのリダイレクト
タグベース	タグベース	プロバイダのリダイレクトは、プロバイダの VNet の CIDR です。	コンシューマのリダイレクトは、コンシューマの VNet の CIDR です。
タグベース	サブネットベース	プロバイダのリダイレクトはプロバイダのサブネットです	コンシューマのリダイレクトは、コンシューマの VNet の CIDR です。

コンシューマ	プロバイダー	コンシューマ VNet でのリダイレクト	プロバイダ VNet でのリダイレクト
サブネットベース	タグベース	プロバイダのリダイレクトは、プロバイダの VNet の CIDR です。	コンシューマのリダイレクトは、コンシューマのサブネットです
サブネットベース	サブネットベース	プロバイダのリダイレクトはプロバイダのサブネットです	コンシューマのリダイレクトは、コンシューマのサブネットです

リダイレクト ポリシー

レイヤ 4 からレイヤ 7 へのサービス リダイレクト機能をサポートするために、サービス デバイス コネクタで新しいリダイレクト フラグを使用できるようになりました。次の表に、サービス デバイス コネクタの既存のフラグと新しいフラグに関する情報を示します。

接続タイプ	説明
redir	この値は、サービス ノードがその接続のリダイレクト ノードにあることを意味します。この値は、サードパーティのファイアウォールとネットワーク ロードバランサでのみ使用可能または有効です。
snat	この値は、サービス ノードがトラフィックに対してソース NAT を実行していることをサービス グラフに通知します。この値は、サードパーティ ファイアウォールのプロバイダ コネクタでのみ、ノードのプロバイダ コネクタでのみ使用可能または有効です。
snat_dnat	この値は、サービス ノードがトラフィックに対してソース NAT と宛先 NAT の両方を実行していることをサービス グラフに伝えます。この値は、サードパーティ ファイアウォールのプロバイダー コネクタでのみ、ノードのプロバイダー コネクタでのみ使用可能または有効です。
none	デフォルト値。

リダイレクトを構成するためのワークフロー

リダイレクトを構成するための一般的なワークフローは次のとおりです。

1. サービス グラフで使用する 1 つ以上のサービス デバイスを作成します。

- ネットワーク ロードバランサ（NLB）
- アプリケーション ロードバランサ（ALB）
- サードパーティ ファイアウォール

2. サービス グラフを作成し、この特定のサービス グラフに適切なサービス デバイスを選択します。

   手順のこの時点でリダイレクトを構成します。

   1. ネットワーク ロード バランサ、アプリケーション ロード バランサ、またはファイアウォール アイコンを **[デバイスのドロップ（Drop Device）]** 領域にドラッグ アンド ドロップして、サービス グラフ用にそのサービス デバイスを選択します。
   2. リダイレクト機能を有効にするには、表示される **[サービス ノード（Service Node）]** ウィンドウで、リダイレクト機能を有効にする場所に応じて、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** または **[プロバイダ コネクタ タイプ（Provider Connector Type）]** 領域の下にある **[リダイレクト（Redirect）]** オプションの横にあるボックスをオンにします。

（注） サービス グラフにアプリケーション ロードバランサがある場合でも、アプリケーション ロード バランサ サービス デバイスでリダイレクトを有効にすることはできません。

   3. **[サービス ノード（Service Node）]** ウィンドウで残りの構成を完了し、**[追加（Add）]** をクリックします。

3. コンシューマとプロバイダの EPG 間の契約を作成する EPG 通信を構成します。
4. サービス グラフを契約に添付します。
5. サービス デバイスのパラメータを構成します。

ユースケースの例

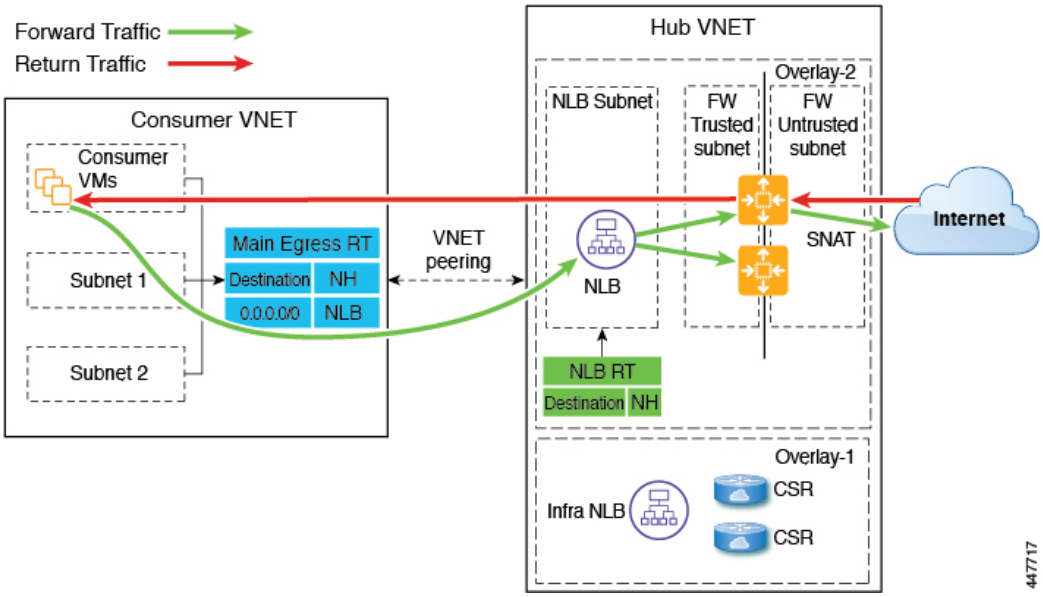
次に、いくつかのユース ケースの例を示します。

- 2 つの個別の VNet でのコンシューマおよびプロバイダ EPG を使用した VNet のハブ （240 ページ）

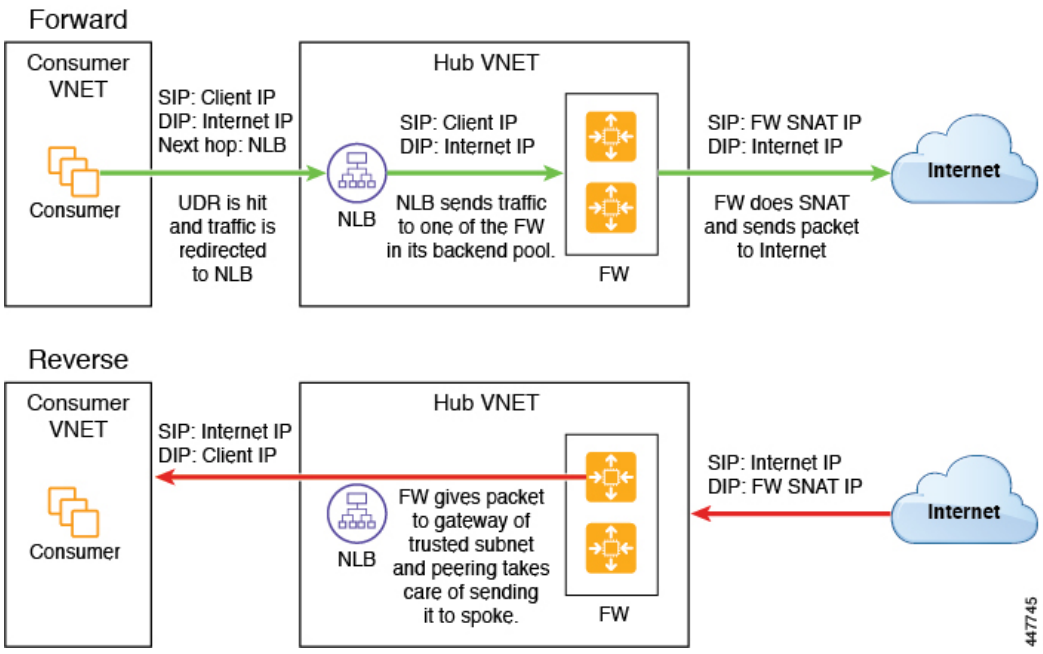
スポークツーインターネット

このユース ケースでは、コンシューマ VNet（コンシューマ VM を含む）とハブ VNet は、VNet ピアリングを使用してピアリングされます。ネットワーク ロードバランサも展開され、スケーリングのために 2 つのファイアウォールに面しています。このユース ケースでは、パッチの更新など、特定の理由でコンシューマ VM がインターネットにアクセスする必要があります。この場合、コンシューマ VNet では、インターネットへのリダイレクトを含むようにルート テーブルが変更され、トラフィックはハブ VNet のファイアウォールの前にある NLB にリダイレクトされます。インターネットに向かうサービス グラフの一部であるこのコンシューマからのトラフィックは、すべてネクスト ホップとして NLB に行きます。VNet ピアリングでは、トラフィックは最初に NLB に送られ、次に NLB がトラフィックをバックエンドのファイアウォールの 1 つに転送します。ファイアウォールは、トラフィックをインターネットに送信するときに、ソース ネットワーク アドレス変換（SNAT）も実行します。

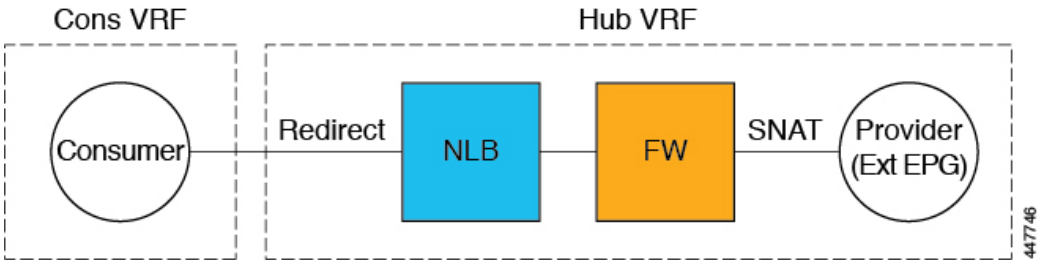
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

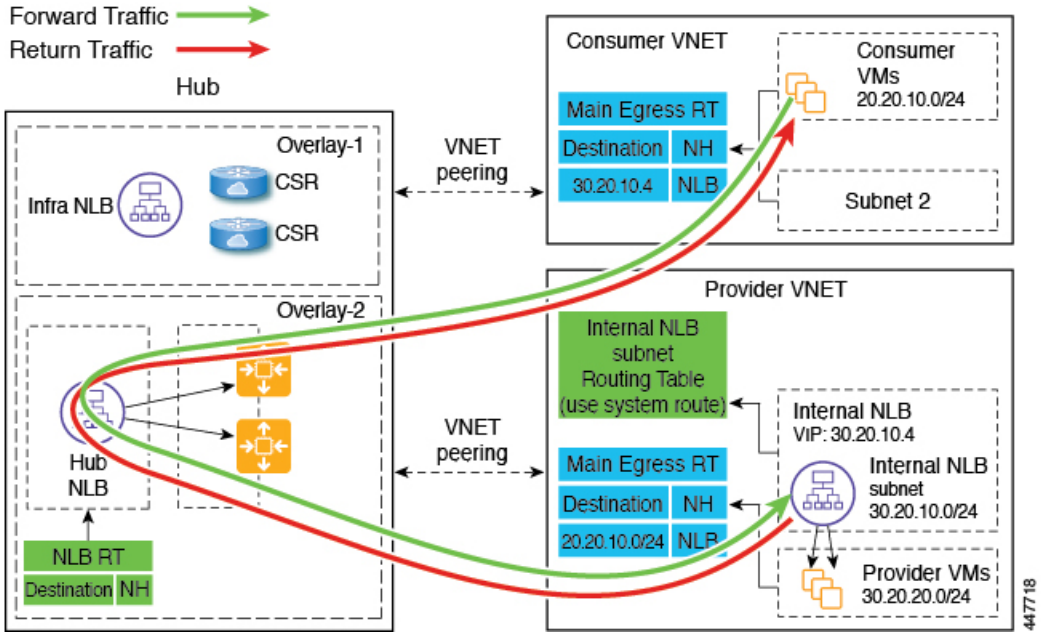
- **[デバイスの作成（Create Device）]** ウィンドウで
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ネットワーク ロードバランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

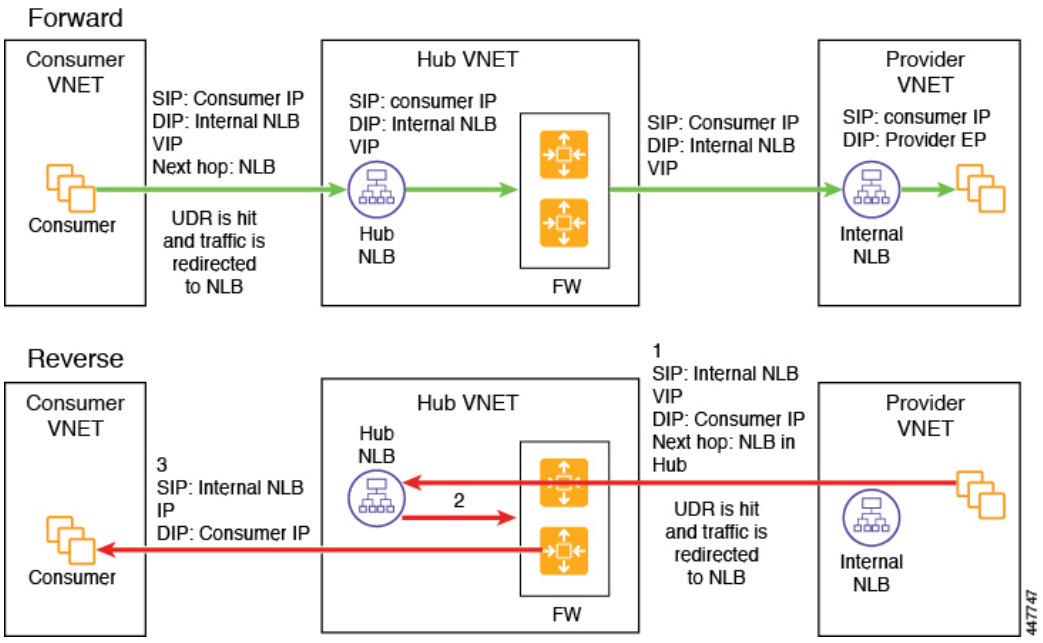
スポークツースポーク

このユース ケースでは、トラフィックはスポークからスポークへ、ハブ NLB が前面にあるハブ ファイアウォールを通過します。コンシューマ エンドポイントはコンシューマ VNet 内にあり、プロバイダ VNet には内部 NLB（またはサード パーティ ロード バランサ）が前面にある VM があります。コンシューマとプロバイダの VNet で出力ルート テーブルが変更され、トラフィックが NLB の前にあるファイアウォール デバイスにリダイレクトされるようになります。このユース ケースでは、リダイレクトが双方向に適用されます。

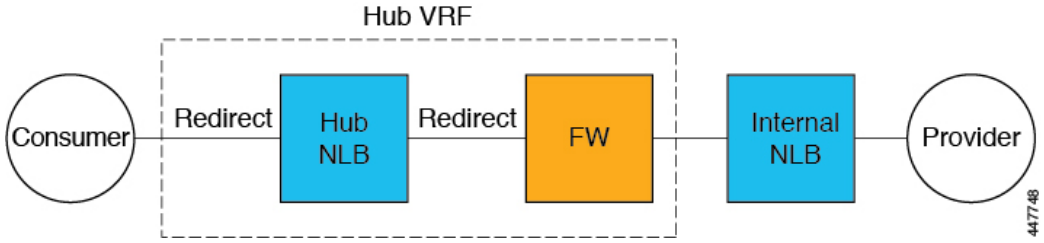
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[デバイスの作成（Create Device）]** ウィンドウで、次にプロバイダー VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、プロバイダー テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドで **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダー VRF のサブネットを選択します。

（注） 内部 NLB の代わりにサードパーティ ロード バランサを使用できます。**[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択します。**[インターフェイスの追加（Add Interface）]** をクリックして、**[VRF]** を選択し、インターフェイスの詳細を設定します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。

- ネットワーク ロードバランサ（ハブ VNet 用）
- サードパーティ ファイアウォール（ハブ VNet 用）
- ネットワーク ロード バランサまたはサードパーティ ロード バランサ（プロバイダ VNet の場合）

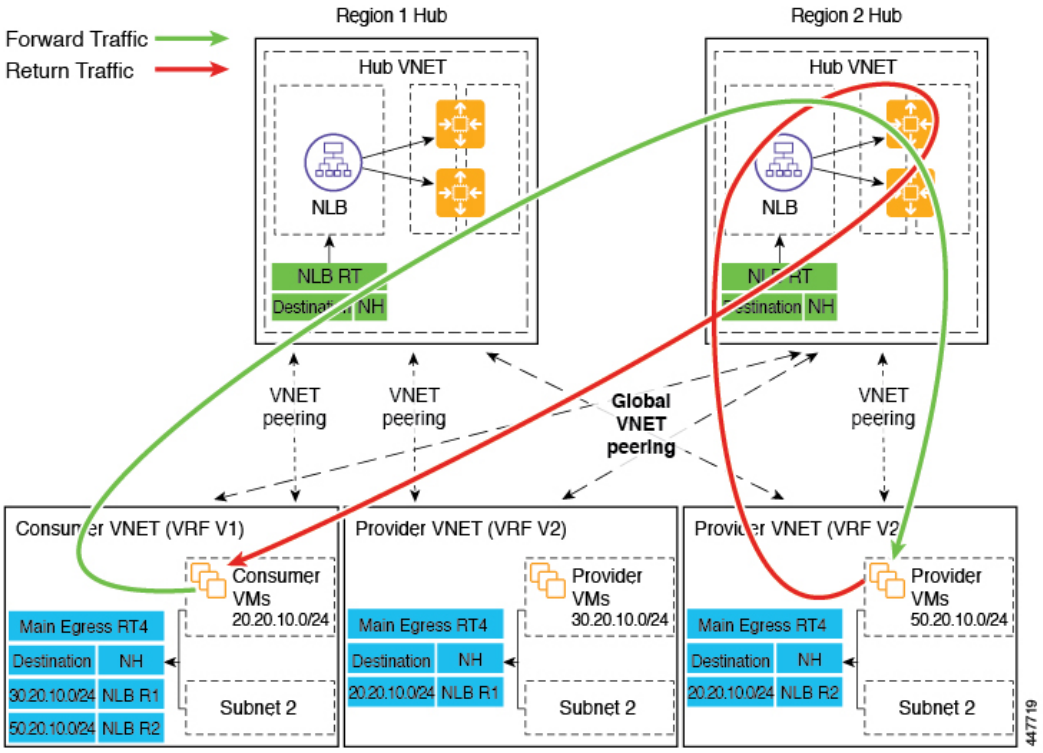
- ハブ VNet のネットワーク ロードバランサの **[サービス ノード（Service Node）]** ウィンドウで、次のようにします。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの横にあるボックスにチェックを入れ、プロバイダー側でリダイレクト機能を有効にします。
- サード パーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）** と **[プロバイダー コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。
- プロバイダー VNet でネットワーク ロードバランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダー コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。

（注） SNATがサードパーティのロードバランサで構成されていることを確認します。

リージョン間スポーク ツー スポーク

このユース ケースでは、両方のリージョンにサービス デバイスが必要です。コンシューマ VNet はリージョン 1 にあり、プロバイダは両方のリージョン（リージョン 1 と 2）にまたがっており、一部のエンドポイントはリージョン 1 にあり、一部のエンドポイントはリージョン 2 にあります。ローカル プロバイダ エンドポイントとリモート リージョン エンドポイントには、異なるリダイレクトがプログラムされています。この場合、使用されるファイアウォールは、プロバイダ エンドポイント側に最も近いファイアウォールになります。

このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



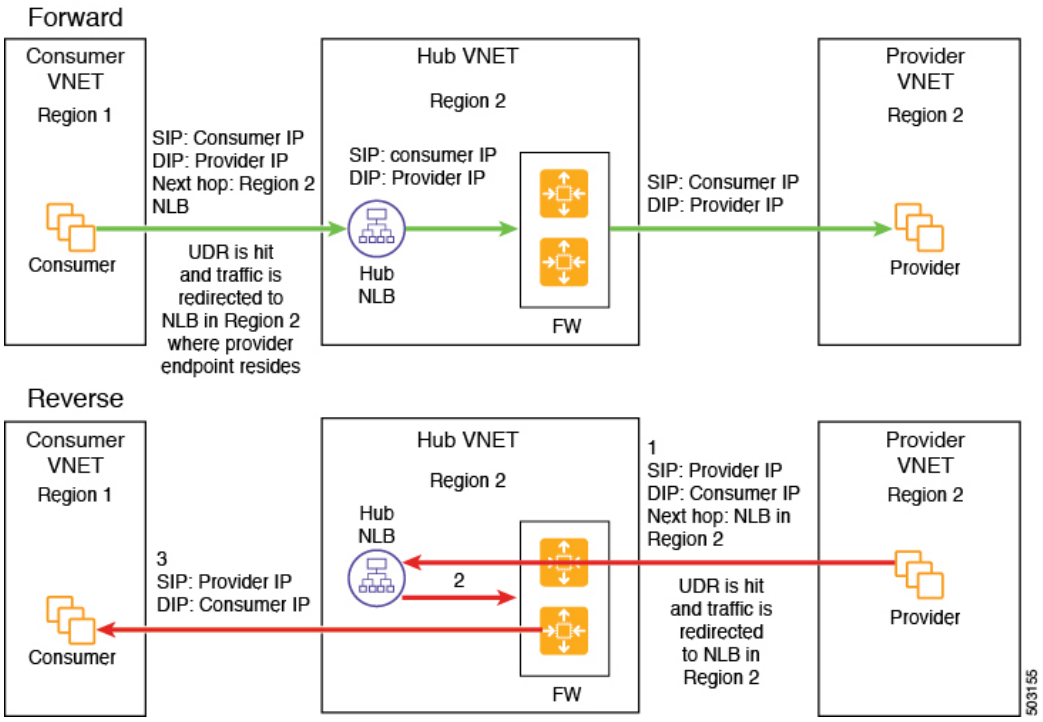
たとえば、コンシューマ VNet（VRF 1）の出力ルート テーブル（RT）の 2 つのサブネットについて考えてみます。

- 30.20.10.0/24（リージョン 1 [R1] の NLB）
- 50.20.10.0/24 （リージョン 2 [R2] の NLB）

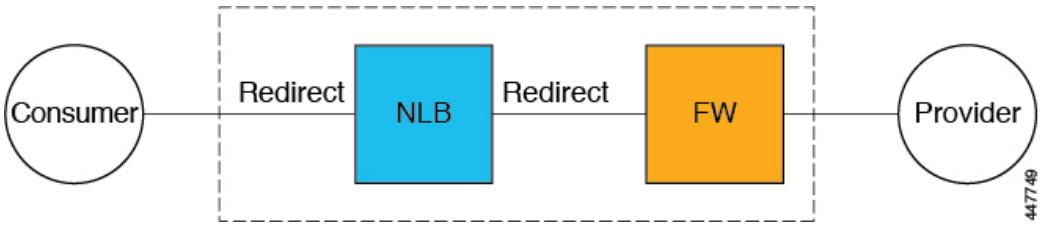
コンシューマが、ローカルにあるプロバイダ VM 30.20.10.0/24 にトラフィックを送信するとします。その場合、トラフィックはリージョン 1 のハブ NLB とファイアウォールにリダイレクトされ、プロバイダに移動します。

ここで、コンシューマがプロバイダー VM 50.20.10.0/24 にトラフィックを送信するとします。この場合、ファイアウォールはプロバイダ エンドポイントに対してローカルであるため、トラフィックはリージョン 2 のハブ NLB とファイアウォールにリダイレクトされます。

次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ハブ NLB の **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの横にあるボックスにチェックを入れ、プロバイダー側でリダイレクト機能を有効にします。
- サード パーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）** と **[プロバイダー コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

上記のユース ケースでは、プロバイダ VM は、クラウド ネイティブまたはサードパーティ ロード バランサによってフロントエンドにすることもできます。

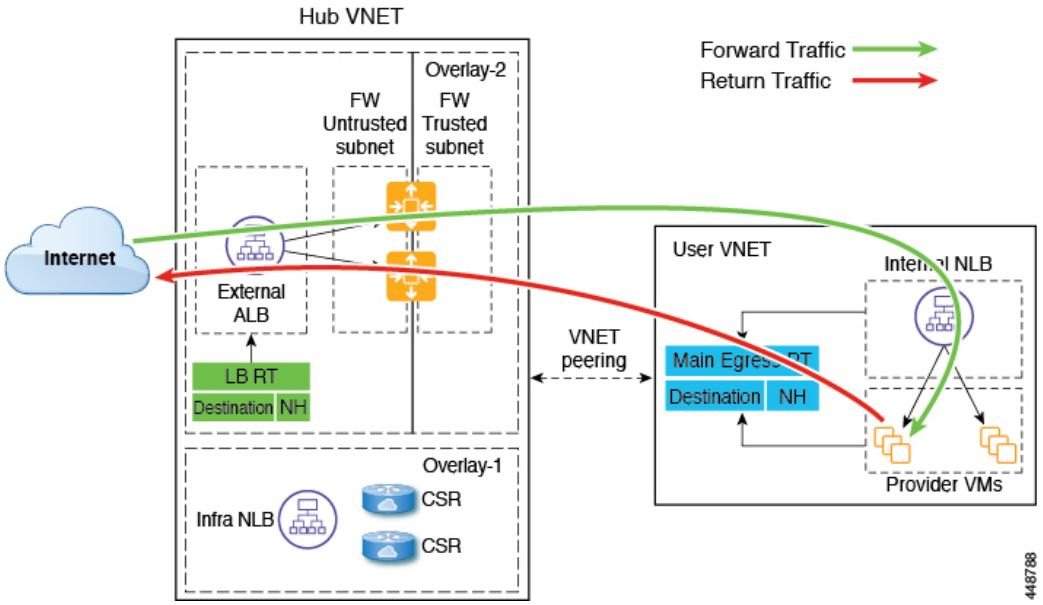
インターネット ツー スポーク（VRF 間）

このユース ケースでは、インターネットからのトラフィックは、プロバイダのエンドポイントに到達する前にファイアウォールを通過する必要があります。このユース ケースではリダイレクトは使用されません。

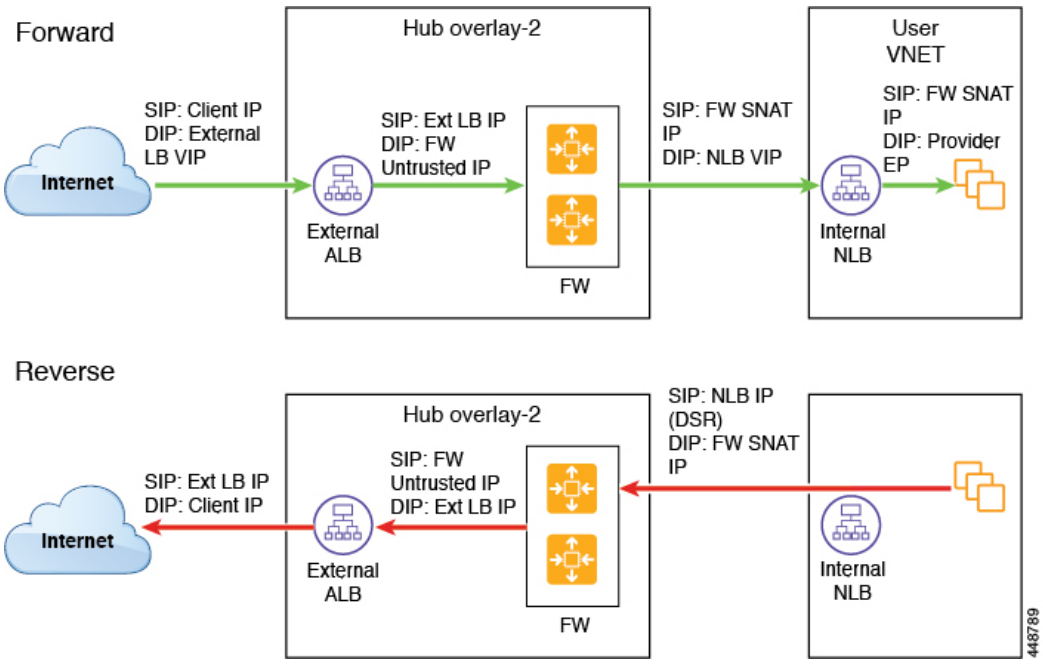
（注） このセクションでは、一般的な用語「外部ロード バランサー」が使用されています。これは、このユース ケースで外部ロード バランサが NLB、ALB、またはサード パーティ ロード バランサのいずれかになる可能性があるためです。次の例は、ALB を使用した構成を示していますが、外部ロード バランサは代わりに NLB またはサードパーティ ロード バランサである可能性があることに注意してください。

外部ロード バランサは、VIP を介してサービスを公開します。インターネット トラフィックはその VIP に送信され、外部ロード バランサはトラフィックをバックエンド プール内のファイアウォールに送信します（外部ロード バランサにはファイアウォールの信頼できないインターフェイスがバックエンド プールとしてあります）。ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP に送られます。次に、内部 NLB はプロバイダ エンドポイントの 1 つにトラフィックを送信します。

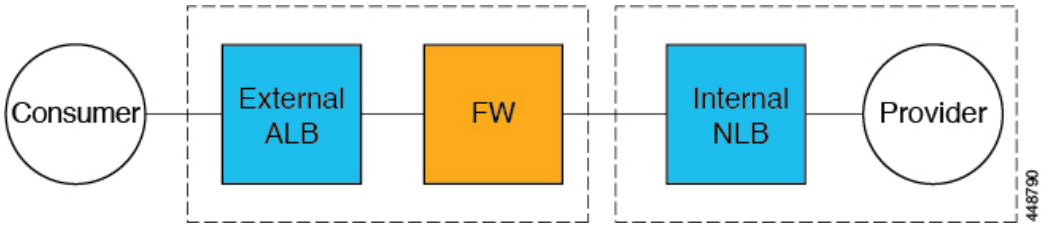
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[アプリケーション ロードバランサ（Application Load Balancer）]** または **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加（Add Interface）]** をクリックしてインターフェイスの詳細を設定します。
- **[デバイスの作成（Create Device）]** ウィンドウで、次にプロバイダー VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、プロバイダー テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドで **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダー VRF のサブネットを選択します。
- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサまたはアプリケーション ロード バランサ（ハブ VNet 用）
  - サードパーティ ファイアウォール（ハブ VNet 用）
  - ネットワーク ロード バランサまたはサードパーティ ロード バランサ（プロバイダ VNet の場合）
- ハブ VNet のネットワーク ロード バランサまたはアプリケーション ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユース ケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、**[プロバイダ コネクタ タイプ（Third-Party Firewall）]** フィールドで、**[SNAT]** および **[DNAT]** オプションの隣のボックスにチェックを入れます。
- プロバイダ VNet でネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。

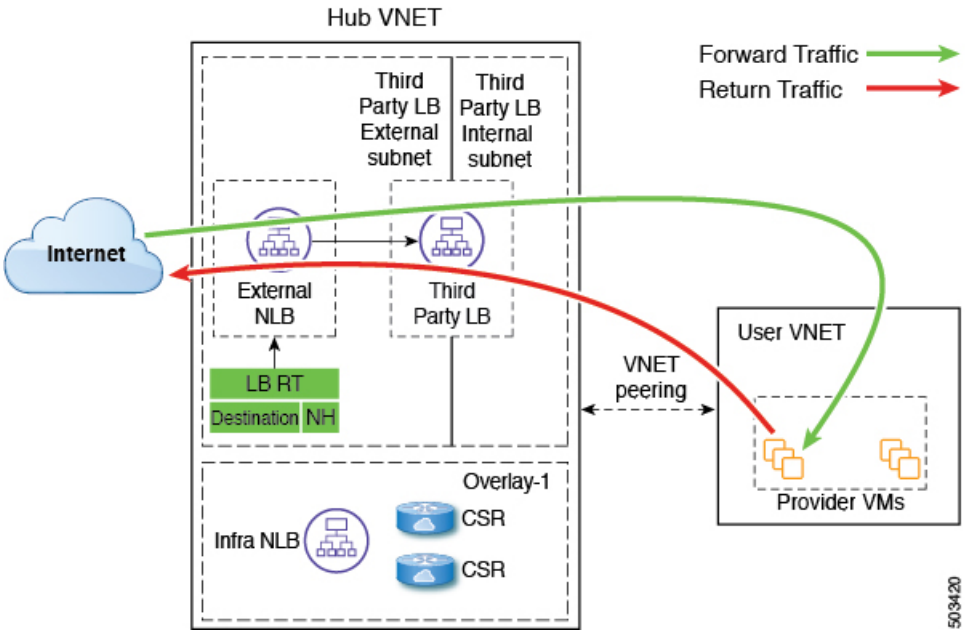
（注） SNAT がサードパーティのロードバランサで構成されていることを確認します。

サードパーティ ロード バランサの高可用性サポート

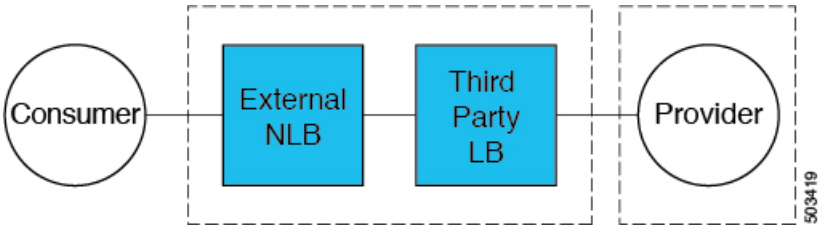
このユースケースでは、インターネットからのトラフィックは、プロバイダのエンドポイントに到達する前にサードパーティ ロード バランサを通過する必要があります。このユース ケースではリダイレクトは使用されません。

サードパーティ ロードバランサは、NLB のバックエンド プールとして構成されます。デバイスのセカンダリ IP アドレスは、NLB のターゲットとして機能します。NLB のターゲットとして、プライマリまたはセカンダリ IP アドレス（またはその両方）を追加することを選択できます。サードパーティ ロードバランサ VM は、アクティブ/アクティブ モードでのみ展開されます。サードパーティ ロード バランサは、アクティブ/スタンバイの高可用性構成では使用できません。

サードパーティ ロードバランサとネットワーク ロードバランサに専用のサブネットがあることを確認します。



次の図は、このユース ケースのサービス グラフを示しています。



このユース ケースの構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加（Add Interface）]** をクリックしてインターフェイスの詳細を設定します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ロード バランサ

（注） ネットワーク ロード バランサとサードパーティのロード バランサが同じ VNet にあることを確認します。

- ハブ VNet のネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

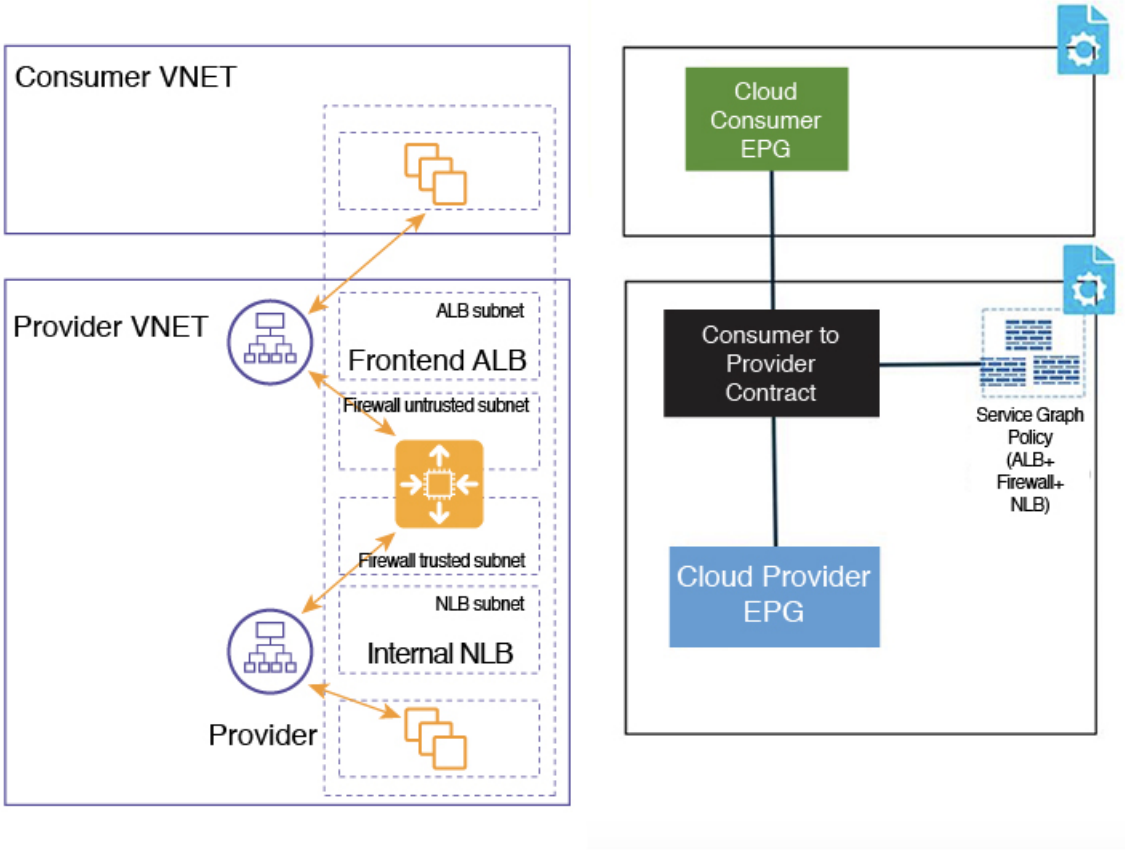
（注） SNAT がサードパーティのロードバランサで構成されていることを確認します。

2 つの個別の VNet 内のコンシューマとプロバイダの EPG

このユース ケースは、2 つの VNet を使用した構成例であり、コンシューマ EPG とプロバイダ EPG が別々の VNet にあります。

- フロントエンド ALB、ファイアウォール、および内部 NLB は、コンシューマとプロバイダの EPG の間に挿入されます。
- コンシューマ エンドポイントは、フロントエンドの ALB VIP にトラフィックを送信し、ファイアウォールに転送します。
- ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP にフローが流れます。
- 内部 NLB は、バックエンド プロバイダのエンドポイントへのトラフィックを負荷分散します。

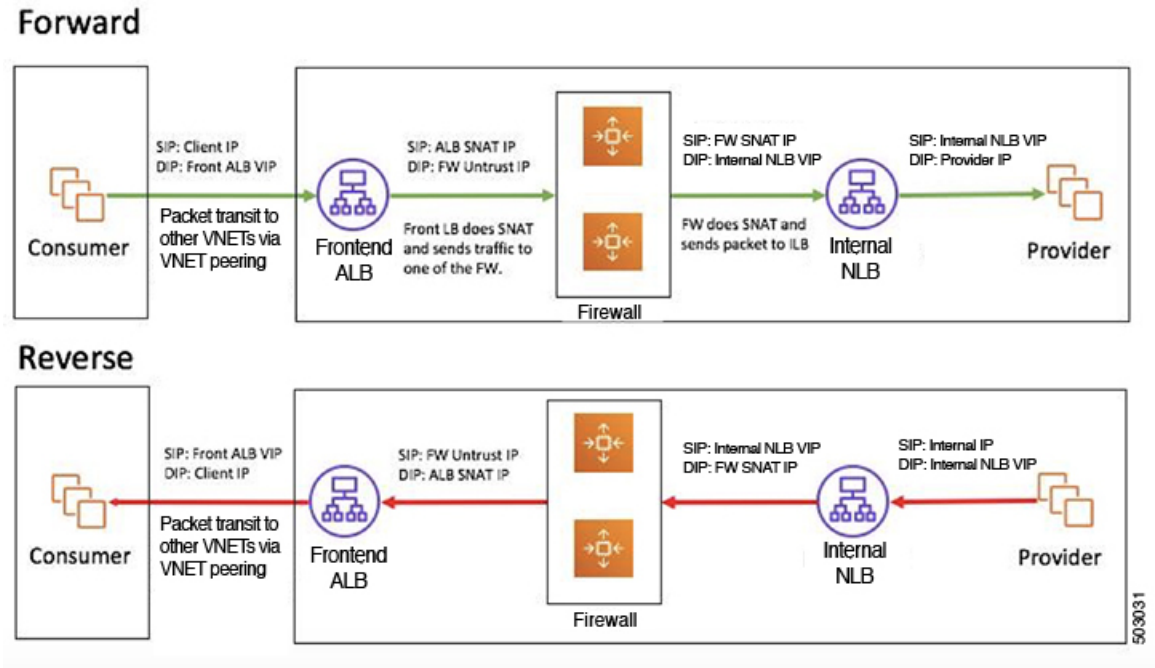
このユース ケースでは、フロントエンド ALB または内部 NLB の代わりにサードパーティのロード バランサを使用できます。このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



この図では次のようになっています。

- コンシューマ EPG はコンシューマ VNet にあります。
- プロバイダ EPG とすべてのサービス デバイスはプロバイダ VNet にあります。
- アプリケーション ロード バランサ、ネットワーク ロード バランサ（またはサードパーティのロード バランサ）、およびファイアウォールは、VNet 内に独自のサブネットを持つ必要があります。

両方向のパケット フローを次の図に示します。

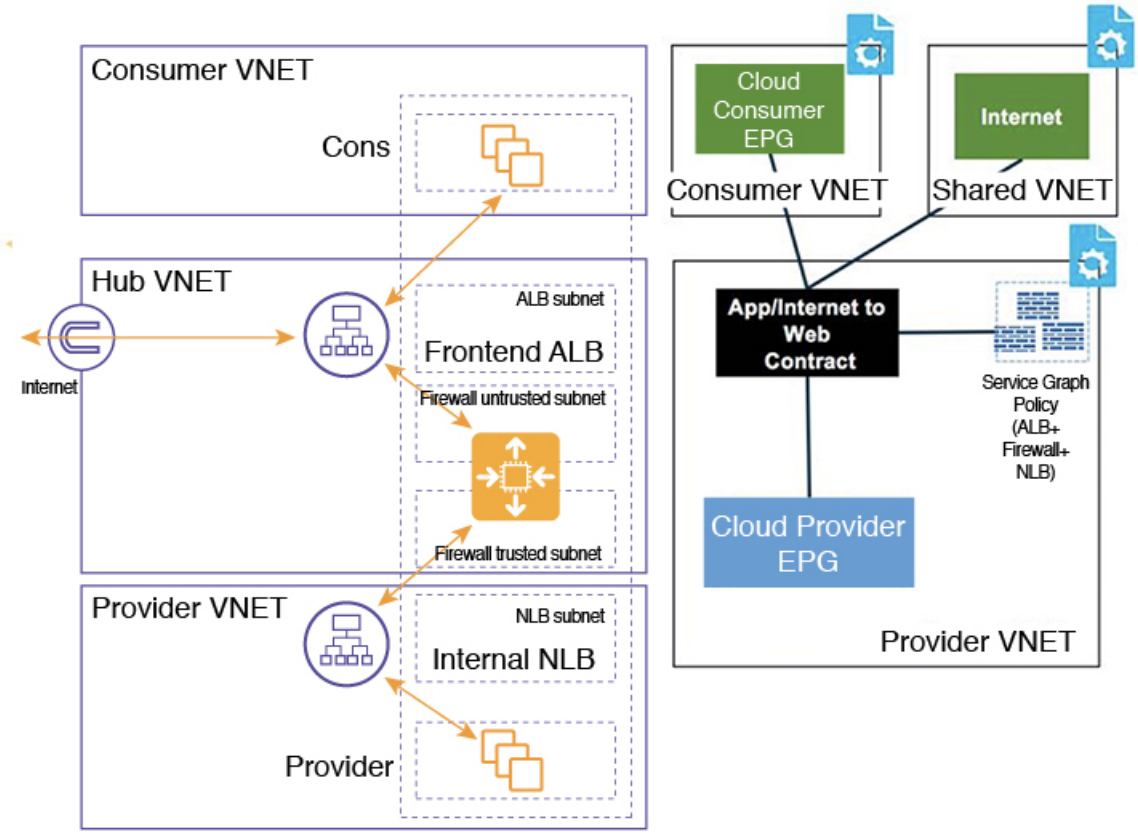


2 つの個別の VNet でのコンシューマおよびプロバイダ EPG を使用した VNet のハブ

このユース ケースは、ハブ VNet、2 つの個別の VNet 内のコンシューマ EPG とプロバイダ EPG の 3 つの VNet を使用した構成例です。

- フロントエンド ALB とファイアウォールは、コンシューマとプロバイダの EPG の間にあるハブ VNet 内に挿入されます。
- 内部 NLB はプロバイダ EPG に挿入されます。
- コンシューマ エンドポイントは、フロントエンドの ALB VIP にトラフィックを送信し、ファイアウォールに転送します。
- ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP にフローが流れます。
- 内部 NLB は、バックエンド プロバイダのエンドポイントへのトラフィックを負荷分散します。

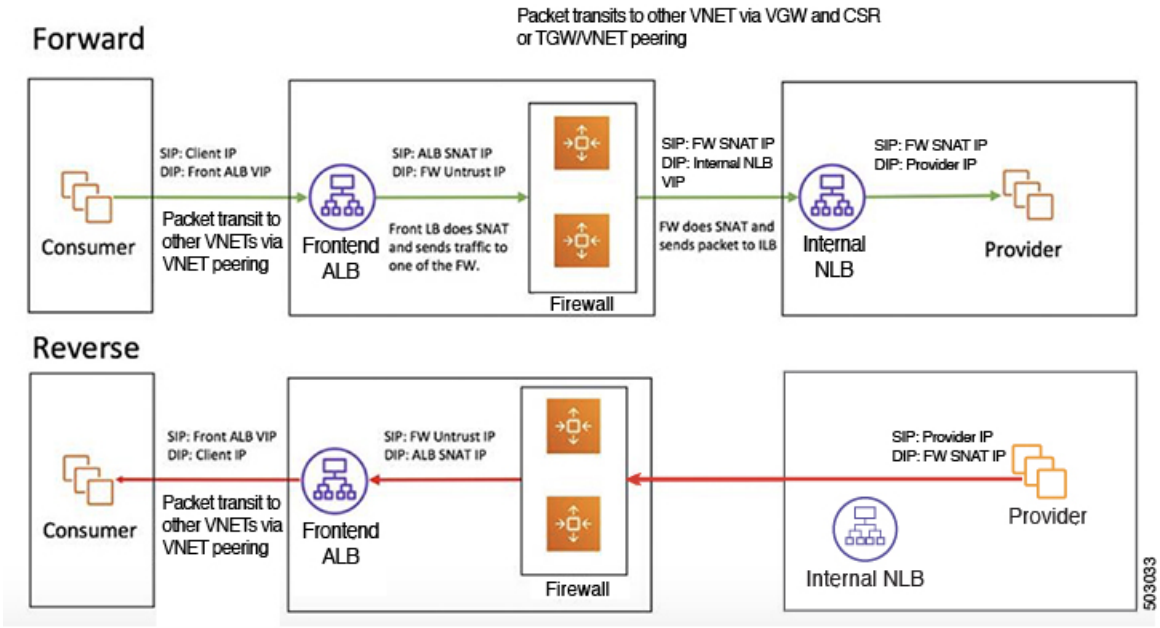
このユース ケースでは、フロントエンド ALB または内部 NLB の代わりにサードパーティのロード バランサを使用できます。このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



この図では次のようになっています。

- コンシューマ EPG はコンシューマ VNet にあります。
- プロバイダ EPG と内部 NLB はプロバイダ VNet にあります。
- フロントエンド ALB とファイアウォールはハブ VNet にあります
- アプリケーション ロード バランサ、ネットワーク ロード バランサ（またはサードパーティのロード バランサ）、およびファイアウォールは、VNet 内に独自のサブネットを持つ必要があります。

両方向のパケット フローを次の図に示します。



クラウドネイティブおよびサードパーティ サービスによるサービス グラフの使用例

以下は、リダイレクトの有無にかかわらず、クラウド ネイティブおよびサードパーティ サービスを使用したサービス グラフの使用例です。詳細、ガイドラインおよび制限事項については、クラウドネイティブおよびサードパーティ サービスでのサービス グラフの使用 （210 ページ） を参照してください。

リダイレクトのないユースケースの例

以下は、リダイレクトのないクラウドネイティブおよびサードパーティのサービスを使用したサービス グラフのユース ケースの例です。

これらの各ユースケースのプロセスの一部として、クラウド サービス EPG を構成します。クラウドサービス EPG を構成している場合は、**サブネットごとの NSG** 構成を有効にする必要があります。詳細については、セキュリティ グループ （50 ページ）およびクラウド サービス エンドポイント グループ （42 ページ）を参照してください。

- インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしての非管理サービス EPG （243 ページ）
- インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ サービス EPG （245 ページ）

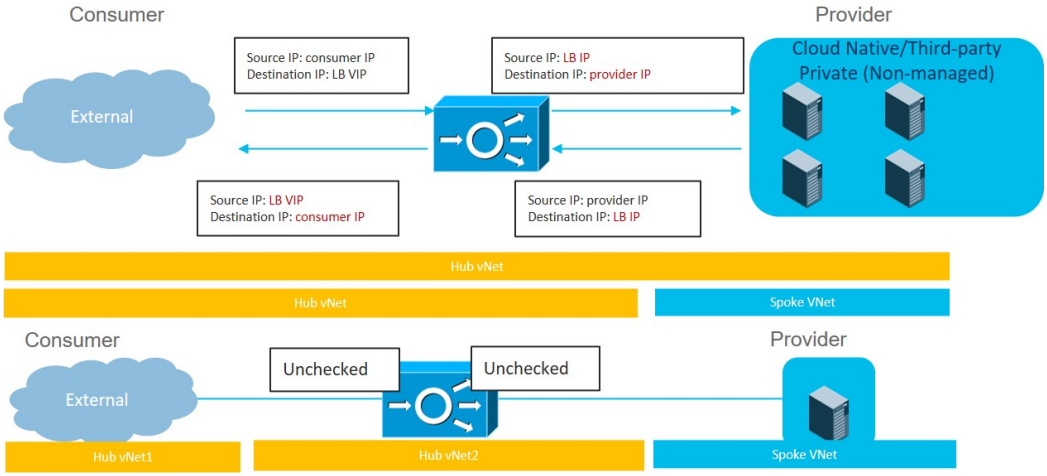
- インターネット インバウンド トラフィックの 2 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG （246 ページ）
- インターネット インバウンド トラフィックの 3 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG （248 ページ）

（注） 次の各ユース ケースでは、プロバイダとしてサービス EPG を使用する、単一ノード、2 ノード、および 3 ノードのサービス グラフを使用する同様のトポロジを、クラウドの東西トラフィックに対してサポートできます。これらのユース ケースでは、コンシューマはクラウド EPG になり、使用されるロード バランサーは内部ロード バランサになります。

インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしての非管理サービス EPG

このユース ケースには、サービス ノードがロードバランサ（アプリケーション ロードバランサ、ネットワーク ロードバランサ、またはサードパーティのロードバランサ）である単一ノード サービス グラフがあります。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。サービス エンドポイントは動的に学習され、アプリケーション ロードバランサまたはネットワーク ロードバランサに追加されます。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ）を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   これらの手順については、次の設定を使用して Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure Storage` は、クラウド ネイティブ 展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：クラウド ネイティブまたはサードパーティ
   - **アクセス タイプ**：`Private`

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   次のように選択します。

   - **[デバイスの作成（Create Device）]** ウィンドウで、ハブ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** として **[アプリケーション ロード バランサ（Application Load Balancer）]** または **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、アプリケーション ロード バランサまたはネットワーク ロード バランサをドラッグ アンド ドロップします。
   - ハブ VNet のアプリケーション ロード バランサまたはネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

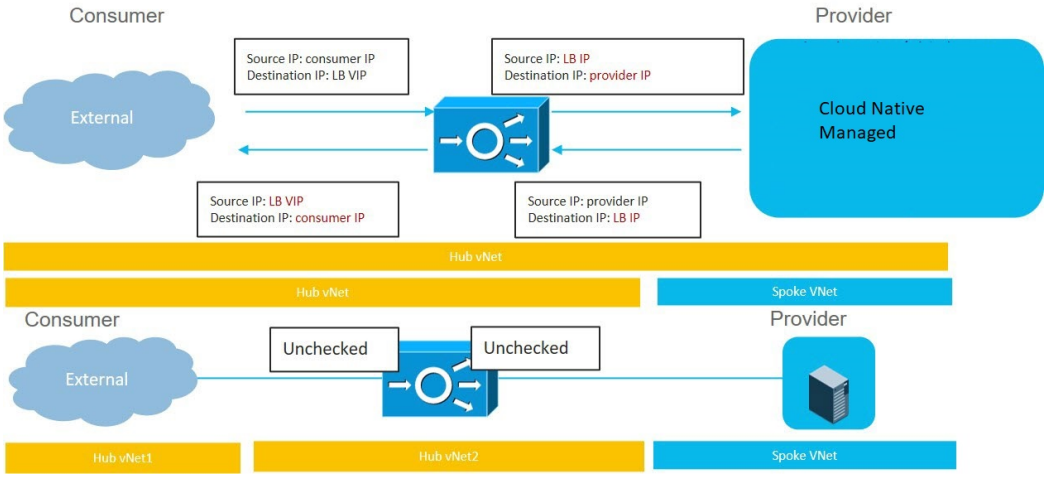
4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ サービス EPG

このユース ケースには、サービス ノードがロードバランサ（アプリケーション ロードバランサ、ネットワーク ロードバランサ、またはサードパーティのロードバランサ）である単一ノード サービス グラフがあります。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ）を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   これらの手順については、次の設定を使用して Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure ApiManagement Services` は、`Cloud Native Managed` 展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：`Cloud Native Managed`
   - **アクセス タイプ**：パブリックおよびプライベート

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   次のように選択します。

- **[デバイスの作成（Create Device）]** ウィンドウで、ハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** として **[アプリケーション ロード バランサ（Application Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、アプリケーション ロード バランサをドラッグ アンド ドロップします。
- ハブ VNet のアプリケーション ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

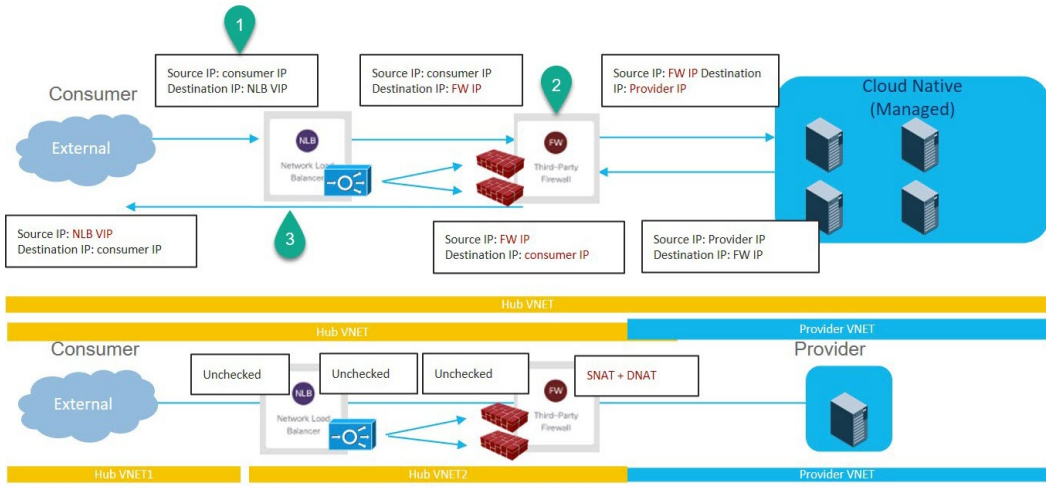
インターネット インバウンド トラフィックの 2 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG

このユースケースには2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。この 2 ノード サービス グラフはリダイレクトを使用しないため、SNAT+DNAT はファイアウォールで実行されます。DNATed アドレスは、ネットワーク ロードバランサまたは同等のサービスであると想定されます。このユース ケースでは、サービス グラフは、ロードバランサのサブネットへのルートの到達可能性のみを確立します。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサのパブリック VIP に送信され、ファイアウォール（DNAT）へのトラフィックが負荷分散されます。
2. SNAT+DNAT はファイアウォールで実行されます。
3. リターン トラフィックの場合、Azure はソース IP をネットワーク ロード バランサのパブリック VIP に変換します。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ）を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   これらの手順については、次の設定を使用して Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure Kubernetes Services（AKS）` は、`Cloud Native Managed` 展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：`Cloud Native Managed`
   - **アクセス タイプ**：`Private`

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   このユースケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。

- **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、**[プロバイダ コネクタ タイプ（Third-Party Firewall）]** フィールドで、**[SNAT]** および **[DNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

インターネット インバウンド トラフィックの 3 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG

このユースケースには3 ノードのサービス グラフがあり、サービス ノードは次のとおりです。

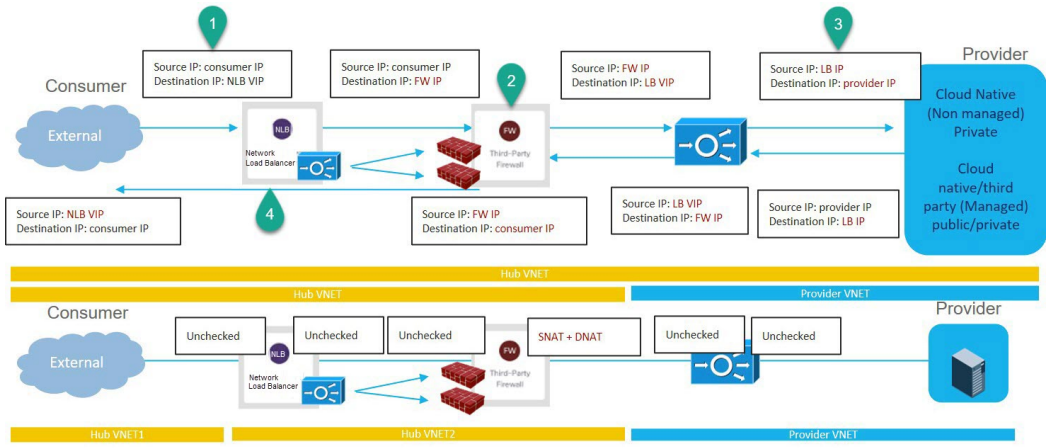
- 最初のサービス デバイス: ハブ VNet のネットワーク ロードバランサ
- 2 番目のサービス デバイス：ハブ VNet のファイアウォール
- サード サービス デバイス：ハブ VNet またはスポーク VNet 内のサードパーティのロードバランサ

この 3 ノード サービス グラフはリダイレクトを使用しないため、SNAT+DNAT はファイアウォールで実行されます。DNATedアドレスは、ロードバランサまたは同等のサービスであると想定されます。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックは最初のサービス デバイスであるネットワーク ロード バランサのパブリック VIP に送信され、次にファイアウォール（DNAT）へのトラフィックの負荷分散が行われます。
2. SNAT+DNAT は、2 番目のサービス デバイスであるファイアウォールで実行されます。
3. トラフィックは、SNAT が構成されているサードパーティのロード バランサであるサード サービス デバイスに移動します。
4. リターン トラフィックの場合、Azure はソース IP をネットワーク ロード バランサのパブリック VIP に変換します。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ）を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダー側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure ApiManagement Services` は、`Cloud Native Managed` 展開タイプでサポートされるサービス タイプです。

- **展開タイプ**：`Cloud Native Managed`
- **アクセス タイプ**：`Private`

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成（274 ページ） を参照してください。

   このユースケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - 最初のデバイスとして、**[サービス タイプ（Service Type）]** として **[アプリケーション ロード バランサ（Application Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - 2 番目のサービス デバイスについては、**[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドで、セカンダリ VRF を選択します。
       - 3 番目のサービス デバイスがハブ VNet にある場合は、**[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third-Party Load Balancer）]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加（Add Interface）]** をクリックしてインターフェイスの詳細を設定します。

   - **[デバイスの作成（Create Device）]** ウィンドウで、次に、必要に応じて (3 番目のサービス デバイスがプロバイダ VNet にある場合)、プロバイダ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、プロバイダー テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドで **[サードパーティ ロード バランサ（Third-Party Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダ VRF のサブネットを選択します。

   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - アプリケーション ロード バランサ（ハブ VNet 用）

- サードパーティ ファイアウォール（ハブ VNet 用）
- サード パーティ ロード バランサ（ハブまたはプロバイダ VNet 用）

- ハブ VNet のアプリケーション ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユース ケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、**[プロバイダ コネクタ タイプ（Third-Party Firewall）]** フィールドで、**[SNAT]** および **[DNAT]** オプションの隣のボックスにチェックを入れます。
- SNAT がサードパーティのロードバランサで構成されていることを確認します。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

リダイレクトの使用例

以下は、リダイレクトを備えたクラウド ネイティブ サービスとサードパーティ サービスを使用したサービス グラフのユース ケースの例です。

これらの各ユース ケースのプロセスの一部として、クラウド サービス EPG を構成します。クラウド サービス EPG を構成している場合は、**サブネットごとの NSG** 構成を有効にする必要があります。詳細については、セキュリティ グループ （50 ページ）およびクラウド サービス エンドポイント グループ （42 ページ）を参照してください。

- インターネット アウトバウンドの 2 ノード サービス グラフ （252 ページ）
- East-West の 2 ノード サービス グラフ （254 ページ）
- SNAT オプションを使用した East-West の 2 ノード サービス グラフ （257 ページ）
- エクスプレス ルート ゲートウェイ経由の受信トラフィックの 2 ノード サービス グラフ （259 ページ）
- SNAT オプションを使用したエクスプレス ルート ゲートウェイ経由のインバウンド トラフィックの 2 ノード サービス グラフ （262 ページ）

- エクスプレス ルート ゲートウェイ経由の受信トラフィックの 3 ノード サービス グラフ（264 ページ）

インターネット アウトバウンドの 2 ノード サービス グラフ

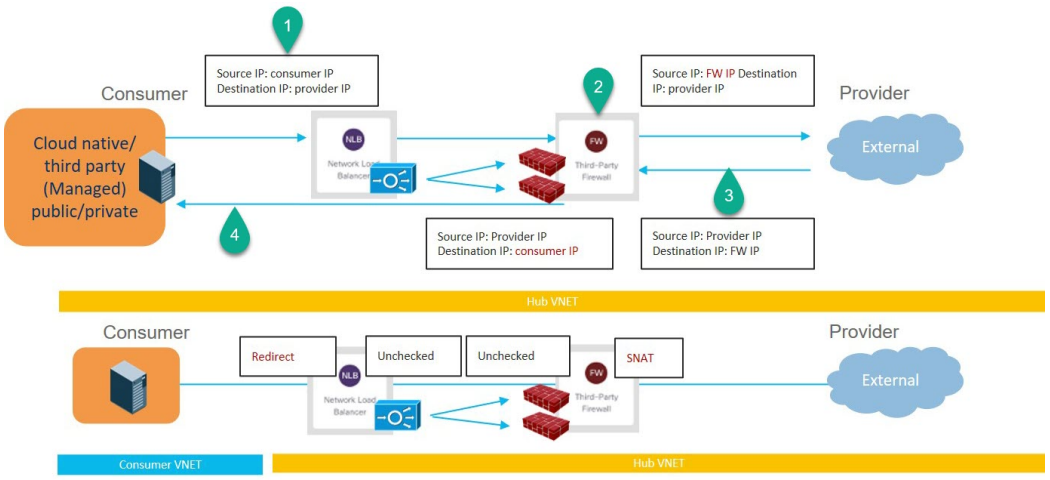
このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、コンシューマ側でリダイレクトが有効になっており、ファイアウォールで SNAT が有効になっています。

このユース ケースでは、サービス EPG はコンシューマであり、外部 EPG はプロバイダ側で構成されます。

（注） レイヤ 4 からレイヤ 7 のサービス グラフが、インターネットの到達可能性のために独自の UDR を使用する PaaS に使用されている場合は、外部 EPG で 0.0.0.0/0 を使用しないことをお勧めします。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターン トラフィックはファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、戻りトラフィックはネットワーク ロード バランサを通過しません。



このユース ケースを構成するには：

1. プロバイダ側で外部 EPG を作成します。

これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ）を参照してください。

- この外部 EPG の [インフラ（infra）] テナントを選択します。
- 0.0.0.0/0 サブネットで外部 EPG を設定しないでください。

2. コンシューマ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、Azure Kubernetes Services (AKS) は、クラウド ネイティブ管理対象展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：クラウド ネイティブ管理対象
   - **アクセス タイプ**：Private

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - ネットワーク ロード バランサ

- サードパーティ ファイアウォール

- ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。

- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

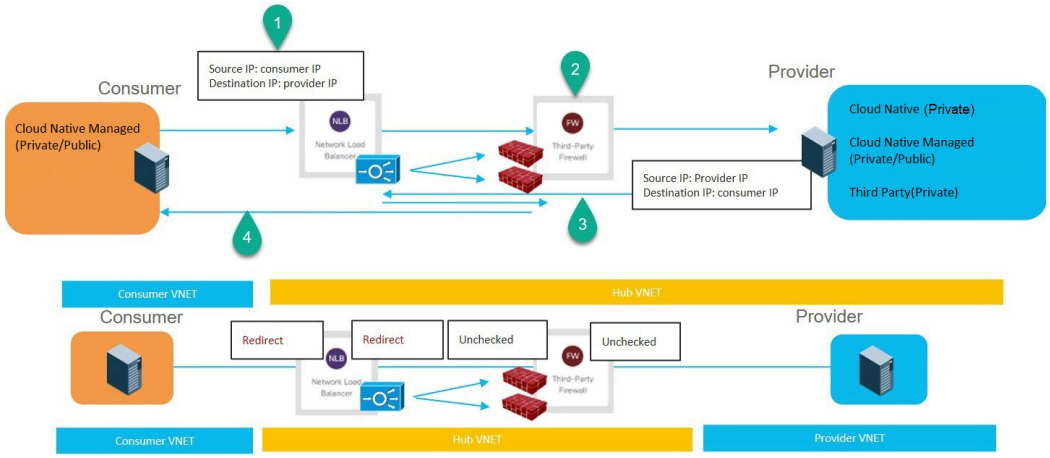
East-West の 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、コンシューマ側とプロバイダ側の両方でリダイレクトが有効になっています。

このユース ケースでは、コンシューマとプロバイダはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユース ケースでは、ファイアウォールで SNAT は実行されません。
3. リターン トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
4. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユース ケースを構成するには：

1. コンシューマまたはプロバイダのサービス EPG を使用している場合は、サービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - コンシューマとしてのサービス EPG には、次の設定があります。
     - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure Kubernetes Services (AKS)` は、`クラウド ネイティブ管理対象` 展開タイプでサポートされるサービス タイプです。
     - **展開タイプ**：`クラウド ネイティブ管理対象`
     - **アクセス タイプ**：`Private`
   - プロバイダとしてのサービス EPG には、次の設定があります。
     - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure Storage File` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
     - **展開タイプ**：`クラウド ネイティブ`
     - **アクセス タイプ**：`Private`

2. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ハブ NLB の **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。
- サード パーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

3. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

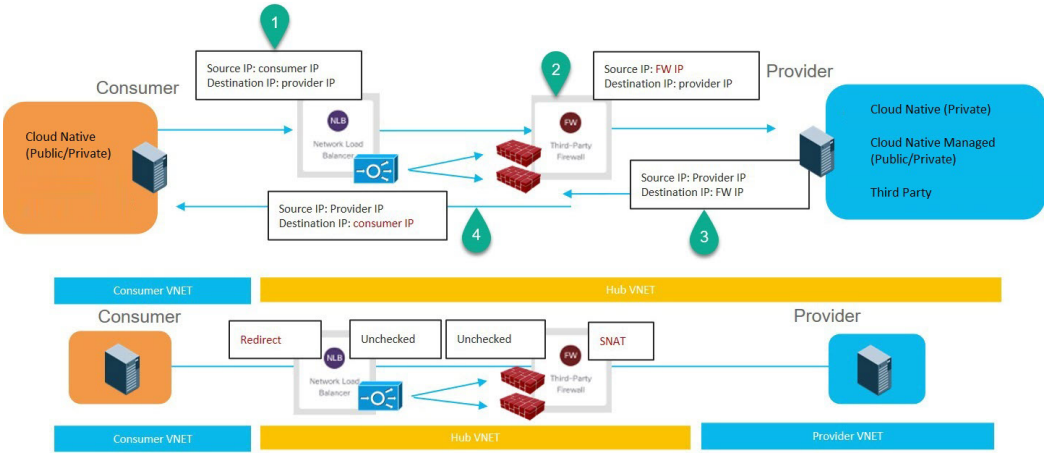
SNAT オプションを使用した East-West の 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、リダイレクトはコンシューマ側でのみ有効になっており、SNAT はファイアウォールで有効になっています。

このユース ケースでは、コンシューマとプロバイダはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターン トラフィックはファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、戻りトラフィックはネットワーク ロード バランサを通過しません。



このユース ケースを構成するには：

1. コンシューマまたはプロバイダのサービス EPG を使用している場合は、サービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - コンシューマとしてのサービス EPG には、次の設定があります。
     - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure Active Directory Domain Services` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
     - **展開タイプ**：`クラウド ネイティブ管理対象`
     - **アクセス タイプ**：`Private`

- プロバイダとしてのサービス EPG には、次の設定があります。
  - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure Storage File` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
  - **展開タイプ**：`クラウド ネイティブ`
  - **アクセス タイプ**：`Private`

2. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - ネットワーク ロード バランサ
     - サードパーティ ファイアウォール
   - ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
     - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。

- **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。

- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

3. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

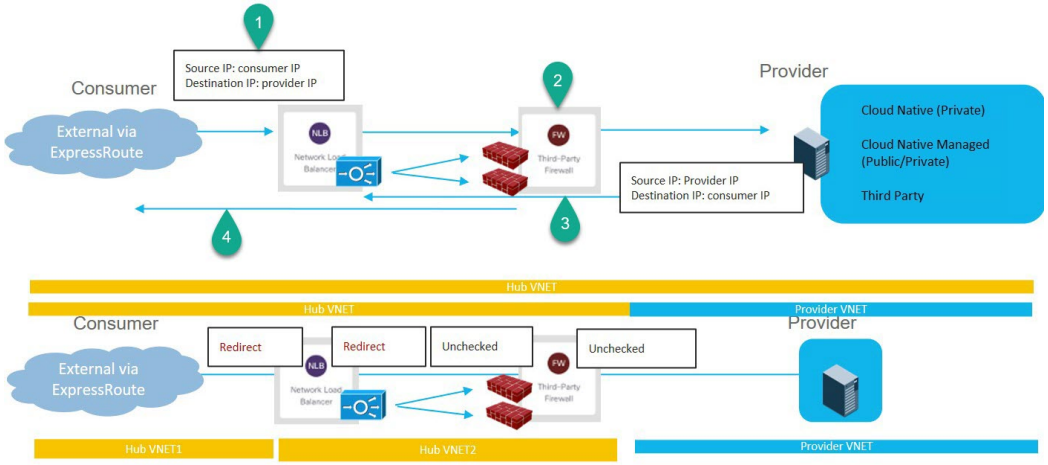
エクスプレス ルート ゲートウェイ経由の受信トラフィックの 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、コンシューマ側とプロバイダ側の両方でリダイレクトが有効になっています。

このユース ケースでは、サービス EPG がプロバイダであり、エクスプレス ルートがコンシューマ側にあります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユース ケースでは、ファイアウォールで SNAT は実行されません。
3. リターン トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
4. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユース ケースを構成するには：

1. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure Active Directory Domain Services` は、クラウド ネイティブ管理対象展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：クラウド ネイティブ管理対象
   - **アクセス タイプ**：`Private`

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

   これらの手順については、リダイレクトを使用してエクスプレス ルート ゲートウェイを展開する （349 ページ） を参照してください。

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。

- **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

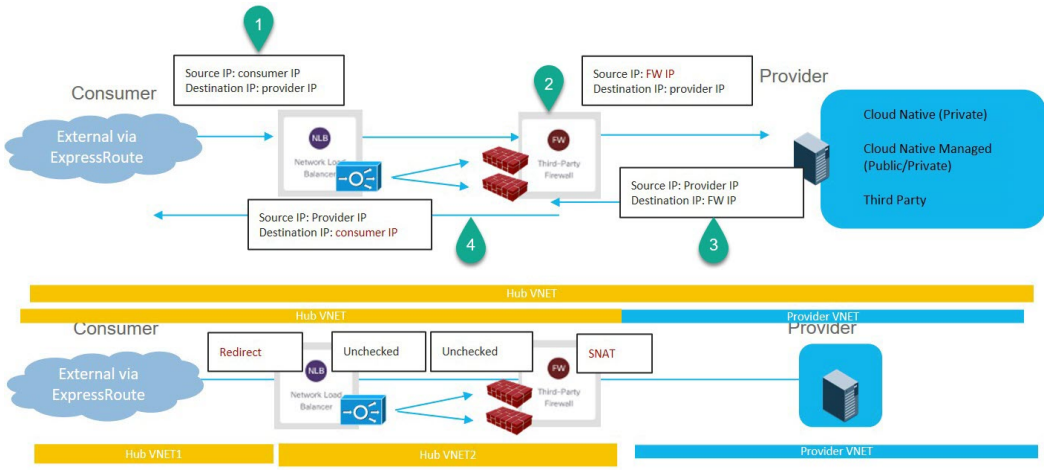
SNATオプションを使用したエクスプレス ルート ゲートウェイ経由のインバウンド トラフィックの 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、リダイレクトはコンシューマ側でのみ有効になっており、SNAT はファイアウォールで有効になっています。

このユース ケースでは、サービス EPG はプロバイダであり、エクスプレス ルートはコンシューマ側にあります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターン トラフィックはファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、戻りトラフィックはネットワーク ロード バランサを通過しません。



このユースケースを構成するには：

1. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Redis キャッシュ`は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：`クラウド ネイティブ管理対象`
   - **アクセス タイプ**：`Private`

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

   これらの手順については、リダイレクトを使用してエクスプレス ルート ゲートウェイを展開する （349 ページ） を参照してください。

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - ネットワーク ロード バランサ
     - サードパーティ ファイアウォール
   - ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
     - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
     - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。
   - サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
     - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。

- このユース ケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

エクスプレス ルート ゲートウェイ経由の受信トラフィックの 3 ノード サービス グラフ

このユース ケースには3 ノードのサービス グラフがあり、サービス ノードは次のとおりです。

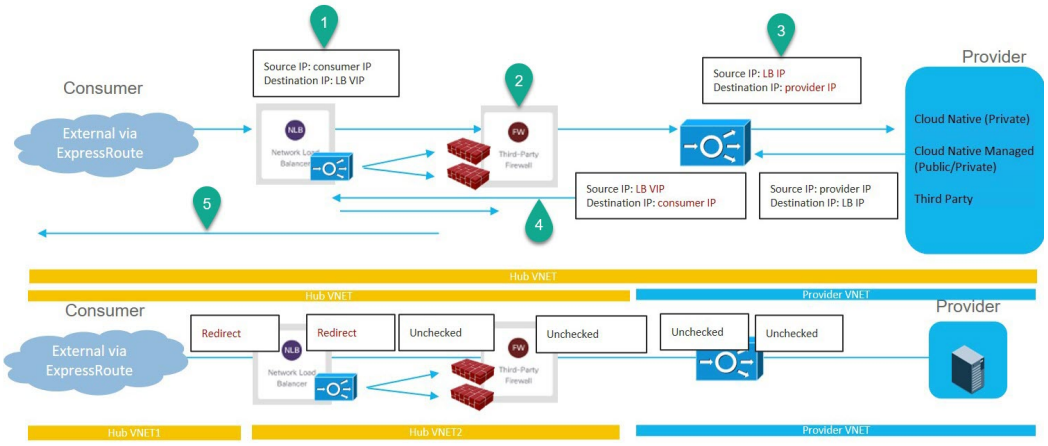
- 最初のサービス デバイス：ハブ VNet のネットワーク ロード バランサ
- 2 番目のサービス デバイス：ハブ VNet のファイアウォール
- 3 番目のサービス デバイス：ハブまたはスポーク VNet のアプリケーション ロード バランサ

このユースケースでは、コンシューマ側とプロバイダ側の両方でリダイレクトが有効になっています。

このユース ケースでは、サービス EPG はプロバイダです。エクスプレス ルートはコンシューマ側にあり、コンシューマはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユース ケースでは、ファイアウォールで SNAT は実行されません。
3. トラフィックは、SNAT が構成されているアプリケーション ロード バランサであるサード サービス デバイスに移動します。
4. リターン トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
5. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユースケースを構成するには：

1. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ） を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ （42 ページ） を参照）。たとえば、`Azure ApiManagement Services` は、クラウド ネイティブ管理対象展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：クラウド ネイティブ管理対象
   - **アクセス タイプ**：プライベート

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

   これらの手順については、リダイレクトを使用してエクスプレス ルート ゲートウェイを展開する （349 ページ） を参照してください。

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。

- **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[デバイスの作成（Create Device）]** ウィンドウで、次にプロバイダ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、プロバイダ テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドで **[アプリケーション ロード バランサ（Application Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダ VRF のサブネットを選択します。

（注） 内部 NLB の代わりにサードパーティのロードバランサを使用できます。**[サービス タイプ（Service Type）]**として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択します。**[インターフェイスの追加（Add Interface）]** をクリックして、**[VRF]** を選択し、インターフェイスの詳細を設定します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ（ハブ VNet 用）
  - サードパーティ ファイアウォール（ハブ VNet 用）
  - アプリケーション ロード バランサ（プロバイダ VNet 用）
- ハブ VNet のネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次のようにします。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。

- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。
- プロバイダ VNet でネットワーク ロードバランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。

（注） SNAT がサードパーティのロード バランサで構成されていることを確認します。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （288 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

リダイレクトの注意事項と制約事項

リダイレクトの注意事項と制約事項は次のとおりです。

- レイヤ 4 ～ レイヤ 7 のすべてのサービス デバイスには、独自の専用サブネットが必要です。
- リージョン内の VRF 内レイヤ 4 ～ レイヤ 7 サービスへのリダイレクション：
  - コンシューマ EPG とプロバイダ EPG が同じ VNet にある場合、レイヤ 4 ～ レイヤ 7 サービスへのリダイレクトは、east-west 展開ではサポートされません。
  - 外部 EPG がプロバイダ EPG である場合、コンシューマ EPG とプロバイダ EPG が同じ VNet にあるかどうかに関係なく、レイヤ 4 からレイヤ 7 へのサービス リダイレクトが North-South 展開でサポートされます。
- リージョンでの VRF 間レイヤ 4 からレイヤ 7 サービスへのリダイレクト：
  - リージョン間レイヤ 4 ～ レイヤ 7 サービスへのリダイレクトがサポートされています。ただし、コンシューマ EPG とプロバイダ EPG は拡大しないでください。
  - リージョンでは、同じ VRF にコンシューマ EPG とプロバイダ EPG の両方を含めることはできません。たとえば、リージョン 1 にコンシューマ EPG のみがあり、リージョン 2 にプロバイダ EPG のみがある場合、これはサポートされますが、リージョン 1 にコンシューマ EPG とプロバイダ EPG の両方を含めることはできません。
  - コンシューマおよびプロバイダの EPG は、サブネット ベースの EPG である必要があります。

- レイヤ 4 ～レイヤ 7 サービスへのリダイレクションを伴うリージョン間サービス グラフの場合、サービス デバイスはプロバイダ EPG のリージョンに展開する必要があります。プロバイダ EPG がリージョン全体に拡張されている場合、サービス デバイスは各リージョンに展開する必要があります。
- プロバイダとしての外部 EPG の場合、サービス デバイスはコンシューマ EPG に対してローカルなリージョンに展開する必要があります。コンシューマ EPG が複数のリージョンにまたがっている場合は、サービス デバイスを各リージョンに展開する必要があります。
- コンシューマ VNet とプロバイダ EPG の間では、サービス グラフを介して挿入できるリダイレクト デバイスは 1 つだけです。たとえば、コンシューマ EPG1 とコンシューマ EPG2 がコンシューマ VNet にあり、プロバイダ EPG3 がプロバイダ VNet にある場合、EPG1 と EPG3 間の契約、および EPG2 と EPG3 間の契約に同じリダイレクト デバイスを使用する必要があります。

（注） この制限は、クラウド プロバイダがユーザー定義ルートの特定の宛先に対して 1 つのネクスト ホップのみを許可するためです。

- 次の表に、サポートされている、またはサポートされていない特定のリダイレクト構成に関する情報を示します。
  - NLB はネットワーク ロード バランサの略
  - ALB はアプリケーション ロード バランサの略
  - FW はファイアウォールの略

（注） サードパーティのロードバランサへのリダイレクトはサポートされていません。

サービス チェイン オプション	スポークツースポーク		スポークツー外部へ（コンシューマが話す）		外部ツースポークへ（コンシューマは外部）	
	VNet 内	VNet 間	VNet 内	VNet 間	VNet 内	VNet 間
NLB/ALB[1] LB(SNAT) 1	サポート対象	サポート対象	非対応	サポート対象外	サポート対象	サポート対象
FW（SNAT なし）[2]	非対応	サポート対象	非対応	サポート対象外	サポート対象外	サポート対象外

サービス チェイン オプション	スポークツースポーク		スポークツー外部へ（コンシューマが話す）		外部ツースポークへ（コンシューマは外部）	
FW（SNAT）リダイレクトは、コンシューマ コネクタで有効になっています。[3]	サポート対象	サポート対象	サポート対象	サポート対象	非対応	サポート対象外
• NLB[2]-FW(no SNAT)[1] • NLB[2]-FW(no SNAT)[1]-NLB/ALB[1] • NLB[2]-FW(no SNAT)[1]-LB(SNAT)[1]	非対応	サポート対象	非対応	サポート対象外	サポート対象外	サポート対象外
NLB[4]-FW(SNAT)[5]	非対応	サポート対象	サポート対象	サポート対象	非対応	サポート対象外
NLB/ALB[1]-FW(SNAT+DNAT)[6]-NLB/ALB[1] NLB/ALB[1]-FW(ANT+DNAT)[6]-LB(SNAT)[1] （リダイレクトなし）	サポート対象	サポート対象	未サポート	非対応	サポート対象	サポート対象
NLB[1]-LB(SNAT)[1] （リダイレクトなし）	サポート対象	サポート対象	未サポート	非対応	サポート対象	サポート対象

[1] コンシューマ コネクタとプロバイダ コネクタの両方でチェックを外すか、オプションは ALB に適用されません。
[2] リダイレクトは、コンシューマ コネクタとプロバイダ コネクタの両方で有効になっています。
[3] プロバイダ コネクタで SNAT が有効になっています。
[4] リダイレクトは、コンシューマ コネクタで有効になっています。プロバイダ コネクタではオフになっています。
[5] コンシューマ コネクタではチェックを外します。プロバイダ コネクタで SNAT が有効になっています。
[6] コンシューマ コネクタではチェックされていません。プロバイダ コネクタで SNAT+DNAT が有効になっています。

Cloud APIC GUI を使用したセカンダリ VRF への新しい CIDR の追加

状況によっては、新しい CIDR を追加したり、セカンダリ VRF で既存の CIDR を編集したりする前に、VNet ピアリングを無効にする必要がある場合があります。これは、アクティブな VNet ピアリングがある場合、VNet 上の CIDR を更新できないという Azure の制限によるものです。CIDR を追加するには、最初にその VNet の VNet ピアリングを削除する必要があります。その後、CIDR を更新できます。CIDR を更新したら、VNet ピアリングを再度有効にすることができます。

これらの手順では、特定のインフラ VNet に関連付けられているすべての VNet ピアリングを削除するハブ ネットワーク ピアリングを無効にする手順について説明します。

- インフラ VNet に追加の CIDR が既に作成されているが、その既存の CIDR にサブネットを追加するだけでよい場合は、それらのサブネットを追加する前に、その特定のインフラ VNet のハブ ネットワーク ピアリングを無効にする必要はありません。既存の CIDR にサブネットを追加するには：

  1. その場合は、適切なクラウド コンテキスト プロファイルに移動します（**[アプリケーション管理（Application Management）]>[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**）。
  2. サブネットを既存の CIDR に追加するクラウド コンテキスト プロファイルをダブルクリックし、ステップ 10 （272 ページ） に移動して、新しいサブネットを既存の CIDR に追加します。

- インフラ VNet に新しい CIDR を追加する場合、またはインフラ VNet で CIDR を削除するか、他の方法（サブネットの追加以外）で CIDR を編集する場合は、その特定のインフラ VNet のハブ ネットワーク ピアリングを無効にする必要があります。 。CIDR を追加した後、ハブ ネットワーク ピアリングを再度有効にします。以下の手順では、それらの手順について説明します。

（注） 新しい CIDR をセカンダリ VRF に追加しており、次のリリースで実行しているマルチサイト展開がある場合：

- Cloud APIC のリリース 5.2(1) 以降
- Nexus Dashboard Orchestrator のリリース 3.3 以降

新しい CIDR を追加し、ハブ ネットワーク ピアリングを再度有効にしたら、Nexus Dashboard Orchestrator でサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開する前に、CIDR が起動するまで少なくとも 5 分間待機します。CIDR が Azure に展開されるには時間がかかるため、サイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開する前に少なくとも数分待たないと、新しく追加された CIDR が Nexus Dashboard Orchestrator を介してリモート サイトに伝達されない可能性があります。

Nexus Dashboard Orchestrator からインフラ構成を展開した後に、次のエラー メッセージが表示された場合：

```
Invalid configuration CT_Remotectx_cidr: Remote Site CIDR
```

これは、Nexus Dashboard Orchestrator からインフラ構成を展開しする前に十分な時間を待たず、新しく追加された CIDR がリモート サイトに伝達されなかったことを意味します。この場合、次のようになります。

1. Cloud APIC でハブ ネットワーク ピアリングを無効にする
2. Nexus Dashboard Orchestrator でサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開します。
3. Cloud APIC でハブ ネットワーク ピアリングを再度有効にする
4. 少なくとも 5 分（または以前に待機したよりも長い時間）待ってからサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を再度展開します。

ステップ 1 まだログインしていない場合は、Cloud APIC にログインします。

ステップ 2 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**に移動します。

既存のクラウドコンテキストプロファイルが表示されます。

ステップ 3 ハブ ネットワーク ピアリングを無効にするクラウド コンテキスト プロファイルをダブルクリックします。

そのクラウド コンテキスト プロファイルの概要ウィンドウが表示されます。この概要ウィンドウの **[ハブ ネットワーク ピアリング（Hub Network Peeri）]** 領域に **[有効（Enabled）]** と表示されます。これは、ハブ ネットワーク ピアリングが有効になっていることを示しています。

ステップ 4 鉛筆アイコンをクリックして、このクラウド コンテキスト プロファイルを編集します。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

ステップ 5 [クラウド コンテキスト プロファイルの編集] ウィンドウで、[ハブ ネットワーク ピアリング] フィールドを見つけ、チェック ボックスをクリックして [有効] フィールドからチェックマークを外します。

[ハブ ネットワーク ピアリング（Hub Network Peering）] オプションを無効にしても、グローバル レベルで VNet ピアリングが削除されるのではなく、この特定のインフラ VNet に関連付けられているすべての VNet ピアリングが削除されます。

ステップ 6 [保存（Save）] をクリックします。

そのクラウドコンテキストプロファイルの概要ウィンドウが再び表示されます。この概要ウィンドウの **[ハブ ネットワーク ピアリング（Hub Network Peeri）]** 領域に **[無効（Disabled）]** と表示されます。これは、ハブ ネットワーク ピアリングが無効になっていることを示しています。

ステップ 7 新しい CIDR を追加するには、鉛筆アイコンをクリックして、このクラウド コンテキスト プロファイルを再度編集します。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

ステップ 8 **[CIDR の追加（Add CIDR）]** をクリックします。

[CIDR の追加（Add CIDR）] ダイアログボックスが表示されます。

ステップ 9 **[CIDR ブロック範囲（CIDR Block Range）]** フィールドに新しい CIDR を追加します。

[プライマリ（Primary）] フィールドのボックスをクリックしないでください（**[プライマリ'（Primary）]** フィールドの **[はい（yes）]** の横のボックスにチェックを入れないでください）。

ステップ 10 **[サブネットの追加（Add subnet）]** をクリックして、必要なサブネットアドレスを **[アドレス（Address）]** に入力します。

必要に応じて、追加のサブネットの **[サブネットの追加（Add Subnet）]** をクリックし続けます。

ステップ 11 **[CIDR の追加（Add CIDR）]** ウィンドウで必要な情報をすべて追加し終わったら、**[追加（Add）]** をクリックします。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

ステップ 12 **[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）]** ウィンドウで情報を確認し、**[保存（Save）]** をクリックします。

そのクラウドコンテキストプロファイルの概要ウィンドウが表示されます。**[CIDR ブロック範囲（CIDR Block Range）]** 領域にリストされた新しい CIDR が表示されます。

ステップ 13 これらの手順の最初にハブ ネットワーク ピアリングを無効にした場合は、この時点で再度有効にします。

a) 鉛筆アイコンをクリックして、このクラウド コンテキスト プロファイルを編集します。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

b) **[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）]** ウィンドウで、**[ハブ ネットワーク ピアリング（Hub Network Peering）]** フィールドを見つけ、チェック ボックスをクリックして **[有効（Enabled）]** フィールドにチェックマークを追加し、この特定のインフラ VNet の VNet ピアリングを再度有効にします。

c) [保存（Save）] をクリックします。

そのクラウド コンテキスト プロファイルの概要ウィンドウが再び表示されます。この概要ウィンドウの **[ハブ ネットワーク ピアリング（Hub Network Peeri）]** 領域に **[有効（Enabled）]** と表示されます。これは、ハブ ネットワーク ピアリングが再び有効になっていることを示しています。

前に説明したように、この時点で Azure portal にアクセスすると、Azure の overlay-1 VNet にてこれらの手順で追加した追加の CIDR とサブネットが 表示されます。これは、正しく予期される動作です。

サービス グラフの展開

サービス グラフを使用すると、デバイス間のトラフィック フロー、ネットワークへのトラフィックの流入方法、トラフィックが通過するデバイス、およびトラフィックがネットワークから出る方法を定義できます。

サービス グラフは、次の 2 つの方法で展開できます。

- 単一ノード サービス グラフ：1 つのデバイスのみが展開されます。
- マルチノード サービス グラフ：最大 3 つのノードをサービス チェーンに追加できます。

単一ノードまたはマルチキャストノードのいずれかでサービス グラフを展開可能になる前に、以下を構成する必要があります。

1. テナント
2. アプリケーション プロファイル
3. コンシューマ EPG
4. プロバイダーEPG
5. VRF
6. クラウド コンテキスト プロファイル
7. フィルタとの契約

GUI を使用してサービス グラフの展開

次のセクションでは、GUI を使用してサービス グラフを展開する方法について説明します。

Cloud APIC GUI を使用したサービス デバイスの作成

始める前に

このセクションでは、Cisco Cloud APIC GUI を介してサービス グラフで使用できるサービス デバイスを作成する方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]** > **[デバイス（Devices）]** > **[デバイスの作成（Create Device）]**をクリックします。**[[デバイスの作成（Create Device）]** ダイアログボックスが表示されます。

ステップ 4 次の *[デバイスの作成ダイアログボックスのフィールド（Create Device Dailog Box Fields）]* の表にリストされた各フィールドに該当する値を入力し、続行します。

各タイプのサービス デバイスに固有の情報については、次の表を参照してください。

- アプリケーション ロード バランサについては、4.a （274 ページ） を参照してください。
- ネットワーク ロード バランサについては、4.b （276 ページ） を参照してください。
- サード パーティのロード バランサについては、4.c （281 ページ） を参照してください。
- サードパーティのファイアウォールについては、4.d （282 ページ） を参照してください。

a) アプリケーション ロード バランサに必要な情報を入力します。

[プロパティ（Properties）]	**説明**
全般	
名前	デバイスの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]**をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[デバイスの作成（Create Device）]** ダイアログボックスに戻ります。
[設定（Settings）]	

[プロパティ（Properties）]	説明
サービス タイプ	デバイス タイプを選択します。 • アプリケーションロードバランサ
ALB SKU	次から選択します。 • Standard • Standard V2
VM インスタンス数	*[VM インスタンス数（VM Instance Count）]* テキスト ボックスに数値を入力します。 （注） これは、Application Gateway にのみ適用されます。
VM インスタンス サイズ	選択する VM インスタンスのサイズ（**大**、**中**、または**小**）のラジオ ボタンをクリックします。 （注） これは、Application Gateway にのみ適用されます。
スキーム	**[インターネット向け]** または **[内部]** を選択します。 • **インターネット向け**：これは、バランサのパブリック IP を構成するために使用されます。これは Azure によって割り当てられます。 • 内部：クリックして、**[IP アドレスの割り当て（IP Address Assignment）]** で **[動的（Dynamic）]** または **[静的（Static）]** を選択します。 • **動的**：Azure によって動的 IP アドレスが割り当てられます。動的 IP アドレスは、VM が起動するたびに変更されます。 • **静的**：クラウド コンテキスト プロファイルで定義されている CIDR に基づいて IP アドレスを入力し、IP アドレスが ALB と同じサブネットにあることを確認します。 ALB SKU Standard は、静的および動的 IP アドレスをサポートします。ALB SKU Standard V2 は、静的 IP アドレスのみをサポートします。

[プロパティ（Properties）]	説明
サブネット	サブネットを選択するには: 1. **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。**[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 2. **[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** ダイアログ ボックスが表示されます。 3. **[サブネットの選択（Select Subnet）]** をクリックします。**[サブネットの選択]** ダイアログボックスが表示されます。静的 IP アドレス テキスト ボックスが表示されます。ロード バランサの IP アドレスを入力します。右の「ティック」マークをクリックして確定します。 4. さらにサブネットを追加するには、手順 a ～ c を繰り返します。

b) ネットワーク ロード バランサに必要な情報を入力します。

表 *39 :* ネットワーク ロード バランサの *[*デバイスの作成（***Create Device***）*]* ダイアログ ボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	ロード バランサーの名前を入力します。
[設定（Settings）]	
サービス タイプ	デバイス タイプを選択します。 • ネットワーク ロード バランサ

[プロパティ（Properties）]	説明
すべてのトラフィックを許可	**[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にするかどうかを決定します。 **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にすると、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスが許可されます。詳細については、「すべてのトラフィックを許可について （217 ページ）」を参照してください。 （注） このオプションを有効にする前に、これによってセキュリティ リスクが発生しないことを確認してください。 • すべてのトラフィックを許可する場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横にあるボックスをクリックします。 • すべてのトラフィックを許可しない場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横のボックスをオフ（選択解除）したままにします。
スキーム	**[インターネット向け]** または **[内部]** を選択します。 • **インターネット向け**：これは、バランサのパブリック IP を構成するために使用されます。これは Azure によって割り当てられます。 • リリース 25.0(3) より前のリリースでは、**インターネット向け**オプションの選択は、1 つのデフォルトのパブリック フロントエンド IP アドレスのみを構成するために使用されます。 • リリース 25.0(3) 以降では、このページの **[フロントエンド IP 名（Frontend IP Names）]** フィールドでの選択に応じて、**インターネット向けオプション**を選択して、単一のデフォルト パブリック フロントエンド IP アドレスまたは複数のパブリック フロントエンド IP アドレスを構成できます。。 • 内部：クリックして、**[IP アドレスの割り当て（IP Address Assignment）]** で **[動的（Dynamic）]** または **[静的（Static）]** を選択します。 • **動的**：Azure によって動的 IP アドレスが割り当てられます。動的 IP アドレスは、VM が起動するたびに変更されます。 • **静的**：クラウド コンテキスト プロファイルで定義されている CIDR に基づいて IP アドレスを入力し、IP アドレスが NLB と同じサブネットにあることを確認します。静的 IP アドレスは、ロード バランサに関連付けられます。 （注） Cloud APIC は、標準の SKU NLB のみを作成します。

[プロパティ（Properties）]	説明
カスタム リソース グループ	必要に応じて、カスタム リソース グループの名前を入力します。
Subnets	サブネットを選択するには: **1.** **[+ サブネットの追加 (+Add Subnet)]** をクリックします。 **2.** **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。 **[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 **3.** **[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** ダイアログ ボックスが表示されます。 **[クラウド コンテキスト プロファイル（Select Cloud Context Profile）]** ダイアログで、左側の列のクラウド コンテキスト プロファイルをクリックして選択し、**[選択（Select）]** をクリックします。 **4.** **[サブネットの選択（Select Subnet）]** をクリックします。**[サブネットの選択]** ダイアログボックスが表示されます。 **[サブネット の選択（Select Subnet）]** ダイアログで、左側の列のサブネットをクリックして選択し、**[選択（Select）]** をクリックします。 **5.** 右の「ティック」マークをクリックして確定します。 **6.** さらにサブネットを追加するには、**[+ サブネットの追加（+ Add Subnet）]** を再度クリックして、これらの手順を繰り返します。
詳細設定	下矢印をクリックして、**[詳細設定（Advanced Settings）]** 領域を展開します。 次のエントリが表示されます。

[プロパティ（Properties）]	説明
フロントエンド IP 名	

[プロパティ（Properties）]	説明
	リリース 25.0(3) 以降、インターネット向けのネットワーク ロード バランサに対して複数のフロントエンド IP アドレスを構成するためのサポートが利用可能になりました。 • デフォルトでは、インターネット向けのネットワーク ロード バランサ用に単一のフロントエンド IP アドレスが自動的に作成されます。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。 • インターネット向けネットワーク ロード バランサに追加のフロントエンド IP アドレスが必要な場合は、**[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** をクリックします。これは、リリース 25.0(3) で導入された新機能です。詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （214 ページ）を参照してください。 この領域にフロントエンド IP 名を追加すると、このインターネット向けネットワーク ロード バランサに複数のフロントエンド IP アドレスを割り当てることが Azure に通知されます。この領域に入力する各フロントエンド IP 名は、単一の追加フロントエンド IP アドレスになります。 この領域のパブリック フロントエンド IP アドレス (既定のフロントエンド IP アドレスと追加のフロントエンド IP アドレス) は、Azure によって割り当てられます。 1. **[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** をクリックして、Azure でネットワーク ロード バランサに割り当てる追加のフロントエンド IP アドレスの名前を追加します。 2. 追加のフロントエンド IP アドレスの名前を入力し、右側のチェック マークをクリックして新しいフロントエンド IP 名を確認します。 3. **[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** を再度クリックして、Azure でネットワーク ロード バランサに割り当てる追加のフロントエンド IP アドレスの名前を追加します。 たとえば、インターネット向けのネットワーク ロード バランサに合計 3 つのフロントエンド IP アドレスが必要だとします。 • 3 つのフロントエンド IP アドレスの最初のアドレスは、リリース 25.0(3) より前に使用できる既存の動作を使用して、デフォルトで自動的に割り当てられます。 • 次に、**[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** を 2 回クリックし、2 つの個別のフロントエンド IP 名（たとえば、`frontend2` と `frontend3`）を入力して、インターネット向けネットワーク ロード バランサに対して合計 3 つのフロントエンド IP アドレスを割り当てることを Azure に通知します。

[プロパティ（Properties）]	説明
	デフォルトおよび構成済みのフロントエンド IP 名に関連付けられたフロントエンド IP アドレスを表示するには： 1. **[アプリケーション管理（Application Management）]** > **[サービス（Services）]** > **[デバイス（Devices）]** に移動します。 2. 構成されたサービス デバイスをダブルクリックして、そのサービス デバイスの **[概要（Overview）]** ページを表示します。 3. **[クラウド リソース（Cloud Resources）]** > **[フロントエンド IP 名（Frontend IP Names）]** をクリックします。 デフォルトのフロントエンド IP アドレスは、この詳細ページの [デフォルト（Default）] タグとともに表示されます。

c) サード パーティ ロード バランサに必要な情報を入力します。

表 *40*：サード パーティ ロード バランサの *[デバイスの作成（Create Device）]* ダイアログ ボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	デバイスの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[デバイスの作成（Create Device）]** ダイアログボックスに戻ります。
[設定（Settings）]	
サービスの種類	デバイス タイプを選択します。 • サードパーティ ロード バランサ
作成モード	**[セレクタ（Selectors）]** を選択します。 **[VRF]** および **[インターフェイス（Interfaces）]** フィールドが表示されます。

[プロパティ（Properties）]	説明
VRF	**[VRF の選択（Select VRF）]** をクリックします。開いている [VRF の選択（Select VRF）] ダイアログで、クリックして左の列の VRF を選択します。[選択（Select）] をクリックします。
インターフェイス	[インターフェイスの追加（Add Interface）] をクリックします。**[インターフェイス（Interfaces）]** ウィンドウが表示されます。 **1. [インターフェイス設定（Interface Settings）]** フィールドで外部インターフェイスの名前を入力します。 **2. [インターフェイス セレクタの追加（Add Interface selector）]** をクリックします。 **3. [インターフェイス セレクタの設定（Interface Selector Settings）]** ページで、インターフェイスの名前を入力します。 **4. [一致式（Match Expressions ）]** フィールドで、**[一致式（Match Expressions ）]** をクリックして選択します。 • **キー**：これは、IP、リージョン、またはカスタム ベースのタグ セレクタです。 • **演算子**：これは、equal、not equals、in、not in、key あり、または key なしのいずれかです。 • **値**：サード パーティのロード バランサの外部または内部ネットワークの IP アドレス。 **5.** チェック マークをクリックしてインターフェイスを追加し、**[保存（Save）]**（[インターフェイス ウィンドウ）をクリックします。 **6. [保存（Save）]**（[デバイスの作成（Create Device）] ウィンドウ）をクリックします。 **[インターフェイスの追加（Add Interface）]** をクリックし、手順 a ～ e を繰り返して、さらにインターフェイスを追加します。 （注） サードパーティのロードバランサインターフェイスは、マルチノード サービス グラフに展開する場合、サブネット ベースのセレクタで構成する必要があります。

d) サード パーティ ファイアウォールに必要な情報を入力します。

表 *41 :* サード パーティ ファイアウォールの *[*デバイスの作成（*Create Device*）*]* ダイアログ ボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	デバイスの名前を入力します。
[設定（Settings）]	
サービス タイプ	デバイス タイプを選択します。 • サードパーティ ファイアウォール （注） サードパーティのファイアウォールをマルチノード サービス グラフの最初のデバイスにすることはできません。
VRF	VRF を選択するには、次の手順を実行します。 1. [VRF の選択（Select VRF）] をクリックします。[VRF の選択（Select VRF）] ダイアログボックスが表示されます。 2. [VRF の選択（Select VRF）] ダイアログで、左側の列の VRF をクリックして選択し、[選択（Select）] をクリックします。

[プロパティ（Properties）]	説明
インターフェイス	[インターフェイスの追加（Add Interface）] をクリックします。 **[設定]** ページが表示されます。 **1.** **[名前（Name）]** フィールドに、インターフェイスの名前を入力します。 **2.** **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にするかどうかを決定します。 **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にすると、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスが許可されます。詳細については、「すべてのトラフィックを許可について （217 ページ）」を参照してください。 （注） このオプションを有効にする前に、これによってセキュリティ リスクが発生しないことを確認してください。 • すべてのトラフィックを許可する場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横にあるボックスをクリックします。 • すべてのトラフィックを許可しない場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横のボックスをオフ（選択解除）したままにします。 **3.** **[インターフェイス セレクタの追加（Add Interface Selector）]** をクリックします。 **4.** インターフェイス セレクタの名前を入力します。 **5.** **[一致式（Match Expressions）]** をクリックして選択します。 • **キー**：これは、IP、リージョン、またはカスタムベースのタグセレクタです。 • **演算子**：これは、equal、not equals、in、not in、key あり、または key なしのいずれかです。 • **値**：アプリ、Web、内部ネットワーク、管理ネットワーク、または外部ネットワークの IP アドレス。 **6.** [追加] をクリックします。 **7.** 手順 a から f を繰り返して、さらにインターフェイスを追加します。

ステップ 5 設定が終わったら [Save] をクリックします。

ステップ 6 **[サービス グラフの作成（Create Service Graph）]** ダイアログボックスが表示されます。**[別のサード パーティ ファイアウォールを作成（Create another Third Party Firewall）]** をクリックして、別のデバイスを作成します。**[[デバイスの作成（Create Device）]** ダイアログボックスが表示されます。

（注） UI は通常、以前に作成したデバイスを作成するように求めます。ただし、それをクリックすると、**[デバイスの作成（Create Device）]** ページに戻ります。ここで、作成する必要があるデバイスを選択できます。最初のデバイスは、サード パーティのファイアウォールにしないでください。

Cisco Cloud APIC GUIを使用したサービス グラフ テンプレートの作成

このセクションでは、Cisco Cloud APIC GUI を使用した単一ノードまたはマルチノード向けサービス グラフ テンプレートの作成方法について説明します。

始める前に

デバイスはすでに作成されています。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが**[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[サービス（Services）]** > **[サービス グラフ（Service Graph）]** > **[サービス グラフの作成（Create Service Graph）]** をクリックします。**[サービス グラフの作成（Create Service Graph）]** ポップアップが表示されます。**[では始めましょう（Let's Get Started）]** をクリックします。

ステップ 4 次の *[サービス グラフの作成ダイアログ ボックスのフィールド（Create Service Graph Dialog Box Fields）]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *42*：サービス グラフの作成ダイアログ ボックスのフィールド（単一ノード向け）

[プロパティ（Properties）]	説明
全般	
名前	サービス グラフ テンプレートの名前を入力します。

[プロパティ（Properties）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[サービス グラフの作成（Create Service Graph）]** ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。
[設定（Settings）]	
デバイスを選択	デバイスを選択します。 1. **[デバイスの選択（Select Device）]** をクリックします。**[デバイスの選択（Select Device）]** ダイアログが表示されます。 2. 左側の列から、デバイスをクリックして選択します。下の**[デバイスのドロップ（Drop Device）]** スペースにデバイスをドラッグ アンド ドロップします。これにより、このデバイス タイプの実際のデバイスを選択できる小さなウィンドウが開きます。 3. [選択（Select）] をクリックします。**[サービス グラフの作成（Create Service Graph）]** ダイアログボックスに戻ります。

表 *43*: サービス グラフの作成ダイアログ ボックスのフィールド（マルチノード向け）

[プロパティ（Properties）]	説明
全般	
名前	サービス グラフ テンプレートの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[サービス グラフの作成（Create Service Graph）]** ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。

[プロパティ（Properties）]	説明
設定：必要なトポロジに基づいて、デバイスを下のボックスにドラッグ アンド ドロップします。	
アプリケーション ロード バランサ	1. アプリケーション ロード バランサ デバイスを下のボックスにドラッグ アンド ドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[アプリケーション ロード バランサの選択（Select Application Load Balancer）]** をクリックし、左側の列で [アプリケーション ロード バランサ（Application Load Balancer）] をクリックして選択し、**[追加（Add）]** をクリックします。
サードパーティ ファイアウォール	1. 下のボックスでデバイスの隣にサードパーティ ファイアウォールをドラッグアンド ドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[サード パーティ ファイアウォール（Third Party Firewall）]** をクリックし、左側の列で [サードパーティ ファイアウォール（Third Party Firewall）] をクリックして選択し、**[追加（Add）]** をクリックします。 （注） サード パーティ ファイアウォールをサービス グラフの最初のノードにすることはできません。 3. サードパーティ ファイアウォールのコンシューマ側でユーザー ベースのリダイレクト機能を有効にする場合は、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 4. サードパーティ ファイアウォールのプロバイダ側でユーザー ベースのリダイレクト機能を有効にする場合は、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 5. **[プロバイダ コネクタ タイプ（Provider Connector Type）]** で、該当するオプションの横にチェックを入れます。詳細については、「レイヤ4～レイヤ7サービス リダイレクト」を参照してください。 6. [追加] をクリックします。

[プロパティ（Properties）]	説明
ネットワーク ロード バランサ	1. ネットワーク ロードバランサデバイスを下のボックスにドラッグアンドドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[ネットワーク ロード バランサの選択（Select Network Load Balancer）]** をクリックし、左側の列で [ネットワーク ロード バランサ（Network Load Balancer）] をクリックして選択し、**[追加（Add）]** をクリックします。 3. ネットワーク ロードバランサのコンシューマ側でユーザーベースのリダイレクト機能を有効にする場合は、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 4. ネットワーク ロードバランサのプロバイダ側でユーザーベースのリダイレクト機能を有効にする場合は、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 5. [追加] をクリックします。
サードパーティ ロードバランサ	1. サード パーティのロード バランサ デバイスを下のボックスにドラッグ アンド ドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[サード パーティ ロード バランサの選択（Select Third Party Load Balancer）]** をクリックし、左側の列でサード パーティ ロード バランサをクリックして選択します。 3. **[コンシューマ インターフェイスの選択（Select Consumer Interface）]** をクリックします。外部としてマークされたインターフェースを選択します。 4. **[プロバイダ インターフェイスの選択（Select Provider Interface）]** をクリックします。内部としてマークされたインターフェイスを選択します。 5. **[追加（Add）]** をクリックします。

ステップ 5 設定が終わったら [Save] をクリックします。

ステップ 6 **[EPG 通信（EPG Communication）]** ダイアログボックスが表示されます。**[詳細に移動（Go to details）]** をクリックして、サービス グラフ テンプレートを確認します。

Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開

このセクションでは、レイヤ4～ レイヤ7サービスを展開する方法について説明します。この手順は、シングル ノードおよびマルチノードの展開に適用できます。

始める前に

- デバイスを構成しました。
- サービス グラフが構成されました。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

[インテント（Intent）] の **[構成（Configuration）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[EPG Communication]** をクリックします。**[EPG通信（EPG Communication）]** ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

ステップ 4 コントラクトを選択します。

a) **[コントラクトの選択（Select Contract）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが表示されます。

b) **[コントラクトの選択（Select Contract）]** ダイアログの左側のペインで、契約をクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが閉じます。

ステップ 5 コンシューマ EPG を追加するには、次の手順を実行します。

a) **[コンシューマ EPG の追加（Add Consumer EPGs）]** をクリックします。**[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログが表示されます。

b) **[コンシューマ EPG の選択（Select Consumer EPGs）]** ダイアログの左側のペインで、チェック ボックスをクリックして、クラウドEPG（内部向けロードバランサの場合）またはクラウド外部EPG(インターネット向けロードバランサの場合) を選択します。**[選択（Select）]** をクリックします。**[コンシューマ EPG の選択（Select Consumer EPGs）]** ダイアログボックスが閉じます。

ステップ 6 プロバイダー EPG を追加するには、次の手順を実行します。

a) **[プロバイダー EPG の追加（Add Provider EPGs）]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログが表示されます。

b) **[プロバイダ EPG の選択（Select Provider EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダ EPG を選択し、**[選択]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログボックスが閉じます。

ステップ 7 サービス グラフを選択するには:

a) **[EPF 通信の構成（EPG Communication Configuration）]** ダイアログで、**[サービス グラフの選択（Select Service Graph）]** をクリックします。**[サービス グラフの選択（Select Service Graph）]** ダイアログボックスが表示されます。

b) **[サービス グラフの選択（Select Service Graph）]** ダイアログの左側のペインで、サービス グラフをクリックして選択し、**[選択（Select）]** をクリックします。**[サービス グラフの選択（Select Service Graph）]** ダイアログボックスが閉じます。

ステップ 8 **[サービス グラフのプレビュー（Service Graph Preview）]** で、**[クラウド ロード バランサ リスナーの追加（Add Cloud Load Balancer Listner）]** をクリックします。**[クラウド ロード バランサ リスナーの追加（Add Cloud Load Balancer Listner）]** ダイアログが表示され、リスナーを追加できます。

リスナーは、デバイスが動作するポートとプロトコルです。

ステップ 9 次の *[クラウドロードバランサ リスナーの追加ダイアログボックスのフィールド（Add Cloud Load Balancer Listener Dialog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *44 :* アプリケーション ゲートウェイ用クラウド ロード バランサ リスナーの追加ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	リスナーの名前を入力します。
[ポート（Port）]	デバイスがトラフィックを受け入れるポートを入力します。
プロトコル	Application Gateway の場合は、クリックして **[HTTP]** または **[HTTPS]** を選択します。
Security Policy	ドロップダウンリストをクリックし、セキュリティポリシーを選択します **(HTTPS** が選択されている場合にのみ選択可能)。
SSL 証明書（SSL Certificate）	SSL 証明書を選択するには **(HTTPS** が選択されている場合にのみ選択可能): **1.** **[SSL 証明書の追加]** をクリックします。 **2.** クリックして、追加する証明書のチェックボックスをオンにします。 **3.** キー リングを選択してください: **1.** **[キー リングの選択]** をクリックします。**[キー リンクの選択（Select Key Ring）]** ダイアログが表示されます。 **2.** **[キー リンクの選択（Select Key Ring）]** ダイアログで、左側の列のキー リングをクリックして選択し、**[選択（Select）]** をクリックします。**[キー リンクの選択（Select Key Ring）]** ダイアログボックスが閉じます。 **4.** **[証明書ストア]** ドロップダウンリストをクリックして、証明書を選択します。 （注） リスナーは複数の証明書を持つことができます。
ルールの追加	ルール設定をデバイス リスナーに追加するには、**[ルールの追加]** をクリックします。**[ルール]** リストに新しい行が表示され、**[ルール設定]** フィールドが有効になります。

[プロパティ（**Properties**）]	説明
ルール設定	

[プロパティ（Properties）]	説明
	[ルール設定（Rule Settings）] ペインで、次のオプションを設定します。 • **名前** ：規則の名前を入力します。 • **ホスト**：ホスト名を入力して、ホストベースの条件を作成します。このホスト名に対して要求が行われると、指定したアクションが実行されます。 • **パス**：パスを入力して、パスベースの条件を作成します。このパスに対して要求が行われると、指定したアクションが実行されます。 • **タイプ**：アクションタイプは、実行するアクションをデバイスに通知します。アクション タイプのオプション: • **固定応答を返す**：次のオプションを使用して応答を返します。 • **固定応答本文**：応答メッセージを入力します。 • **固定応答コード**：応答コードを入力します。 • **固定の応答コンテンツ タイプ**：コンテンツ タイプを選択します。 • **転送**：次のオプションを使用してトラフィックを転送します。 • **ポート**：デバイスがトラフィックを受け入れるポートを入力します。 • **プロトコル**：**[HTTP]** または **[HTTPS]** を選択します。 • **プロバイダー EPG**：トラフィックを処理する Web サーバーを持つ EPG。 • **EPG**：EPG を選択するには: 1. **[EPG の選択]** をクリックします。**[EPG の選択]** ダイアログボックスが表示されます。 2. **[EPG の選択]** ダイアログで、左側の列の EPG をクリックして選択し、**[選択（Select）]** をクリックします。**[EPG の選択]** ダイアログボックスが閉じます。 • **リダイレクト**：次のオプションを使用して、リクエストを別の場所にリダイレクトします。 • **リダイレクト コード**：**[リダイレクト コード]** ドロップダウン リストをクリックして、コードを選択します。 • **リダイレクト ホスト名** ：リダイレクトのホスト名を入力します。 • **リダイレクト パス**：リダイレクト パスを入力します。 • **リダイレクト ポート**：デバイスがトラフィックを受け入れるポートを入力します。

[プロパティ（Properties）]	説明
	• **リダイレクト プロトコル**：**[リダイレクト プロトコル（Redirect Protocol）]** ドロップダウン リストをクリックして、**[HTTP]**、**[HTTPS]**、または **[継承（Inherit）]** を選択します。 • **リダイレクト クエリ**：リダイレクト クエリを入力します。
正常性チェック（Health Checks）	アプリケーション ロードバランサは、高可用性のためにバックエンドプール ターゲットでヘルス チェックを実行します。これは、ヘルス チェックで構成できます。 • **プロトコル**：**[HTTP]** または **[HTTPS]** を選択します。 • **パス**：パスを入力します。 デフォルトは / です • **ポート**：ヘルスチェックを実行するポートを入力します。 • **詳細設定** **異常なしきい値**：このしきい値を構成して、バックエンド ターゲットが異常であると通知されるタイミングを決定します。 • **タイムアウト**：ヘルス チェックのタイムアウトの値を入力します。 • **間隔**：チェックを実行する間隔を決定する時間を秒単位で入力します。 • **成功コード**：成功コードを入力します。デフォルトは 200 ～ 399 です。 • **ルールからホストを使用**：ホスト名をルールから選択する必要がある場合は、チェックボックスをクリックします。 • **ホスト**：**[ルールのホストを使用（Use host from rule）]** がチェックされていない場合は、ヘルス チェックに使用するホスト名を指定します。 完了したら、**[ルールの追加]** をクリックします。

表 *45 :* ネットワーク ロード バランサ用クラウド ロード バランサ リスナーの追加ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	リスナーの名前を入力します。
プロトコル	クリックして **[TCP]** または **[UDP]** を選択します。
[ポート（Port）]	デバイスがトラフィックを受け入れるポートを入力します。

[プロパティ（Properties）]	説明
フロントエンド IP 名	クラウド ロード バランサ リスナーを構成するフロントエンド IP アドレスを選択します。 • **デフォルト IP を使用**：デフォルトのフロントエンド IP アドレスでクラウド ロード バランサ リスナーを構成するには、このオプションを選択します。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。 • **<frontend_ip_name>**：このオプションを選択して、Cloud APIC GUI を使用したサービス デバイスの作成 （274 ページ） でこのインターネット向けネットワーク ロードバランサのサービスデバイスを作成したときに構成した、フロントエンド IP 名に関連付けられた追加のフロントエンド IP アドレスにクラウド ロード バランサー リスナーを構成します。これは、リリース 25.0(3) で導入された新機能です。 詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （214 ページ）を参照してください。
ルール設定	**[ルール設定（Rule Settings）]** ペインで、次のオプションを設定します。 • **名前** ：規則の名前を入力します。 • **アクション タイプ**：デフォルトで `[転送先（Forward to）]` に設定されています。トラフィックは、以下で選択したプロトコルを使用して、選択した EPG のポートに転送されます。 • **ポート**：バックエンド プール サーバがロードバランサからのトラフィックを受け入れるポートを入力します。 • **プロトコル**：クリックして **[TCP]** または **[UDP]** を選択します。 • **EPG**：Web サーバがトラフィックを処理する EPG。
正常性チェック（Health Checks）	ロード バランサは、高可用性のためにバックエンド プール ターゲットでヘルス チェックを実行します。ここで構成できます。· • **プロトコル**：クリックして **[TCP]**、**[HTTP]** または **[HTTPS]** を選択します。 • **ポート**：ヘルス チェックを実行するポートを入力します。 • **詳細設定** 異常なしきい値 - このしきい値を構成して、バックエンド ターゲットが異常であると通知されるタイミングを決定します。 • **間隔**：チェックを実行する間隔を決定する時間を秒単位で入力します。 終了したら、[Add] をクリックします。

ステップ 10 終了したら、[Add] をクリックします。
サービス グラフが展開されます。

REST API を使用したサービス グラフの展開

次のセクションでは、REST API を使用してサービス グラフを展開する方法について説明します。

REST API を使用したインターネット向けロード バランサの作成

この例では、REST API を使用して内部向けのロード バランサを作成する方法を示します。

ステップ 1 アプリケーション ゲートウェイ（アプリケーション ロード バランサ）の内部向けロード バランサを作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
        <cloudLB scheme="internal" type="application" name="alb-151-15" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
        </cloudLB>
      </fvTenant>
</polUni>
```

ステップ 2 Azure ロードバランシング（ネットワーク ロードバランサ）の内部向けロードバランサを作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[subscription id]-vendor-azure" />
        <cloudLB scheme="internal" type="network" name="nlb-151-15" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
        </cloudLB>
    </fvTenant>
</polUni>
```

ステップ 3 すべてのトラフィックを許可について （217 ページ） で説明されている **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを使用して、Azure ロード バランシング（ネットワーク ロード バランサ）用の内部向けロード バランサを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[subscription id]-vendor-azure" />
        <cloudLB scheme="internal" type="network" name="nlb-151-15" allowAll="true" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
        </cloudLB>
    </fvTenant>
</polUni>
```

REST API を使用したインターネット向けロード バランサの構成

この例では、REST API を使用してインターネット向けのロード バランサを作成する方法を示します。

ステップ 1 アプリケーション ゲートウェイ（アプリケーション ロード バランサ）のインターネット向けロード バランサを作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />

        <cloudLB scheme="internet" type="application" name="alb-151-15" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
        </cloudLB>


      </fvTenant>
</polUni>
```

ステップ 2 インターネット向けネットワーク ロード バランサ：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->

<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
        <cloudLB scheme="internet" type="network" name="nlb-151-15" status="">
            <cloudVip name="IP1"/>
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
        </cloudLB>
    </fvTenant>
</polUni>
```

この例では、以下のようになっています。

- cloudLB ラインは、単一のデフォルト IP アドレスを持つインターネット向けのネットワーク ロード バランサを作成するために使用されます。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。
- cloudVip ラインは、インターネットに接続するネットワーク ロード バランサの追加フロントエンド IP アドレスを作成するために使用されます。これは、リリース 25.0(3) で導入された新機能です。詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （214 ページ）を参照してください。

REST API を使用したサードパーティ ファイアウォールの作成

この例では、REST API を使用したサードパーティ ファイアウォールを作成する方法を示します。

ステップ 1 サードパーティ ファイアウォールを作成するには：

例：

```
<cloudLDev name="HubFW" svcType="FW" status="">
    <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
    <cloudLIf name="provider">
       <cloudEPSelector name="east" matchExpression="IP=='{{eastus_FwUntrustSubnet}}'" status=""/>

    </cloudLIf>
    <cloudLIf name="consumer">
        <cloudEPSelector name="east" matchExpression="IP=='{{eastus_FwTrustSubnet}}'" status=""/>
    </cloudLIf>
</cloudLDev>
```

ステップ 2 すべてのトラフィックを許可について （217 ページ） で説明されている **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを使用してサードパーティ ファイアウォールを作成するには、次の手順を実行します。

例：

```
<cloudLDev name="HubFW" svcType="FW" status="">
    <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
    <cloudLIf name="provider"  allowAll="true" status="">
        <cloudEPSelector name="1" matchExpression="IP=='10.1.1.0/28'" status=""/>
    </cloudLIf>
    <cloudLIf name="consumer"  allowAll="true" status="">
        <cloudEPSelector name="east" matchExpression="IP=='10.1.2.0/28'" status=""/>
    </cloudLIf>
</cloudLDev>
```

REST API を使用したサードパーティ ロード バランサの作成

この例では、REST API を使用してサードパーティ ロード バランサを作成する方法を示します。

この例では、REST API を使用してサードパーティ ロード バランサを作成する方法を示します。

例：

```
<cloudLDev name="ThirdPartyLB" svcType="ADC" status="">
    <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
    <cloudLIf name="external">
        <cloudEPSelector name="ExtInterfaceSelector" matchExpression="IP=='{{ExtInterfaceSubnet}}'"
 status=""/>
    </cloudLIf>
    <cloudLIf name="internal">
        <cloudEPSelector name="IntInterfaceSelector" matchExpression="IP=='{{IntInterfaceSubnet}}'"
 status=""/>
    </cloudLIf>
</cloudLDev>
```

アプリケーション ゲートウェイの REST API を使用してサービス グラフの作成

この例では、REST API を使用してサービス グラフを作成する方法を示します。

この例では、REST API を使用してサービス グラフを作成する方法を示します。

アプリケーション ゲートウェイのサービス グラフを作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">

       <vnsAbsGraph name="c15_g1" type="cloud" status="">
      <vnsAbsTermNodeProv name="p1">
        <vnsAbsTermConn/>
      </vnsAbsTermNodeProv>
      <vnsAbsTermNodeCon name="c1">
        <vnsAbsTermConn/>
      </vnsAbsTermNodeCon>
      <vnsAbsNode managed="yes" name="N1" funcType="GoTo">
          <vnsRsNodeToCloudLDev tDn="uni/tn-tn15/clb-alb-151-15"/>
        <vnsAbsFuncConn name="provider"/>
        <vnsAbsFuncConn name="consumer"/>
      </vnsAbsNode>
      <vnsAbsConnection  connDir="consumer" connType="external" name="con1">
          <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeCon-c1/AbsTConn"/>
         <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-consumer"/>

      </vnsAbsConnection>
      <vnsAbsConnection connDir="provider" connType="internal"  name="con2">
          <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeProv-p1/AbsTConn"/>
         <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-provider"/>

      </vnsAbsConnection>
```

```
  </vnsAbsGraph>

  </fvTenant>
</polUni>
```

Azure ロード バランサの REST API を使用してサービス グラフを作成する

Azure ロード バランサのサービス グラフを作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- api/node/mo/uni/.xml -->

<polUni>

<fvTenant name="tn15">

<vnsAbsGraph name="c15_g1" type="cloud" status="">

<vnsAbsTermNodeProv name="p1">

<vnsAbsTermConn />

</vnsAbsTermNodeProv>

<vnsAbsTermNodeCon name="c1">

<vnsAbsTermConn />

</vnsAbsTermNodeCon>

<vnsAbsNode managed="yes" name="N1" funcType="GoTo">

<vnsRsNodeToCloudLDev tDn="uni/tn-tn15/clb-nlb-151-15" />

<vnsAbsFuncConn name="provider" />

<vnsAbsFuncConn name="consumer" />

</vnsAbsNode>

<vnsAbsConnection connDir="consumer" connType="external" name="con1">

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeCon-c1/AbsTConn"
/>

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-consumer"
 />

</vnsAbsConnection>

<vnsAbsConnection connDir="provider" connType="internal" name="con2">

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeProv-p1/AbsTConn"
/>

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-provider"
 />

</vnsAbsConnection>
```

```
</vnsAbsGraph>

</fvTenant>

</polUni>
```

サード パーティ ロード バランサの REST API を使用してサービス グラフを作成する

サードパーティのロードバランサのサービス グラフを作成するには、次の手順を実行します。

```
<polUni>
<fvTenant name="infra" >
<!-- Abs Graph Creation -->
<vnsAbsGraph name="{{graphName}}" uiTemplateType="UNSPECIFIED" type="cloud" status="">
<vnsAbsTermNodeProv name="T2">
<vnsOutTerm/>
<vnsInTerm />
<vnsAbsTermConn attNotify="no" name="1" />
</vnsAbsTermNodeProv>
<vnsAbsTermNodeCon name="T1" >
<vnsOutTerm/>
<vnsInTerm />
<vnsAbsTermConn attNotify="no" name="1" />
</vnsAbsTermNodeCon>
<vnsAbsNode funcTemplateType="ADC_TWO_ARM" name="{{F5Name}}" managed="no">
<vnsRsNodeToCloudLDev tDn="uni/tn-infra/cld-{{F5Name}}" />
<vnsAbsFuncConn attNotify="no" name="consumer" deviceLIfName="external"/>
<vnsAbsFuncConn attNotify="no" name="provider" deviceLIfName="internal"/>
</vnsAbsNode>
<vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="ConsTermToF5">
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsTermNodeCon-T1/AbsTConn"/>
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsNode-{{F5Name}}/AbsFConn-consumer"/>
</vnsAbsConnection>
<vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="F5ToProv">
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsNode-{{F5Name}}/AbsFConn-provider" />
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsTermNodeProv-T2/AbsTConn"/>
</vnsAbsConnection>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

REST API を使用してマルチノード サービス グラフを作成する

この例では、REST API を使用してマルチノード サービス グラフを作成する方法を示します。

マルチノード サービス グラフを作成するには、次の例のような投稿を入力します。

```
<polUni>
 <fvTenant name="tn12_iar_iavpc" status="">
  <fvRsCloudAccount  tDn="uni/tn-infra/[SubscriptionId]-vendor-azure"/>
  <fvCtx name="vrf50" status=""/>
  <fvCtx name="vrf60" status=""/>
  <cloudVpnGwPol name="VgwPol0"/>
```

```
<cloudCtxProfile name="c50" status="">
 <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
 <cloudRsToCtx tnFvCtxName="vrf50"/>
 <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
 <cloudCidr addr="12.3.0.0/16" primary="true" status="">
  <cloudSubnet ip="12.3.30.0/24" status="" name="GatewaySubnet" usage="gateway">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.2.0/24" status="" name="ALBSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.1.0/24" status="" name="FwMgmtSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.3.0/24" status="" name="FwUntrustSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.4.0/24" status="" name="FwTrustSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.5.0/24" status="" name="ConsumerSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
 </cloudCidr>
</cloudCtxProfile>
<cloudCtxProfile name="c60" status="">
 <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus2"/>
 <cloudRsToCtx tnFvCtxName="vrf60"/>
 <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
 <cloudCidr addr="12.4.0.0/16" primary="true" status="">
  <cloudSubnet ip="12.4.1.0/24" status="" name="ProviderSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.4.2.0/24" status="" name="NLBSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.4.30.0/24" status="" name="GatewaySubnet" usage="gateway">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
  </cloudSubnet>
 </cloudCidr>
</cloudCtxProfile>
<cloudApp name="ap50" status="">
 <cloudEPg name="ap50vrf50epg1" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
  <fvRsCons tnVzBrCPName="con50"/>
  <fvRsProv tnVzBrCPName="con60"/>
  <cloudEPSelector matchExpression="IP=='12.3.5.0/24'" name="100"/>
 </cloudEPg>
 <cloudEPg name="ap50vrf50epg2" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
  <fvRsProv tnVzBrCPName="con60"/>
  <cloudEPSelector matchExpression="IP=='12.3.1.0/24'" name="100"/>
 </cloudEPg>
 <cloudExtEPg routeReachability="internet" name="ap50extepg1">
  <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
  <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
  <fvRsCons tnVzBrCPName="con60"/>
 </cloudExtEPg>
</cloudApp>
<cloudApp name="ap60" status="">
 <cloudEPg name="ap60vrf60epg1" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="vrf60"/>
  <fvRsProv tnVzBrCPName="con50"/>
  <fvRsProv tnVzBrCPName="con70"/>
```

```
    <cloudEPSelector matchExpression="IP=='12.4.1.0/24'" name="100"/>
   </cloudEPg>
   <cloudExtEPg routeReachability="internet" name="ap60extepg1">
    <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
    <cloudRsCloudEPgCtx tnFvCtxName="vrf60"/>
    <fvRsCons tnVzBrCPName="con70"/>
   </cloudExtEPg>
  </cloudApp>
  <vzBrCP name="con50" scope="tenant" status="">
   <vzSubj name="con50">
    <vzRsSubjFiltAtt tnVzFilterName="f10"/>
    <vzRsSubjGraphAtt tnVnsAbsGraphName="g1" status=""/>
   </vzSubj>
  </vzBrCP>
  <vzBrCP name="con60" scope="tenant" status="">
   <vzSubj name="con60">
    <vzRsSubjFiltAtt tnVzFilterName="f20"/>
   </vzSubj>
  </vzBrCP>
  <vzBrCP name="con70" scope="context" status="">
   <vzSubj name="con70">
    <vzRsSubjFiltAtt tnVzFilterName="f20"/>
   </vzSubj>
  </vzBrCP>
  <vzFilter name="f10" status="">
   <vzEntry etherT="ip" prot="icmp" name="f10entry1" status=""/>
   <vzEntry etherT="ip" prot="udp" dFromPort="1" dToPort="65535" name="f10entry2" status=""/>
   <vzEntry etherT="ip" prot="tcp" dFromPort="1" dToPort="65535" name="f10entry3" status=""/>
  </vzFilter>
  <vzFilter name="f20" status="">
   <vzEntry etherT="ip" prot="tcp" dFromPort="http" dToPort="http" name="f20entry1" status=""/>
   <vzEntry etherT="ip" prot="tcp" dFromPort="https" dToPort="https" name="f20entry2" status=""/>
   <vzEntry etherT="ip" prot="tcp" dFromPort="22" dToPort="22" name="f20entry3" status=""/>
  </vzFilter>
  <cloudLB name="FrontALB" type="application" scheme="internal" >
   <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn12_iar_iavpc/ctxprofile-c50/cidr-[12.3.0.0/16]/subnet-[12.3.2.0/24]"/>
  </cloudLB>
  <cloudLDev name="FW" svcType="FW" status="">
   <cloudRsLDevToCtx tDn="uni/tn-tn12_iar_iavpc/ctx-vrf50" />
   <cloudLIf name="provider" >
    <cloudEPSelector name="1" matchExpression="custom:tagp=='trustFW'"/>
   </cloudLIf>
   <cloudLIf name="consumer" >
    <cloudEPSelector name="1" matchExpression="custom:tagp=='untrustFW'"/>
   </cloudLIf>
  </cloudLDev>
  <cloudLB name="BackNLB" type="network" scheme="internal" >
   <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn12_iar_iavpc/ctxprofile-c60/cidr-[12.4.0.0/16]/subnet-[12.4.2.0/24]"/>
  </cloudLB>
  <vnsAbsGraph name="g1" type="cloud" status=""  >
   <vnsAbsTermNodeProv name="Input1" >
    <vnsAbsTermConn  name="C1"/>
   </vnsAbsTermNodeProv>
   <vnsAbsTermNodeCon descr="" name="Output1" nameAlias="" ownerKey="" ownerTag="">
    <vnsAbsTermConn name="C2" />
   </vnsAbsTermNodeCon>
   <vnsAbsNode funcType="GoTo" name="N1" managed="yes" funcTemplateType="ADC_ONE_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/clb-FrontALB" />
    <vnsAbsFuncConn attNotify="no" descr="" name="provider" nameAlias="" ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" name="consumer" nameAlias="" ownerKey="" ownerTag=""/>
    <cloudSvcPolicy tenantName="tn12_iar_iavpc" contractName="con50" subjectName="con50" >
     <cloudListener name="http_listener1" port="80" protocol="http">
```

```
      <cloudListenerRule name="rule1" priority="20" default="yes" >
       <cloudRuleAction type="forward" port="80" protocol="http"/>
      </cloudListenerRule>
     </cloudListener>
    </cloudSvcPolicy>
   </vnsAbsNode>
   <vnsAbsNode funcType="GoTo" name="N2" managed="no" funcTemplateType="ADC_TWO_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/cld-FW" />
    <vnsAbsFuncConn attNotify="no" descr="" connType="snat_dnat" name="provider" nameAlias=""
ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" connType="none" name="consumer" nameAlias="" ownerKey=""
 ownerTag=""/>
   </vnsAbsNode>
   <vnsAbsNode funcType="GoTo" name="N3" managed="yes" funcTemplateType="ADC_ONE_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/clb-BackNLB" />
    <vnsAbsFuncConn attNotify="no" descr="" name="provider" nameAlias="" ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" name="consumer" nameAlias="" ownerKey="" ownerTag=""/>
    <cloudSvcPolicy tenantName="tn12_iar_iavpc" contractName="con50" subjectName="con50" >
     <cloudListener name="http_listener1" port="80" protocol="tcp">
      <cloudListenerRule name="rule1" priority="20" default="yes" >
       <cloudRuleAction type="forward" port="80" protocol="tcp"
epgdn="uni/tn-tn12_iar_iavpc/cloudapp-ap60/cloudepg-ap60vrf60epg1"/>
      </cloudListenerRule>
     </cloudListener>
    </cloudSvcPolicy>
   </vnsAbsNode>
   <vnsAbsConnection connDir="provider" connType="external" name="CON4">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N3/AbsFConn-provider"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsTermNodeProv-Input1/AbsTConn"/>

   </vnsAbsConnection>
   <vnsAbsConnection  connDir="consumer" connType="external" name="CON1">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsTermNodeCon-Output1/AbsTConn"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N1/AbsFConn-consumer"/>

   </vnsAbsConnection>
   <vnsAbsConnection  connDir="consumer" connType="external" name="CON2">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N1/AbsFConn-provider"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N2/AbsFConn-consumer"/>

   </vnsAbsConnection>
   <vnsAbsConnection  connDir="consumer" connType="external" name="CON3">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N2/AbsFConn-provider"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N3/AbsFConn-consumer"/>

   </vnsAbsConnection>
  </vnsAbsGraph>
 </fvTenant>
</polUni>
```

REST API を使用してリダイレクトでマルチノード サービス グラフを作成する

この例では、REST API を使用してマルチノード サービス グラフを作成する方法を示します。

ステップ 1 インフラ テナントを設定するには、次の手順を実行します。

```
<polUni>
    <fabricInst>
        <commPol name="default">
            <commSsh name="ssh" adminSt="enabled" passwordAuth="enabled" />
        </commPol>
        <dnsProfile name="default">
            <dnsProv addr="172.23.136.143" preferred="yes" status=""/>
        </dnsProfile>
    </fabricInst>
   <fvTenant name="infra">
      <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
      <cloudAccount name="insbu" id="{{subscriptionId}}" vendor="azure" accessType="credentials"
status="">
        <cloudRsCredentials tDn="uni/tn-infra/credentials-cApicApp"/>
      </cloudAccount>
      <cloudCredentials name="cApicApp" keyId="{{accessKeyId}}" key="{{accessKey}}" httpProxy="">
        <cloudRsAD tDn="uni/tn-infra/ad-{{adId}}"/>
      </cloudCredentials>
    <cloudAD name="CiscoINSBUAd" id="{{adId}}" />
    <cloudApicSubnetPool subnet="10.10.1.0/24" />
    <cloudtemplateInfraNetwork name="default" numRoutersPerRegion="2" vrfName="overlay-1"
numRemoteSiteSubnetPool="1" status="">
         <cloudtemplateProfile name="default" routerUsername="cisco" routerPassword="ins3965" />
         <cloudtemplateExtSubnetPool subnetpool="11.11.0.0/16" status=""/>
         <cloudtemplateExtNetwork name="default" status="">
            <cloudRegionName provider="azure" region="{{region}}" />
            <cloudtemplateVpnNetwork name="default">
               <cloudtemplateIpSecTunnel peeraddr="{{peerAddress}}"/>
               <cloudtemplateOspf area="0.0.0.1" />
            </cloudtemplateVpnNetwork>
         </cloudtemplateExtNetwork>
         <cloudtemplateIntNetwork name="default">
            <cloudRegionName provider="azure" region="{{region}}"/>
         </cloudtemplateIntNetwork>
    </cloudtemplateInfraNetwork>
   </fvTenant>
   <cloudDomP>
      <cloudBgpAsP asn="1111"/>
      <cloudProvP vendor="azure">
         <cloudRegion adminSt="managed" name="{{region}}">
            <cloudZone name="default"/>
         </cloudRegion>
      </cloudProvP>
  </cloudDomP>
</polUni>
```

ステップ 2 ハブ VNet でサービス デバイスを構成するには:

```
<polUni>
    <fvTenant name="infra">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
        <cloudCtxProfile name="ct_ctxprofile_{{region}}" status="modified">
          <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

            <cloudCidr name="cidr1" addr="{{HubCidrSvc}}" primary="no" status="">
                <cloudSubnet ip="{{HubNLBSubnet}}" name="HubNLBSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{HubFWSubnetInt}}" name="HubFWSubnetInt" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
```

```
                </cloudSubnet>
                <cloudSubnet ip="{{HubFWSubnetExt}}" name="HubFWSubnetExt" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{HubFWMgmtSubnet}}" name="HubFWMgmtSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{ConsHubEPgSubnet}}" name="ConsHubEPgSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
             </cloudCidr>
        </cloudCtxProfile>
        <cloudLDev name="{{FWName}}" status="">
            <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-{{ServicevVNetName}}"/>
            <cloudLIf name="external" >
                <cloudEPSelector matchExpression="custom:EPG=='FwExt'"  name="1"/>
            </cloudLIf>
            <cloudLIf name="internal" >
               <cloudEPSelector matchExpression="custom:EPG=='FwInt'"  name="1"/>
            </cloudLIf>
        </cloudLDev>
       <cloudLB name="{{NLBName}}" type="network" scheme="internal" size="small" instanceCount="2"
 status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-infra/ctxprofile-ct_ctxprofile_{{region}}/cidr-[{{HubCidrSvc}}]/subnet-[{{HubNLBSubnet}}]"
 status=""/>
        </cloudLB>
    </fvTenant>
</polUni>
```

ステップ 3 プロバイダとスポークのグラフを構成するには:

```
<polUni>
    <fvTenant name="{{tnNameProv}}" status="" >
        <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
        <fvCtx name="{{ProviderVNetName}}"/>
        <cloudCtxProfile name="{{ProviderVNetName}}" status="">
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
           <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

            <cloudRsToCtx tnFvCtxName="{{ProviderVNetName}}"/>
            <cloudCidr name="cidr1" addr="{{VnetCidrProv}}" primary="yes" status="">
                <cloudSubnet ip="{{ProviderSubnet}}" name="ProviderSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{BackALBSubnet}}" name="BackALBSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
        <!-- contract-->
        <vzFilter descr="" name="HttpsFilter" ownerKey="" ownerTag="">
            <vzEntry dFromPort="443" dToPort="443" etherT="ip" name="https" prot="tcp" status=""/>
            <vzEntry dFromPort="80" dToPort="80" etherT="ip" name="http" prot="tcp" status=""/>
            <vzEntry dFromPort="22" dToPort="22" etherT="ip" name="ssh" prot="tcp" status=""/>
        </vzFilter>
        <vzBrCP name="{{contractName}}" scope="global" status="">
            <vzSubj name="Sub1" revFltPorts="yes">
```

```
                <vzRsSubjGraphAtt directives="" tnVnsAbsGraphName="{{graphName}}"/>
                <vzRsSubjFiltAtt tnVzFilterName="HttpsFilter"/>
            </vzSubj>
        </vzBrCP>
        <!-- cloud App Profile-->
        <cloudApp name="provApp" status="">
            <cloudEPg name="App" status="">
                <cloudRsCloudEPgCtx tnFvCtxName="{{ProviderVNetName}}"/>
                <cloudEPSelector matchExpression="custom:EPG=='App'" name="1"/>
                <fvRsProv status="" tnVzBrCPName="{{contractName}}"/>
                <fvRsProv tnVzBrCPName="mgmt_common"/>
            </cloudEPg>
        </cloudApp>
        <!-- Abs Graph Creation -->
        <vnsAbsGraph name="{{graphName}}" uiTemplateType="UNSPECIFIED" type="cloud">
            <vnsAbsTermNodeProv name="T2">
                <vnsOutTerm/>
                <vnsInTerm />
                <vnsAbsTermConn attNotify="no" name="1" />
            </vnsAbsTermNodeProv>
            <vnsAbsTermNodeCon name="T1" >
                <vnsOutTerm/>
                <vnsInTerm />
                <vnsAbsTermConn attNotify="no" name="1" />
            </vnsAbsTermNodeCon>
            <vnsAbsNode  name="{{NLBName}}" managed="yes" >
                <vnsRsNodeToCloudLDev tDn="uni/tn-infra/clb-{{NLBName}}" status=""/>
                <cloudSvcPolicy tenantName="{{tnNameProv}}" contractName="{{contractName}}"
subjectName="Sub1" status="">
                  <cloudHealthProbe name="http_listener1-rule1" protocol="tcp" port=22 interval=15
 unhealthyThreshold=2/>
                   <cloudListener name="http_listener1" port="80" protocol="tcp" status="">
                       <cloudListenerRule name="rule1" default="true">
                           <cloudRuleAction type="haPort" port="80" protocol="tcp"
healthProbe="http_listener1-rule1"/>
                       </cloudListenerRule>
                   </cloudListener>
                </cloudSvcPolicy>
                <vnsAbsFuncConn attNotify="no" name="provider" connType="redir"/>
                <vnsAbsFuncConn attNotify="no" name="consumer" connType="redir"/>
            </vnsAbsNode>
            <vnsAbsNode funcTemplateType="FW_ROUTED" name="{{FWName}}" managed="no">
                <vnsRsNodeToCloudLDev tDn="uni/tn-infra/cld-{{FWName}}" />
                <vnsAbsFuncConn attNotify="no" name="consumer" deviceLIfName="internal"/>
                <vnsAbsFuncConn attNotify="no" name="provider" deviceLIfName="internal"/>
            </vnsAbsNode>
            <vnsAbsNode  name="{{BackALBName}}" managed="yes">
                <vnsRsNodeToCloudLDev tDn="uni/tn-{{tnNameProv}}/clb-{{BackALBName}}"/>
                <cloudSvcPolicy tenantName="{{tnNameProv}}" contractName="{{contractName}}"
subjectName="Sub1" status="">
                   <cloudListener name="http_listener1" port="80" protocol="http" status="">
                       <cloudListenerRule name="rule1" default="true">
                           <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-{{tnNameProv}}/cloudapp-provApp/cloudepg-App"/>
                       </cloudListenerRule>
                   </cloudListener>
                </cloudSvcPolicy>
                <vnsAbsFuncConn attNotify="no" name="provider"/>
                <vnsAbsFuncConn attNotify="no" name="consumer"/>
            </vnsAbsNode>
          <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="ConsTermToNLB">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsTermNodeCon-T1/AbsTConn"/>
```

```
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{NLBName}}/AbsFConn-consumer"/>
              </vnsAbsConnection>
             <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="NLBToFW">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{NLBName}}/AbsFConn-provider" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{FWName}}/AbsFConn-consumer"/>
              </vnsAbsConnection>
             <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="FWToBackALB">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{FWName}}/AbsFConn-provider" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{BackALBName}}/AbsFConn-consumer"/>
              </vnsAbsConnection>
             <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="BackALBToProv">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{BackALBName}}/AbsFConn-provider" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsTermNodeProv-T2/AbsTConn"/>
              </vnsAbsConnection>
        </vnsAbsGraph>
        <cloudLB name="{{BackALBName}}" type="application" scheme="internal" size="small"
instanceCount="2">
              <cloudRsLDevToCloudSubnet
tDn="uni/tn-{{tnNameProv}}/ctxprofile-{{ProviderVNetName}}/cidr-[{{VnetCidrProv}}]/subnet-[{{BackALBSubnet}}]"
 status=""/>
        </cloudLB>
  </fvTenant>
</polUni>
```

ステップ 4 コンシューマを構成し、プロバイダで定義されたコントラクトをインポートするには:

```
<polUni>
    <fvTenant name="{{tnNameCons}}" >
        <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
        <fvCtx name="{{ConsumerVNetName}}"/>
        <cloudCtxProfile name="{{ConsumerVNetName}}" status="">
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
           <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

            <cloudRsToCtx tnFvCtxName="{{ConsumerVNetName}}"/>
            <cloudCidr name="cidr1" addr="{{VnetCidrCons}}" primary="yes" status="">
                <cloudSubnet ip="{{ConsumerSubnet}}" name="ConsumerSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
        <vzCPIf name="imported_{{contractName}}">
            <vzRsIf tDn="uni/tn-{{tnNameProv}}/brc-{{contractName}}" />
        </vzCPIf>
        <!-- cloud App Profile-->
        <cloudApp name="consApp" status="">
            <cloudEPg name="Web" status="">
                <cloudRsCloudEPgCtx tnFvCtxName="{{ConsumerVNetName}}"/>
                <cloudEPSelector matchExpression="custom:EPG=='Web'" name="1"/>
                <fvRsConsIf tnVzCPIfName="imported_{{contractName}}"/>
                <fvRsProv tnVzBrCPName="mgmt_common"/>
            </cloudEPg>
```

```
        </cloudApp>
  </fvTenant>
</polUni>
```

REST API を使用してサービス グラフを添付する

この例では、REST API を使用してサービス グラフを作成する方法を示します。

ステップ 1 Application Gateway のサービス グラフをアタッチするには:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">

    <vzBrCP name="c1">
        <vzSubj name="c1">
            <vzRsSubjGraphAtt tnVnsAbsGraphName="c15_g1"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

ステップ 2 Azure Load Balancing のサービス グラフをアタッチするには:

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- api/node/mo/uni/.xml -->

<polUni>

<fvTenant name="tn15">

<vzBrCP name="c1">

<vzSubj name="c1">

<vzRsSubjGraphAtt tnVnsAbsGraphName="c15_g1" />

</vzSubj>

</vzBrCP>

</fvTenant>

</polUni>
```

REST API を使用した HTTPS サービス ポリシーの構成

この例では、REST API を使用して HTTP サービス ポリシーを作成する方法を示します。

ステップ 1 Application Gateway の HTTP サービス ポリシーを作成するには：

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="http_listener1" port="80" protocol="http" status="">
            <cloudListenerRule name="rule1" priority="10" default="yes" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectRule" priority="20">
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="redirect" RedirectPort="8080"/>
            </cloudListenerRule>
            <cloudListenerRule name="FixedRspRule" priority="30">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleAction type="fixedResponse" FixedResponseCode="200"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectHPRule" priority="40" status="">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
          </cloudListener>
        </cloudSvcPolicy>
      </vnsAbsNode>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```

ステップ 2 ネットワーク ロード バランサの HTTP サービス ポリシーを作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>

<polUni>
    <fvTenant name="tn15">
        <vnsAbsGraph name="CloudGraph" type="cloud" status="">
            <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
               <cloudSvcPolicy tenantName=" tn15" contractName="httpFamily" subjectName="consubj">

                    <cloudListener name="tcp_listener" port="80" protocol="tcp" status="">
                        <cloudListenerRule name="rule1" priority="10" default="yes" status="">
                            <cloudRsListenerToVip tDn="uni/tn-infra/clb-NLB/vip-IP1" status=""/>
                           <cloudRuleAction type="forward" port="80" protocol="tcp" epgdn="uni/tn-
 tn15/cloudapp-ap/cloudepg-provEPG" />
                        </cloudListenerRule>
                    </cloudListener>
                    <cloudListener name="udp_listener" port="55" protocol="udp" status="">
                        <cloudListenerRule name="rule1" priority="10" default="yes" status="">
                            <cloudRsListenerToVip tDn="uni/tn-infra/clb-NLB/vip-IP1" status=""/>
                           <cloudRuleAction type="forward" port="55" protocol="udp" epgdn="uni/tn-
 tn15/cloudapp-ap/cloudepg-provEPG" />
                        </cloudListenerRule>
                    </cloudListener>
                </cloudSvcPolicy>
            </vnsAbsNode>
        </vnsAbsGraph>
```

```
    </fvTenant>
</polUni>
```

このドキュメントで前述したように、ネットワーク ロードバランサで定義されている場合、リスナー ルールとルールアクションの設定は、ロードバランサのフロントエンド構成からバックエンドプールへのマッピングを構築します。この例では、以下のようになっています。

- `cloudListenerRule` 行は、単一のフロントエンド IP アドレスを使用してリスナーを構成するために使用されますが、Cisco Cloud APIC 上のインターネットに接続されたネットワーク ロード バランサ用に異なるポートとプロトコルの組み合わせを使用します。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。
- `cloudRsListenerToVip` 行は、Cisco Cloud APIC 上のインターネット向けネットワーク ロード バランサの複数のフロントエンドでリスナー ルールを構成するために使用されます。各フロントエンドは、フロントエンド IP アドレス、ポート、およびプロトコルのタプルの組み合わせとして表されます。これは、リリース 25.0(3) で導入された新機能です。詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （214 ページ）を参照してください。

REST API を使用したキー リングの設定

この例では、REST API を使用したキー リングのリーク ルートを構成する方法を示します。キー リング構成の詳細については、*Cisco APIC* 基本構成ガイドを参照してください。

（注） この手順は、アプリケーション ゲートウェイにのみ適用されます。

キー リングを設定するには:

```
<polUni>
     <fvTenant name="tn15" >
    <cloudCertStore>
    <pkiKeyRing status="" name="lbCert" tp="lbTP" key="-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA4DGxaK+RHv/nToHLnmDBq2BfLimgX/zNJQC9bGuzr8Mj7dm0
XuHfQYGv0h1PtL4Pdxf5qjB0NbHjAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCRe
Ginn/CgF75QPIed568eScNDZPt/eMeHAuRX/PykKUatWWncGanjvHqc+SOLPF6TD
gQ5nwOHHFvyM2DY8bfdYWrWmGsO7JqZzbPMptA2QWblILsSoIrdkIIgf6ZfYy/EN
bH+nYN2rJT8lzYsxz0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8KOfdCZPEq
8takiWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQABAoIBAQDQqA9IslYrdtqN
q6mZ3s2BNfF/4kgb7gn0DWs+9EJJLCJNZVhFEo2ZxxyfPp6HRnjYS50W83/E1anD
+GD1bSucTuxqFWIQVh7r1ebYZIWk+NYSjr5yNVxux8U2hCNNV8WWVqkJjKcUqICB
Bm47FKj53LV46zE0gyCaibFrYxZJ9+farGneyBdnoV+3thmez7534KCi0t3J3Eri
lgSY3ql6hPXB2ZXAP4jdAoLgWDU4I1M6OqOiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5GlfV2A4xTBQMCTZUZJ9fYAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphEDlAoGBAPVlvKfGW46qqRnYovfryxxz4OMlsVSgcJpQTQtBQi2koJ8OwEZJ
2s+CX0r+oDqwP23go/QEVYVkcic9RGkJBNge1+dm/bTjzgMQYtqSCNtecTsZD5JN
y1jkciizznDkjcjReSZ2kh3dGXIbRiYk7ezp2z7EKfDrHe5x5ouGMgCnAoGBAOnh
buDEohv8KJaB+DiUfhtoa3aKNPBO+zWPCHp0HFGjPXshJcIYZc1GcycmuDKVNnDd
MxhE/yOnQHowi4T9FMLpz5yh5zuCUVqOBgB1P6MzbC5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCWlOAFJRw3c/OiESwLMzchsl8RnbwOi6kDAoGBANVlzmPb07zB3eGTCU0t
KGiqwFLncUkVaDZZRFZYPpNwiRkoe73j9brkNbgCqxW+NLp5UjoeFry0N6y106q/
ZA4I7FnXryLBw2HYuw41Vixl+XOZ/HeO3RmFN1z717dGmaGbv43aKIB9x+X5n8wF
```

```
6z1NtBHmBk7yNwom1IRag1sbAoGAX0p4cJ/tJNXSe7AswHDQCL68uimJdDfZ5nKG
k83nE+Qc0qQozDJAmCiSFmuSNRnSep3FiafjBFXK0X4h+mdbJCc7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztzTn+as6xKOUATEezy9DK9zMWzQhhtaY
m9yZTp0CgYEA1UtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdGJt88ezM1Oej
Pdoab0G2PcfgJZoTSGk7N4XArVKeq7pgZ0kwcYAshO6A2Hal+D1z/bGoZP+kmD/x
Ny82phxYOXCnEc5Vv92lU59+j7e067UFLAYJe6fu+oFImvofRnP4DIQ=
-----END RSA PRIVATE KEY-----" cert="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRIwEAYDVQQK
EwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVoXDTE5MTAwMjIwNTMwNVowgY0xCzAJBgNVBAYTAlVTMQswCQYDVQQI
EwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBgNVBAoTCU15Q29tcGFueTEOMAwG
A1UECxMFTXlPcmcxGDAWBgNVBAMUDyouYW1hem9uYXdzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDgMbFor5Ee/+dOgcueYMGrYF8uKaBf/M0lAL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXvlA8h53nrx5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqeO8epz5I4s8XpMOBDmfA
4ccW/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZHShFAdOI3Y2INj9lXrfLEJd8uD2qk1kK4Pwo590Jk8Sry1qSJ
YHGJHn8dE+xxYB1ZCyiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMEgbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BAcTCFNhbiBKb3NlMRIwEAYDVQQKEwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvbmF3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAe/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5ml5baCYZZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoelewv+wRl0oVRChlTfKtXO68TUk6vrqpw76hKfOHIa7b2h1IIMdq6VA/
+A5FQ0xqYfqKdVd2RaINpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfGPlVesFEyJEL
gHBUiPt8TIbaMYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjmDL3tpFwg
qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
-----END CERTIFICATE-----">
    </pkiKeyRing>


    <pkiTP status="" name="lbTP" certChain="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRIwEAYDVQQK
EwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVoXDTE5MTAwMjIwNTMwNVowgY0xCzAJBgNVBAYTAlVTMQswCQYDVQQI
EwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBgNVBAoTCU15Q29tcGFueTEOMAwG
A1UECxMFTXlPcmcxGDAWBgNVBAMUDyouYW1hem9uYXdzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDgMbFor5Ee/+dOgcueYMGrYF8uKaBf/M0lAL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXvlA8h53nrx5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqeO8epz5I4s8XpMOBDmfA
4ccW/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZHShFAdOI3Y2INj9lXrfLEJd8uD2qk1kK4Pwo590Jk8Sry1qSJ
YHGJHn8dE+xxYB1ZCyiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMEgbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BAcTCFNhbiBKb3NlMRIwEAYDVQQKEwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvbmF3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAe/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5ml5baCYZZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoelewv+wRl0oVRChlTfKtXO68TUk6vrqpw76hKfOHIa7b2h1IIMdq6VA/
+A5FQ0xqYfqKdVd2RaINpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfGPlVesFEyJEL
gHBUiPt8TIbaMYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjmDL3tpFwg
qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
-----END CERTIFICATE-----">
    </pkiTP>
```

```
    </cloudCertStore>
     </fvTenant>
</polUni>
```

REST API を使用した HTTPS サービス ポリシーの作成

このセクションでは、REST API を使用して HTTPS サービス ポリシーを作成する方法を示します。

（注） リスナーは複数の証明書をもつことができます。証明書のオプションは次のとおりです。

- ELBSecurityPolicy-2016-08 – セキュリティ ポリシーが選択されていない場合のデフォルト。
- ELBSecurityPolicy-FS-2018-06
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2015-05
- ELBSecurityPolicy-TLS-1-0-2015-04

複数の証明書を使用する場合は、デフォルトの証明書を指定する必要があります。デフォルトは、**cloudRsListenerToCert** の **defaultCert** プロパティを使用して指定されます。

始める前に

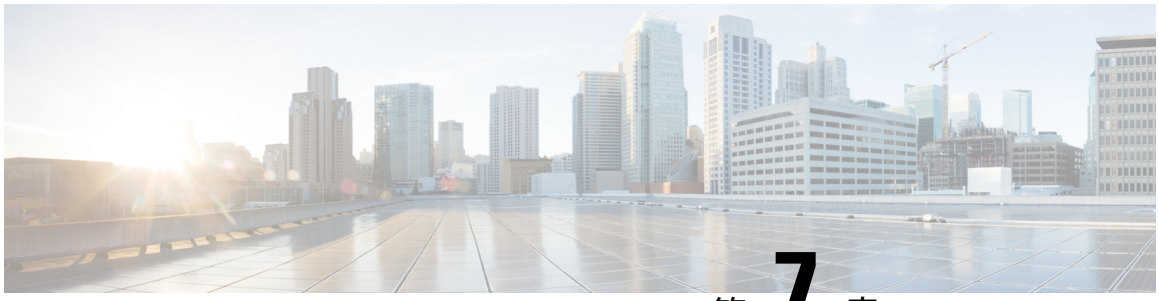
キー リング証明書は既に構成されています。

（注） これは、アプリケーション ゲートウェイにのみ適用されます。

HTTPS サービス ポリシーを作成するには:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="https_listener" port="443" protocol="https"
secPolicy="eLBSecurityPolicy-2016-08" status="">
            <cloudRsListenerToCert defaultCert="yes" certStore="default"
tDn="uni/tn-t2/certstore/keyring-lbCert" status=""/>
            <cloudListenerRule name="defaultRule" default="yes" priority="100" status="">
```

```
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t1/cloudapp-ap/cloudepg-ep1">
                                                  </cloudRuleAction>
            </cloudListenerRule>
          </cloudListener>
        </cloudSvcPolicy>
      </vnsAbsNode>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```



第 7 章

Cisco Cloud APIC セキュリティ

この章は、次の内容で構成されています。

アクセス、認証およびアカウンティング

Cisco Cloud Application Policy Infrastructure Controller（Cloud APIC）ポリシーは、認証、認可、アカウンティング（AAA）機能を管理します。ユーザ権限、ロール、およびドメインとアクセス権限の継承を組み合わせることにより、管理者は細分化された方法で管理対象オブジェクトレベルで AAA 機能を設定することができます。これらの設定は、REST API または GUI を使用して実行できます。

（注） ログイン ドメイン名に 32 文字を超えることはできないという既知の制限があります。また、ログイン ドメイン名とユーザ名を合わせた文字数は 64 文字を超えることはできません。

アクセス、認証、およびアカウント構成情報の詳細については、 https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html の ***Cisco APIC Security Configuration Guide, Release 4.0(1)*** をお読みください。

構成

初期構成スクリプトで、管理者アカウントが構成され、管理者はシステム起動時の唯一のユーザーとなります。

ローカル ユーザの設定

Cisco Cloud APIC GUI を使用したローカル ユーザーの作成 （164 ページ） を参照して、ローカル ユーザーを設定し、 Cisco Cloud APIC GUI を使用して OTP、SSH 公開キー、および X.509 ユーザー証明書に関連付けます。

TACACS+、RADIUS、LDAP、および SAML アクセスの構成

次のトピックは、Cisco Cloud APIC の TACACS+、RADIUS、LDAP および SAML アクセスを構成する方法を説明します。

概要

このトピックでは、RADIUS、TACACS +、LDAP、および SAML ユーザー（ADFS、Okta、PingID など）の Cisco Cloud APIC へのアクセスを有効にする方法について、順を追って説明します。

TACACS +、RADIUS、LDAP、および SAML の詳細については、https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html の『 ***Cisco APIC* セキュリティ構成ガイド、リリース *4.0(1)*** 』を参照してください。

Cloud APIC for TACACS+ Access の構成

始める前に

- Cloud Application Policy Infrastructure Controller (Cloud APIC) はオンラインになっています。
- TACACS+ サーバのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cloud APIC 管理エンドポイント グループが使用できます。

ステップ 1 クラウドAPICで、**TACACS+プロバイダー**を作成します。

a) メニュー バーで、**[管理（Administrative）] > [認証（Authentication）]** を選択します。

b) 作業ペインで、**[プロバイダー（Providers）]** タブをクリックして、**[アクション（Actions）]** ドロップダウンをクリックして、**[プロバイダーの作成（Create Provider）]** を選択します。

[プロバイダーの作成（Create Provider）] ダイアログボックスが表示されます。

c) **[ホスト名/IP アドレス（Host name/IP Address）]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。

d) **[説明（Description）]** フィールドに、プロバイダーの説明を入力します。

e) **[タイプ（Type）]** ドロップダウン リストをクリックし、**[TACACS+]** を選択します。

f) **[設定（Settings）]** セクションで、**[キー（Key）]**、**[ポート（Port）]**、**[認証プロトコル（Authentication Protocol）]**、**[タイムアウト（Timeout）]**、**[再試行（Retries）]**、**[管理 EPG（Management EPG）]** を

指定します。**有効化（Enabled）** または **無効化（Disabled）** のいずれかを **[サーバー監視（Server Monitoring）]** に対して選択します。

ステップ 2 TACACS+ の [Login Domain] を作成します。

a) **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

b) [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

c) **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ログイン ドメインの作成（Create Login Domain）]** をクリックします。

[ログイン ドメインの作成（Create Login Domains）] ダイアログボックスが表示されます。

d) 次の *[ログイン ドメインダイアログボックスのフィールド（Login Domains Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ（Properties）]	**説明**
全般	
名前	ログイン ドメインの名前を 入力します
説明	ログイン ドメインの説明を入力します。
Settings	
Realm	ドロップダウン メニューから **TACACS+** を選択します。
プロバイダ（Providers）	プロバイダーを選択するには： 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. **[選択（Select）]** をクリックします。**[ログイン ドメインの作成]** ダイアログボックスに戻ります。

e) [保存（Save）] をクリックして、設定を保存します。

次のタスク

これで、APIC TACACS+ 構成手順は完了です。次に、RADIUS サーバーも使用する場合は、RADIUS の APIC を設定します。

Cloud APIC for RADIUS Access の構成

始める前に

- Cloud Application Policy Infrastructure Controller (Cloud APIC) はオンラインになっています。
- RADIUS サーバーのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cloud APIC 管理エンドポイント グループが使用できます。

ステップ 1 Cloud APIC で、**RADIUS プロバイダー**を作成します。

a) メニュー バーで、**[管理（Administrative）]** > **[認証（Authentication）]** を選択します。

b) 作業ペインで、**[プロバイダー（Providers）]** タブをクリックして、**[アクション（Actions）]** ドロップダウンをクリックして、**[プロバイダーの作成（Create Provider）]** を選択します。

[プロバイダーの作成（Create Provider）] ダイアログボックスが表示されます。

c) **[ホスト名/IP アドレス（Host name/IP Address）]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。

d) **[説明（Description）]** フィールドに、プロバイダーの説明を入力します。

e) **[タイプ（Type）]** ドロップダウン リストをクリックし、**[RADIUS]** を選択します。

f) **[設定（Settings）]**セクションで、**[キー（Key）]**、**[ポート（Port）]**、**[認証プロトコル（Authentication Protocol）]**、**[タイムアウト（Timeout）]**、**[再試行（Retries）]**、**[管理 EPG（Management EPG）]** を指定します。**有効化（Enabled）** または **無効化（Disabled）** のいずれかを **[サーバー監視（Server Monitoring）]** に対して選択します。

ステップ 2 **RADIUS** の **[ログイン ドメイン]**を作成します。

a) **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

b) **[インテント（Intent）]** 検索ボックスの下にあるドロップダウン矢印をクリックし、**[管理（Administrative）]** を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

c) **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ログイン ドメインの作成（Create Login Domain）]** をクリックします。

[ログイン ドメインの作成（Create Login Domains）] ダイアログボックスが表示されます。

d) 次の *[ログイン ドメインダイアログボックスのフィールド（Login Domains Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ（Properties）]	説明
全般	
名前	ログイン ドメインの名前を 入力します
説明	ログイン ドメインの説明を入力します。
Settings	
Realm	ドロップダウン メニューから **RADIUS** を選択します。
プロバイダ（Providers）	プロバイダーを選択するには： 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. **[選択（Select）]** をクリックします。**[ログイン ドメインの作成]** ダイアログボックスに戻ります。

e) [保存（Save）] をクリックして、設定を保存します。

次のタスク

これで、 Cloud APIC RADIUS 構成手順は完了です。次に、RADIUS サーバを設定します。

Cloud APIC への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の設定

『 ***Cisco APIC Security Configuration Guide、Release 4.0（1）*** 』の「*Configuring a Cisco Secure Access Control Server for RADIUS and TACACS + Access to the APIC*」の項を /docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html で参照してください。

LDAP Access の構成

LDAP 設定には 2 つのオプションがあります。

- Cisco AVPair の設定
- Cisco Cloud ネットワーク コントローラで LDAP グループ マップを構成する

次のセクションには、両方の構成オプションの手順が含まれています。

Cisco AVPair を使用した APIC アクセス用の Windows Server 2008 LDAP の設定

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-security/Cisco-APIC-Security-Configuration-Guide-401.html にある『 ***Cisco APIC Security Configuration Guide、Release 4.0(1)*** 』の「*Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair*」を参照してください。

LDAP アクセスのための Cisco Cloud Network Controller の構成

始める前に

- Cisco Cloud Network Controller はオンラインです。
- LDAP サーバのホスト名または IP アドレス、ポート、バインド DN、ベース DN、およびパスワードを使用できること。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。

ステップ 1 Cisco Cloud Network Controller で、**[LDAP プロバイダ（LDAP Provider）]** を作成します。

a) メニュー バーで、**[管理（Administrative）]** > **[認証（Authentication）]** を選択します。

b) 作業ペインで、**[プロバイダー（Providers）]** タブをクリックして、**[アクション（Actions）]** ドロップダウンをクリックして、**[プロバイダーの作成（Create Provider）]** を選択します。

[プロバイダーの作成（Create Provider）] ダイアログボックスが表示されます。

c) **[ホスト名/IP アドレス（Host name/IP Address）]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。

d) **[説明（Description）]** フィールドに、プロバイダーの説明を入力します。

e) **[タイプ（Type）]** ドロップダウン リストをクリックし、**[LDAP]** を選択します。

f) **バインド DN**、**ベース DN**、**パスワード**、**ポート**、**属性**、**フィルタ タイプ**、および**管理 EPG** を指定します。

（注）
- バインド DN は、Cisco Cloud Network Controller が LDAP サーバにログインするために使用する文字列です。Cisco Cloud Network Controller は、ログインしようとするリモートユーザーの検証にこのアカウントを使用します。ベース DN は、Cisco Cloud Network Controller がリモート ユーザー アカウントを検索する LDAP サーバのコンテナ名とパスです。これはパスワードが検証される場所です。フィルタを使用して、Cisco Cloud Network Controller が *cisco-av-pair* に使用するために要求している属性を見つけます。これには、Cisco Cloud Network Controller で使用するユーザー認証と割り当て済み RBAC ロールが含まれます。Cisco Cloud Network Controller は、この属性を LDAP サーバから要求します。
- **[属性]** フィールド：次のうちいずれかを入力します。
  - LDAPサーバの設定では、Cisco AVPair、入力 **CiscoAVPair** 。
  - LDAP グループ マップ LDAPサーバ設定、入力 **memberOf** 。

ステップ 2 LDAP の **ログイン ドメイン** を作成します。

a) メニュー バーで、**[管理（Administrative）]** > **[認証（Authentication）]** を選択します。

b) [Work]ペインで、[Login Domains]タブをクリックし、[Actions]ドロップダウンをクリックして[Create Login Domain]を選択します。

c) 次の *[ログイン ドメインダイアログボックスのフィールド（Login Domains Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ（Properties）]	説明
全般	
名前	ログイン ドメインの名前を 入力します
説明	ログイン ドメインの説明を入力します。
Settings	
Realm	ドロップダウン メニューから **[LDAP]** 選択します。
プロバイダ（Providers）	プロバイダーを選択するには： 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. **[選択（Select）]**をクリックします。**[ログインドメインの作成]**ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
認証タイプ	1. プロバイダーが**属性**として **CiscoAVPair** を使用して設定されている場合は、**[Cisco AV ペア（Cisco AV Pairs）]** を選択します。 2. プロバイダーが**属性**として **memberOf** で設定されている場合は、**[LDAP Group Map Rules]** を選択します。 1. **[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** をクリックします。ダイアログボックスが表示されます。 2. マップの**名前**と**説明**（オプション）および**グループ DN** を指定します。 3. **[セキュリティ ドメインの追加（Add Security Domain）]** の横にある [+] をクリックします。ダイアログボックスが表示されます。 4. [+] をクリックして、**[ロール（Role）]**の名前およびロールの **[権限（Privilege）]** タイプ（**Read** または **Write**）フィールドにアクセスします。チェックマークをクリックします。 5. さらにロールを追加するには、手順 4 を繰り返します。次に、[追加（Add）] をクリックします。 6. 手順3を繰り返して、さらにセキュリティドメインを追加します。次に、[追加（Add）] をクリックします。

d) [ログイン ドメインの作成（Create Login Domain）] ダイアログボックスで **[保存（Save）]** をクリックします。

Cloud APIC for SAML Access の構成

次のセクションでは、SAML Access 用の Cloud APIC の設定について詳しく説明します。

SAML について

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html で『***Cisco APIC Security Configuration Guide*、*Release 4.0(1)***』の「*About SAML*」セクションを参照してください。

SAML の基本要素

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html で『***Cisco APIC Security Configuration Guide*、*Release 4.0(1)***』の「*Basic Elements of SAML*」セクションを参照してください。

サポートされている IdPs および SAML コンポーネント

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html で『***Cisco APIC Security Configuration Guide*、*Release 4.0(1)***』の「*Supported IdPs and SAML Components*」セクションを参照してください。

Cloud APIC for SAML Access の構成

（注） SAML ベースの認証は Rest に対するものではなく、Cloud APIC GUI のみに対するものです。

始める前に

- SAML サーバー ホスト名または IP アドレスと、IdP メタデータの URL を使用できます。
- Cloud APIC 管理エンドポイント グループが使用できます。
- 次の設定を行います。
  - 時刻同期と NTP
  - GUI を使用した DNS プロバイダーの構成
  - GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

ステップ 1 Cloud APIC で、**SAML プロバイダー**を作成します。

a) メニュー バーで、**[管理（Administrative）]** > > **[認証（Authentication）]**を選択します。
b) **[作業（Work）]**ペインで、**[プロバイダー（Providers）]** タブをクリックし、**[アクション（Actions）]** ドロップダウンをクリックして **[プロバイダーの作成（Create Provider）]** を選択します。
c) **[ホスト名/IP アドレス（Host name/IP Address）]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
d) **[説明（Description）]** フィールドに、プロバイダーの説明を入力します。
e) **[タイプ（Type）]** ドロップダウン リストをクリックし、**[SAML]** を選択します。

f) **[設定（Settings）]** ペインで、次の手順を実行します。

- IdP メタデータ URL を指定します。
  - AD FS の場合、IdP メタデータ URL は *https://<FQDN ofADFS>/FederationMetadata/2007-06/FederationMetadata.xml* という形式になります。
  - Okta の場合、IdP メタデータの URL を取得するには、Okta サーバから該当 SAML アプリケーションの [Sign On] セクションに、**アイデンティティ プロバイダー メタデータ**のリンクをコピーします。
- SAML ベースのサービスの**エンティティ ID** を指定します。
- IdP メタデータの URL にアクセスする必要がある場合は、**メタデータ URL の HTTPS プロキシ（HTTPS Proxy for Metadata URL）** を構成します。
- IdP はプライベート CA によって署名された場合は、**[認証局（Certificate Authority）]** を選択します。
- ドロップダウン リストから、**[署名アルゴリズム認証ユーザー要求（Signature Algorithm Authentication User Requests）]**を選択します。
- **SAML 認証要求の署名**、**SAML 応答メッセージの署名**、**SAML 応答の署名アサーション**、**SAML アサーションの暗号化**を有効にするには、チェックボックスをオンにします。

g) [保存（Save）] をクリックして、設定を保存します。

ステップ 2 SAML のログイン ドメインを作成します。

a) メニュー バーで、**[管理（Administrative）]** > **[認証（Authentication）]**を選択します。

b) **作業**ペインで、**[ログイン ドメイン（Login Domains）]** タブをクリックして、**[アクション（Actions）]** ドロップダウンをクリックして、**[ログイン ドメインの作成（Create Login Domains）]** を選択します。

c) 次の [ログイン ドメインダイアログボックスのフィールド（Login Domains Dialog Box Fields）] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ（Properties）]	**説明**
全般	
名前	ログイン ドメインの名前を 入力します
説明	ログイン ドメインの説明を入力します。
Settings	
Realm	ドロップダウン メニューから **SAML** を選択します。

[プロパティ（Properties）]	説明
プロバイダ（Providers）	プロバイダーを選択するには： 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. **[選択（Select）]** をクリックします。**[ログインドメインの作成]** ダイアログボックスに戻ります。

d) [**保存（Save）**] をクリックして、設定を保存します。

Okta で SAML アプリケーションの設定

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html で『***Cisco APIC Security Configuration Guide***、***Release 4.0(1)***』のセクション「*Setting Up a SAML Application*」を参照してください。

AD FS で Relying Party Trust の設定

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html で『***Cisco APIC Security Configuration Guide***、***Release 4.0***（***1***）』の「Setting Up a Relying Party Trust in AD FS」 セクションを参照してください。

HTTPS Access の構成

ここでは、HTTPS Access を構成する方法について説明します。

HTTPSアクセスについて

この記事は、Cisco ACI を使用する際の HTTPS アクセスのカスタム証明書を設定する方法の例を示します。

詳細については、https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html の『***Cisco APIC Security Configuration Guide*、*Release 4.0(1)***』の「*HTTPS Access*」の項を参照してください。

カスタム証明書の構成のガイドライン

- ワイルドカード証明書（*.cisco.com など。複数のデバイス間で使用）およびそれに関連する他の場所で生成される秘密キーは、Cisco Cloud APIC ではサポートされません。これは、Cisco Cloud APIC に秘密キーまたはパスワードを入力するためのサポートがないためです。また、ワイルドカード証明書などのいかなる証明書の秘密キーもエクスポートできません。
- 証明書署名要求（CSR）を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。Cisco Cloud APIC は、送信された証明書が設定された CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
  - 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。
  - Cisco Cloud APIC で公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
  - 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキー リングを削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。
- ポッドあたり 1 つの証明書ベースのルートのみをアクティブにすることができます。
- このリリースでは、クライアント証明書認証はサポートされていません。

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

始める前に

注意：ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。この操作中に Cloud APIC のすべての Web サーバの再起動が予期されます。

ステップ 1　メニュー バーで、**[管理（Administrative）] > セキュリティ（Security）]** を選択します。

ステップ 2 [作業（Work）] ペインで、**[証明書認証局（Certificate Authorities）]** タブをクリックし、**[アクション（Actions）]** ドロップダウンをクリックして **[証明書認証局の作成（Create Certificate Authorities）]** を選択します。

ステップ 3 **[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスの **[名前（Name）]** フィールドに、認証局の名前を入力します。

ステップ 4 **[用途（Used for）]** フィールドで **[システム（System）]** を選択します。

ステップ 5 **[証明書チェーン（Certificate Chain）]** フィールドに、クラウド アプリケーション ポリシー インフラストラクチャ コントローラー（APIC）の証明書署名要求（CSR）に署名する認証局の中間証明書とルート証明書をコピーします。証明書は、Base64 エンコード X.509（CER）形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 メニュー バーで、**[管理（Administrative）]** > **セキュリティ（Security）]** を選択します。

ステップ 8 [作業（Work）]ペインで、**[キー リング（Key Rings）]** タブをクリックし、[アクション（Actions）] ドロップダウンをクリックして **[キー リングの作成（Create Key Ring）]** を選択します。

ステップ 9 **[キー リングの作成（Create Key Ring）]** ダイアログボックスで、**[名前（Name）]** フィールドにキー リングの名前を入力し、**[説明（Description）]** フィールドに説明を入力します。

ステップ 10 **[用途（Used for）]** フィールドで **[システム（System）]** を選択します。

ステップ 11 **[証明書認証局（Certificate Authority）]** フィールドで、**[証明書認証局の選択（Select Certificate Authority）]** をクリックし、以前に作成した認証局を選択します。

ステップ 12 **[秘密キー（Private Key）]** フィールドで、**[新規キーの生成（Generate New Key）]** または **[既存のキーのインポート（Import Existing Key）]** を選択します。**[既存のキーのインポート（Import Existing Key）]** を選択した場合は、**[秘密キー（Private Key）]** テキスト ボックスに秘密キーを入力します。

ステップ 13 **[モジュラス（Modulus）]** ドロップダウンからモジュラスを選択します。メニュー

ステップ 14 [Certificate] フィールドには、コンテンツを追加しないでください。

ステップ 15 [保存（Save）] をクリックします。

[Work] ペインの [Key Rings] 領域では、作成したキー リングに対する [Admin State] に [Started] と表示されます。

ステップ 16 作成したキー リングをダブルクリックして、**[作業（Work）]** ペインから [キー リング*]* **[key_ring_name]** ダイアログボックスを開きます。

ステップ 17 **[作業（Work）]** ペインで、**[証明書要求の作成（Create Certificate Request）]** をクリックします。

ステップ 18 **[情報カテゴリ（Subject）]** フィールドに、Cloud APIC の完全修飾ドメイン名（FQDN）を入力します。

ステップ 19 必要に応じて、残りのフィールドに入力します。

ステップ 20 [保存（Save）] をクリックします。

[Key Ring] *[key_ring_name]* ダイアログボックスが表示されます。

ステップ 21 フィールド [要求（Request）] からコンテンツを署名するために**証明書認証局** にコピーします。

ステップ 22 **[キー リング（Key Ring）]** *[key_ring_name]* ダイアログボックスで、[編集（Edit）] アイコンをクリックして **[キー リング（Key Ring）]** *[key_ring_name]* ダイアログボックスを表示します。

ステップ 23 **[証明書（Certificate）]** フィールドに、認証局から受信した署名付き証明書を貼り付けます。

ステップ 24 **[保存（Save）]** をクリックして、**[キー リング（Key Rings）]** 作業ウィンドウに戻ります。

キーが確認されて **[作業（Work）]** ペインで **[管理状態（Admin State）]** が **[完了済み（Completed）]** に変わり、HTTP ポリシーを使用できるようになります。

ステップ 25 **[インフラストラクチャ（Infrastructure）]** > **[システム構成（System Configuration）]** に移動し、**[管理アクセス（Management Access）]** タブをクリックします。

ステップ 26 **[HTTPS]** 作業ウィンドウの編集アイコンをクリックして、**[HTTPS 設定（HTTPS Settings）]**ダイアログボックスを表示します。

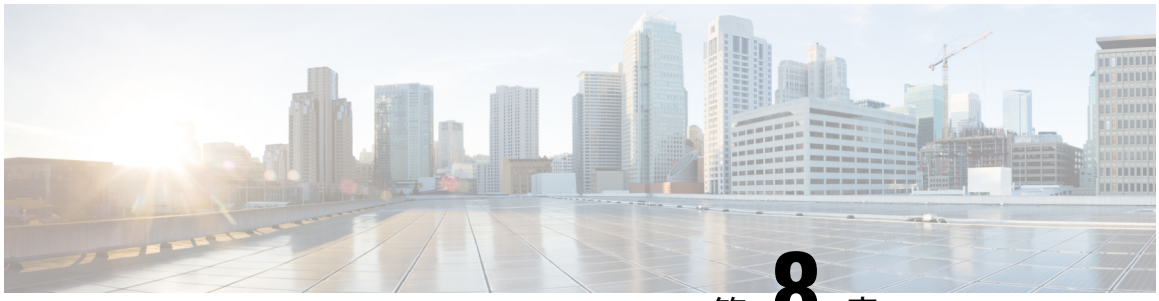
ステップ 27 **[管理キー リング（Admin Key Ring）]** をクリックし、以前に作成したキー リングを関連付けます。

ステップ 28 [保存（Save）] をクリックします。

すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキー リングが HTTPS アクセスに関連付けられています。

次のタスク

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じCSR を再送信する必要があります。キー リングを削除すると、Cloud APIC に内部的に保存されている秘密キーも削除されるため、新しいキー リングの削除または作成は行わないでください。



第 8 章

アクセスの制限

ドメイン別にアクセスを制限する

制限付きセキュリティ ドメインを使用すると、テナント A などのファブリック管理者は、両方のグループのユーザーに同じ権限が割り当てられている場合、あるユーザー グループがテナント B などの別のセキュリティ ドメインのユーザー グループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、テナントAの制限付きセキュリティ ドメインのテナント管理者は、テナント B のセキュリティ ドメインで構成されたポリシー、プロファイル、またはユーザーを表示できません。テナント B のセキュリティ ドメインも制限されていない限り、テナントBは、テナントA で設定されたポリシー、プロファイル、またはユーザーを表示できます。 ユーザーが適切な権限を持つシステム作成の構成に対して、ユーザーは常に読み取り専用で閲覧可能であることに注意してください。

たとえば、制限付きセキュリティ ドメインのユーザーがテナント A に関連付けられているとします。テナント A には、ユーザーが作成したアプリケーション プロファイル 1 と管理者が作成したアプリケーション プロファイル 2 の 2 つのアプリケーション プロファイルが含まれています。アプリケーションプロファイル2も同じテナントのものですが、ユーザーはアプリケーション プロファイル 1 しか表示できません。ユーザーが制限付きセキュリティ ドメインにいる場合、管理者によって作成されたプロファイルも表示されません。

上記の例では、アプリケーションプロファイル2は別のユーザー（管理者）によって作成されていますが、制限のないユーザー（制限付きのセキュリティドメインに属していないユーザー）は、アプリケーション プロファイル 1 とアプリケーション プロファイル 2 の両方を表示できます。

RBAC ルール

Cloud Application Policy Infrastructure Controller (cAPIC) では、ロールベース アクセス コントロール（RBAC）を介してユーザーのロールに従ってアクセスが提供されます。ファブリック ユーザーは以下に関連付けられています。

- ロールのセット
- ロールごとの権限タイプ：アクセスなし、読み取り専用、または読み取り/書き込み
- ユーザがアクセスできる管理情報ツリー (MIT) の一部を識別する 1 つ以上のセキュリティ ドメイン タグ

Cloud APIC は、管理対象オブジェクト（MO）レベルでアクセス権限を管理します。権限は、システム内の特定の機能に対するアクセスを許可または制限する MO です。たとえば、ファブリック機器は権限ビットです。このビットは、物理ファブリックの機器に対応するすべてのオブジェクト上で cAPIC によって設定されます。

ロールは権限ビットの集合です。たとえば、「管理者」ロールが「ファブリック機器」と「テナントセキュリティ」に対する権限ビットに設定されていると、「管理者」ロールにはファブリックの機器とテナントセキュリティに対応するすべてのオブジェクトへのアクセス権があります。

セキュリティ ドメインは、 cAPIC オブジェクト階層の特定のサブツリーに関連付けられたタグです。たとえば、デフォルトのテナント「common」にはドメイン タグ `common` が付いています。同様に、特殊なドメイン タグ `all` の場合、MIT オブジェクト ツリー全体が含まれます。管理者は、MIT オブジェクト階層にカスタム ドメイン タグを割り当てることができます。

ユーザを作成してロールを割り当てても、アクセス権は有効になりません。1 つ以上のセキュリティ ドメインにそのユーザを割り当てることも必要です。デフォルトでは、cAPIC ファブリックには事前作成された次の 2 つの特殊なドメインが含まれています。

- All：MIT 全体へのアクセスを許可
- インフラ：ファブリック アクセス ポリシーなどの、ファブリック インフラストラクチャのオブジェクトおよびサブツリーへのアクセスを許可

Cisco Cloud APIC は、次の AAA ロールと権限をサポートしています。

特権	説明
ロール：管理	
admin	すべてのファブリックの機能へのフル アクセスを提供します。管理者権限は、その他のすべての権限を組み合わせたものとみなされます。
ロール：aaa	

特権	説明
aaa	ポリシーの認証、許可、アカウンティング、インポート/エクスポートの設定に使用されます。
Role: access-admin	
access-connectivity	インフラでのレイヤ 1 ～ 3 の構成、テナントの L3Out でのスタティックルート構成、管理インフラ ポリシー、テナント ERSPAN ポリシーに使用されます。
access-equipment	アクセス ポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタポリシーやファームウェアポリシーなどの操作関連のアクセスポリシーでレイヤ 1 ～ 3 のプロトコル構成に使用されます。
access-qos	CoPP および QoS に関連するポリシーの変更に使用されます。
ロール：**fabric-admin**	
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ1～3の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ 1 ～ 3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN およびヘルススコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイント トラッキングポリシーに使用されます。
ロール：**nw-svc-admin**	

特権	説明
nw-svc-policy	レイヤ 4 ～ レイヤ 7 ネットワークサービス オーケストレーションの管理に使用されます。
ロール： nw-svc-params	
nw-svc-params	レイヤ 4 ～ レイヤ 7 のサービス ポリシーの管理に使用されます。
Role: ops	
ops	設定されているポリシーの表示に使用されます（ポリシーのトラブルシューティングなど）。
ロール：port-mgmt	
port-mgmt	ノードをセキュリティドメインに割り当てるために使用されます。また、ノードルールを持つセキュリティドメインのユーザーは、`port-mgmt` のロールを持つドメイン `all` に割り当てる必要があります。
Role: tenant-admin	
aaa	ポリシーの認証、許可、アカウンティング、インポート/エクスポートの設定に使用されます。
access-connectivity	インフラでのレイヤ 1 ～ 3 の構成、テナントの L3Out でのスタティックルート構成、管理インフラ ポリシー、テナント ERSPAN ポリシーに使用されます。
access-equipment	アクセス ポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタポリシーやファームウェアポリシーなどの操作関連のアクセスポリシーでレイヤ 1 ～ 3 のプロトコル構成に使用されます。
access-qos	CoPP および QoS に関連するポリシーの変更に使用されます。

特権	説明
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ1～3の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ 1 ～ 3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN およびヘルススコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイント トラッキングポリシーに使用されます。
nw-svc-policy	レイヤ 4 ～ レイヤ 7 ネットワークサービス オーケストレーションの管理に使用されます。
tenant-network-profile	ネットワークプロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ1～3プロトコルの構成、テナント トレース ルート ポリシー、およびファームウェア ポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントの QoS に関連する設定に使用されます。
tenant-security	テナントのコントラクトに関連する設定に使用されます。
Role: tenant-ext-admin	

特権	説明
tenant-connectivity	ブリッジドメイン、サブネット、およびVRFなどの レイヤ 1 ～ 3 の接続変更に使用されます。これには、リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシー、テナントのインバンドおよびアウトオブバンド管理接続構成。アトミック カウンタやヘルス スコアなどのデバッグ/モニタリング ポリシーなどがあります。
tenant-epg	エンドポイント グループ、VRF、ブリッジ ドメインの削除/作成など、テナント設定の管理に使用されます。
tenant-ext-connectivity	書き込みアクセス ファームウェア ポリシーに使用されます。テナント L2Out および L3Out 設定の管理。デバッグ/モニタリング/オブザーバ ポリシー。
tenant-ext-protocol	BGP、OSPF、PIM、IGMP などのテナント外部レイヤ 1 ～ 3 プロトコルの管理、およびトレースルート、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバ ポリシーに使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。
tenant-network-profile	ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ1～3プロトコルの構成、テナント トレースルートポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントの QoS に関連する設定に使用されます。
tenant-security	テナントのコントラクトに関連する設定に使用されます。

カスタム権限は、任意のMOクラスに割り当てることができます。22個のカスタム権限がCisco Cloud APIC GUIに表示されます。これらのカスタム権限のいずれかがクラスに割り当てられている場合、その MO のアクセスには新しく追加されたカスタム権限が含まれます。1 つのカスタム権限を 1 つ以上の MO クラスに関連付けることができます。

（注） カスタム権限はCisco Cloud APIC GUIで表示されますが、現在サポートされていません。

事前に定義された一連の管理対象オブジェクト クラスをドメインに関連付けることができます。これらのクラスがオーバーラップすることはできません。ドメインの関連付けをサポートするクラスの例：

- レイヤ 2 およびレイヤ 3 のネットワークで管理されたオブジェクト
- ネットワーク プロファイル (物理、レイヤ 2、レイヤ 3、管理など)
- Quality of Service（QoS）ポリシー

ドメインに関連付けることができるオブジェクトが作成されると、ユーザは、ユーザのアクセス権の範囲内でオブジェクトにドメインを割り当てる必要があります。ドメインの割り当てはいつでも変更できます。

RBACルール

RBAC ルールは、リソース（アプリケーション プロファイル、EPG、契約など）を、別のセキュリティ ドメインにいるためにアクセスできないユーザーに選択的に公開します。RBAC ルールは、アクセスされるオブジェクトを特定する識別名（DN）と、オブジェクトにアクセスするユーザーを含むセキュリティ ドメインの名前の 2 つの部分で構成されます。

RBAC ルールには 2 つのタイプがあります。

- 暗黙的 - ユーザーは、RBAC 階層に基づいてルールまたは権限を継承します
- 明示的 - ルールは特定のポリシーに基づいてユーザーに直接割り当てられます

制限付きおよび制限なしの両方のセキュリティ ドメインがサポートされています。

（注） 管理情報ツリー内の異なる部分に存在するユーザに対し、RBAC規則によりオブジェクトを公開することは可能ですが、CLIの使用によってツリーの構造を横断することでそのようなオブジェクトに移動することはできません。ただし、RBAC規則に含まれるオブジェクトのDNをユーザが把握していれば、ユーザはMO検索コマンドにより、CLIを使用してそれを見つけることができます。

制限付きドメインの注意事項と制限事項

制限付きドメインのユーザーに対するガイドラインと制限は次のとおりです。

- あるセキュリティ ドメインのユーザーに別のセキュリティ ドメインが割り当てられている場合、そのユーザーは新しいドメインに関連付けられた構成にアクセスできます。

- ユーザーは、「制限付き」とマークされた1つ以上のセキュリティ ドメインの一部になることができます。
- 制限付きドメインユーザーは、システムで作成された構成への読み取り専用アクセス権を持っています。
- 複数のセキュリティ ドメインを持つユーザーの場合、すべてのセキュリティ ドメインを合わせた長さが 1024 文字を超えることはできません。長さが 1024 を超えると、ユーザーはポリシーの作成に問題が発生します。
- Cloud APIC の制限付きドメインは、クラウド リソースではサポートされていません。つまり、ある制限付きドメインのユーザーは、別の制限付きドメインのユーザーによって作成されたクラウド リソースを表示できます。

Cisco Cloud APIC GUI を使用した RBAC ルールの作成

このセクションでは、GUI を使用して RBAC ルールを作成する方法について説明します。

（注） RBAC ルールを構成できますが、Cloud APIC GUI は構成をサポートしていません。この手順（手順 4）を使用して構成された DN は、API を使用して照会できます。

始める前に

セキュリティ ドメインの作成詳細なタスクについては、「Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成」を参照してください。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[インテント（Intent）] メニューに**管理**オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストから、**[セキュリティ（Security）]** > **[RBAC ルール（RBAC Rules）]** > **[RBAC ルールの作成（Create RBAC Rule）]** をクリックします。**[RBAC ルールの作成（Create RBAC Rule）]** ダイアログボックスが表示されます。

ステップ 4 **DN** フィールドに、ルールの DN を入力します。

明示的な RBAC ルールを作成するには、ObjectStore でアプリケーションの DN を見つけます。ここでその DN 値を使用します。

ステップ 5 セキュリティ ドメインを選択します。

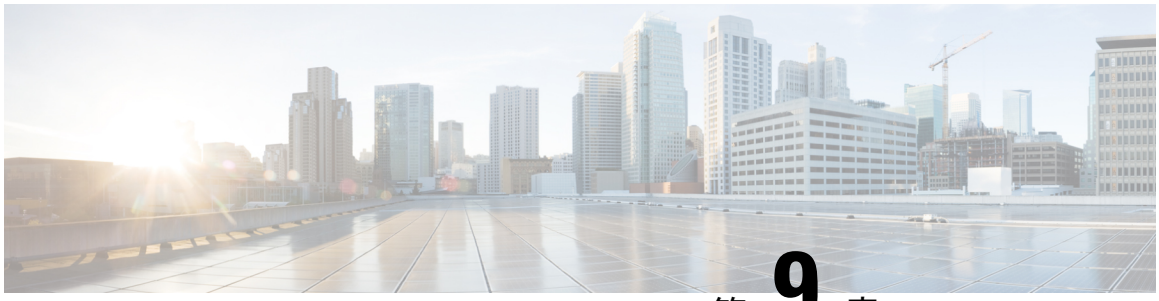
a) **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログ ボックスが表示されます。

b) **[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログで、左側の列のセキュリティ ドメインをクリックして選択し、**[選択（Select）]** をクリックします。**[RBAC ルールの作成]** ダイアログボックスに戻ります。

ステップ 6 **[書き込みを許可]** フィールドで、**[はい]** をクリックして書き込みを許可するか、**[いいえ]** をクリックして書き込みを許可しません。

ステップ 7 設定が終わったら [Save] をクリックします。

（注） 明示的な RBAC ルールを作成した後、セキュリティ ドメインに割り当てられたユーザーは、以前に（ObjectStore から）定義されたアプリケーションとその子のみを表示できます。



第 9 章

設定のばらつき

構成のばらつき通知と障害

パブリック クラウドに Cisco ACI を展開する場合、Cloud APIC からほとんどのファブリック構成を実行します。ただし、お客様または別のクラウド管理者が、AWS または Azure が提供するツールを使用して、クラウド プロバイダーの GUI で展開された構成を直接変更する場合があります。このような場合、Cloud APIC から展開した意図した構成とクラウド サイトの実際の構成が同期しなくなる可能性があります。これを構成のばらつきと呼びます。

リリース 5.0(2) 以降、Cloud APIC は、Cloud APIC から展開したものとクラウド サイトで実際に構成されたものとの間のセキュリティ ポリシー (コントラクト) 構成の不一致を可視化します。将来のリリースでは、他の Cloud APIC オブジェクトへの構成のばらつきの可視性と、クラウドに展開されているが Cloud APIC で定義されていない無関係な構成に関する情報が提供されます。

構成のばらつきの分析には 2 つの側面があります。

- Cloud APIC で構成され、クラウド ファブリックにデプロイされる予定のすべてのファブリック要素が適切に展開されましたか?

  このシナリオは、クラウドに展開できなかった Cloud APIC のユーザー構成エラー、クラウド プロバイダー側の接続または API の問題、またはクラウド管理者がクラウド プロバイダーの UI で直接セキュリティ ルールを手動で削除または変更した場合に発生する可能性があります。意図されていても欠落している構成は、Cloud APIC ファブリックに問題を引き起こす可能性があります。

- クラウドに存在するが、Cloud APIC から展開することを意図していない追加の構成はありますか?

  前のシナリオと同様に、これは、接続または API の問題がある場合、またはクラウド管理者がクラウド プロバイダーの UI で直接追加のセキュリティ ルールを手動で作成した場合

に発生する可能性があります。既存の、意図されていない構成では、問題が発生する可能性があります。

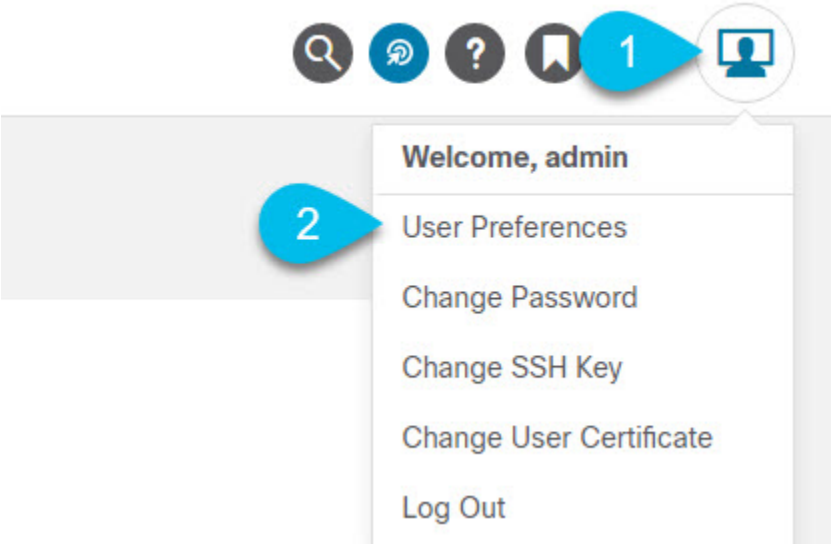
構成のばらつきの検出の有効化

構成のばらつき検出を使用する場合は、Cloud APIC で実行されているソフトウェア リリースによっては、有効にする必要がある場合があります。

- リリース 25.0(2) 以降では、構成のばらつきの検出がデフォルトで有効になっています。この場合、このセクションの手順を使用して構成ドライブを手動で有効にしないでください。
- リリース 25.0(1) 以前では、構成のばらつきの検出はベータ段階であるため、デフォルトでは無効になっています。このセクションでは、Cloud APIC ユーザー設定で構成のばらつき検出を有効にする方法について説明します。

ステップ 1 Cloud APIC GUI にログインします。

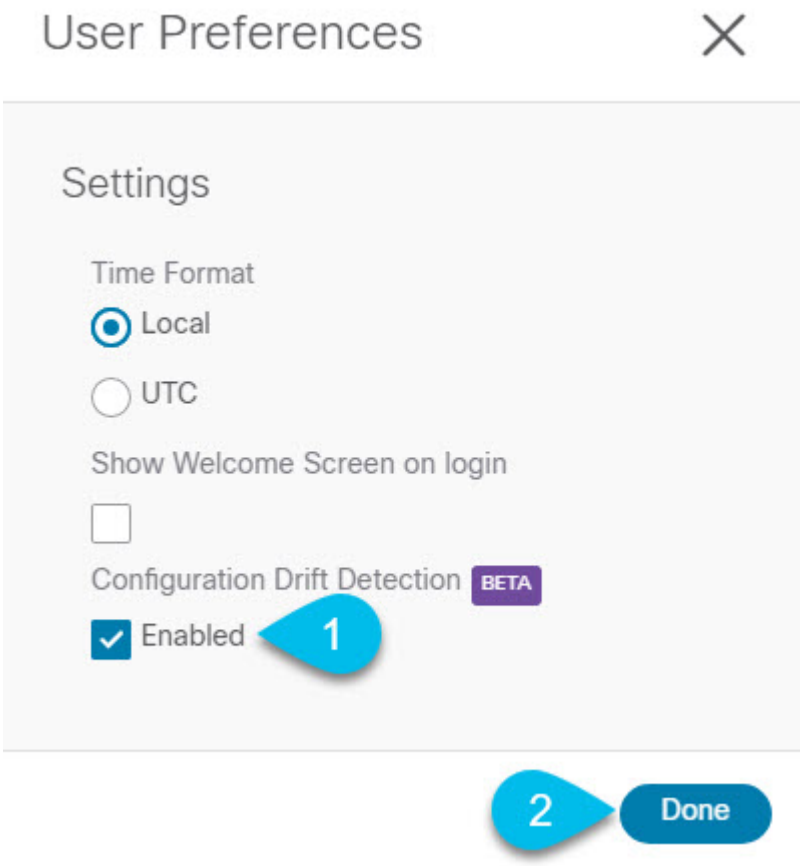
ステップ 2 **[ユーザーの基本設定（User Preferences）]** ダイアログボックスを開きます。



a) 画面の右上にある [ユーザー] アイコンをクリックします。

b) メニューから、**[ユーザーの基本設定（User Preferences）]** を選択します。

ステップ 3 **[ユーザーの基本設定（User Preferences）]** ダイアログで、**構成のばらつき検出**を有効にします。

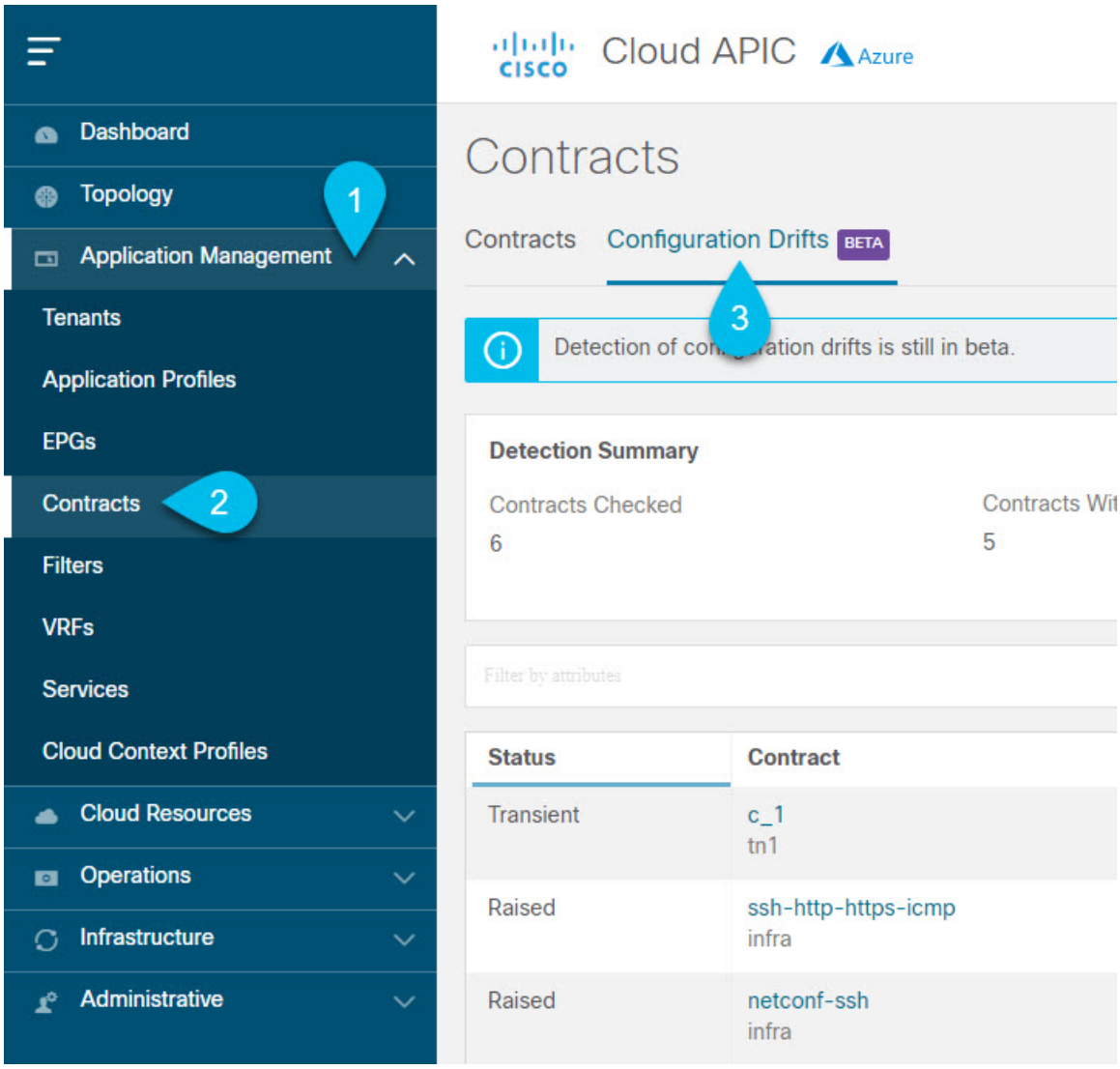


a) [有効（Enabled）] チェックボックスをオンにします。
b) **[完了]** をクリックして変更を保存します。

欠落しているコントラクト構成の確認

このセクションでは、Cloud APIC から構成したが、クラウド ファブリックに適切にデプロイされていないコントラクト設定を確認する方法について説明します。

ステップ 1 Cloud APIC GUI にログインします。
ステップ 2 **[構成のばらつき（Configuration Drifts）]** 画面に移動します。



a) 左側の**ナビゲーション** サイドバーで、**[アプリケーション管理 (Application Management)]** カテゴリを展開します。

b) **[アプリケーション管理]** カテゴリから、**[コントラクト]** を選択します。

c) **[コントラクト]** 画面で、**[構成のばらつき（Configuration Drifts）]** タブを選択します。

[構成のばらつき] タブでは、ファブリック内のコントラクトに関する構成の問題の概要を確認できます。

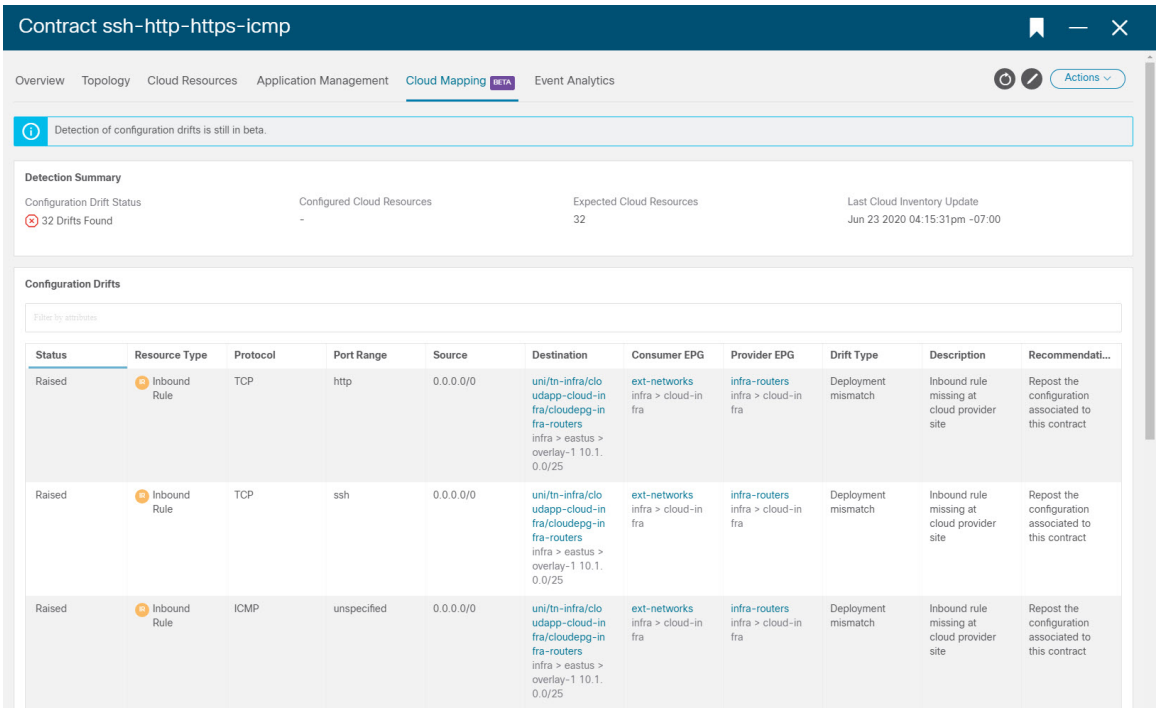
ばらつきのあるコントラクトごとに、欠落している構成の数と問題の重大度が表示されます。

メイン ウィンドウの右上にある更新ボタンをクリックして、情報を更新できます。

ステップ 3 **[構成のばらつき]** 画面で、コントラクトの名前をクリックして、構成のばらつきの問題を含むその詳細を表示します。

ステップ 4 開いた **[コントラクトの詳細]** ビューで、**[クラウド マッピング]** タブを選択します。

クラウド マッピング ビューには、コントラクトとそれが使用するクラウド リソースに関するすべての情報が表示されます。



画面は、**[検出の概要]**、**[構成のばらつき]**、および **[マップされたクラウド リソース]** の 3 つのセクションに分かれています。各セクションには、選択したコントラクトに関するそれぞれの情報をリストした表が含まれています。

検出の概要**の表には、検出された構成のばらつきの数、構成された意図された実際のクラウド リソースの数、およびこの情報が最後に更新された時刻の概要が表示されます。**在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある **[更新]** アイコンをクリックして情報を更新できます。

構成のばらつきテーブルには、コントラクト ルールに関するすべての問題が一覧表示されます。具体的には、展開することを意図していたが、実際のファブリック構成に欠落しているすべてのコントラクト ルール。この表には、使用されるプロトコル、ポート範囲、送信元と宛先の IP またはグループ、コンシューマーとプロバイダーの EPG、問題の説明、問題を解決するための推奨アクションなどの詳細情報が含まれています。構成ののばらつきごとに、[ステータス] フィールドに重大度と推奨されるアクションが示されます。

- 一時的(低): 最近の構成変更が原因である可能性が高いばらつき。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。
- 推定(中): 一時的である場合とそうでない場合があるばらつき。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。

  上げた (高): クリティカル ばらつき。Cloud APIC の構成を確認し、関連する障害を確認することをお勧めします。構成を再デプロイすると、Cloud APIC とクラウド サービス間の通信の問題を解決できる場合があります。問題が解決しない場合は、テクニカル サポート ログを確認してください。

マップされたクラウドリソースの表には、クラウドで適切に構成されたすべてのリソースに関する情報が表示されます。この表は、特定のコントラクトのためにクラウドで構成されているルールをよりよく把握できるように設計されています。

構成のばらつきのトラブルシューティング

このセクションでは、構成のばらつきプロセスが Cloud APIC で稼働していることを確認し、アプリケーション ログを確認し、必要に応じてテクニカル サポート情報を生成するためのいくつかの便利なコマンドを提供します。

ステップ 1 root ユーザーとしてコンソール経由で Cisco Cloud APIC にログインします。

ステップ 2 構成のばらつきアプリケーションのステータスを確認します。

```
ACI-Cloud-Fabric-1# moquery -d pluginContr/plugin-Cisco_CApicDrift | egrep "dn |pluginSt |operSt
|version"
dn: pluginContr/plugin-Cisco_CApicDrift
operSt: active
pluginSt: active
Verison: 5.1.0
```

ステップ 3 アプリケーション コンテナのステータスを確認します。

```
ACI-Cloud-Fabric-1# docker ps | grep drift
CONTAINER ID    IMAGE           COMMAND                  CREATED         STATUS
         NAMES
649af6feb72c    a5ea08bbf541    "/opt/bin/conit.bi..."  13 hours ago    Up 13
hours     drift-api-b703e569-0aa6-859f-c538-a5fecbc5708f
```

ステップ 4 すべての Docker コンテナによって消費されるメモリを確認します。

消費されるメモリの合計量は 12GB 未満である必要があります。

```
ACI-Cloud-Fabric-1# systemctl status ifc-scheduler_allocations.slice| grep Memory
```

ステップ 5 必要に応じて、テクニカル サポート ログを収集します。

ログは、コントローラの /data/techsupport ディレクトリに保存されます。

```
ACI-Cloud-Fabric-1# trigger techsupport controllers application CApicDrift
ACI-Cloud-Fabric-1# trigger techsupport controllers application CApicDrift vendorName Cisco
```

ステップ 6 アプリケーション ログを確認します。

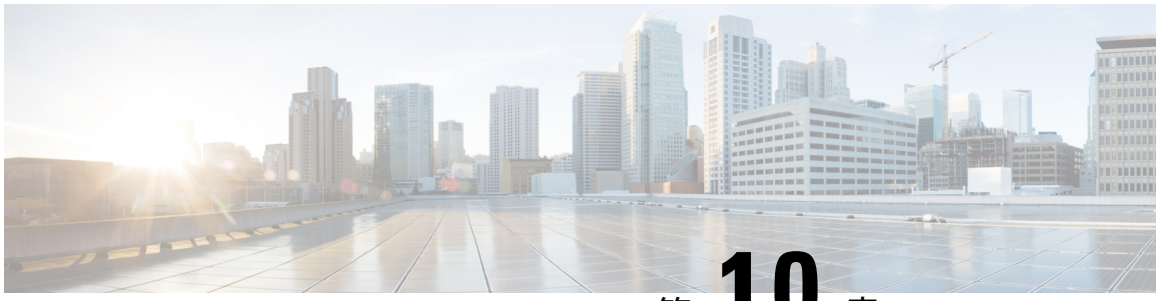
構成のばらつきプロセスのログは、/data2/logs/Cisco_CApicDrift ディレクトリに保存されます。

runhist.log ファイルには、アプリケーションが開始されるたびに情報が記録されます。次に例を示します。

```
# cat runhist.log
1 - Thu Jun 11 23:55:59 UTC 2020
2 - Fri Jun 12 01:19:41 UTC 2020
```

drift.log ファイルはアプリケーション ログ ファイルであり、構成ドリフトが更新された回数と各更新にかかった時間を表示するために使用できます。

```
# cat drift.log | grep ITER
{"file":"online_snapshot.go:178","func":"Wait","level":"info","msg":"ITER# 109
ENDED ===  RDFGEN TIME: 1m40.383751649s,  MODEL UPLOAD TIME 5m54.245550374s;
TOTAL       TIME:: 7m34.629447083s","time":"2020-06-12T19:53:13Z"}
```



第 10 章

Cisco Cloud APIC で管理されたクラウド サイトと非 ACI リモート サイト間の接続の設定

この章のセクションでは、エクスプレス ルート ゲートウェイを使用して、またはエクスプレス ルート ゲートウェイを使用せずに、Cisco Cloud APIC で管理されたクラウド サイトと非 ACI リモート サイト間の接続を構成する方法について説明します。

エクスプレス ルート ゲートウェイを使用して接続を構成する

リリース 5.1(2) 以降では、リダイレクトを使用して、またはリダイレクトを使用せずに、ハブ VNet にエクスプレス ルート ゲートウェイを展開可能なエクスプレス ルート ゲートウェイ展開がサポートされています。エクスプレス ルート ゲートウェイは、Cisco Cloud Network Controller が管理するクラウド サイトと非 ACI リモート サイト間の接続を提供するために使用されます。非 ACI リモート サイト（この場合、エクスプレス ルート ゲートウェイによって接続されている）の外部 EPG には、ハブまたはスポーク VNet 内のクラウド EPG との契約があります。

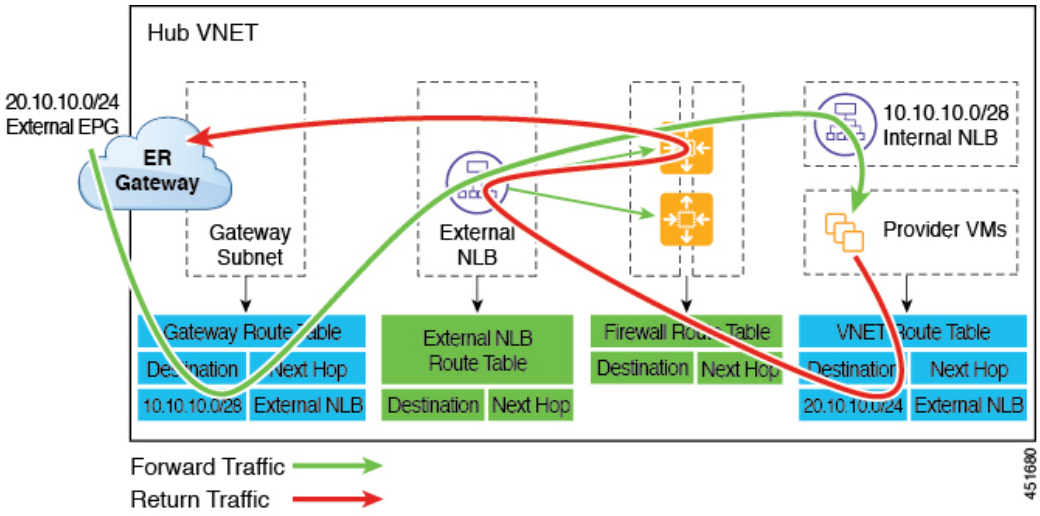
リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて

ExpressRoute ゲートウェイを介してクラウド エンドポイントと外部ネットワーク間の接続を展開している状況では、リダイレクトを使用してそれらの間にサービス デバイスを挿入できます。

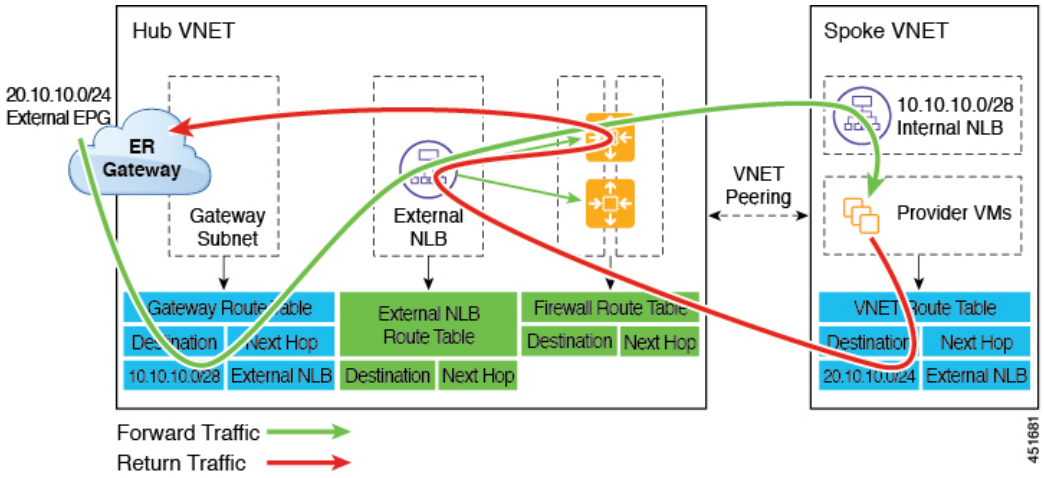
このユース ケースでは、エクスプレス ルート ゲートウェイによって接続された外部 EPG は、ハブまたはスポーク VNet のいずれかでクラウド EPG と契約しています。このケースから得られた結果を以下に示します。

- リダイレクトは、Cloud APIC によってゲートウェイ サブネット ルート テーブルで構成されます。プロバイダ クラウド EPG 宛てのトラフィックは、ハブ VNet に展開されたサービス デバイスにネクスト ホップとしてリダイレクトされます。
- リダイレクトで使用されるサービス デバイスは、エクスプレス ルート ゲートウェイ（この場合はハブ VNet）によって接続された外部 EPG と同じ VNet にある必要があります。
- この場合、プロバイダ クラウド EPG をリージョン全体に拡張することがサポートされています。

次の図は、ハブ VNet のプロバイダ EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の図は、スポーク VNet 内のプロバイダ EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の表は、、リダイレクトがどのようにプログラムされるかを示しています。

コンシューマ	プロバイダー	ゲートウェイ サブネット ルート テーブルでのリダイレクト	プロバイダ VNet のリダイレクト
エクスプレス ルート ゲートウェイによって接続された外部 EPG	サブネットベースのエンドポイント セレクタを備えたクラウド EPG	プロバイダのサブネットを使用したコンシューマからプロバイダへのトラフィックのリダイレクト	外部 EPG のサブネットを使用したプロバイダからコンシューマへのトラフィックのリダイレクト

リダイレクトを使用してエクスプレス ルート ゲートウェイを展開する

始める前に

これらの手順を続行する前に、リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて （347 ページ） の情報を確認します。

ステップ 1 Cisco Cloud Network Controller で VNet ピアリングを有効にします。

これらの指示については、「Azure 向け Cisco Cloud Network Controller の VNET ピアリングを構成する」を参照してください。

エクスプレス ルート ゲートウェイに必要なハブ VNet のゲートウェイ サブネットは、VNet ピアリングが有効な場合 Cisco Cloud Network Controller で展開されます。これは、エクスプレス ルート ゲートウェイの展開用にハブ VNet を準備するために行われます。

ステップ 2 非 ACI リモートサイトのネットワークを表すハブ VNet に外部 EPG を作成します。

- GUI を使用して外部 EPG を作成するには、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ） を参照してください。

外部 EPG の **[ルート到達可能性（Route Reachability）]** で、**[外部サイト（External-Site）]** を選択します。

- REST API を使用して外部 EPG を作成するには、REST API を使用した外部クラウド EPG の作成 （185 ページ） を参照してください。

  タイプ **site-external** の外部クラウド EPG を作成します。

ステップ 3 Azure portal を通じて、ステップ 1 （349 ページ） で構成したゲートウェイ サブネットを使用してハブ VNet でエクスプレス ルート ゲートウェイを展開します。

ステップ 1 （349 ページ） で VNet ピアリングを有効にするときに選択したリージョンの数に応じて、Cisco Cloud Network Controller が管理する複数のリージョンでエクスプレス ルート ゲートウェイ アクセスが必要な場合は、それらの各リージョンにエクスプレス ルート ゲートウェイを個別に展開します。

a) Azure portal で、仮想ネットワーク ゲートウェイを作成する Resource Manager 仮想ネットワークに移動します。
b) 左側で、**[リソースの作成（Create a resource）]** を選択し、検索に**仮想ネットワーク ゲートウェイ**と入力します。
c) 検索結果で **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** を見つけて、エントリをクリックします。
d) **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** ページで、**[作成（Create）]** を選択します。
e) **[仮想ネットワーク ゲートウェイの作成（Create virtual network gateway）]** ページで、次のフィールドに適切な情報を入力します。
   - **サブスクリプション**：適切なサブスクリプションが選択されていることを確認します。
   - **リソース グループ**：仮想ネットワークを選択すると、リソース グループが自動的に選択されます。
   - **名前**：エクスプレス ルート ゲートウェイの名前。
   - **リージョン**：仮想ネットワークが配置されている場所を指すように**[リージョン（Region）]** フィールドを変更します。場所が仮想ネットワークのあるリージョンを指していない場合、仮想ネットワークは **[仮想ネットワークの選択（Choose a virtual network）]** ドロップダウンに表示されません。
   - **ゲートウェイ タイプ**：**[ExpressRoute]** を選択します。
   - **SKU**：ドロップダウンからゲートウェイ SKU を選択します。
   - **仮想ネットワーク**：ステップ 1 （349 ページ） で Cisco Cloud Network Controller によって作成された仮想ネットワークを選択します。
   - **パブリック IP アドレス**：**[新規作成（Create new）]** を選択します。
   - **パブリック IP アドレス名**：パブリック IP アドレスの名前を指定します。
f) **[確認 + 作成（Review + Create）]** を選択し、**[作成（Create）]** でゲートウェイの作成を開始します。

設定が確認され、ゲートウェイが展開します。仮想ネットワーク ゲートウェイの作成には、完了までに最長 45 分かかります。

エクスプレス ルート ゲートウェイが正常に展開されたことを確認するには、Azure ポータルのネットワーク ゲートウェイ ページに移動し、タイプ **エクスプレス ルート** のネットワーク ゲートウェイが作成されたことを確認します。

追加のリージョンでエクスプレスルート ゲートウェイ アクセスが必要な場合、それらのリージョンそれぞれにこれらの手順を繰り返します。

ステップ 4 リダイレクト用のサービス デバイスを構成します。

GUI または REST API を使用してリダイレクトのサービス デバイスを構成するには、レイヤ 4 から レイヤ 7 サービスの展開 （209 ページ） を参照してください。

ステップ 5 エクスプレス ルート ゲートウェイで接続したクラウド EPG および外部 EPG 間のコントラクトを構成します。

- GUI を使用してコントラクトを作成するには、Cisco Cloud APIC GUI を使用したコントラクトの作成 （121 ページ） を参照してください。
- REST API を使用して契約を構成するには、REST API を使用したコントラクトの作成 （180 ページ） を参照してください。

リダイレクトなしの Express Route ゲートウェイの展開について

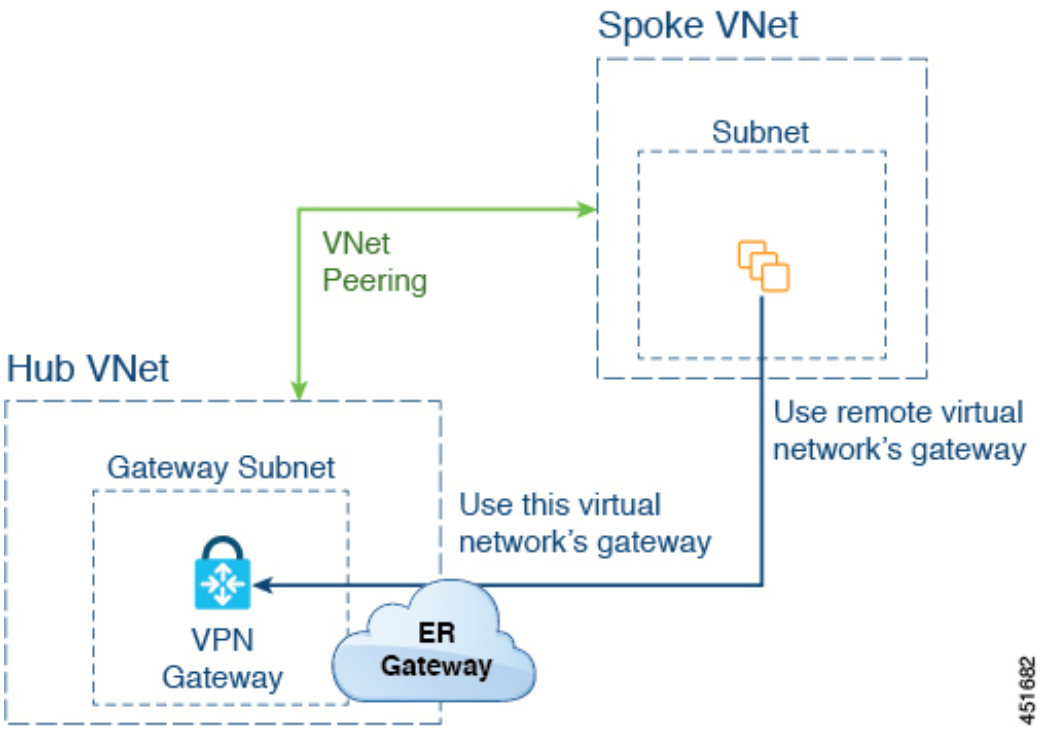
このタイプの展開では、スポーク VNet へのルート伝達が Cisco Cloud Network Controller によって自動的に有効になります。これにより、ゲートウェイ移行を使用した VNet ピアリング（移行ピアリングとも呼ばれます）を使用して、ハブ VNet を介してスポーク VNet で非 ACI リモート サイト サブネット ルートを使用できるようになります。ゲートウェイトランジットを使用した VNet ピアリングは、この場合Cisco Cloud Network Controller によって自動的に有効になります。

この構成の一部として、ハブ VNet にエクスプレス ルート ゲートウェイを展開します。Cisco Cloud Network Controller は、エクスプレス ルート ゲートウェイがハブ VNet で構成されていることを検出すると、Azure portal で移行ピアリング プロパティを自動的に設定します。1 つはハブ → スポーク ピアリング用、もう 1 つはスポーク → ハブ ピアリング用です。

- **Hub VNet**：**[この仮想ネットワークのゲートウェイを使用する（Use this virtual network's gateway）]** に自動的に設定されます。
- **スポーク VNet**：Cisco Cloud Network Controller によって管理されるスポーク VNet で **[リモート仮想ネットワークのゲートウェイを使用する（Use remote virtual network's gateway）]** に自動的に設定されます。

スポーク VNet の出力ルート テーブルに対してルート伝達を有効にするには、スポーク VNet のクラウド EPG と、非 ACI リモート サイトに接続する外部 EPG との間の契約を構成する必要があります。

次の図に、この展開タイプの例を示します。



この例では、以下のようになっています。

- 次の構成は、Cisco Cloud Network Controller によって自動的に行われます。
  - スポーク VNet は、ゲートウェイ トランジット（トランジット ピアリング）で VNet ピアリングを使用する
  - ハブ VNet の VPN ゲートウェイがオンプレミスの非 ACI リモート サイトに接続されている
  - エクスプレス ルート ゲートウェイがハブ VNet に展開されていることを Cisco Cloud Network Controller が検出すると、移行ピアリング プロパティがピアリングの各側で自動的に設定されます（ハブ → スポークおよびスポーク → ハブ）。
    - **Hub VNet**：**[この仮想ネットワークのゲートウェイを使用する（Use this virtual network's gateway）]** に自動的に設定されます。
    - **スポーク VNet**：Cisco Cloud Network Controller によって管理されるスポーク VNet で **[リモート仮想ネットワークのゲートウェイを使用する（Use remote virtual network's gateway）]** に自動的に設定されます。

- スポーク VNet の EPG が外部 EPG と契約している場合、VPN ゲートウェイによって学習されたオンプレミスの非 ACI ルートは、スポーク VNet で使用できます。
- ハブ VNet は、VPN ゲートウェイを介してオンプレミスの非 ACI リモート サイトを宛先としたスポーク VNet 内の EPG からのトラフィックを許可します。

リダイレクトなしのエクスプレス ルート ゲートウェイのデプロイ

始める前に

これらの手順を続行する前に、リダイレクトなしの Express Route ゲートウェイの展開について （351 ページ） の情報を確認します。

ステップ 1 Cisco Cloud Network Controller で VNet ピアリングを有効にします。

これらの指示については、「Azure 向け Cisco Cloud Network Controller の VNET ピアリングを構成する」を参照してください。

エクスプレス ルート ゲートウェイに必要なハブ VNet のゲートウェイ サブネットは、VNet ピアリングが有効な場合 Cisco Cloud Network Controller で展開されます。これは、エクスプレス ルート ゲートウェイの展開用にハブ VNet を準備するために行われます。

ステップ 2 非 ACI リモート サイトのネットワークを表すハブ VNet に外部 EPG を作成します。

- GUI を使用して外部 EPG を作成するには、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ） を参照してください。

  外部 EPG の **[ルート到達性（Route Reachability）]** で、**[外部サイト（External-Site）]** を選択します。

- REST API を使用して外部 EPG を作成するには、REST API を使用した外部クラウド EPG の作成 （185 ページ） を参照してください。

  タイプ **site-external** の外部クラウド EPG を作成します。

ステップ 3 Azure portal を通じて、ステップ 1 （353 ページ） で構成したゲートウェイ サブネットを使用してハブ VNet でエクスプレス ルート ゲートウェイを展開します。

ステップ 1 （353 ページ） で VNet ピアリングを有効にするときに選択したリージョンの数に応じて、Cisco Cloud Network Controller が管理する複数のリージョンでエクスプレス ルート ゲートウェイ アクセスが必要な場合は、それらの各リージョンにエクスプレス ルート ゲートウェイを個別に展開します。

a) Azure portal で、仮想ネットワーク ゲートウェイを作成する Resource Manager 仮想ネットワークに移動します。
b) 左側で、**[リソースの作成（Create a resource）]** を選択し、検索に**仮想ネットワーク ゲートウェイ**と入力します。
c) 検索結果で **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** を見つけて、エントリをクリックします。
d) **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** ページで、**[作成（Create）]** を選択します。

e) **[仮想ネットワーク ゲートウェイの作成（Create virtual network gateway）]** ページで、次のフィールドに適切な情報を入力します。

- **サブスクリプション**：適切なサブスクリプションが選択されていることを確認します。
- **リソース グループ**：仮想ネットワークを選択すると、リソース グループが自動的に選択されます。
- **名前**：エクスプレス ルート ゲートウェイの名前。
- **リージョン**：仮想ネットワークが配置されている場所を指すように **[リージョン（Region）]** フィールドを変更します。場所が仮想ネットワークのあるリージョンを指していない場合、仮想ネットワークは **[仮想ネットワークの選択（Choose a virtual network）]** ドロップダウンに表示されません。
- **ゲートウェイの種類**：**ExpressRoute** を選択します。
- **SKU**：ドロップダウンからゲートウェイ SKU を選択します。
- **仮想ネットワーク**：ステップ 1 （353 ページ） で Cisco Cloud Network Controller によって作成された仮想ネットワークを選択します。
- **パブリック IP アドレス**：**[新規作成（Create new）]** を選択します。
- **パブリック IP アドレス名**：パブリック IP アドレスの名前を指定します。

f) **[確認 + 作成（Review + Create）]** を選択し、**[作成（Create）]** でゲートウェイの作成を開始します。

設定が確認され、ゲートウェイが展開します。仮想ネットワーク ゲートウェイの作成には、完了までに最長 45 分かかります。

エクスプレス ルート ゲートウェイが正常に展開されたことを確認するには、Azure portal のネットワーク ゲートウェイ ページに移動し、タイプ **エクスプレス ルート** のネットワーク ゲートウェイが作成されたことを確認します。

追加のリージョンでエクスプレス ルート ゲートウェイ アクセスが必要な場合、それらのリージョンそれぞれにこれらの手順を繰り返します。

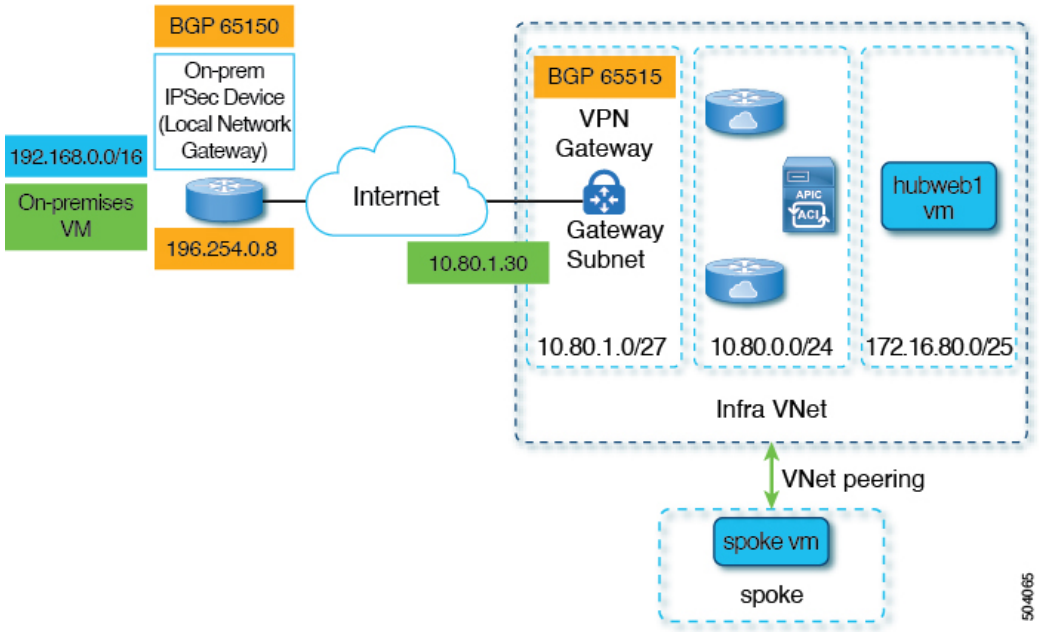
ステップ 4 エクスプレス ルート ゲートウェイで接続したクラウド EPG および外部 EPG 間の契約を構成します。

- GUI を使用して契約を作成するには、Cisco Cloud APIC GUI を使用したコントラクトの作成 （121 ページ） を参照してください。
- REST API を使用して契約を構成するには、REST API を使用したコントラクトの作成 （180 ページ） を参照してください。

VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成

リリース 25.0(2) 以降、VPN ゲートウェイを使用して、Cisco Cloud Network Controller で管理されたクラウド サイトと非 ACI リモート サイト間の接続を提供するためのサポートを利用できます。このタイプの接続では、仮想ネットワーク ゲートウェイ（VNG）がインフラ（ハブ）VNet に展開され、Cisco Cloud Network Controller で管理されたクラウド サイトから非 ACI リモート ブランチ サイトに接続できるようにします。BGP は、インフラ VNet の CCR ルータと VNG と、非 ACI リモート ブランチ サイトのオンプレミス IPsec デバイス（ローカル ネットワーク ゲートウェイ）との間のルーティング プロトコルとして IPsec トンネル上で実行されます。

次の図では、このタイプの接続による構成例を示します。



次の手順では、このタイプの接続を構成する方法について説明します。最終的には、192.168.20.0/24 サブネットにあるオンプレミスの仮想マシンと、172.16.80.0/25 サブネットにある `hubweb` 仮想マシンの間で到達可能です。

VPN ゲートウェイを使用した接続の構成

始める前に

これらの手順を続行する前に、VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （355 ページ） の情報を確認します。

ステップ 1 必要に応じて、Cloud APIC で VNet ピアリングを有効にします。

これらの手順については、「Azure 用 Cloud APIC の VNET ピアリングの構成」を参照してください。

ステップ 2 VPN ゲートウェイ サブネットの 2 番目のサブネットを追加します。

a) Cisco Cloud Network Controller GUI で、インテント アイコン（）をクリックし、**[Cloud APIC セットアップ（Cloud APIC Setup）]** を選択します。

b) **[リージョン管理（Region Management）]** エリアで、**[設定の編集（Edit Configuration）]** をクリックします。

c) **[管理するリージョン（Regions to Manage）]** ウィンドウで、**[次へ（Next）]** をクリックします。

[一般接続（General Connectivity）] ウィンドウが表示されます。

d) **[全般（General）]** 領域の **[クラウド ルータのサブネット プール（Subnet Pools for Cloud Routers）]** フィールドで、**[クラウド ルータのサブネット プールの追加（Add Subnet Pool for Cloud Routers）]** をクリックします。

e) VPN ゲートウェイ ルータの 2 番目のサブネットの情報を入力します。

たとえば、VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （355 ページ）の構成例を使用して、このフィールドの VPN ゲートウェイ ルーターの 2 番目のサブネットに `10.80.1.0/24` を追加します。

f) **[次へ（Next）]** をクリックし、次のページに必要な情報を入力して、**[保存して続行（Save and Continue）]** をクリックします。

Cloud APIC セットアップ プロセスが完了すると、Cisco Cloud Network Controller によって VPN ゲートウェイ ルータのサブネットが作成されます。VPN ゲートウェイ ルータのサブネットの構成が Azure に正常にプッシュされたことを確認するには、Azure portal の **[サブネット（Subnets）]** ページに移動し、**GatewaySubnet** エントリを見つけます。

ステップ 3 インフラでホストされる VRF を作成し、その VRF をサイト外部 EPG に使用します。

親インフラ VNet 内でホストされる VRF があるインフラ ホスト VRF を作成し、次の手順で作成するサイト外部 EPG にその VRF を使用します。

a) Cisco Cloud Network Controller GUI で、**[アプリケーション管理（Application Management）]** > **[VRF]** に移動します。

b) **[アクション（Actions）]** > **[VRF の作成（Create VRF）]** をクリックします。
[VRF の作成（Create VRF）] ウィンドウが表示されます。

c) このインフラでホストされる VRF の名前を入力し、**[テナントの選択（Select Tenant）]** をクリックし、テナントの **[インフラ（infra）]** を選択して [選択（Select）] をクリックします。

d) 必要に応じて説明を入力し、**[保存（Save）]** をクリックします。

ステップ 4 非 ACI リモート サイトのネットワークを示すハブ VNet で外部 EPG を作成します。

- GUI を使用して外部 EPG を作成するには、Cisco Cloud APIC GUI を使用した外部 EPG の作成 （97 ページ） を参照してください。

- 外部 EPG の **[VRF]** フィールドで、この外部 EPG 用に作成したインフラ ホスト VRF を選択します。
- 外部 EPG の **[ルート到達性（Route Reachability）]** で、**[外部サイト（External-Site）]** を選択します。

- REST API を使用して外部 EPG を作成するには、REST API を使用した外部クラウド EPG の作成（185 ページ） を参照してください。
  - このサイト外部 EPG には、インフラでホストされる VRF を使用します。
  - タイプ **site-external** の外部クラウド EPG を作成します。

ステップ 5 Azure portal を介して、ステップ 2（356 ページ） で構成した VPN ゲートウェイ サブネットのインフラ VNet に仮想ネットワーク ゲートウェイを作成します。

これらの手順では、オンプレミス サイトから Azure VPN ゲートウェイへの IPsec および BGP 接続を構築します。詳細については、Azure サイトの次の記事を参照してください。

https://docs.microsoft.com/en-gb/azure/virtual-network/virtual-network-configure-vnet-connections

a) Azure portal で、仮想ネットワーク ゲートウェイを作成する Resource Manager virtual network に移動して、仮想ネットワーク ゲートウェイを作成します。
b) 左側で、**[リソースの作成（Create a resource）]** を選択し、検索に**仮想ネットワーク ゲートウェイ**と入力します。
c) 検索結果で **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** を見つけて、エントリをクリックします。
d) **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** ページで、**[作成（Create）]** を選択します。
e) **[仮想ネットワーク ゲートウェイの作成（Create virtual network gateway）]** ページで、次のフィールドに適切な情報を入力します。
   - **サブスクリプション**：適切なサブスクリプションが選択されていることを確認します。
   - **リソース グループ**：仮想ネットワークを選択すると、リソース グループが自動的に選択されます。
   - **名前**：仮想ネットワーク ゲートウェイの名前。
   - **リージョン**：仮想ネットワークが配置されている場所を指すように **[リージョン（Region）]** フィールドを変更します。場所が仮想ネットワークのあるリージョンを指していない場合、仮想ネットワークは **[仮想ネットワークの選択（Choose a virtual network）]** ドロップダウンに表示されません。
   - **ゲートウェイ タイプ**：**[VPN]** を選択します。
   - **VPN タイプ**：**[Route-based]** を選択します。
   - **SKU**：**[VpnGw1]** を選択します。
   - **世代**：**[Generation1]** を選択します。

- **仮想ネットワーク**：**[overlay-1]** を選択します。
- **パブリック IP アドレス**：**[新規作成（Create new）]** を選択します。
- **パブリック IP アドレス名**：パブリック IP アドレスの名前を指定します。
- **アクティブ-アクティブ モードを有効にする**：**[無効（Disabled）]** に設定します。
- **BGP の構成**：**[有効（Enabled）]** に設定します。
- **自律システム番号（ASN）**: VPN ゲートウェイの適切な BGP ASN 値を入力します。デフォルトでは、Azure は 65515 の ASN 値を使用します。

f) **[確認 + 作成（Review + Create）]** を選択し、**[作成（Create）]** でゲートウェイの作成を開始します。

設定が確認され、ゲートウェイが展開します。仮想ネットワーク ゲートウェイの作成は、完了するまでに最長 45 分かかることがあります。

仮想ネットワーク ゲートウェイが正常に展開されたことを確認するには、[仮想ネットワーク ゲートウェイ（virtual network gateway）] ページに移動して、作成したばかりの仮想ネットワーク ゲートウェイを選択し、**[設定: 構成（Settings: Configuration）]** をクリックして、仮想ネットワーク ゲートウェイの構成設定を表示および確認します。

ステップ 6 ローカル ネットワーク ゲートウェイを作成します。

この構成では、ローカル ネットワーク ゲートウェイは、オンプレミスの IPsec デバイスを表すオブジェクトです。ローカル ネットワーク ゲートウェイを作成する前に、次のパラメータを準備します。

- BGP 自律システム番号（ASN）
- パブリック IP アドレス（Public IP address）
- 仮想ネットワーク ゲートウェイにアドバタイズする必要があるオンプレミス サブネットの適切なアドレス スペース

a) Azure portal で、ローカル ネットワーク ゲートウェイを作成する Resource Manager ローカル ネットワークに移動して、ローカル ネットワーク ゲートウェイを作成します。
b) 左側で**[リソースの作成（Create a resource）]** を選択し、検索に「**ローカル ネットワーク ゲートウェイ（Local Network Gateway）**」と入力します。
c) 検索結果で **[ローカル ネットワーク ゲートウェイ（Local network gateway）]** を見つけて、エントリをクリックします。
d) **[ローカル ネットワーク ゲートウェイ（Local network gateway）]** ページで、**[作成（Create）]** を選択します。
e) **[ローカル ネットワーク ゲートウェイの作成（Create local network gateway）]** ページで、次のフィールドに適切な情報を入力します。

- **名前**： ローカル ネットワーク ゲートウェイの名前。
- **エンドポイント**：**[IP アドレス（IP address）]** を選択します。
- **IP アドレス**：ローカル ネットワーク ゲートウェイの適切な IP アドレスを入力します。

- **アドレス スペース**：アドレス スペースに適切な値を入力します。たとえば、VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （355 ページ） の構成例を使用して、このフィールドに `192.168.0.0/16` を追加します。
- **BGP 設定の構成**：この設定を有効にするには、チェックボックスをクリックします。
- **自律システム番号（ASN）**：ローカル ネットワーク ゲートウェイの適切な BGP ASN 値を入力します。これは、リモート デバイスの ASN 値です。たとえば、VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （355 ページ） の構成例を使用して、このフィールドに `65150` を追加します。
- **BGP ピア IP アドレス**：このフィールドには、オンプレミス デバイスに使用する BGP ピア IP アドレスを入力します（Azure 仮想ネットワーク ゲートウェイではありません）。たとえば、VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （355 ページ） の構成例を使用して、このフィールドに `196.254.0.8` を追加します。
- **サブスクリプション**：ステップ 5 （357 ページ） の仮想ネットワーク ゲートウェイに使用したものと同じサブスクリプションを選択します。
- **リソース グループ**：ステップ 5 （357 ページ） の仮想ネットワーク ゲートウェイに使用したのと同じリソース グループを選択します。
- **場所**：ステップ 5 （357 ページ） の仮想ネットワーク ゲートウェイに使用したのと同じ場所（リージョン）を選択します。

f) **[確認 + 作成（Review + Create）]** を選択し、**[作成（Create）]** でゲートウェイの作成を開始します。

設定が確認され、ゲートウェイが展開します。

ローカル ネットワーク ゲートウェイが正常に展開されたことを確認するには、[ローカル ネットワーク ゲートウェイ（local network gateway）] ページに移動して、作成したばかりのローカル ネットワーク ゲートウェイを選択し、**[設定: 構成（Settings: Configuration）]** をクリックして、ローカル ネットワーク ゲートウェイの構成設定を表示および確認します。

ステップ 7 Azure 仮想ネットワーク ゲートウェイからローカル ネットワーク ゲートウェイ（オンプレミスの IPsec デバイス）への VPN 接続を作成します。

a) Azure portal で、仮想ネットワーク ゲートウェイのページに移動し、ステップ 5 （357 ページ） で作成した Azure 仮想ネットワーク ゲートウェイを見つけます。

b) 作成した仮想ネットワーク ゲートウェイを選択し、**[設定: 接続（Settings: Connections）]** をクリックします。

c) [追加] をクリックします。

[接続の追加（Add connection）] ウィンドウが開きます。

d) この VPN 接続を Azure 仮想ネットワーク ゲートウェイからローカル ネットワーク ゲートウェイ（オンプレミスの IPsec デバイス）に追加するために必要な情報を入力します。

- **[接続タイプ（Connection type）]** フィールドで、`[サイト間（IPsec） (Site-to-site (IPsec))]` を選択します。

- **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** フィールドで、ステップ 5 （357 ページ） で作成した Azure 仮想ネットワーク ゲートウェイを選択します。
- **[ローカル ネットワーク ゲートウェイ（Local network gateway）]** フィールドで、ステップ 6 （358 ページ） で作成したローカル ネットワーク ゲートウェイを選択します。
- **[BGP を有効にする（Enable BGP）]** フィールドでチェックボックスをクリックして、この接続の BGP を有効にします。
- **[IKE プロトコル（IKE Protocol）]** フィールドで、`[IKEv2]` を選択します。

e) この VPN 接続の構成情報の入力が完了したら、**[OK]** をクリックします。

ステップ 8 Azure から VPN 構成テンプレートをダウンロードします。

a) Azure portal で、仮想ネットワーク ゲートウェイのページに移動し、作成した Azure 仮想ネットワーク ゲートウェイを見つけます。ステップ 5 （357 ページ）

b) 作成した仮想ネットワーク ゲートウェイを選択し、[設定: 接続] をクリックします。

c) 構成した VPN 接続の名前を選択します。

VPN 接続の概要ページが表示されます。

d) **[ダウンロード構成（Download configuration）]** をクリックします。

[ダウンロード構成（Download configuration）] ページが表示されます。

e) **[ダウンロード構成（Download configuration）]** ページで次の選択を行います。

- **[デバイス ベンダー（Device vendor）]** フィールドで、`[Cisco]` を選択します。
- **[デバイス ファミリ（Device family）]** フィールドで、`[IOS（ISR、ASR）]` を選択します。
- **[ファームウェア バージョン（Firmware version）]** フィールドで、`[15.x (IKEv2)]` を選択します。

f) **[ダウンロード構成（Download configuration）]** をクリックします。

ステップ 9 ダウンロードした構成テンプレート ファイルをテキスト エディタで開き、構成テンプレートの指示に従って必要な編集を行います。

通常、構成テンプレートで必要な変更は、BGP 構成の次のフィールドのみです。

- **LOCAL_ROUTE**：Azure にアドバタイズする必要があるネットワークである必要があります。たとえば、VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （355 ページ） の構成例を使用すると、このフィールドに `192.168.0.0` と入力します。
- **LOCAL_MASK**：`255.255.255.0` でなければなりません

ステップ 10 編集した構成テンプレートを保存して閉じます。

ステップ 11 編集した構成テンプレートをオンプレミスの IPsec デバイスに適用します。

VPN Gateway（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （355 ページ） の設定例に基づいて編集された構成テンプレートの例を次に示します。

```
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.0.0 0.0.0.127
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.0.128 0.0.0.127
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.1.0 0.0.0.127
access-list 101 permit esp host 52.152.235.192 host 173.39.125.130
access-list 101 permit udp host 52.152.235.192 eq isakmp host 173.39.125.130
access-list 101 permit udp host 52.152.235.192 eq non500-isakmp host 173.39.125.130
!
crypto ikev2 proposal Azure-Ikev2-Proposal
  encryption aes-cbc-256
  integrity sha1
  group 2
  exit
!
crypto ikev2 policy Azure-Ikev2-Policy
  proposal Azure-Ikev2-Proposal
  match address local 173.39.125.130
  exit
!
crypto ikev2 keyring singaporeisr-keyring
  peer 52.152.235.192
    address 52.152.235.192
    pre-shared-key 0123456789cisco
    exit
  exit

crypto ikev2 profile Azure-Ikev2-Profile
  match address local 173.39.125.130
  match identity remote address 52.152.235.192 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  lifetime 28800
  dpd 10 5 on-demand
  keyring local singaporeisr-keyring
  exit
!
crypto ipsec transform-set Azure-TransformSet esp-aes 256 esp-sha256-hmac
  mode tunnel
  exit
!
crypto ipsec profile Azure-IPsecProfile
  set transform-set Azure-TransformSet
  set ikev2-profile Azure-Ikev2-Profile
  set security-association lifetime seconds 3600
  ! Note: PFS (perfect-forward-secrecy) is an optional feature (commented out)
  !set pfs None
  exit
!
int tunnel 11
  ip address 169.254.0.1 255.255.255.255
  tunnel mode ipsec ipv4
  ip tcp adjust-mss 1350
  tunnel source 173.39.125.130
  tunnel destination 52.152.235.192
  tunnel protection ipsec profile Azure-IPsecProfile
  exit

interface Loopback 11
  ip address 196.254.0.8 255.255.255.255
  exit
!
router bgp 65150
  bgp log-neighbor-changes
  neighbor 10.80.1.30 remote-as 65515
```

```
  neighbor 10.80.1.30 ebgp-multihop 255
  neighbor 10.80.1.30 update-source loopback 11

  address-family ipv4
    network 192.168.0.0 mask 255.255.0.0
    neighbor 10.80.1.30 activate
    exit
  exit
!
ip route 10.80.0.0 255.255.255.128 Tunnel 11
ip route 10.80.0.128 255.255.255.128 Tunnel 11
ip route 10.80.1.0 255.255.255.128 Tunnel 11
ip route 10.80.1.30 255.255.255.255 Tunnel 11
```

ステップ 12 VPN 接続を確認します。

a) Azure portal で、仮想ネットワーク ゲートウェイのページに移動し、作成した Azure 仮想ネットワーク ゲートウェイを見つけます。ステップ 5 （357 ページ）

b) 作成した仮想ネットワーク ゲートウェイを選択し、[設定: 接続] をクリックします。

c) 作成した VPN 接続が [ステータス（Status）] 列に **[接続済み（Connected）]** と表示されていることを確認します。

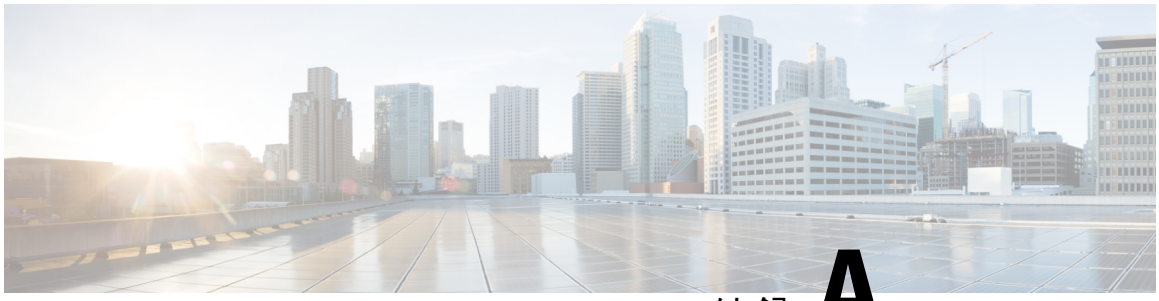
ステップ 13 リダイレクトを使用して仮想ネットワーク ゲートウェイを展開するかどうかを決定します。

- リダイレクトなしで仮想ネットワーク ゲートウェイを展開する場合は、ステップ 14 （362 ページ）に進みます。
- リダイレクトを使用して仮想ネットワーク ゲートウェイを展開する場合は、リダイレクト用にサービス デバイスを構成します。

  GUI または REST API を使用してリダイレクト用にサービス デバイスを設定するには、レイヤ 4 から レイヤ 7 サービスの展開 （209 ページ） を参照してください。

ステップ 14 クラウド EPG と、仮想ネットワーク ゲートウェイによって接続された外部 EPG との間の契約を構成します。

- GUI を使用して契約を作成するには、Cisco Cloud APIC GUI を使用したコントラクトの作成 （121 ページ） を参照してください。
- REST API を使用して契約を構成するには、REST API を使用したコントラクトの作成 （180 ページ）を参照してください。



付録 A

Cisco Cloud APIC エラーコード

Cisco Cloud APIC エラーコード

ここでは、Cisco Cloud APIC のエラー コードについて説明します。

表 *46 : Cisco Cloud APIC* エラー コード

コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_INFRANETWORK_COUNT	`cloudtemplateInfraNetwork` MOの数は最大 1 です。
cloud-template	CT_INFRANETWORK_VRF	`cloudtemplateInfraNetwork` MOでは、vrfName を overlay-1 にする必要があります。
cloud-template	CT_INFRANETWORK_PARENT	`cloudtemplateInfraNetworkMO` の場合、親 MO は uni/tn-infra である必要があります。
cloud-template	CT_INFRANETWORK_NUMROUTERSPERREGION_MINIMUM	`cloudtemplateInfraNetwork` MO では、属性 `numRoutersPerRegion` の最小許容値は 2 です。
cloud-template	CT_INFRANETWORK_NUMROUTERSPERREGION_MAXIMUM	`cloudtemplateInfraNetwork` MO では、属性 `numRoutersPerRegion` の最大許容値は 4 です。
cloud-template	CT_INTNETWORK_COUNT	`cloudtemplateIntNetwork` MO の数は最大 1 です

コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_EXTNETWORK_COUNT	`cloudtemplateExtNetwork` MO の数は最大 1 です
cloud-template	CT_VPNNETWORK_COUNT	`cloudtemplateVpnNetwork` MO の数は最大 1 です
cloud-template	CT_OSPF_COUNT	`cloudtemplateOspf` MO の数は最大 1 です
cloud-template	CT_INTNETWORK_REGION_MATCH	`cloudtemplateIntNetwork` で `cloudRegionName` によって指定されたリージョンには、`cloudProvP` で対応する `cloudRegion` が必要です。
cloud-template	CT_INTNETWORK_REGION_MANAGED	`cloudtemplateIntNetwork` の `cloudRegionName` の子によって指定されたリージョンには、`adminSt` が管理対象の対応する `cloudRegion` が必要です。
cloud-template	CT_INTNETWORK_REGION_MAXIMUM	`cloudtemplateIntNetwork` で指定されるリージョンの最大数（`cloudRegionName`）は 4 です
cloud-template	CT_EXTNETWORK_REGION_SUBSET	`cloudtemplateExtNetwork` の `cloudRegionName` の子によって指定されたリージョンは、`cloudtemplateIntNetwork` の下の `cloudRegionName` の子によっても指定する必要があります。
cloud-template	CT_EXTNETWORK_REQUIRES_EXTSUBNETPOOL	`cloudtemplateExtNetwork` の存在には、`cloudtemplateExtSubnetPool` の存在が必要です。
cloud-template	CT_EXTSUBNETPOOL_COUNT	`cloudtemplateExtSubnetPool` の数は最大 1 です
cloud-template	CT_EXTSUBNETPOOL_SUBNETPOOL_ADDRESS	`cloudtemplateExtSubnetPool` では、サブネットプールにネットワーク アドレスが含まれている必要があります。

コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_EXTSUBNETPOOL_SUBNETPOOL_IP_VERSION	`cloudtemplateExtSubnetPool` では、サブネットプールに IPv4 アドレスが含まれている必要があります
cloud-template	CT_EXTSUBNETPOOL_SUBNETPOOL_ADDRESS_TYPE	`cloudtemplateExtSubnetPool` では、サブネットプール の IP アドレスはマルチキャストまたはループバック アドレス空間からのものであってはなりません
cloud-template	CT_EXTSUBNETPOOL_SUBNETPOOL_MINIMUM_SIZE	`cloudtemplateExtSubnetPool` では、サブネット プールは /22 以上である必要があります（ネットマスクは 22 以下である必要があります）。
cloud-template	CT_EXTSUBNETPOOL_AND_REMOTESITE	`cloudtemplateExtSubnetPool` は、cloudtemplateRemoteSite ごとに少なくとも 1 つの `cloudtemplateRemoteSiteSubnetPool` を持つのに十分な大きさである必要があります。
cloud-template	CT_INTNETWORK_MISSING_HOME	`cloudtemplateIntNetwork` の下に `cloudRegionName` がある場合は、`cloudRegonName`の 1 つを cAPIC のホーム リージョン（`capicDeployed`）に関連付ける必要があります。
cloud-template	CT_CLOUD_APICSUBNETPOOL_INSUFFICIENT	`cloudApicSubnetPool MO` は、`cloudApicSubnet MO` を生成するために十分な数である必要があります。これにより、`cloudtemplateIntNetwork` で指定されたすべての `cloudRegionName MO` を一意の `cloudApicSubnet MO` に関連付けることができます。`cloudApicSubnet` MO からのサブネットは、対応するリージョンの `cloudCtxProfile` で CIDR として使用されます。

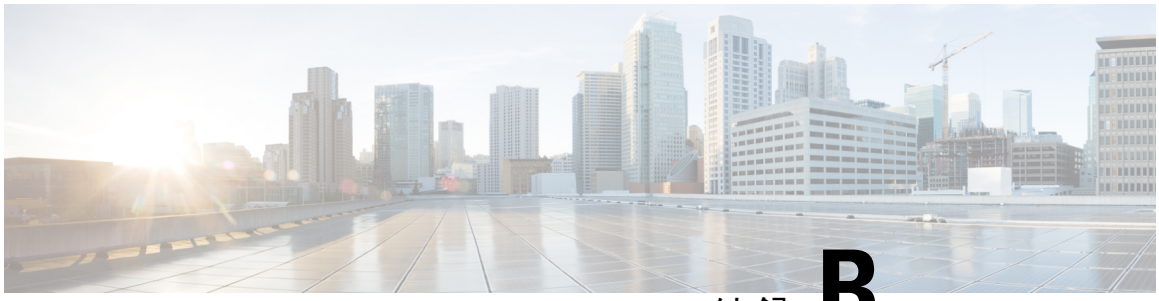
コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_IPSECTUNNEL_PEERADDR_IP_VERSION	`cloudtemplateIpSecTunnel` では、peeraddr に IPv4 アドレスを含める必要があります。
cloud-template	CT_IPSECTUNNEL_PEERADDR_IS_HOST	`cloudtemplateIpSecTunnel` では、peeraddr はホストアドレス（/32 など）である必要があります。
cloud-template	CT_PROFILE_COUNT	`cloudtemplateProfile` MO のカウントは最大 1 です
cloud-template	CT_PROFILE_DELETE	`cloudtemplateProfile` MO は、親の `cloudtemplateInfraNetwork` も削除されない限り、削除できません。
cloud-template	CT_AZURE_PROFILE_ROUTERUSERNAME_INVALID	Azure では、一部のユーザー名（admin、root など）が無効であり、ピリオドで終わらないようにしてください。
cloud-template	CT_AZURE_PROFILE_ROUTERUSERNAME_TOO_LONG	Azure では、ユーザー名は最大 20 文字に制限されています。
cloud-template	CT_PROFILE_ROUTERUSERNAME_NONEMPTY	`cloudtemplateProfile` では、`routerUsername` は空でない必要があります。
cloud-template	CT_PROFILE_ROUTERPASSWORD_NONEMPTY	`cloudtemplateProfile` では、`routerLicenseToken` に無効な文字を含めることはできません。
cloud-template	CT_PROFILE_ROUTERTHROUGHPUT_MODIFY	`cloudtemplateProfile` では、`routerThroughput` は、いずれかのリージョン（つまり、`cloudtemplateIntNetwork` の下にある `cloudRegionName`）にルータが展開されている場合は変更できません。（どのリージョンにもルータが導入されていない場合は、変更が許可されます）。

コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_PROFILE_ROUTERLICENSETOKEN_INVALID_CHARACTER	`cloudtemplateProfile` では、`routerPassword` は空でない必要があります。
cloud-template	CT_APICSUBNET_INVALID_HOME_REGION	`cloudApicSubnet` MO では、`capicDeployed` としてマークされたリージョンは有効なリージョンである必要があります。
cloud-template	CT_APICSUBNET_REPEATED_REGION	`cloudApicSubnet` MO では、リージョンを最大1つのサブネットに関連付けることができます。
cloud-template	CT_APICSUBNET_MULTIPLE_HOME_REGION	`cloudApicSubnet` MO では、最大で 1 つのリージョンが `capicDeployed`を true に設定できます。
cloud-template	CT_HUBNETWORK_COUNT	`cloudtemplateHubNetwork` MO の数は最大1です
クラウド	CLOUD_APICSUBNETPOOL_CREATEDBY_USER	`cloudApicSubnetPool` では、`createdBy` 属性は USER である必要があります
クラウド	CLOUD_APICSUBNETPOOL_SUBNET_IP_VERSION	`cloudApicSubnetPool` では、サブネットに IPv4 アドレスが含まれている必要があります。
クラウド	CLOUD_APICSUBNETPOOL_SUBNET_SIZE	`cloudApicSubnetPool`では、サブネットは /24 である必要があります。
クラウド	CLOUD_APICSUBNETPOOL_DELETE_USAGE	`cloudApicSubnetPool` は、その `cloudApicSubnet` 子の少なくとも1つがリージョンで使用されている場合は削除できません。
クラウド	CLOUD_APICSUBNETPOOL_DELETE_CREATEDBY	`createdBy` 属性が USER ではない `cloudApicSubnetPool` は削除できません。
クラウド	CLOUD_AZURE_CTXPROFILE_SUBNET_RENAME	`cloudSubnet` 名は変更できません

コンポーネント	エラー コード（**Error Code**）	制約
クラウド	CLOUD_AZURE_CTXPROFILE_SUBNET_DUPLICATE	同じ `cloudCtxProfile` 内の 2 つの `cloudSubnet` に同じ名前を付けることはできません
クラウド	CLOUD_CAPIC_IP_EXT_EPG_SELECTOR_MAXIMUM	クラウド APIC IP に対応する `cloudExtEPg` には最大1つの `cloudExtEpSelector` があります
クラウド	CLOUD_AZURE_ACCOUNT_IN_USE	アカウントが使用中で、コンテキスト プロファイルが展開されている間は、アカウントとテナント間の関連付けを更新または削除することはできません。
クラウド	CLOUD_AZURE_INFRA_ACCOUNT_CHANGE	テナント インフラのアカウントは変更または削除できません
クラウド	CLOUD_SOURCE_PORT_NOT_SUPPORTED	送信元ポート範囲はクラウド APIC では許可されていません
クラウド	CLOUD_ONLY_PERMIT_ACTION_SUPPORTED	「許可」とは異なるアクションはクラウド APIC ではサポートされていません
クラウド	CLOUD_CIDR_OVERLAP	`cloudCidr` のサブネットはオーバーラップできません
クラウド	CLOUD_SUBNET_USAGE	特定のゾーンには最大で1つのゲートウェイ サブネットが存在でき、各ユーザー サブネットは同じユーザー サブネットのゾーンに正確に 1 つのゲートウェイ サブネットを持つ必要があります。
クラウド	CLOUD_AZURE_ACCOUNT_CRED_CROSS_TENANT	`cloudAccount` によって使用される `cloudCredentials` は、同じテナントにある必要があります
クラウド	CLOUD_AZURE_ACCOUNT_AD_CROSS_TENANT	`cloudAccount` によって使用される `cloudAd` は、同じテナントにある必要があります

コンポーネント	エラー コード（Error Code）	制約
cloud-template	CT_CLOUD_APICSUBNETPOOL_INSUFFICIENT_HUBNETWORK	cloudApicSubnetPool MO は、cloudApicSubnet MO を生成するために十分な数である必要があります。これにより、cloudtemplateIntNetwork で指定されたすべての cloudRegionName MO を一意の cloudApicSubnet MO に関連付けることができます。cloudApicSubnet MO からのサブネットは、対応するリージョンの cloudCtxProfile で CIDR として使用されます。HubNetworking を有効にすると、cloudtemplateIntNetwork の下の cloudRegionName と同じ数の cloudApicSubnetPool が必要になります。
クラウド	CLOUD_SYSTEM_MO_IS_IMMUTABLE	システムによって作成されたインスタンスは不変です
cloud-template	CT_BGPEVPN_PEERADDR_IP_VERSION	cloudtemplateBgpEvpn では、peeraddr に IPv4 アドレスを含める必要があります。
cloud-template	CT_BGPEVPN_PEERADDR_ADDRESS_TYPE	cloudtemplateBgpEvpn では、peeraddr IP アドレスはホストアドレスである必要があります
クラウド	CLOUD_APICSUBNETPOOL_SUBNET_HOST_PART	cloudApicSubnetPool サブネットでは、ホスト部分は 0 である必要があります。
cloud-template	CT_EXTSUBNETPOOL_CLOUD_APICSUBNETPOOL_OVERLAP	cloudtemplateExtSubnetPool と cloudApicSubnetPool の間にサブネットのオーバーラップがあります。

Cisco Cloud APIC エラーコード



付録 B

サービス EPG 構成例

サービス EPG の詳細については、以下を参照してください。

- クラウド サービス エンドポイント グループ （42 ページ）
- Cisco Cloud APIC GUI を使用したサービス EPG の作成 （106 ページ）
- REST API を使用したサービス EPG の作成 （185 ページ）

次のセクションにサービス EPC の構成例を示します。

- Azure Kubernetes Services（AKS）サービス EPG 構成例 （371 ページ）

Azure Kubernetes Services（AKS）サービス EPG 構成例

このセクションでは、次の設定を持つサービス EPG 例を構成する手順を説明します。

- **サービス タイプ**：Azure Kubernetes Services（AKS）
  - Azure Kubernetes Services（AKS）には、他のサービスへのアクセスが必要です。
  - Cisco Cloud APIC は、ここにリストされているルールのプログラミングを自動化します。

    https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic#required-outbound-network-rules-and-fqdns-for-aks-clusters
- **展開タイプ**：管理対象クラウド ネイティブこのタイプの展開では、サービスは VNet またはサブネットでインスタンス化されます（Cisco Cloud APIC を介して作成）。たとえば、Azure Kubernetes Services（AKS）サービスは、Cisco Cloud APIC によって管理されるサブネットに展開できます。
- **アクセス タイプ**：プライベート

AKS のこのサンプル サービス EPG を構成する手順は、次のセクションで提供されます。

クラウド コンテキスト プロファイルでサブネットの作成

これらの手順では、Azure Kubernetes Services（AKS）サービス EPG によって使用されるクラウド コンテキスト プロファイルにサブネットを作成する方法について説明します。これらの手順では、Cisco Cloud APIC GUI を使用して設定を行います。

始める前に

- 1 つのブラウザ ウィンドウで、Cisco Cloud APIC GUI にログインします。
- 別のブラウザ ウィンドウで、Cisco Cloud APIC インフラ テナントの Azure アカウントにログインし、Azure 管理ポータルに移動します。

  https://portal.azure.com/#home

ステップ 1 Cisco Cloud APIC GUI で、**[インテント（Intent）]** アイコンをクリックします。

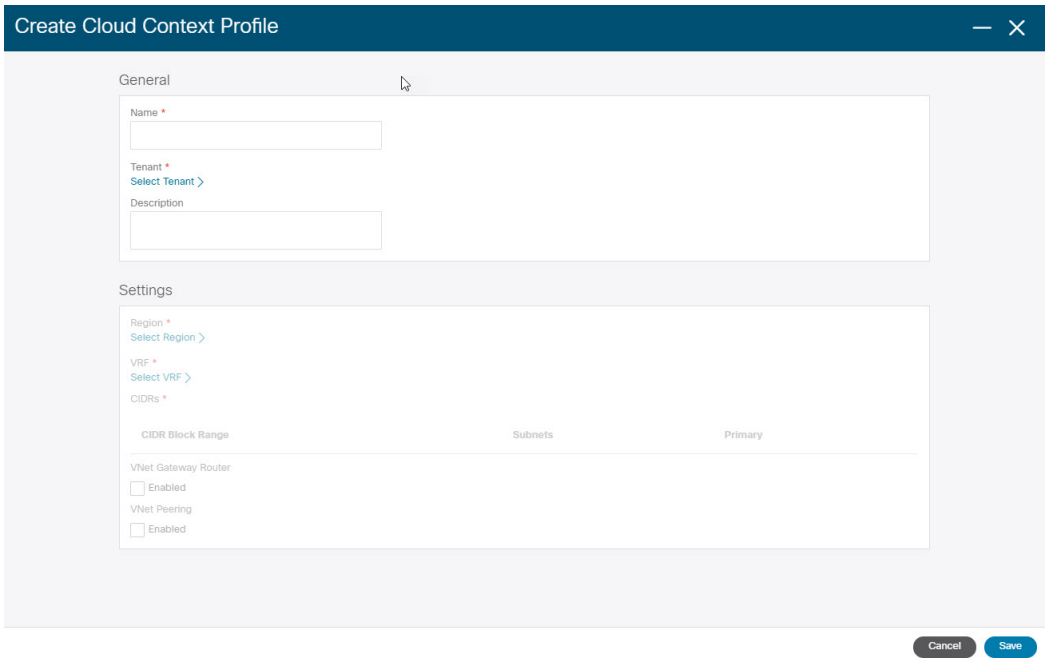
[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[クラウド コントラクト プロファイルの作成（Create Cloud Context Profile）]** をクリックします。

[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）] ウィンドウが表示されます。



ステップ 4 **[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ウィンドウに次の情報を入力します。

- **名前**：クラウド コンテキスト プロファイルの名前を入力します。たとえば、**ct_ctxprofile_eastus** です。
- **テナント**：**[テナントの選択（Select Tenant）]** をクリックし、このユース ケースのクラウド コンテキスト プロファイルのテナントを選択して、**[選択（Select）]** をクリックします。
- **リージョン**：**[リージョンの選択（Select Region）]** をクリックし、リージョン（例：**eastus**）を選択し、**[選択（Select）]** をクリックします。
- **VRF**：**[VRF の選択（Select VRF）]** をクリックし、適切な VRF を選択し、**[選択（Select）]** をクリックします。
- **CIDR の追加**： CIDR 情報を入力します。
  1. **[CIDR の追加（Add CIDR）]** をクリックします。
  2. **[CIDR ブロック範囲（CIDR Block Range）]** フィールドにアドレスを入力します。

     たとえば、`30.1.0.0/16` です。
  3. **[プライマリ（Primary）]** チェック ボックスをオフ（無効）にします。
  4. **[サブネットの追加（Add subnet）]** をクリックして、サブネット アドレスを **[アドレス（Address）]** に入力します。

     たとえば、`30.1.0.0/17` です。AKS クラスタには 338 個のアドレスが必要であることに注意してください。
  5. [追加] をクリックします。
- **VNet ゲートウェイ ルータ**： このフィールドのボックスをオフ（選択解除）したままにします。
- **VNet ピアリング**：VNet ピアリングを有効にするには、このボックスをオンにします。

ステップ 5 設定が終わったら [Save] をクリックします。

次のタスク

「AKS のクラウド サービス EPG の作成 （373 ページ）」に進みます。

AKS のクラウド サービス EPG の作成

これらの手順では、Azure Kubernetes Services (AKS) サービス タイプでクラウド サービス EPG を作成する方法について説明します。これらの手順では、Cisco Cloud APIC GUI を使用して設定を行います。

サービス EPG 構成例

始める前に

これらの手順に進む前に、クラウドコンテキストプロファイルでサブネットの作成（372ページ） の手順を完了してください。

ステップ 1 Cisco Cloud APIC GUI で、**[インテント（Intent）]** アイコンをクリックします。

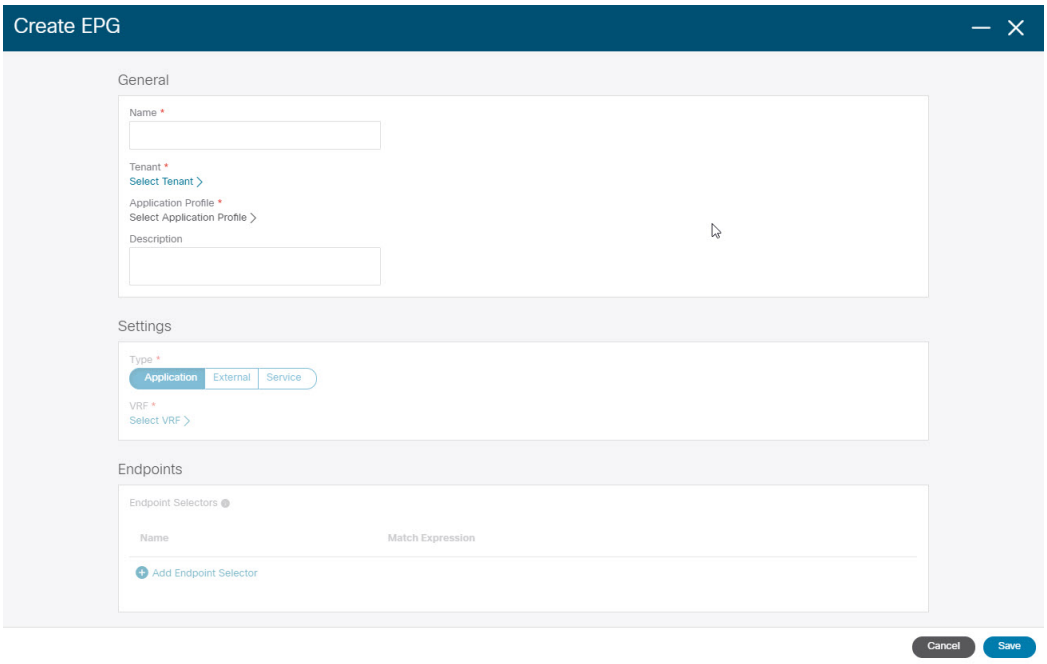
[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。

[EPG の作成（Create EPG）] ウィンドウが表示されます。



ステップ 4 **[EPG の作成（Create EPG）]** ウィンドウに次の情報を入力します。

- **名前**：クラウド サービス EPG の名前を入力します。たとえば、**svc-Hub-AzureAKS** などです。
- **テナント**：**[テナントの選択（Select Tenant）]** をクリックし、このユース ケースのクラウド サービス EPG のテナントを選択してから、**[選択（Select）]** をクリックします。
- **アプリケーション プロファイル**：**[アプリケーション プロファイルの選択（Select Application Profile）]** をクリックし、アプリケーション プロファイルを選択してから、**[選択（Select）]** をクリックします。

- **タイプ**：EPG タイプとして **[サービス（Service）]** を選択します。
- **VRF**：**[VRF の選択（Select VRF）]** をクリックし、適切な VRF を選択し、**[選択（Select）]** をクリックします。
- **サービス タイプ**：**Azure Kubernetes Services (AKS)** サービス タイプを選択します。
- **展開タイプ**：**クラウド ネイティブ管理対象**の展開タイプを選択します。
- **アクセス タイプ**：**[プライベート（Private）]** アクセス タイプを選択します。

ステップ 5 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックします。

[エンドポイント セレクタの追加（Add Endpoint Selector）] ウィンドウが表示されます。

このユース ケースでは、IP アドレスが前のステップで構成されたサブネット情報 `30.1.0.0/17` と一致するエンドポイント セレクタを作成します。エンドポイント セレクタの IP アドレスが前の手順のサブネットと一致することで、Cisco Cloud APIC は NSG をプログラムして、このサービス タイプに必要なすべてのルールを許可するようになります。

ステップ 6 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ウィンドウの **[Name（名前）]** フィールドに名前を入力します。

ステップ 7 **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。

この時点で、**IP** はこのアクセス タイプのキーとして唯一のオプションです。

ステップ 8 **[演算子（Operator）]** ドロップダウン リストをクリックし、**[equals]** を選択します。

ステップ 9 **[値（Value）]** フィールドに `30.1.0.0/17` と入力し、チェックマークをクリックしてエントリを検証します。

ステップ 10 [Add] をクリックします。

ステップ 11 設定が終わったら [Save] をクリックします。

次のタスク

「アウトバウンド セキュリティ ルールの確認 （375 ページ）」に進みます。

アウトバウンド セキュリティ ルールの確認

これらの手順では、必要なアウトバウンド セキュリティ ルールが正しく構成されていることを確認する方法について説明します。Cisco Cloud APIC は、AKS を Azure ポータルに展開するために必要なすべてのアウトバウンド セキュリティ ルールを Azure で構成します。

始める前に

これらの手順に進む前に、AKS のクラウド サービス EPG の作成 （373 ページ） の手順を完了してください。

ステップ 1 Azure ポータルで、自動的に作成されたサブネットのネットワーク セキュリティ グループに移動します。

a) 適切なリソース グループに移動します。
b) AKS サービス EPG に使用されたサブネットを選択します。
c) 必要なアウトバウンド セキュリティ グループを見つけます。

ステップ 2 ページで **[アウトバウンド セキュリティ ルール（Outbound security rules）]** 領域を見つけ、NSG のアウトバウンド セキュリティ ルールが正しく構成されていることを確認します。

アウトバウンド セキュリティ ルールの詳細については、次を参照してください。

https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic

次のタスク

「Kubernetes サービスの作成 （376 ページ）」に進みます。

Kubernetes サービスの作成

これらの手順では、Kubernetes サービスを作成する方法について説明します。これらの手順では、Azure portal を使用して構成を行います。

（注） 次の手順では、Azure portal を使用して Kubernetes サービスを作成する方法について説明します。Kubernetes サービスを作成するための代替方法も、「Cisco Cloud APIC での Azure Kubernetes サービス の使用」に関するドキュメントで提供されています。

始める前に

これらの手順に進む前に、アウトバウンド セキュリティ ルールの確認 （375 ページ） の手順を完了してください。

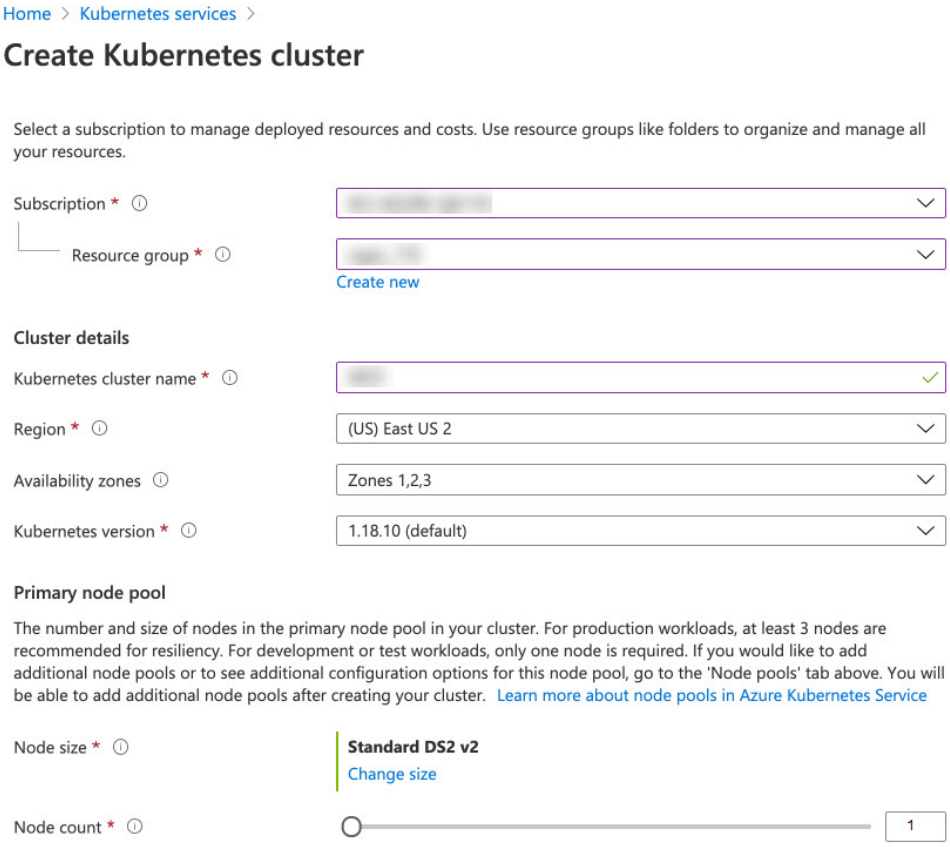
ステップ 1 Azure portal で、`Microsoft による Kubernetes サービス` という用語を検索し、検索結果をクリックします。

[Kubernetes サービス（Kubernetes Service）] ページが表示されます。

ステップ 2 **[Kubernetes サービス（Kubernetes Service）]** ページで **[作成（Create）]** をクリックします。

[Kubernetes クラスタの作成（Create Kubernetes cluster）] ページが表示されます。

サービス EPG 構成例

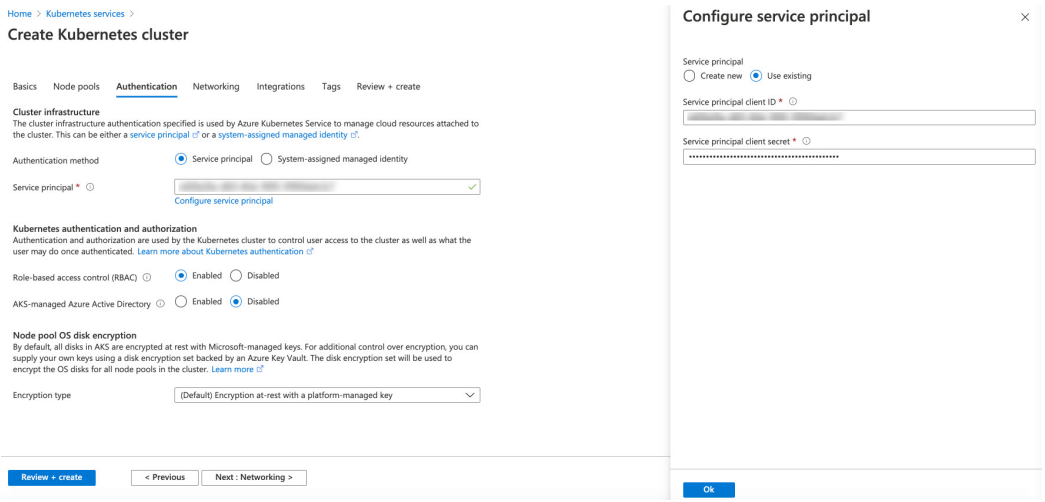


ステップ 3 **[基本（Basics）]** タブで、次の領域を構成します。

- **サブスクリプション**：適切なサブスクリプションを選択します。
- **リソース グループ**：適切なリソース グループを選択します。
- **Kubernetes クラスタ名**：この Kubernetes クラスタの一意の名前を入力します。
- **リージョン**：適切なリージョンを選択します。
- **Kubernetes バージョン**：デフォルトの選択をそのままにします。
- **ノード サイズ**：デフォルトの選択をそのままにします。
- **ノード数**：このフィールドのエントリが 1 になるように、スクロール バーが左端にあることを確認します。

ステップ 4 **[次へ：ノード プール（Next: Node pools）]** をクリックします。デフォルトのエントリをそのままにして、**[次へ：認証（Next: Authentication）]** をクリックして **[認証（Authentication）]** タブに進みます。

サービス EPG 構成例



ステップ 5 **[認証（Authentication）]** タブで、次の領域を構成します。

- **認証方法**：**[サービス プリンシパル（Service principal）]** を選択します。

  [サービス プリンシパル（Service principal）] フィールドが表示されます。

- **サービス プリンシパル**：**[サービス プリンシパルの構成（Configure service principal）]** をクリックします。

  [サービス プリンシパルの構成（Configure service principal）] ウィンドウで、次の領域を構成します。

  - **サービス プリンシパル**：**[新規作成（Create new）]** または **[既存のものを使用（Use existing）]** を選択します。

    [既存のものを使用（Use existing）] を選択した場合は、既存のサービス プリンシパルについて次の情報を入力します。

    - **サービス プリンシパルのクライアント ID**
    - **サービス プリンシパルのクライアント シークレット**

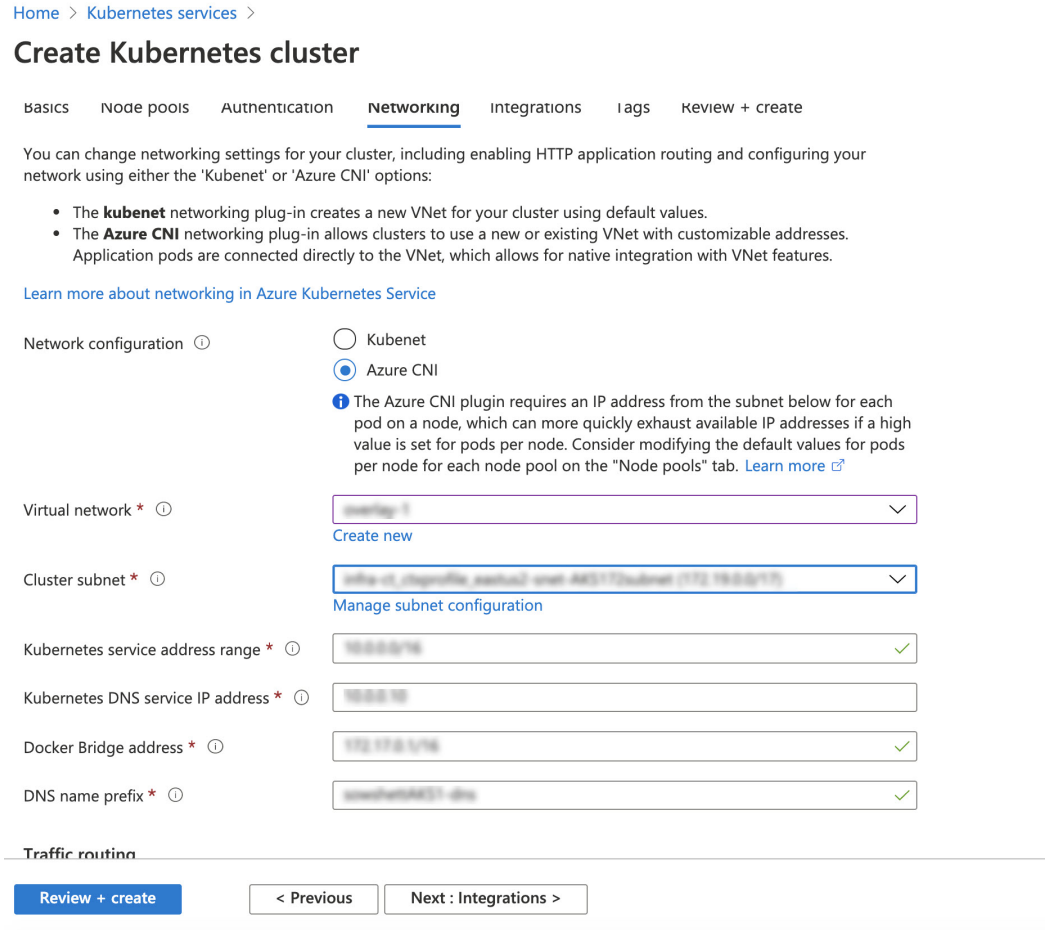
  （注） これら 2 つのフィールドに入力するエントリをメモします。これらのフィールドのエントリは、これらの手順の後半で使用します。

  [OK] をクリックして、**[Kubernetes クラスタの作成（Create Kubernetes cluster）]** ウィンドウの **[認証（Authentication）]** タブに戻ります。

- **ロールベース アクセス コントロール（RBAC）**：**[有効（Enabled）]** を選択します。
- **AKS で管理される Azure Active Directory**：**[無効（Disabled）]** を選択します。
- **暗号化タイプ**：デフォルトの選択をそのままにします。

ステップ 6 **[次へ：ネットワーク（Next: Networking）]** をクリックして、**[ネットワーキング（Networking）]** タブに進みます。

サービス EPG 構成例



ステップ 7 **[ネットワーキング（Networking）]** タブで、次の領域を構成します。

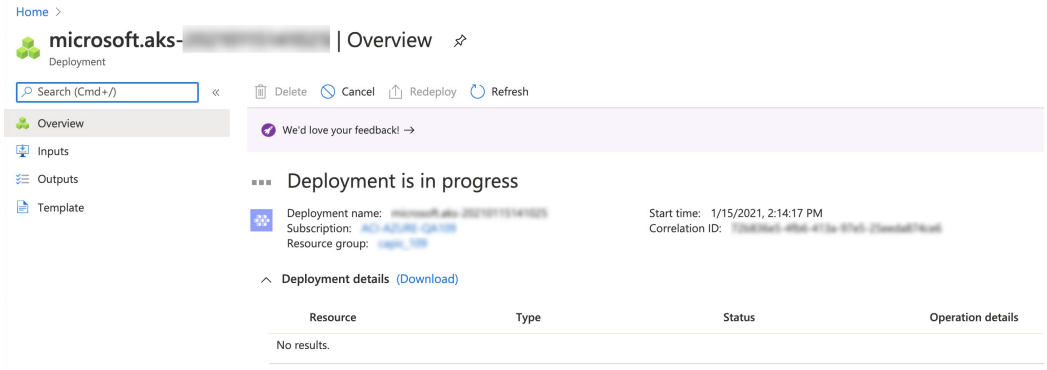
- **ネットワーク構成**：**[Azure CNI]** を選択します。
- **仮想ネットワーク**：対応する仮想ネットワークを選択します。
- **クラスタ サブネット**：Cisco Cloud APIC で管理されるサブネットを選択します。
- **Kubernetes サービスのアドレス範囲**：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **Kubernetes DNS サービスの IP アドレス**：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **Docker Bridge アドレス**：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **DNS 名のプレフィックス**：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **ロード バランサ**：Standard

- **HTTP アプリケーション ルーティングを有効にする**：デフォルトの選択をそのままにするか（有効にしない）、必要に応じてエントリを変更します。
- **プライベート クラスタを有効にする**：必要に応じて、デフォルトの選択をそのまま（無効）にするか、エントリを変更します。

ステップ 8 **[次へ： 統合（Next: Integration）]**、**[次へ：タグ（Next: Tags）]** の順にクリックして、デフォルトのエントリを変更せずにこれらの画面を進め、**[次へ：確認 + 作成（Next: Review+Create）]** をクリックします。

ステップ 9 **[確認 + 作成（Review+Create）]** ウィンドウで **[作成（Create）]** をクリックし、検証に合格した後にもう一度 **[作成（Create）]** をクリックして Kubernetes クラスタを作成します。

「展開が進行中」というメッセージが表示され、Kubernetes サービスの [概要（Overview）] 画面が表示されます。



先に進む前に、Kubernetes サービスが正常に展開されるまで待ちます（展開にかかる時間は異なります）。このプロセスが完了すると、メインの AKS サービスは元のリソース グループに含まれます。Azure はすべての agentpools VM スケール セットを使用して、Kubernetes サービス専用の追加のリソース グループも作成します。

次のタスク

「新しい Kubernetes サービスの確認 （380 ページ）」に進みます。

新しい Kubernetes サービスの確認

これらの手順では、新しい Kubernetes サービスが、Kubernetes サービス専用に作成されたリソース グループにあることを確認する方法について説明します。

始める前に

これらの手順に進む前に、Kubernetes サービスの作成 （376 ページ） の手順を完了してください。

サービス EPG 構成例

ステップ 1 Azure portal で、左側のナビゲーション バーの **[リソース グループ（Resource groups）]** をクリックして、リソース グループ ページに移動します。

ステップ 2 **[リソース グルー（Resource groups）]** ページで、Kubernetes サービス専用に作成されたリソース グループを見つけ、そのリソース グループのリンクをクリックします。

Kubernetes サービス専用に作成されたリソース グループは、次の形式になります。

`MC_resourcegroupname_clustername_region`

それぞれの説明は次のとおりです。

- *resourcegroupname* は、Kubernetes サービス専用に作成されたリソース グループの名前です（`MC_aks` は、Azure によってデフォルトで使用されるリソース グループ名です）。
- *clustername* は、ステップ 3 （377 ページ） の Kubernetes サービスの作成 （376 ページ） で指定した Kubernetes クラスタ名です。
- *region* は、ステップ 3 （377 ページ） の Kubernetes サービスの作成 （376 ページ） で選択した地域です。

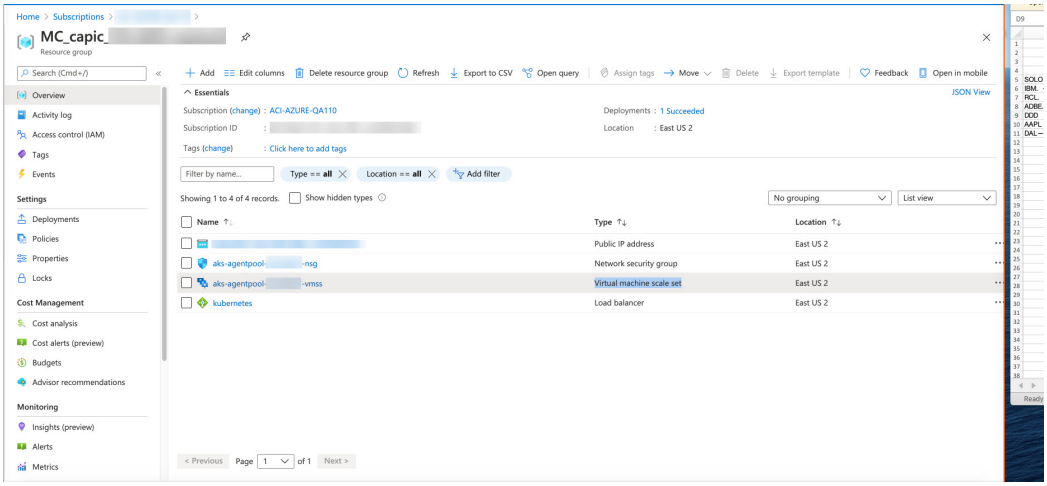
次に例を示します。

`MC_aks_acme-aks-cluster_centralus`

Kubernetes サービス リソース グループの概要ページが表示されます。

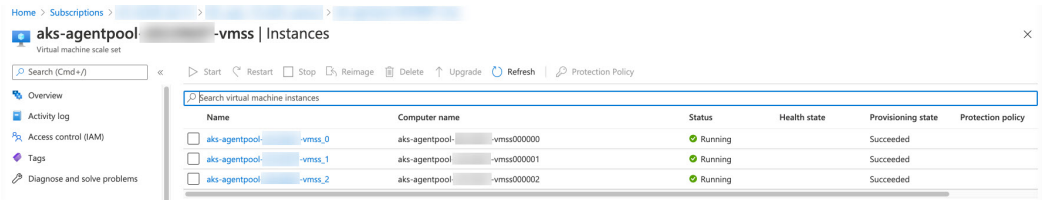
ステップ 3 **仮想マシン スケール セット**の行を見つけて、そのリンクをクリックします。

これは、AKS エージェントが実行されている場所です。



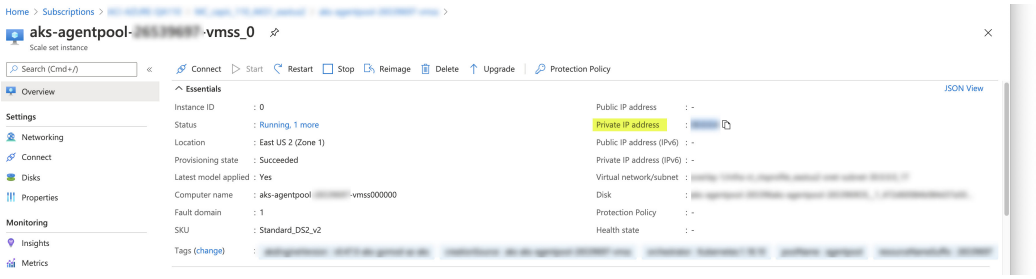
ステップ 4 左側のナビゲーション バーで **[インスタンス（Instances）]** をクリックして、この Kubernetes サービス リソース グループの仮想マシン インスタンスを表示します。

サービス EPG 構成例



ステップ 5 このウィンドウで 3 つのインスタンスのいずれかをクリックし、**[プライベート IP アドレス（Private IP address）]** フィールドに表示されている IP アドレスがハブ サブネットの IP アドレスと一致することを確認します。

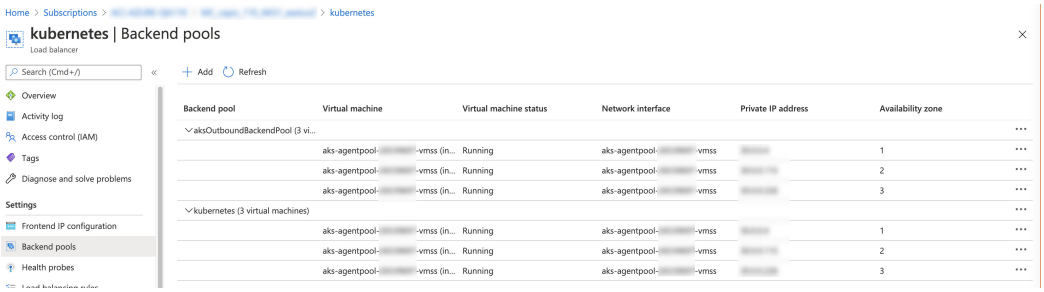
このウィンドウに表示される 3 つのインスタンスはすべて、ステップ 7 （379 ページ） の Kubernetes サービスの作成 （376 ページ） で選択したサブネットからの IP アドレスを持っている必要があります。



ステップ 6 Kubernetes サービス リソース グループの概要ページに戻り、タイプとしてロード バランサが表示されている `kubernetes` エントリを見つけて、そのリンクをクリックします。

Kubernetes ロード バランサの概要ページが表示されます。

ステップ 7 左側のナビゲーション バーで **[バックエンド プール（Backend pools）]** をクリックして、AKS エージェントを表示します。



ステップ 8 契約を構成するプロセスの一部として仮想マシンが作成された場合（たとえば、仮想マシンがコンシューマ用に作成された場合）、プロバイダとして AKS がある場合は、ルールが正しく構成されていることを確認します。

a) Azure portal で、インフラ リソース グループに戻ります。

b) インフラ リソース グループの [概要] ページに表示されるレコードの **[タイプ別にグループ化（Group by type）]** を選択します。

c) **[仮想マシン（Virtual machine）]** 領域が表示されるまで下にスクロールし、契約のコンシューマの仮想マシンをクリックします。

その仮想マシンの概要ウィンドウが表示されます。

d) 左側のナビゲーション バーの **[設定（Settings）]** で、**[ネットワーク（Networking）]** をクリックします。

その仮想マシンの [ネットワーク（utbound port rules）] ウィンドウが表示され、インバウンドおよびアウトバウンドのポート ルールに関する情報が示されます。

e) **[アウトバウンド ポートのルール（utbound port rules）]** タブをクリックし、表にリストされているアウトバウンド ポートの規則のいずれかをクリックします。

ウィンドウが右からスライドして表示され、これらのアウトバウンド ポート ルールに関する追加情報が表示されます。たとえば、**[宛先 IP アドレス/CIDR 範囲（Destination IP addresses/CIDR ranges）]** 領域のエントリは、AKS クラスタに関連付けられているアドレスに関する情報を提供します。

次のタスク

「Azure および AKS CLI のインストール （383 ページ）」に進みます。

Azure および AKS CLI のインストール

これらの手順では、Azure と AKS CLI をインストールする方法について説明します。

始める前に

これらの手順に進む前に、新しい Kubernetes サービスの確認 （380 ページ） の手順を完了してください。

ステップ 1 インターネットにアクセスできるコンシューマ VM に、Azure CLI をインストールします。

詳細については、以下を参照してください。

https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-linux

たとえば、Azure の Ubuntu Linux VM に Azure CLI をインストールするには、次のようにします。

```
# curl -sL https://aka.ms/InstallAzureCliDeb | sudo bash
```

ステップ 2 Kubernetes コマンドライン ツールである **kubectl** と、azure 認証を実装する client-go 資格情報（exec）プラグインである **kubelogin** をダウンロードしてインストールします。

```
# az aks install-cli
```

ステップ 3 次の手順で ステップ 5 （378 ページ） の Kubernetes サービスの作成 （376 ページ） に入力したサービス プリンシパル情報でログインします。

```
# az login --service-principal --username <service_principal_client_id>
--password '<service_principal_client_secret>' --tenant <tenant_ID>
```

それぞれの説明は次のとおりです。

サービス EPG 構成例

- <*service_principal_client_id*> は、ステップ 5 （378 ページ） の Kubernetes サービスの作成 （376 ページ） で **[サービス プリンシパル クライアント ID（Service principal client ID）]** フィールドからのエントリです。
- <*service_principal_client_secret*> は、ステップ 5 （378 ページ） の Kubernetes サービスの作成 （376 ページ） で **[サービス プリンシパル クライアント シークレット（Service principal client secret）]** フィールドからのエントリです。
- <*tenant_ID*> は、サービス プリンシパル（Azure Active Directory テナント ID）に関連付けられたテナントです。このコマンドのテナント ID 情報を見つけるには：

  1. Azure portal にサインインします。
  2. **[Azure Active Directory]** を選択します。
  3. [プロパティ（Properties）] を選択します。
  4. **[テナント ID（Tenant ID）]** フィールドまで下にスクロールします。ボックスにテナント ID が表示されます。

     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/fundamentals/active-directory-how-to-find-tenant

次に例を示します。

```
# az login --service-principal --username 12a3b456-7c89-1234-5de6-7f89012gh3i4
--password 'secretkey12341234!' --tenant 98765zy4-xwv-3ut2-1uts-rq0pon98m765
```

ステップ 4 サブスクリプションを現在アクティブなサブスクリプションに設定します。

```
# az account set --subscription <AKS_rg_subscription_ID>
```

<*AKS_rg_subscription_ID*> は、Azure が 新しい Kubernetes サービスの確認 （380 ページ） の Kubernetes サービス用に作成したリソース グループのサブスクリプション ID です。

次に例を示します。

```
# az account set --subscription 56klm789n-o0p1-234q-5r6s-7t890123u4v5
```

ステップ 5 コンシューマ VM から次のように入力してログインし、AKS に接続します。

```
root@hub-vm:/home/capic# az aks get-credentials --resource-group <resource_group> --name
<AKS_cluster_name> --admin
```

それぞれの説明は次のとおりです。

- <*resource_group*> インフラ リソース グループの名前です。
- <*AKS_cluster_name*> は、ステップ 3 （377 ページ） の Kubernetes サービスの作成 （376 ページ） に入力された Kubernetes クラスタの名前です。

次に例を示します。

```
root@hub-vm:/home/capic# az aks get-credentials --resource-group capic_infra_westus --name azureaksclus
 --admin
```

次のようなメッセージが表示されます。

```
Merged "azureaksclus-admin" as current context in /root/.kube/config
```

ステップ 6 各ノードの内部 IP アドレスを確認してください。

```
root@hub-vm:/home/capic# kubectl get nodes -o wide
```

次のような出力が表示されます。

```
NAME                                STATUS   ROLES   AGE   VERSION   INTERNAL-IP   EXTERNAL-IP   OS-IMAGE             KERNAL-VERSION        CONTAINER-RUNTIME
aks-agentpool-12345678-vmss000000   Ready    agent   14h   v1.17.9   30.1.1.1      <none>        Ubuntu 16.04.7 LTS   4.15.0-1092-azure     docker://19.3.12
aks-agentpool-12345678-vmss000001   Ready    agent   14h   v1.17.9   30.1.1.21     <none>        Ubuntu 16.04.7 LTS   4.15.0-1092-azure     docker://19.3.12
aks-agentpool-12345678-vmss000002   Ready    agent   14h   v1.17.9   30.1.1.31     <none>        Ubuntu 16.04.7 LTS   4.15.0-1092-azure     docker://19.3.12
```

[INTERNAL-IP] 列にリストされている IP アドレスは、ハブ サブネットにあります。

（注） 上記の出力例では、EXTERNAL-IP 列のエントリは <none> と表示されます。これは、**[アクセス タイプ（Access Type）]** が ステップ 4 （374 ページ） の AKS のクラウド サービス EPG の作成 （373 ページ） で [プライベート（Private）] に設定されていたためです。[アクセス タイプ（Access Type）] が **[パブリックおよびプライベート（Public and Private）]** に設定されている場合、IP アドレスは [EXTERNAL-IP] 列に表示されます。

ステップ 7 （任意） 必要に応じて、新しいユーザーに管理者ロールを割り当てます。

a) Azure portal で、インフラ リソース グループに戻ります。
b) ページのレコード領域で、**Kubernetes サービス** エントリが見つかるまで下にスクロールします。
c) 構成した Kubernetes サービスをクリックします。

Kubernetes サービスの [概要（Overview）] ページが表示されます。

d) 左側のナビゲーション バーで、**[アクセス制御（IAM）（Access Control (IAM)）]** をクリックします。

その Kubernetes サービスのアクセス制御（IAM）が表示されます。

e) **[+ Add]** をクリックし、ドロップダウンメニューから **[Add role Assignment]** を選択します。
f) **[ロール割り当ての追加（Add role Assignment）]** ページで、次の選択を行います。

- **[ロール（Role）]** フィールドで、ドロップダウン メニューから **[Azure Kubernetes Service Cluster 管理者ロール（Azure Kubernetes Service Cluster Admin Role）]** を選択します。
- **[アクセス先の割り当て（Assign access to）]** フィールドで、**[ユーザー、グループ、またはサービス プリンシパル（User, group, or service principal）]** を選択します。
- 適切なキーを選択します。

g) 画面の下部にある**[保存（Save）]** をクリックします。

サービス EPG 構成例

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。

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。