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

初版：2021 年 9 月 20 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 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.

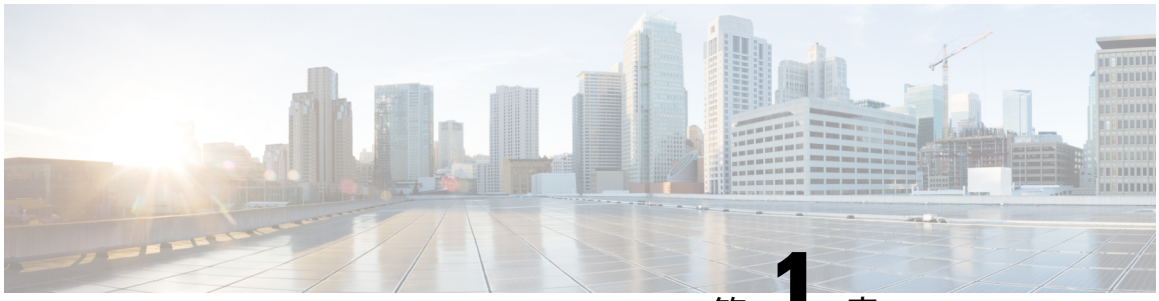
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

© 2021 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

新機能および変更された機能に関する情報

この章は、次の項で構成されています。

新機能および変更された機能に関する情報

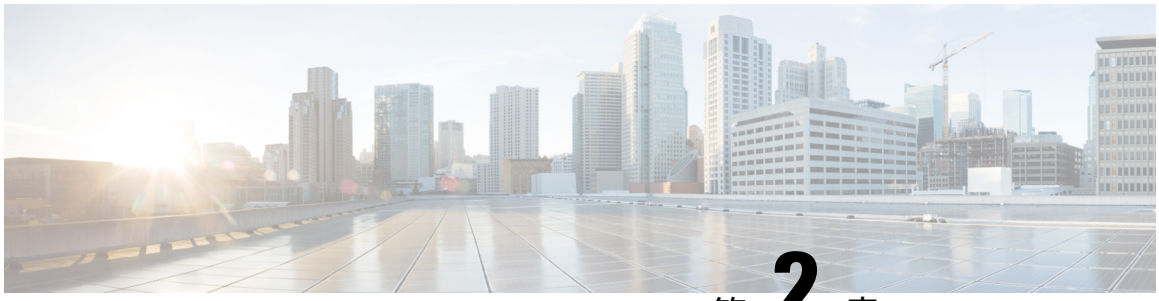
次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC for Cisco APIC Release 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(x)（このリリース）	

新機能および変更された機能に関する情報

機能または変更	説明	参照先
Cisco Cloud APIC での Google Cloud のサポート	リリース 25.0(1) 以降、Cisco Cloud APIC で Google Cloud のサポートが利用可能になりました。	
Cisco Cloud APIC での Prometheus Node Exporter のサポート	Prometheus ノードエクスポータは、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 （135 ページ）



第 2 章

Cisco Cloud APIC の概要

概要

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

Cisco Application Policy Infrastructure Controller（APIC）リリース 4.1(1)Cisco ACI 以降では、Cisco Cloud APIC を使用して Cisco ACI ファブリックを特定のパブリッククラウドに拡張できます。

Cisco Cloud APIC は、次のクラウドコンピューティング プラットフォームをサポートしています。

- リリース 4.1(1)：Amazon Web Services (AWS) のサポート
- リリース 4.2 (1)：Microsoft Azure のサポート
- リリース 25.0 (1)： Google Cloud

Cisco Cloud APICとは

Cisco Cloud APICは、クラウドベースの仮想マシン（VM）に導入できるのソフトウェアコンポーネントです。Cisco APICCisco Cloud APICは次の機能を提供します。

- Google Cloud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。
- クラウド接続の導入と設定を自動化します。
- クラウド ルーターのコントロール プレーンを設定します。

- ポリシーをクラウドネイティブポリシーに変換します。Cisco ACI
- エンドポイントを検出します。

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。

- 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。

  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）]、[トポロジ（Topology）]、[クラウドリソース（Cloud Resources）]、[アプリケーション管理（Application Management）]、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 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、**[EPG]** 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 （5 ページ） を参照してください。

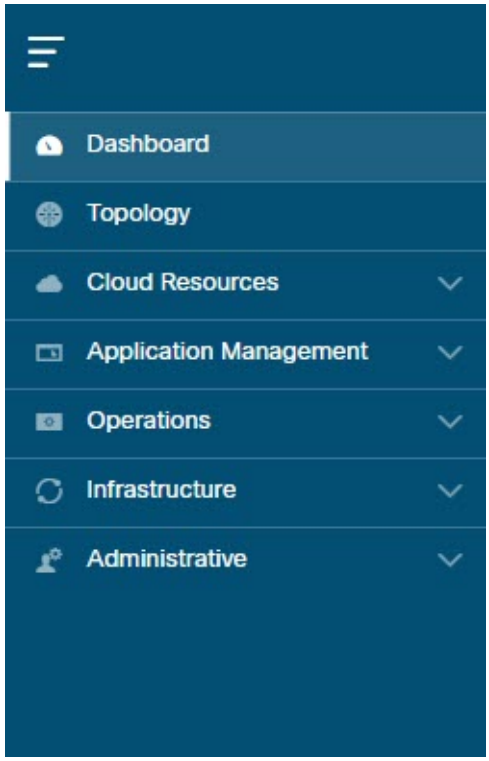
Cisco Cloud APIC コンポーネントの構成の詳細については、Cisco Cloud APIC コンポーネントの設定 （49 ページ） を参照してください。

Cisco Cloud APIC GUI アイコンについて

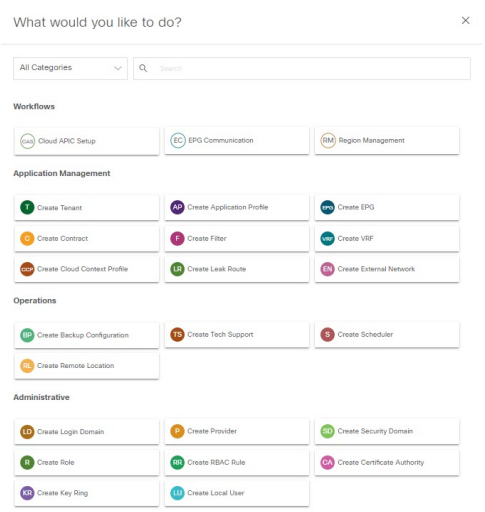
ここでは、Cisco Cloud APIC GUI で一般的に使用されるアイコンの概要について説明します。

表 *2 : 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、VPC、ルータ、エンドポイント、およびインスタンスに関する情報が表示されます。 • **[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、クラウドコンテキストプロファイル、および外部ネットワーク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：システム設定と外部接続に関する情報が表示されます。 • **[管理（Administrative）]** タブ：認証、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（135 ページ） を参照してください。

アイコン	説明
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。
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 （49 ページ）を参照してください。

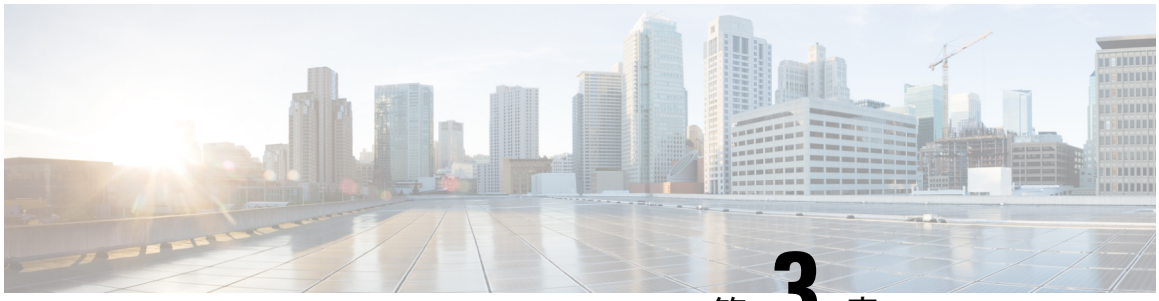
アイコン	説明
図 *5 : [*インテント（***Intent***）*]* ダイアログボックス 	

アイコン	説明

	[インテント（Intent）] 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。
	• 全カテゴリ
	• ワークフロー：次のオプションが表示されます。
	  • クラウドのセットアップ
	  • EPG 通信
	  • リージョン管理
	• **[アプリケーション管理（Application Management）]**：次のオプションが表示されます。
	  • テナントの作成
	  • アプリケーション プロファイルの作成
	  • EPG の作成
	  • コントラクトの作成
	  • フィルタの作成
	  • VRF の作成
	  • クラウドコンテンツ プロファイルの作成
	  • リーク ルートの作成
	  • 外部ネットワークの作成
	• **[操作（Operations）]**：次のオプションが表示されます。
	  • バックアップ構成ファイルの作成
	  • テクニカル サポートの作成
	  • スケジューラの作成
	  • リモート ロケーションの作成

アイコン	説明
	• 管理（**Administrative**）：次のオプションを表示します。 • ログインドメインの作成 • プロバイダーを作成します。 • セキュリティ ドメインの作成 • ロールの作成 • **RBAC** ルールの作成 • 認証局の作成 • キー リングの作成 • ローカル ユーザーの作成
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。 • **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。 • **モデル ドキュメント**：**[Cloud APIC Object Model Documentation]** ウィンドウを開きます。

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）]：ローカル/UTC の時刻形式を設定します。 • **[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およびGoogle Cloudの概要

リリース25.0(1) 以降、Cisco Cloud APIC で Google Cloud のサポートが利用可能になりました。この章の次のトピックでは、Google Cloud を使用した Cisco Cloud APIC の展開方法について説明します。

リリース 25.0(1) の変更のサマリー

次に、リリース 25.0(1) の変更点の概要を示します。

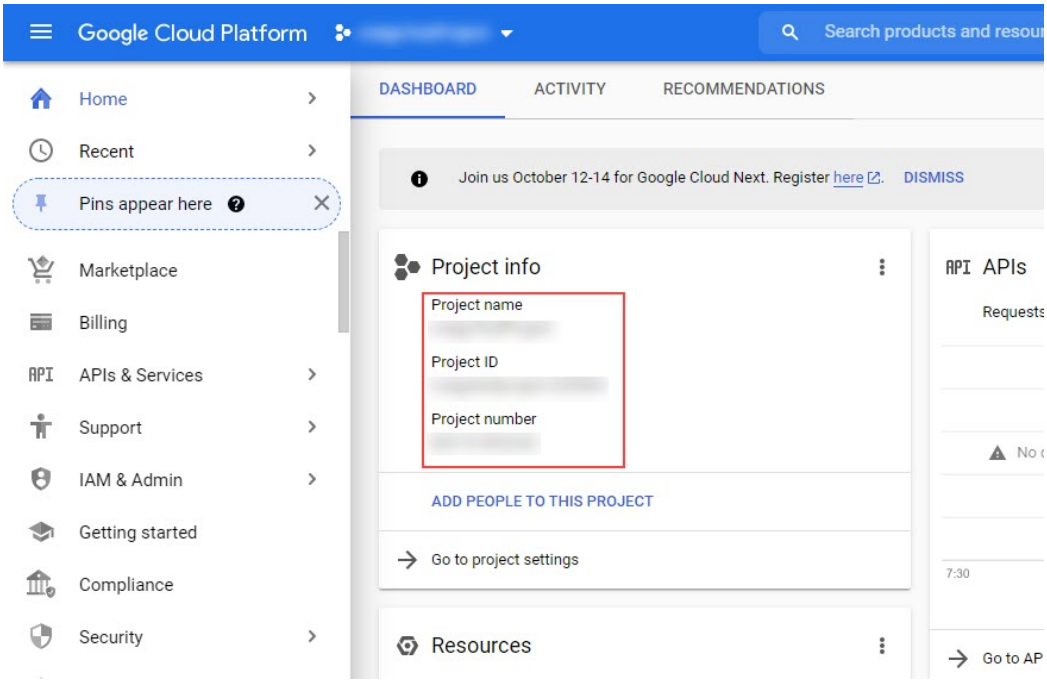
- Cisco Cloud APIC で Google Cloud のサポート。
- Google Cloud から他の外部サイトへの外部接続のサポートが可能です。詳細については、「外部ネットワーク接続 （16 ページ）」を参照してください。
- ルーティングポリシーとセキュリティポリシーの個別設定のサポート。詳細については、「ルーティング ポリシーとセキュリティ ポリシーの個別の構成 （21 ページ）」を参照してください。
  - Cisco Cloud APIC では、ルート マップを使用して、VRF のペア間のセキュリティ ポリシーとは無関係にルーティング ポリシーを設定できます。両方の VRF が内部 VRF であるか、一方の VRF が内部 VRF で、もう一方の VRF が 外部 VRF です。詳細については、「ルーティング ポリシーの設定 （21 ページ）」を参照してください。
  - ファイアウォール ルールを使用したセキュリティ ポリシーの設定のサポート。詳細については、「セキュリティ ポリシーの設定 （22 ページ）」を参照してください。

重要な Google Cloud プロジェクト情報の検索

Google Cloud プロジェクトを作成すると、そのプロジェクトには次の 3 つの固有識別子が割り当てられます。

- プロジェクト名
- プロジェクト ID
- プロジェクト番号

Cisco Cloud APIC 構成プロセスのさまざまな時点で、Google Cloud プロジェクトにこれらの 3 つの識別子が必要になります。これらの Google Cloud プロジェクトIDを含む **[プロジェクト情報（Project Info）]** ペインを見つけるには、Google Cloud アカウントにログインし、**[プロジェクトの選択（Select a Project）]** ウィンドウで特定のGoogle Cloudプロジェクトを選択します。このプロジェクトの **[ダッシュボード（Dashboard）]** が表示され、[プロジェクト情報（Project Info）] ペインに Google Cloud プロジェクトのこれら3つの一意の識別子が表示されます。



Cloud APIC での Google Cloud の展開について

Google Cloud は、ファイル システムに似た方法でリソースを編成します。

- 最上位の組織は複数のフォルダを持つことができます。
- すべてのフォルダには、他のフォルダを含めることも、すべてのプロジェクトに一意の ID があるプロジェクトを含めることもできます。

- クラウド リソース（VM、VPC、サブネットなど）はプロジェクトに含まれます。

組織とフォルダのレベルは、Google Cloud の観点から理解するのに有用な領域ですが、プロジェクトレベルは、Cloud APIC の観点から最も関連性があります。

各 Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングされます。

- Cloud APIC テナントは複数の Google Cloud プロジェクトにまたがることはできません
- Google Cloud プロジェクトに複数の Cloud APIC テナントを含めることはできません

Cloud APIC では、Google Cloud は **サービス アカウント**を使用してプロジェクトにアクセスできます。これらのアカウントは、Google Cloud サービスにアクセスする必要があるアプリケーション用です。これらを使用して、Cloud APIC と他のテナントのポリシーを実行および展開し、プッシュすることができます。Google Cloud 内部で実行されるアプリケーションで使用されるサービスアカウントにはログイン情報は必要ありませんが、事前に生成された秘密キーを必要とする Google Cloud の外部で実行されるアプリケーションにはログイン情報が必要です。サービス アカウントは1つの Google Cloud プロジェクトに存在しますが、他のプロジェクト（Cloud APIC の場合、他のテナント用）のポリシーを管理するためのアクセス権も付与されます。

次の項では、Google Cloud を使用して Cloud APICテナントを設定するさまざまな方法について詳しく説明します。

- 管理対象ログイン情報を持つユーザテナント （15 ページ）
- 管理対象ログイン情報を持つユーザー テナント （16 ページ）

管理対象ログイン情報を持つユーザテナント

このタイプのユーザー テナントには、次の特性があります。

- このテナント アカウントは Cisco Cloud APIC によって管理されます。
- このタイプのユーザーテナントのテナント構成プロセスの一環として、最初に Cisco Cloud APIC GUIで **[管理対象アイデンティティ（Managed Identity）]** を選択します。
- Cisco Cloud APIC で必要なパラメータを構成したら、Google Cloud でこのテナントに必要な権限を設定する必要があります。クラウド APIC によって作成されたサービス アカウントを、次のルールを使用して IAM ユーザーとして追加します。
  - クラウド機能サービス エージェント
  - コンピューティング インスタンス管理（v1）
  - コンピューティング ネットワーク管理
  - コンピューティング セキュリティ管理
  - ロギング管理
  - パブ/サブ管理

- ストレージ管理者

このようなテナントの作成手順については、Google Cloud および Cisco Cloud APIC GUI を使用した管理対象テナントの作成 （50 ページ） を参照してください。

管理対象ログイン情報を持つユーザー テナント

このタイプのユーザー テナントには、次の特性があります。

- このテナント アカウントは Cisco Cloud APIC では管理されません。
- このタイプのテナントの Cisco Cloud APIC に必要なパラメータを構成する前に、まず、このテナントに関連付けられたサービス アカウントの Google Cloud から必要な秘密キー情報を含むJSONファイルをダウンロードする必要があります。
- 次に、このタイプのユーザーテナントのテナント構成プロセスの一環として、Cisco Cloud APIC GUI で **[管理対象外アイデンティティ（Unmanaged Identity）]** を選択します。Cisco Cloud APIC でこのタイプのテナントの構成プロセスの一環として、ダウンロードした JSON ファイルから次の情報を提供します。
  - キー ID
  - RSA 秘密キー
  - Client ID
  - Email

このようなテナントの作成手順については、Google Cloud および Cisco Cloud APIC GUI を使用した管理対象外テナントの作成 （52 ページ） を参照してください。

外部ネットワーク接続

サポートは、Google Cloud サイトと非Google Cloud サイトまたは外部デバイス間の外部接続に使用できます。このIPv4接続を確立するには、Google Cloudルータと外部デバイス（CSR を含む）の間に VPN 接続を作成します。

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、クラウド内に存在しない一意の VRF です。このVRFは、Cisco Cloud APIC によって使用されるクラウド コンテキスト プロファイルでは参照されません。

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。 を参照してください。

クラウド ネイティブ ルータ

Cisco Cloud APIC を Google Cloud で使用して設定すると、インフラ VPC は Google Cloud ネイティブ ルータ（クラウド ルータおよびクラウド VPN ゲートウェイ）を使用して、オンプレミス サイト、他のクラウド サイト、または任意のリモート デバイスへの IPsec トンネルと BGP セッションを作成します。IPv4 セッションが 外部 VRF で作成されているクラウド ネイティブ ルータを使用したこのタイプの接続では、IPv4 接続のみがサポートされます。

Google Cloud は、スタティック ルートと BGP の両方で VPN 接続をサポートします。BGP との VPN 接続を作成するために、Cisco Cloud APIC はクラウド ルータと VPN ゲートウェイの両方が必要です。VPC は複数のクラウド ルータと VPN ゲートウェイを持つことができます。ただし、Google Cloudには、クラウド ルータと VPN ゲートウェイの両方が同じリージョンおよび同じ VPC に存在する必要があるという制限があります。さらに、Cisco Cloud APIC ではリージョンごとに 1 つのクラウド ルータと 1 つのクラウド VPN ゲートウェイのみがサポートされるという制限があります。

VPN 通信

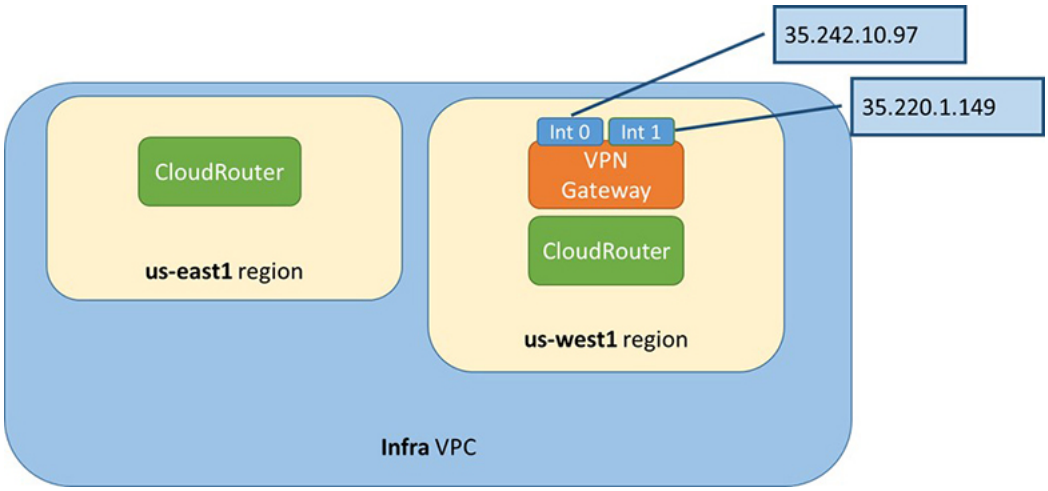
Cisco Cloud APIC を Google Cloud で設定する場合、インフラ VPC を使用して Cisco Cloud APIC をホストし、外部デバイスおよびサイトへの VPN 接続をホストします。ただし、インフラ VPC は、スポーク間通信を実装するための中継として使用されません。代わりに、Cisco Cloud APIC を Google Cloudを使用して設定すると、スポーク間通信はスポーク間 VPC ピアリングによって行われます。

インフラ VPC は、Google Cloud ルータとGoogle Cloud VPN ゲートウェイを使用して、オンプレミス サイトまたは他のクラウド サイトへの IPsec トンネルと BGP セッションを作成します。スポーク VPC は、インフラ VPC とピアリングして、外部サイトへの VPN 接続を共有します。

- VPN 接続で受信したルートがスポーク VPC にリークされる
- スポーク VPC ルートが VPN 接続でアドバタイズされる

VRF 間ルーティングを使用すると、VPN 接続の 外部 VRF とクラウド ローカル スポーク VRF 間でルートがリークされます。

VPN ゲートウェイには 2 つのインターフェイスがあり、Google Cloud は各インターフェイスにパブリック IP アドレスを割り当てます。Google Cloud VPN ゲートウェイは 1 つまたは 2 つのインターフェイスを持つことができますが、ハイアベイラビリティを実現するには2 つのインターフェイスが必要であるため、Cisco Cloud APIC は 2 つのインターフェイスを持つ VPN ゲートウェイのみをサポートします。



ハブ ネットワーク構成

リリース 25.0(1) 以降では、スポーク接続に基づいてリージョンにハブ ネットワークを作成するのではなく、`cloudtemplateHubNetworkName` の下の `cloudRegionName` MOが、ハブ ネットワークが展開されるリージョンを表します。ここで、`cloudtemplateHubNetworkName`は Google Cloud ルータを表します。リリース 25.0(1) の場合、Cisco Cloud APIC では 1 つの `cloudtemplateHubNetworkName` の制限があります。

ハブ ネットワークは、外部サイトへの接続を確立する方法を提供します。ハブ ネットワークの作成は、外部ネットワークを作成するための前提条件です。リリース 25.0(1) 以降では、ハブの名前と、ハブ ネットワークを展開するリージョンを指定して、ハブ ネットワークを作成できます。たとえば、ハブ ネットワークを us-central1 と us-east1 に展開することを選択できます。Cisco Cloud APIC はこれらの地域の Google Cloud ルータをプロビジョニングします。作成できるハブ ネットワークは1つだけです。つまり、Cisco Cloud APICではリージョンごとに 1 つのクラウド ルータのみが展開されます。

次の POST は、このモデルを使用したリリース 25.0(1) 以降のネットワーク接続の例を示しています。`cloudtemplateHubNetwork` は、ハブ ネットワークを作成するために使用されます。この例では、ハブ ネットワークは 4 つの地域に展開されています。外部ネットワークは、`cloudtemplateExtNetwork` MOを使用して 4 つのリージョンのそれぞれから作成されます。

```
<polUni>
    <fvTenant name="infra" status="">
        <fvCtx name="extv1" pcEnfPref="enforced" status=""/>
         <fvCtx name="extv2" pcEnfPref="enforced" status=""/>
          <fvCtx name="extv3" pcEnfPref="enforced" status=""/>

           <cloudtemplateInfraNetwork name="default" vrfName="overlay-1"
hostRouterMode="manual" status="">
            <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.7.0/24"
poolname="pool1" />
             <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.8.0/24"
poolname="pool2" />
              <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.10.0/24"
poolname="pool3" />
```

```
            <cloudtemplateHubNetwork name="default" status="" >
                <cloudtemplateHubNetworkName name="foo1" asn="64514" status="">
                    <cloudRegionName provider="gcp" region="us-west4" status="" />
                    <cloudRegionName provider="gcp" region="us-west2" status="" />
                    <cloudRegionName provider="gcp" region="us-east1" status="" />
                     <cloudRegionName provider="gcp" region="us-west1" status=""/>
                </cloudtemplateHubNetworkName>
            </cloudtemplateHubNetwork>

            <cloudtemplateIntNetwork name="default">
                <cloudRegionName provider="gcp" region="us-west1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-west2">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-east1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                  </cloudRegionName>
                    <cloudRegionName provider="gcp" region="us-west4">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
            </cloudtemplateIntNetwork>

            <cloudtemplateExtNetwork name="default">
            </cloudtemplateExtNetwork>
               <cloudtemplateExtNetwork name="extnwfoo1" vrfName="extv1"
hubNetworkName="foo1" vpnRouterName="default" status="">
                    <cloudRegionName provider="gcp" region="us-west1" status=""/>
                   <cloudtemplateVpnNetwork name="onprem01" remoteSiteId="1" status="">

                    <cloudtemplateIpSecTunnel peeraddr="128.1.1.1" preSharedKey="abcd"
poolname="pool1" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529"
status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
          <cloudtemplateExtNetwork name="extnwfoo2" vrfName="extv2" hubNetworkName="foo1"
 vpnRouterName="default" status="">
             <cloudRegionName provider="gcp" region="us-west2" status=""/>
                <cloudtemplateVpnNetwork name="onprem02" remoteSiteId="2" status="">
                      <cloudtemplateIpSecTunnel peeraddr="128.1.1.2" preSharedKey="def"
 poolname="pool2" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529"
status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
             <cloudtemplateExtNetwork name="extnwfoo3" vrfName="extv3"
hubNetworkName="foo1" vpnRouterName="default" status="">
                <cloudRegionName provider="gcp" region="us-east1" status=""/>
                   <cloudtemplateVpnNetwork name="onprem03" remoteSiteId="3" status="">
                      <cloudtemplateIpSecTunnel peeraddr="128.1.1.3" preSharedKey="abc"
 poolname="pool3" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529"
status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
                  </cloudtemplateExtNetwork>
        </cloudtemplateInfraNetwork>
    </fvTenant>
</polUni>
```

この POST の例：

- **cloudtemplateExtNetwork**：複数の cloudtemplateExtNetwork エントリを持つことができ、それぞれが一意の名前を持ち、外部 VRF 上の外部ネットワークを表します。

  cloudtemplateExtNetwork エリアには、次のフィールドがあります。

  - **vrfName**：このプロパティは、外部ネットワークに使用される VRF（トランスポート VRF など）を表します。複数のリモート サイトで同じトランスポート VRF を使用できます。つまり、これらのリモート サイトはすべてクラウド上で 1 つの VRF として扱われ、すべてのリモート サイトがクラウドから同じルートを受信します。

  - **hubNetworkName**：このプロパティは、この外部ネットワークで使用されるハブ ネットワークの名前を表します。この名前は、cloudtemplateHubNetworkName 領域で作成されたハブ ネットワークの 1 つを参照します。

  - **vpnRouterName**：このプロパティは、この外部ネットワークで使用される VPN ルータの名前を表します。この名前は、cloudtemplateVpnRouter によって作成された VPN ルータを参照します。

  また、外部ネットワークは複数のリージョンに展開でき、外部ネットワークで使用されるルータはそれらのリージョンに展開する必要があります（つまり、hubNetworkName と vpnRouterName はそれらのリージョンに存在する必要があります）。

- **cloudtemplateVpnNetwork**：このMOはリモートサイトを表します。

  cloudtemplateVpnNetwork エリア内に **remoteSiteId** フィールドがあります。このプロパティは、リモート サイト ID を表します。

- **cloudtemplateVpnRouter**：この MO は Google CloudVPN ゲートウェイに変換されます。リリース 25.0(1) では、名前がdefault の 1 つの cloudtemplateVpnRouter のみが許可されます。

- **cloudtemplateIpSecTunnel**：この MO はリモート ピアを表します。

- **cloudtemplateBgpIpv4**：この MO はリモート サイトの IPv4 BGP ピアを表します。

  cloudtemplateBgpIpv4 の下の peeraddr エントリにデフォルト アドレス（0.0.0.0/0）がある場合、リモート BGP ピアはリモート デバイスのトンネルの内部アドレスであると見なされます。

上記のモデルは次をサポートしていることに注意してください。

- 外部デバイスへの ikev1 と ikev2 の両方。
- 複数の cloudtemplateIpSecTunnelSubnetPool サブネット プール。
  cloudtemplateIpSecTunnelSubnetPool サブネット プールで許可されるIP範囲は、クラウド プロバイダーと使用例によって異なります。たとえば、169.254.0.0 / 16 以下のサブネットが Google Cloud VPN接続でサポートされます。

ルーティングポリシーとセキュリティポリシーの個別の構成

異なるVRFの2つのエンドポイント間の通信を許可するには、ルーティング ポリシーとセキュリティ ポリシーを別々に確立する必要があります。

- **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**：ゾーン分割ルール、セキュリティ グループ ルール、ACL など、セキュリティ目的で使用されるルール

Google Cloud の場合、ルーティングはセキュリティとは無関係に設定する必要があります。つまり、Google Cloud の場合、「契約」はセキュリティのためだけに使用されます。ルーティングを構成するには、ルートマップを構成する必要があります。

ルーティング ポリシーの設定

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、VRF のペア間でリークするルートを指定できます。ルーティングを確立するには、VRFのペア間にルートマップを設定する必要があります。

ルート マップを使用して、VRF のペア間でリークするルートを設定できる状況では、VRF 間ルーティングに次のタイプの VRF が使用されます。

- **外部VRF** は、1 つ以上の外部ネットワークに関連付けられている VRF です。
- **内部 VRF** は、1 つ以上のクラウド コンテキスト プロファイルまたはクラウド サブネットが関連付けられているVRFです。

次のタイプの VRF で VRF 間ルーティングを設定する場合：

- 内部 VRF のペア間では、常にすべてのルートをリークする必要があります。
- 内部 VRF から外部 VRF へ、特定のルートまたはすべてのルートをリークできます。
- 外部 VRF から内部 VRF に、すべてのルートをリークする必要があります。

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 2 つの VRF 間で双方向にリークされます。あるテナント/VRF から別のテナント/VRF へのルート リーク エントリごとに、対応するルート リーク エントリが反対方向に存在する必要があります。

たとえば、2 つのテナント（t1とt2）と 2 つの対応する VRF（v1 とv2）があるとします。VRF t2:v2 のすべてのルート リーク エントリ t1:v1 に対して、VRF t1:v1 の対応するルート リーク エントリ t2:v2 が必要です。

- 外部 VRF を外部ネットワークに関連付けた後、外部 VRF を変更する場合は、外部ネットワークを削除してから、新しい外部 VRF で外部ネットワークを再作成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。

セキュリティ ポリシーの設定

Cisco Cloud APIC の EPG は AWS と Azure のセキュリティ グループに対応しますが、EPGに対する Google Cloud の対応コンポーネントはありません。Google Cloud で最も近いものは、ファイアウォール ルールとネットワーク タグの組み合わせです。

Google Cloudのファイアウォール リソースは、プロジェクト（テナント）に対してグローバルです。ファイアウォール ルールは単一の VPC に関連付けられ、その範囲は VPC 全体にグローバルに適用されます。ファイアウォール ルールの範囲は、Target パラメータによってさらに定義されます。つまり、ルールが適用されるインスタンスのセットは、次の 1 つ以上のターゲット タイプによって選択できます。

- **ネットワーク タグ**：ネットワークタグは、Google Cloudの VM のファイアウォールとルーティング設定を制御するキー文字列です。インスタンス（VM など）は、一意の文字列でタグ付けできます。ファイアウォール ルールは、等しいタグを持つすべてのインスタンスに適用されます。複数のタグ値は論理「or」演算子として機能し、少なくとも 1 つのタグが一致する限りファイアウォール ルールが適用されます。
- **ネットワーク内のすべてのインスタンス**：ファイアウォールルールは VPC 内のすべてのインスタンスに適用されます。

ファイアウォール ルールは、トラフィックの送信元と宛先も識別します。ルールが入力トラフィック（VM に向かう）または出力トラフィック（VM を離れる）のどちらであるかによって、送信元フィールドと宛先フィールドの値は異なります。次のリストに、これらの値の詳細を示します。

- **入力ルール**：
  - **ソース**：次を使用して識別できます。
    - ネットワーク タグ
    - IP アドレス
    - 論理「or」演算子を使用した IP アドレスとネットワーク タグの組み合わせ

- **宛先**：Target パラメータは、宛先インスタンスを識別します。

- **出力ルール**：
  - **送信元**：Target パラメータは、送信元インスタンスを識別します。
  - **宛先**：IP アドレスのみを使用して識別できます（ネットワーク タグは使用できません）。

Cisco Cloud APIC が Google Cloud を使用したファイアウォールルールの実装方法

次のリストは、Cisco Cloud APIC の Google Cloud を使用したファイアウォールルールの実装方法を示しています。

- **グローバル リソース**：Google Cloud の VPC とファイアウォールはグローバル リソースであるため、Cisco Cloud APIC は複数のリージョンにまたがるエンドポイントのファイアウォール ルールをプログラムする必要はありません。エンドポイントが存在するすべてのリージョンに同じファイアウォール ルールが適用されます。
- **ファイアウォール出力ルールとネットワーク タグ**：ファイアウォール出力ルールは、宛先フィールドとしてネットワーク タグをサポートしていないため、エンドポイントの個々の IP アドレスをリストする必要があります。
- **ファイアウォール入力ルールおよびエイリアス IP 範囲の送信元タグ**：ファイアウォール入力ルールには、送信元フィールドで使用されるネットワークタグに一致する VM のエイリアス IP 範囲は含まれません。
- **ファイアウォール ルールの優先度フィールド**：Google Cloud は優先度の値に従ってファイアウォール ルールを評価します。

Google Cloud ファイアウォール ルールがプライオリティ リストの後に続く場合、Cisco Cloud APIC は VPC の作成時に、低プライオリティの deny-all 入力ルールと出力ルールのペアを設定します。その後、Cisco Cloud APIC は EPG の優先度の高いコントラクトに従ってトラフィックを開くルールを設定します。したがって、EPGコントラクトの結果として特定のトラフィックを許可する明示的なルールがない場合は、優先順位の低いルールが一致し、デフォルトの動作はdeny-allになります。

エンドポイントおよびエンドポイント セレクタ

Cisco Cloud APICでは、クラウド EPG は、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウド EPG は、1 つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウド EPG に割り当てるために使用される、エンドポイント セレクタと呼ばれる機能があります。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 Google Cloud VPC 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。

次に、2 種類のクラウド EPG で使用可能なエンドポイント セレクタのタイプを示します。

- **アプリケーション EPG**：
  - **IP**): IP アドレスまたはサブネットによって選択するために使用されます。
  - **リージョン**: エンドポイントのリージョンで選択するために使用されます。
  - **カスタム**：カスタム タグまたはラベルで選択するために使用されます。たとえば、Google Cloud のロケーション タグを追加する場合、Google Cloud で以前に追加したロケーション タグと一致するこのフィールドにカスタム タグのロケーションを作成できます。
- **外部 EPG**：

  サブネット：サブネット セレクタはエンドポイント セレクタのタイプで、一致表現ではサブネットの IP アドレスが使用されるため、サブネット全体が EPG の一部として割り当てられます。基本的に、サブネット セレクタをエンドポイント セレクタとして使用する場合、そのサブネット内のすべてのエンドポイントは関連付けられたEPGに属します。

Google Cloud で Cisco Cloud APIC エンドポイント セレクタを使用する場合、Google Cloudの一致する VM に EPG を関連付けるネットワーク タグが適用されます。ネットワーク タグが VM で設定されると、Google Cloud は VM のトラフィックにファイアウォール ルールが適用されます。

Google Cloud 上の VM もラベルをサポートします。ラベルは、組織的なツールとなるキーと値のペアです。Cisco Cloud APIC のカスタムエンドポイントセレクタは、Google Cloud のVMに割り当てられたラベルを認識します。

Cisco Cloud APIC は、EPG ごとに一意のネットワーク タグ文字列を予約します。Google Cloud では、この値が EPG 用に作成されたファイアウォール ルールのターゲット フィールドとして使用されます。新しいVMがEPGのエンドポイント セレクタに一致すると、Cisco Cloud APIC はこの値を既存の VM のネットワーク タグに追加します。さらに、EPG のネットワークタグは、Google Cloudファイアウォール ルールの送信元フィールドで使用されます。

たとえば、次の設定例について考えます。

```
<cloudEPg  name="epg1" >
    <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
    <fvRsProv tnVzBrCPName="httpSSHFamily"/>
    <cloudEPSelector name="web-selector" matchExpression="custom:server=='web'"/>
    <cloudEPSelector name="web-selector" matchExpression="custom:server==backend"/>
</cloudEPg>
<cloudEPg  name="epg2" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
    <fvRsCons tnVzBrCPName="httpSSHFamily"/>
   <cloudEPSelector name="database-selector" matchExpression="custom:server=='database'"/>
</cloudEPg>
```

次の設定の VPC に 3 つのエンドポイントがあると仮定すると、Cisco Cloud APIC は次のネットワーク タグを設定します。Cisco Cloud APIC-configured ネットワーク タグは次の形式です。

```
capic-<app-profile-name>-<epg-name>
```

エンドポイント	アプリケーション プロファイル	EPG	Primary IP	ラベル	クラウド APIC で設定されたネットワーク タグ
EP1	最初のアプリケーション プロファイル（app01）	最初の EPG（epg01）	10.0.0.1	server:web	capic-app01-epg01
EP2	2 番目のアプリケーション プロファイル（app02）	2 番目の EPG（epg02）	20.0.0.1	server:backend	capic-app02-epg02
EP3	2 番目のアプリケーション プロファイル（app02）	3 番目の EPG（epg03）	30.0.0.1	server:database	capic-app02-epg03

Cisco Cloud APIC がネットワーク タグを設定するには、VMに対する管理者権限が必要です。この権限は、コンピューティング インスタンス管理者ロールによって付与されます。

Cisco Cloud APIC にこの権限がなく、VM のタグを管理できない場合があります。これらのシナリオでは、最初にVMでネットワークタグを設定し、その後で Cisco Cloud APIC に適切なエンドポイント セレクタ設定を指定できます。

ファイアウォール ルールを確認するには：

- **Google Cloud**内：Google Cloud アカウントで、**[VPC ネットワーク（VPC Network）]** > **[ファイアウォール（Firewall）]**に移動します。
  - VM が EPG の一部である場合は、ファイアウォール ルールを展開し、**[フィルタ（Filters）]** 列に表示される複数のエントリを表示することで、エンドポイントを検索できます。
  - **[タイプ（Type）]** 列のエントリを使用して、特定のファイアウォール ルールが入力ファイアウォール ルールか出力ファイアウォール ルールかを判別します。
    - ファイアウォール ルールが入力タイプの場合、トラフィックはこれらのエンドポイントに送信されます。
    - ファイアウォール ルールが出力タイプの場合、これらのエントリはトラフィックを受信できる場所を示します。

- **Cisco Cloud APIC**内：ファイアウォールルールはVPCに関連付けられているため、**[クラウド リソース（Cloud Resources）]** > **[VPC]**に移動し、VPC をダブルクリックして詳細画面を表示します。次に、**[クラウド リソース（Cloud Resources）]** タブをクリックします。入力ルールと出力ルールが表示されます。

Google Cloud の下の VPC とサブネット、およびクラウド APIC でのクラウドコンテキストプロファイルについて

Google Cloud では、VPC はグローバル リソースですが、サブネットはリージョン内にあり、リージョン内のすべてのアベイラビリティ ゾーンにまたがっていますが、同じ VPC またはピア VPC 内の他のサブネットと重複することはできません。

各サブネットには、プライマリ CIDR ブロック（IP 範囲）が 1 つだけ必要で、最大 30 個のセカンダリ CIDR ブロックを含めることができます。VPC には最大 300 のプライマリおよびセカンダリ CIDR を設定できます。各 VM の NIC はプライマリ CIDR ブロックからプライマリ内部 IP アドレスを取得しますが、セカンダリ IP 範囲は**エイリアス IP 範囲**にのみ使用できます。これは、VM 内で実行されているコンテナまたはアプリケーションにアドレス プールを割り当てるための Google Cloud 組織的なツールです。

次に、Cisco Cloud APIC オブジェクトと Google Cloud オブジェクト間の関連付けについて詳しく説明します。

- **Google Cloud VPC からCisco Cloud APIC VRF への 1 対 1 のマッピング**：Google CloudVPC が各Cisco Cloud APICVRF（`fvCtx` オブジェクト）に展開されます。クラウド コンテキスト プロファイル（`cloudCtxProfile`オブジェクト）は、展開するリージョン サブネットのセットを定義します。同じ VRF 内のすべてのクラウド コンテキスト プロファイルは、同じ VPC にマッピングされます。
- **Google Cloudサブネットとそのセカンダリ IP 範囲**：Cisco Cloud APIC は Cisco Cloud APICCIDR とサブネット オブジェクトを使用して、プライマリおよびセカンダリ IP 範囲でサブネットを展開します。Cisco Cloud APIC サブネット オブジェクトは IP 範囲を表すために使用され、Cisco Cloud APIC CIDR のプライマリ プロパティはプライマリまたはセカンダリかどうかを示します。セカンダリ Cisco Cloud APIC サブネット オブジェクトは、対応するプライマリ サブネット オブジェクトに関連付けられます。これは、Google Cloud だけが実際のサブネットを展開するためです。

VPC グループについて

クラウド コンテキスト プロファイルは Cisco Cloud APIC 内で VPC のマッピング ツールとして使用され、1 つのクラウド コンテキスト プロファイルが 1 つの VPC に関連付けられます。クラウド コンテキスト プロファイルには、リージョンの関連付けに関する情報も含まれます。クラウド コンテキスト プロファイルは、VPC が展開されるリージョンを決定するために使用されます。

Google Cloudでは、VPC を作成するときに、複数のリージョンにサブネットを展開する場合は、複数のクラウド コンテキスト プロファイルを Cisco Cloud APIC を通じて作成する必要があります。ただし、VPC は Google Cloud で本質的にグローバルであり、VPC はすべてのリージョンにまたがっています。

したがって、**VPC グループ**（vpcGroup）と呼ばれるプロパティは、Cisco Cloud APIC が複数のクラウド コンテキスト プロファイルをグループ化して 1 つの VPC を形成できるクラウド コンテキスト プロファイル内で使用できます。Google Cloud 内VPC グループ機能を使用して相互に関連付けられた複数のクラウド コンテキスト プロファイルは、Google Cloud でVPC グループ名が表示されているVPC構造を形成します。

リリース 25.0(1) では 1 つの Google Cloud VRF 内で1つの Cisco Cloud APIC VPC のみが許可されるため、VRF にリストされている各クラウド コンテキスト プロファイルの VPC グループ プロパティに同じ名前を使用する必要があります。同じ VPC グループ名を持つプロファイルは、同じ VPC に存在します。

この照合メカニズムの範囲はテナント レベルです。同じ値をテナント間で再利用できますが、異なるGoogle Cloudプロジェクトの一部であるため、異なるグループを暗黙的に定義します。

Cisco Cloud APIC は少なくとも1つのcloudSubnetが定義されている限り、fvCtx、cloudRsToCtx、および vpcGroup の各タプルに対して VPC を展開します。クラウド コンテキスト プロファイルは、VRF に関連付けられたサブネットなどのリージョン リソースのコンテナになり、VPC にマッピングされなくなります。

次の例では、1 つの VPC グループ（vpc-1）を持つ同じ VRF（v1）内の 2 つのコンテキストプロファイル（c1 と c2）を定義します。この設定では、プロファイル c1 と c2 で定義されたサブネットが同じ VPC グループの一部であるため、1 つの VPC を展開します。

```
<fvTenant name="t1">
    <fvCtx name="v1"/>
    <cloudCtxProfile name="c1" vpcGroup="vpc-1">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
        <cloudRsToCtx tnFvCtxName="v1"/>
        <cloudCidr addr="10.0.0.0/16" primary="yes" >
            <cloudSubnet ip="10.0.1.0/24">
                <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
            </cloudSubnet>
        </cloudCidr>
    </cloudCtxProfile>
    <cloudCtxProfile name="c2" vpcGroup="vpc-1">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-east1" />
        <cloudRsToCtx tnFvCtxName="v1"/>
        <cloudCidr addr="20.0.0.0/16" primary="yes" >
            <cloudSubnet ip="20.0.1.0/24">
                <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
            </cloudSubnet>
        </cloudCidr>
    </cloudCtxProfile>
</fvTenant>
```

プライマリおよびセカンダリ サブネットとサブネット グループについて

Cisco Cloud APIC は cloudRsCtxProfileToRegion 関係が指すリージョンの VPC（タプル fvCtx、cloudRsToCtx、および vpcGroup によって識別される）内のすべてのサブネット（cloudSubnet）を展開します。

Google Cloudでは、VPC の**プライマリ** CIDR の概念はありませんが、クラウド コンテキスト プロファイルの CIDR（cloudCidr）フィールドのプライマリ フラグは、セカンダリ IP 範囲をサポートするために Cisco Cloud APIC を使用できます。プライマリ CIDR で設定されたすべてのサブネットは、指定されたプライマリ IP 範囲（プライマリ サブネット）の実際の Google Cloud サブネットとして展開されます。Google Cloud のリリース 25.0(1) では、特定のクラウド コンテキスト プロファイル（cloudCtxProfile）で複数の CIDR をプライマリとして設定できます。したがって、複数のプライマリ サブネットを持つ特定のクラウド コンテキスト プロファイルの下に、複数のプライマリ CIDR を設定できます。

次の POST は、1 つの VPC と 3 つのサブネットが Google Cloud で展開されている例を示しています。

```
<polUni>
    <fvTenant name="t1">
        <fvCtx name="v1"/>
        <cloudCtxProfile name="c1" vpcGroup="vpc-1">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
            <cloudRsToCtx tnFvCtxName="v1"/>
            <cloudCidr addr="10.0.0.0/16" primary="yes" >
                <cloudSubnet ip="10.0.1.0/24">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="10.0.2.0/24">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr addr="20.0.0.0/16" primary="yes" >
                <cloudSubnet ip="20.0.1.0/24">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
</polUni>
```

上記の例では、1 つの VPC v1 が、us-west リージョンに展開された 3 つのプライマリサブネット（10.0.1.0/24、10.0.2.0/24、および 20.0.1.0/24）で設定されています。

セカンダリ CIDR には、既存のプライマリ サブネットで設定されているセカンダリ IP 範囲（セカンダリ サブネットと呼ばれる）が含まれます。CIDR をプライマリまたはセカンダリとして指定する場合は、次の 2 つの違いを考慮すると役立ちます。

- 通常、プライマリ CIDR は VM です。
- セカンダリ CIDR は、アプリケーションに使用されるコンテナです。

プライマリ サブネットとセカンダリ サブネットを 1 つの**サブネット グループ**にグループ化できます。このグループ化メカニズムは、実際の Google Cloud サブネットにマッピングされたプ

ライマリ サブネットにセカンダリ サブネット（IP 範囲など）を割り当てます。サブネット グループの範囲は、クラウド コンテキスト プロファイル レベルです。同じテナント内に複数のクラウド コンテキスト プロファイルを持つことができますが、サブネットは同じクラウド コンテキスト プロファイル内のサブネット グループにのみ属します。

サブネット グループ ラベルを使用して、特定のサブネット グループに一意のラベルを割り当てます。同じサブネット グループ ラベルを持つ複数のサブネットがある場合、それらがすべて同じクラウド コンテキスト プロファイル内にある限り、それらのサブネットはすべて同じサブネット グループに属します。サブネット グループ ラベルは Cisco Cloud APIC 内でプライマリ サブネットとセカンダリサブネットをグループ化するために使用されますが、Google Cloud では使用されません。

プライマリおよびセカンダリ CIDR に関する次のガイドラインに注意してください。

- **プライマリ CIDR**：
  - サブネット グループは、プライマリ CIDR から最大 1 つのサブネットのみを持つことができます。
  - プライマリ CIDR には複数のサブネットを含めることができますが、すべてのサブネットを別のサブネット グループに含める必要があります。
- **セカンダリ CIDR**：同じサブネット グループにセカンダリ CIDR の複数のサブネットを設定できます。

次の POST は、それぞれが異なるリージョンにあり、セカンダリCIDRを持つ 2 つのサブネットを持つ 2 つの VPC が Google Cloud で展開されている例を示しています。

```
<polUni>
    <fvTenant name="t1">
        <fvCtx name="v1"/>
        <fvCtx name="v2"/>
        <cloudCtxProfile name="c1" vpcGroup="vpc-1">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
            <cloudRsToCtx tnFvCtxName="v1"/>
            <cloudCidr addr="10.0.0.0/16" primary="yes" >
                <cloudSubnet ip="10.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="10.0.2.0/24" subnetGroup="subnet-2">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr addr="40.0.0.0/16" primary="no">
                <cloudSubnet ip="40.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
        <cloudCtxProfile name="c2" vpcGroup="vpc-2">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-east1" />
            <cloudRsToCtx tnFvCtxName="v2"/>
            <cloudCidr addr="20.0.0.0/16" primary="yes">
```

```
                <cloudSubnet ip="20.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr addr="30.0.0.0/16" primary="no">
                <cloudSubnet ip="30.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
</polUni>
```

クラウド コンテキスト プロファイル c2 のサブネット グループ subnet-1 は、クラウド コンテキスト プロファイル c1 のサブネット グループとは異なります。これは、サブネット グループの範囲がクラウド コンテキスト プロファイル レベルにあるためです。

上記の例の目的は次のとおりです。

- テナント t1 は VRF v1 および v2 を定義します。
- クラウド コンテキスト プロファイルc1は、VRF v1 および VPC グループ vpc-1 のリージョンus-west1のサブネットを定義します。これにより、VPC vpc-1 が展開されます。
- クラウド コンテキストプロファイル c2 は、VRF v2 および VPC グループ vpc-2 のリージョン us-east1 のサブネットを定義します。これにより、VPC vpc-2 が展開されます。
- 次のサブネットは、リージョン us-west1 の VPC vpc-1 に展開されます。
  - サブネット-1 サブネット グループ：
    - プライマリ IP 範囲：10.0.1.0/24
    - セカンダリ IP 範囲：40.0.1.0/24
  - サブネット 2 サブネット グループ：
    - プライマリ IP 範囲：10.0.2.0/24
- 次のサブネットは、リージョン us-east1 の VPC vpc-2 に展開されます。
  - サブネット1：
    - プライマリ IP 範囲：20.0.1.0/24
    - セカンダリ IP 範囲：30.0.1.0/24

Google Cloud による Cisco Cloud APIC の設定に関するガイドラインと制限事項

Google Cloud で Cisco Cloud APIC を設定する際の注意事項と制約事項を次に示します。

- Google Cloud は、コントラクトに基づくルーティングをサポートしていません。
- 2 つの Google Cloud サイト間の外部接続は、リリース 25.0(1) ではサポートされていません。
- 外部 VRF は、Cisco Cloud APIC のインフラテナントでのみ設定できます。
- Cisco Cloud APIC に共通するテナントは、どの Google Cloud プロジェクトにも関連付けることができません。
- Inでは、インフラVPCとスポークVPCはVPCピアリングを介して接続されます。Google Cloud
- リリース 25.0(1) では、オンプレミス データセンターとパブリック クラウド間の接続を設定するには、外部デバイス設定ファイルをダウンロードし、Google Cloud と外部デバイス間の接続を手動で有効にすることによって、リモートデバイスを手動で設定する必要があります。

  ダウンロードする外部デバイス設定ファイルは、最終設定ではありません。代わりに、外部デバイス設定ファイルがガイダンスとして提供されます。Google Cloud ルータを IPSec で設定するには、設定ファイルの情報を手動で変更する必要があります。これは、オンプレミスのデータ センターとパブリック クラウド間の接続を確立するために使用されます。

  - Google Cloud ルータとトンネルは、インフラ（ハブ）VPC に導入されます。
  - リリース 25.0(1) では、リージョンごとに 1 つのクラウド ルータがサポートされます。クラウド ルータは、最大 4 つのリージョンに展開できます。
  - スポーク VPC は、インフラ VPC とピアリングして、オンプレミス データセンターなどの外部サイトへの VPN 接続を共有します。

Google Cloud ファイアウォール ルールによる命名の長さの制限

Google Cloud ファイアウォール ルールは名前付きリソースであり、Cisco Cloud APIC は内部ポリシーから名前を取得し、それを使用して Google Cloud ファイアウォール ルールを展開します。Cisco Cloud APICは内部ポリシーに次の命名規則を使用します。

```
{VPC-name}-{in/eg}-{target App-name}-{target EPG-name}-{contract-name}
```

ファイアウォールルール名の最大長は62文字です。Google Cloudこれにより、Google Cloudファイアウォール ルール名で名前が使用される次の Cisco Cloud APIC コンポーネントを設定するときに使用できる名前が制限されます。

- VPC グループ

- アプリケーション プロファイル
- アプリケーション EPG または 外部 EPG
- コントラクト

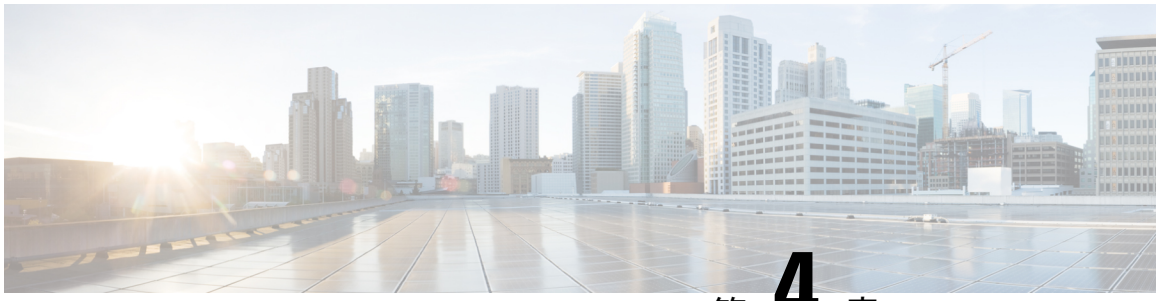
Google Cloudファイアウォール ルール名の最大文字数が 62 であることを認識し、Google Cloud ファイアウォール ルール名を構成する文字列の固定領域を考慮します。

- ハイフン（合計 4 文字）
- `in` (ingress) または `eg` (egress) の値（2 文字）

つまり、すべての個々の Cisco Cloud APIC コンポーネントを組み合わせた名前に使用できる文字の合計数は56文字を超えることはできません。

62 - 4 (ハイフンの数) - 2 (`in` または `eg` 文字数) = 56 文字

したがって、VPC グループ、アプリケーション プロファイル、アプリケーション EPG または外部 EPG、およびコントラクトの名前の長さの合計は、56 文字未満である必要があります。平均すると、各コンポーネントの名前には約 14 文字を使用できます。



第 4 章

Cisco Cloud APIC ポリシー モデル

ACI ポリシー モデルについて

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行えます。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。

- モデル駆動型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。

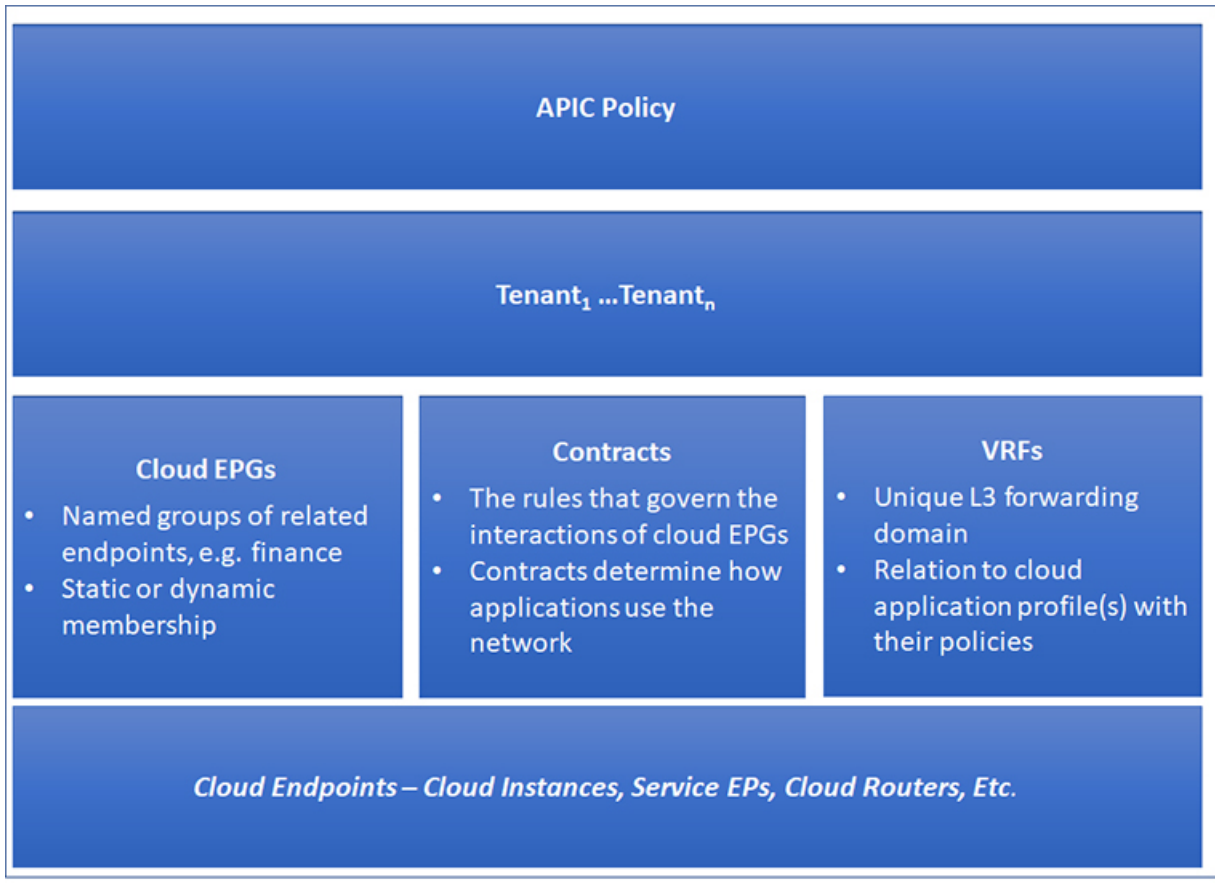
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具象エンティティに対して設定は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシーモデルが更新されるまで、新たに接続されたエンドポイントとの通信を禁止します。
- ネットワーク管理者は、論理システムリソースを直接構成しません。代わりに、システム動作のさまざまな側面を制御する論理（ハードウェアに依存しない）構成とCisco Cloud 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設定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。

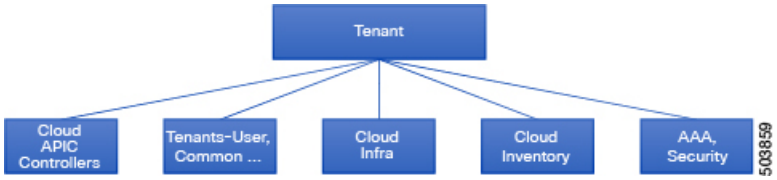
Cisco ACI ポリシー管理情報モデル

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。

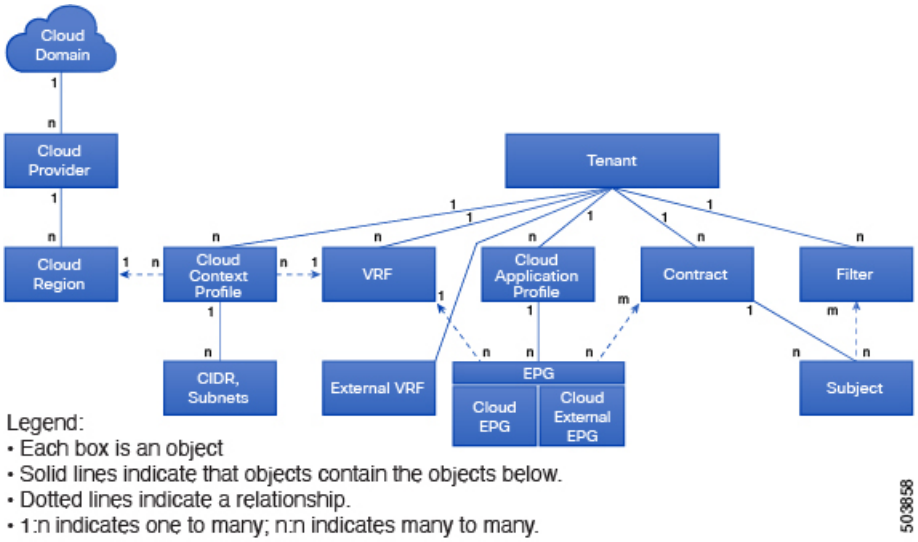
- テナントは、ポリシーのコンテナで、管理者はロールベースのアクセス コントロールを実行できます。システムにより、次の 4 種類のテナントが提供されます。
  - 管理者は、ユーザーのニーズに応じてユーザ テナントを定義します。アプリケーション、データベース、Web サーバ、ネットワーク接続ストレージ、仮想マシンなどのリソースの動作を管理するポリシーが含まれます。
  - システムは共通テナントを提供しますが、クラウドインフラストラクチャ管理者が設定できます。ファイアウォール、ロードバランサ、侵入検知アプライアンスなど、すべてのテナントにアクセス可能なリソースの動作を管理するポリシーが含まれます。
  - 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。
- 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 （151 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。テナントに含まれる主要な要素は、フィルタ、コントラクト、外部ネットワーク、ブリッジ ドメイン、Virtual Routing and Forwarding（VRF）インスタンス、Google Cloud プロバイダー構成、およびエンドポイント グループ（EPG）を含むアプリケーション プロファイルです。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、Google Cloud のリソース グループを表します。VPC 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。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。

クラウド コンテキスト プロファイル

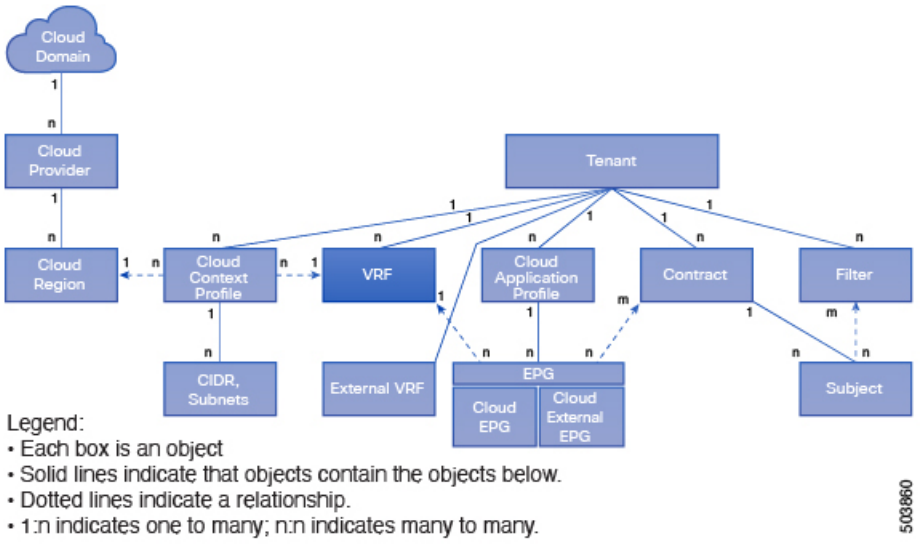
クラウドコンテキストプロファイルには、次の Cisco Cloud APIC コンポーネントに関する情報が含まれています。

- CIDR
- VRF
- EPG
- [Regions]
- VPC
- エンドポイント

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。

外部VRF

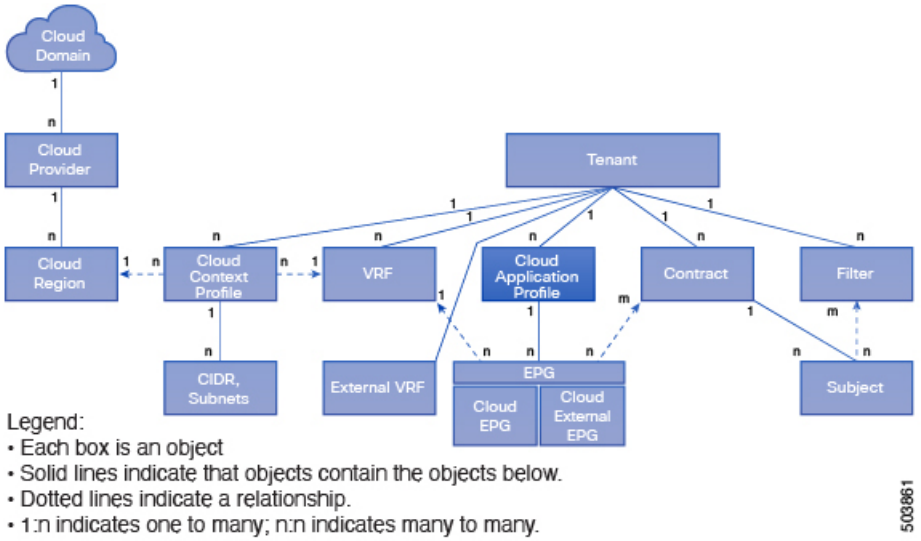
リリース 25.0(1) 以降では、**外部 VRF**Cisco Cloud APIC が使用可能な新しいタイプの VRF として導入されています。外部 VRF はクラウドのプレゼンスをもたない固有の VRF です。この VRF は Cisco Cloud APIC で使用されるクラウド コンテキスト プロファイルで参照されません。

外部 VRF は、他のクラウド サイトまたはオンプレミス サイトに接続された外部ネットワークを表します。複数のクラウド VRF はリークを外部 VRF にルートできるか、外部 VRF からルートを取得できます。外部 VRF で外部ネットワークを作成すると、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。

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。

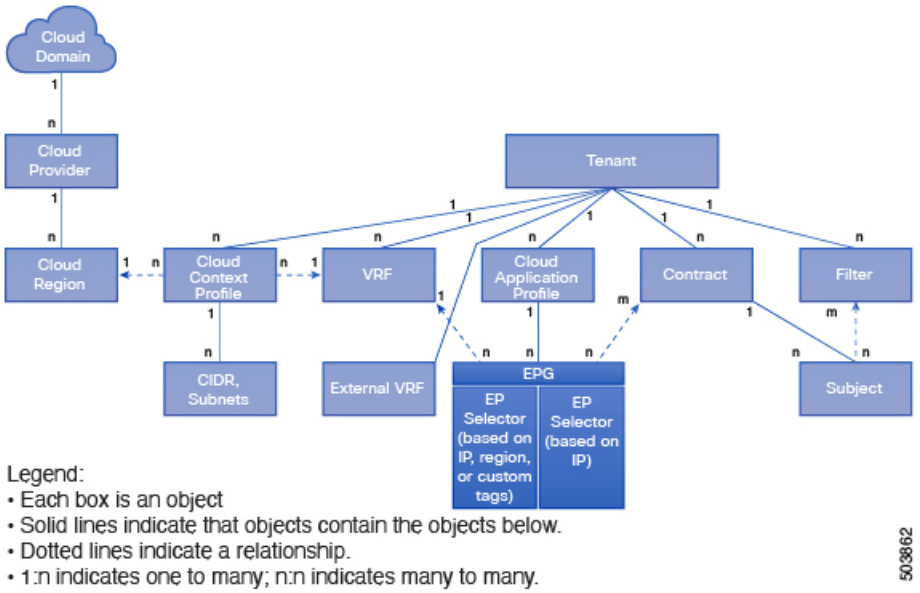
クラウド EPG は次のいずれかに従って組織化できます。

- 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 EPG には、セキュリティ 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 Google Cloud VPC 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。

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。

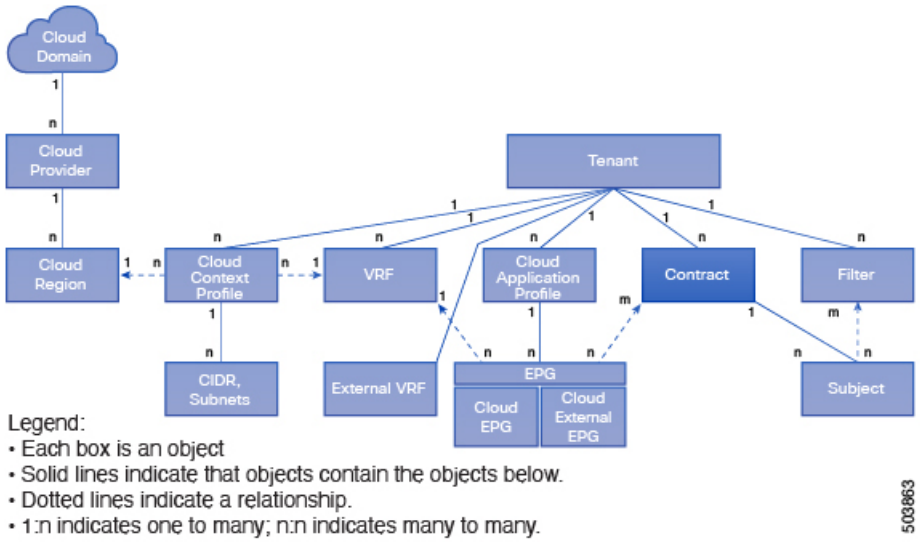


図 *17:* コントラクト

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`）

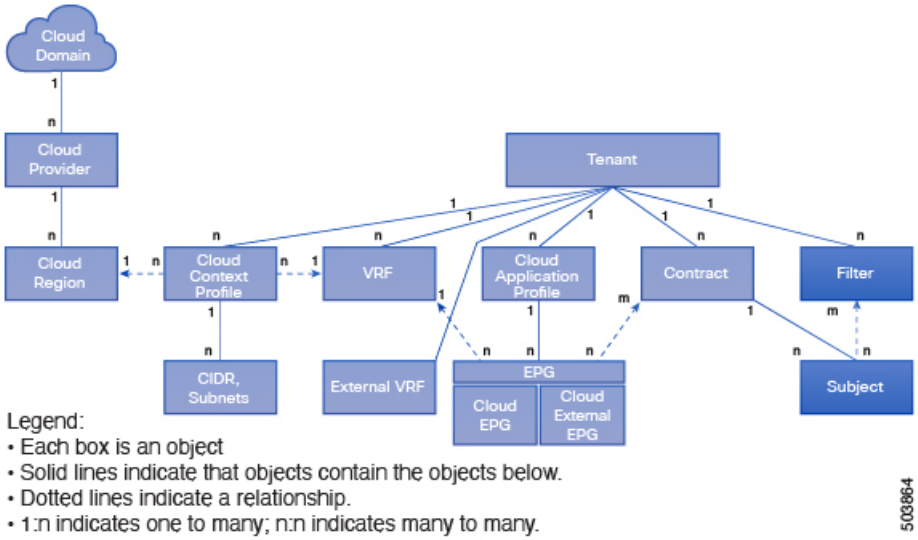
コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付されたクラウド EPG 間の通信を制御します。クラウド EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。クラウド EPG がコントラクトを提供すると、そのクラウド EPG 内のクラウド エンドポイントとの通信は、通信が提供されたコントラクトに準拠している限り、他のクラウド EPG 内のクラウド エンドポイントから開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウド エンドポイントは、コントラクトを指定したクラウド EPG のクラウド エンドポイントと通信を開始できます。

（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。

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現でき、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。Google Cloud 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。

- Google Cloud構造体でレンダリングされるACIコントラクト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。

Google Cloudネットワーク設定の中心的な機能の1つは、仮想プライベート クラウド（VPC）です。Google Cloudは世界中の多くの地域をサポートし、1つのVPCは1つの地域に固有です。

クラウドテンプレートは1つ以上のリージョン名を受け入れ、それらのリージョンのインフラVPCの設定全体を生成します。これらはインフラ VPC です。Google Cloud VPC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 VPCの`cloudCtxProfile` MOは、クラウド テンプレートによって生成されます。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。

Google Cloud VPCの主要なプロパティはCIDRです。Cisco Cloud APICでは、ユーザー VPCでCIDRを選択して展開できます。インフラVPCのCIDRは、クラウドサイトの初期設定時にクラウド 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Google Cloudに展開されます。

CIDRでは、`createdBy`というプロパティも使用できます。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。

インフラ VPC では複数の CIDR およびサブネット ブロックを設定できます。CIDR を作成し、インフラ VPC でサブネットを関連付けることができます。クラウド テンプレートのサブネットは、overlay-1 VRF にマッピングされます。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。

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 （70 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 *3:* 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。
`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。

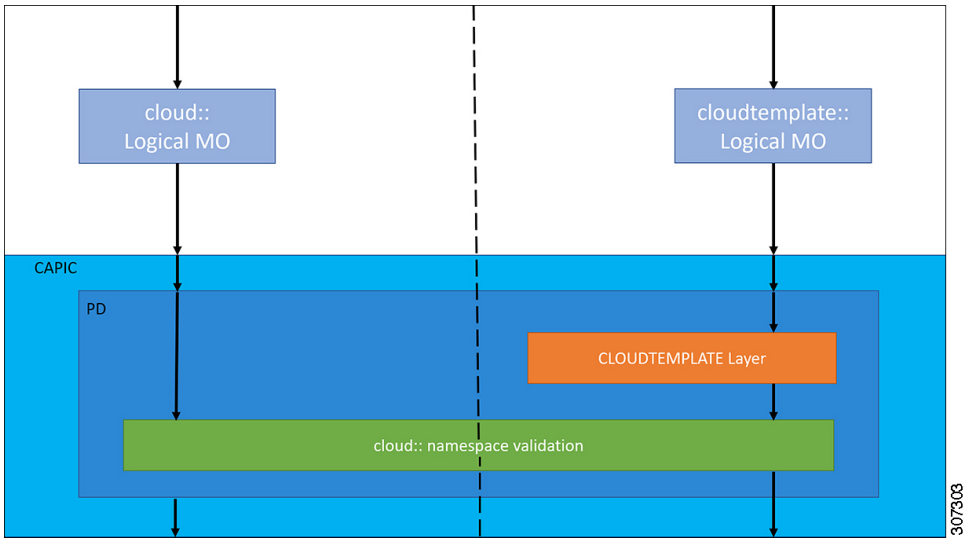
MO	目的
cloudtemplateIpSecTunnel	ACI オンプレミス サイトの IPSec ピアの IP アドレスをキャプチャします。

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 （49 ページ） を参照してください。

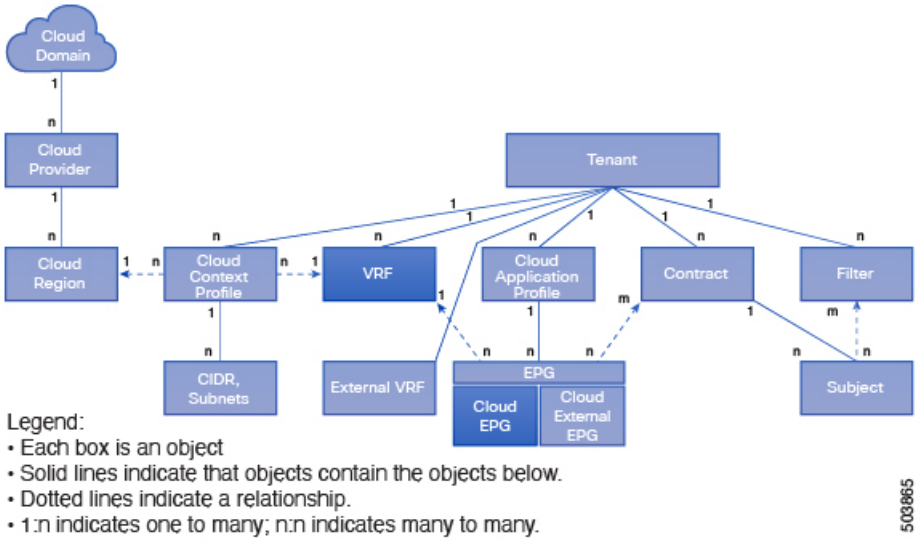
管理対象オブジェクトの関係とポリシー解決

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す。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の異常終了を招く可能性があります。

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。これらのデフォルト ポリシーの例は次のとおりです。

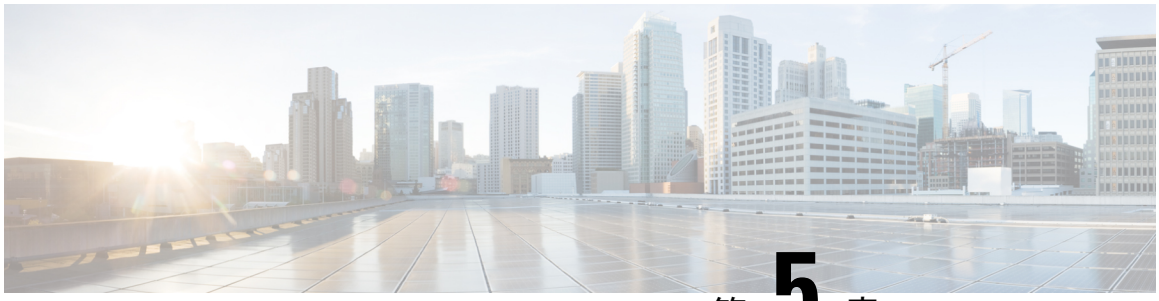
- Google Cloud プロバイダー（インフラ テナント用）
- モニタリング

（注） デフォルト ポリシーを使用する設定を実行する際の混乱を避けるため、デフォルト ポリシーのドキュメントの変更が行われました。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更新ポリシーを削除すると、今後、問題の有るファームウェア更新が発生す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。

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。



第 5 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） 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 （4 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

テナントの作成

次のセクションでは、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方法。

Cloud APIC での Google Cloud の展開について （14 ページ） で説明したように、各 Cisco Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングします。Cisco Cloud APIC テナント用の Google Cloud プロジェクトがまだ作成されていない場合は、次の手順に従って Google Cloud プロジェクトを作成します。

1. Google アカウントにログインします。
2. **[IAM と管理（IAM & Admin）] > [リソースの管理（Manage resources）]**に移動します。

3. ページの上部にある **[組織の選択（Select Organization）]** ドロップダウン リストを使用して、プロジェクトを作成する組織を選択します。
4. **[+プロジェクトの作成（+ CREATE PROJECT）]** をクリックします。
5. 表示される **[新規プロジェクト（New Project）]** ウィンドウで、プロジェクト名を入力し、必要に応じて課金アカウントを選択します。

   プロジェクト名には、文字、数字、一重引用符、ハイフン、スペース、または感嘆符のみを含めることができ、4ー30 文字にする必要があります。
6. **[ロケーション（Location）]** フィールドに親組織またはフォルダを入力します。

   そのリソースは、新しいプロジェクトの階層的な親になります。
7. [CREATE] をクリックします。

Google Cloud および Cisco Cloud APIC GUI を使用した管理対象テナントの作成

このセクションでは、GUIを使用して Cisco Cloud APIC により管理されるテナントを作成する方法について説明します。

ステップ 1 必要に応じて、この Cisco Cloud APIC テナントに関連付ける新しい Google Cloud プロジェクトを作成します。

Cloud APIC での Google Cloud の展開について （14 ページ） で説明したように、各 Cisco Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングされます。必要な場合は、これらの手順について テナントの作成 （49 ページ） を参照してください。

ステップ 2 Cisco Cloud APIC GUI で **[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]** に移動します。

すでに設定されているテナントのテーブルが表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[テナントの作成（Create Tenant）]**を選択します。

[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 *4:* テナント ダイアログボックス フィールドの作成

Properties	説明
[名前（Name）]	テナント名を入力します。正規表現の一致: `[a-z]([-a-z0-9]*[a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

Properties	説明
説明	テナントの説明を入力します。
Settings	
セキュリティドメインの追加（Add Security Domain）	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。
Google Cloud プロジェクト	
Google Cloud プロジェクト ID	この Cisco Cloud APIC テナントに関連付けるGoogle Cloud プロジェクトIDを入力します。
アクセス タイプ（Access Type）	Cisco Cloud APIC によって管理されるテナントの場合、アクセス タイプとして **[管理対象外 ID（Unmanaged Identity）]** を選択します。 詳細については、Cloud APIC での Google Cloud の展開について （14 ページ）を参照してください。
Google Cloud Project のセキュリティ ドメインを追加	（注） テナントの作成時のGoogle Cloudのセキュリティ ドメインの追加はオプションです。 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. **[Google Cloud Project のセキュリティ ドメインの追加（Add Security Domain for Google Cloud Project）]** 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 **[保存（Save）]** をクリックします。

ステップ 6 アクセス タイプとして **[管理対象アイデンティティ（Managed Identity）]** を選択したため、次に Google Cloud でこのテナントに必要な権限を設定します。

a) Google Cloud GUIで、この Cisco Cloud APIC テナントに関連付けられている Google Cloud プロジェクトにログインします。
このプロジェクトの **ダッシュボード** が表示されます。

b) 左ナビゲーション バーで、**[IAM と管理（IAM & Admin）]** をクリックし、**[IAM]** を選択します。

[IAM] ウィンドウが表示され、いくつかのサービス アカウントが表示されます。

c) Cisco Cloud APIC インフラ アカウントに関連付けられているプロジェクトで Cisco Cloud APIC によって作成されたサービス アカウントを見つけます。

d) サービス アカウント名をコピーします。

e) このサービス アカウント名を、ユーザー テナント プロジェクトの IAM ユーザーとして追加します。

f) このサービス アカウントの権限を設定します。

1. このサービス アカウントの行にある鉛筆アイコンをクリックします。

   [権限の編集（Edit Permissions）] ウィンドウが表示されます。

2. **[+別のロールの追加（+ ADD ANOTHER ROLE）]** をクリックし、ロールとして **[クラウド機能サービス エージェント（Cloud Functions Service Agent）]** を選択します。

   サービス アカウントが表示された **[IAM]** ウィンドウに戻ります。

3. **[+別のロールの追加（+ ADD ANOTHER ROLE）]** を再度クリックし、このサービス アカウントに必要な残りのロールを追加します。

   以下は、このプロセスの最初のステップで追加したクラウド機能サービス エージェントを含む、このサービス アカウントに割り当てる必要があるロールの完全なリストです。

   - クラウド機能サービス エージェント
   - コンピューティング インスタンス管理（v1）
   - コンピューティング ネットワーク管理
   - コンピューティング セキュリティ管理
   - ログインしている管理
   - パブ/サブ管理
   - ストレージ管理者

4. 必要なすべてのロールを追加した後で、**[保存（Save）]** をクリックします。

   IAM ウィンドウに戻り、サービス アカウントが表示され、必要なロールがこのサービス アカウントに割り当てられます。

Google Cloud および Cisco Cloud APIC GUI を使用した管理対象外テナントの作成

ここでは、GUI を使用して Cisco Cloud APIC の管理対象外のテナントを作成する方法について説明します。

ステップ 1 必要な場合は、この Cisco Cloud APIC と関連付けられる新しい Google Cloud プロジェクトを作成します。

Cloud APIC での Google Cloud の展開について （14 ページ） で説明したように、各 Cisco Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングします。必要な場合は、これらの手順について テナントの作成 （49 ページ） を参照してください。

ステップ 2 Google Cloud で、Cisco Cloud APIC テナントに関連付けられている Google Cloudプロジェクトを選択します（まだ選択していない場合）。

ステップ 3 左ナビゲーション バーで、**[IAM および Admin]** をクリックして、**[サービス アカウント（Service Accounts）]** を選択します。

この Google Cloud プロジェクトのサービス アカウントが表示されます。

ステップ 4 既存のサービス アカウントを選択するか、**[+サービス アカウントの作成（+ CREATE SERVICE ACCOUNT）]** をクリックして新しいアカウントを作成します。

このサービス アカウントの情報が表示され、**[詳細（Details）]** タブがデフォルトで選択されています。

ステップ 5 **[キー（KEYS）]** タブをクリックします。

ステップ 6 **[ADD KEY（キーの作成）]** > **[新しいキーの作成（Create New Key）]**をクリックします。

このサービスアカウントの秘密キーを作成するためのオプションを提供するウィンドウが表示されます。

ステップ 7 **JSON** キー タイプを選択したまま、**[作成（Create）]** をクリックします。

秘密キーがコンピュータに保存されたことを示すウィンドウが表示されます。

ステップ 8 コンピュータにダウンロードした JSON ファイルを見つけて、コンピュータ上の安全な場所に移動します。

この JSON ファイルには、管理対象外テナントのフィールドに入力する必要があるキー情報が含まれています。

ステップ 9 Cisco Cloud APIC GUI で **[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]** に移動します。

すでに設定されているテナントのテーブルが表示されます。

ステップ 10 **[アクション（Actions）]** をクリックし、**[テナントの作成（Create Tenant）]**を選択します。

[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 11 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 *5:* テナント ダイアログボックス フィールドの作成

Properties	**説明**
[名前（Name）]	テナント名を入力します。正規表現の一致: `[a-z]([-a-z0-9]*[a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。
説明	テナントの説明を入力します。
Settings	
セキュリティ ドメインの追加（Add Security Domain）	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。
Google Cloud プロジェクト	
Google Cloud プロジェクト ID	この Cisco Cloud APIC テナントに関連付ける Google Cloud プロジェクト ID を入力します。
アクセス タイプ（Access Type）	Cisco Cloud APIC によって管理されないテナントの場合は、アクセスタイプとして **[管理対象外 ID（Unmanaged Identity）]** を選択します。 詳細については、Cloud APIC での Google Cloud の展開について （14 ページ）を参照してください。
キー ID	これらの手順の最初にダウンロードした JSON ファイルの `private_key_id` フィールドの情報を入力します。

Properties	説明
RSA プライベート キー	これらの手順の最初にダウンロードしたJSONファイルの `private_key` フィールドの情報を入力します。
Client ID	これらの手順の最初にダウンロードしたJSONファイルの `client_id` フィールドの情報を入力します。
Email	Google Cloudプロジェクトに関連付けられているEメール アドレスを入力します。
Google Cloud Project のセキュリティ ドメインを追加	（注） テナントの作成時のGoogle Cloudのセキュリティ ドメインの追加はオプションです。 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. **[Google Cloud Project のセキュリティ ドメインの追加（Add Security Domain for Google Cloud Project）]** 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 12 設定が終わったら **[保存（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。

次の制約事項に注意してください。

- 正規表現の一致:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。

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 **[保存（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。

（注） 外部 VRF を設定するには、下の **[テナント（Tenant）]** フィールドで [インフラ（infra）] を選択します。VRF は次の場合に 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
- 外部ネットワークに関連付けられています（Cisco Cloud APIC GUI を使用した外部ネットワークの作成 （58 ページ） を参照）。
- 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ません

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

Properties	説明
General	

Properties	説明
Name	**[Name]** フィールドに、VRF の表示名を入力します。 次の制約事項に注意してください。 • 正規表現の一致: `[az]([-a-z0-9] * [a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 • 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。 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。
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 CSR 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。Cisco Cloud APIC は 1 つのハブ ネットワークのみをサポートするため、**[ハブ ネットワーク（Hub Network）]** 列には 1 つのハブ ネットワークのみが表示されます。

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。

（注） ハブネットワークがまだ設定されていない場合は、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する必要があることを示す警告がページの上部に表示されます。メッセージ内の青い **[Cloud APIC のセットアップ（Cloud APIC Setup）]** リンクをクリックしてハブ ネットワークを作成し、ここに戻ります。ハブネットワークの作成の詳細については、『Cisco Cloud APIC for Google CloudInstallation Guide、Release 25.0(x)』の「Configuring Cisco Cloud APIC Using the Setup Wizard」の章を参照してください。

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 *7 : [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*

Properties	説明
General	
Name	外部ネットワーク名を入力します。

Properties	説明
VRF	この 外部 VRF は、オンプレミス CSR 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。この時点では、外部 VRF はインフラ テナント以外のテナントで作成することはできず、外部 VRF はクラウド 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。 **[+ 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。
ハブ ネットワーク	ハブ ネットワークは、初回セットアップで設定した後に自動的に表示されます。 （注） ハブ ネットワークがまだ設定されていない場合は、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する必要があります。ハブネットワークの作成の詳細については、『Cisco Cloud APIC for Google CloudInstallation Guide、Release 25.0(x)』の「Configuring Cisco Cloud APIC Using the Setup Wizard」の章を参照してください。
VPN ルータ	このフィールドは編集できません。デフォルトの VPN ルータが自動的に選択されます。
Settings	

Properties	説明
[Regions]	リージョンを選択するには: 1. **[リージョンの追加（Add Region）]** をクリックします。 **[リージョンの選択（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リージョンがここに表示されます。 • 複数のリージョンを選択して、複数のリージョンでクラウドルータを起動できます。 2. **[リージョンの選択（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。

Properties	説明
VPN ネットワーク	VPNネットワークエントリは、内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 2 つのトンネルが作成されます。 **4.** 追加する IPSec ピア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** • **Pre-Shared Key; 事前共有キー** • **IKE バージョン（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** • **サブネット プール名（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。 **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 Google Cloud で構成されます。

Google Cloud でクラウドルータがで構成されていることを確認するには、インフラ VPC の Google Cloud アカウントで、**[ハイブリッド接続（Hybrid Connectivity）]** > **[クラウドルータ（Cloud Routers）]** に移動します。さまざまなリージョン用に作成されたクラウドルータが表示されます（新しく設定されたクラウドルータを表示するには、[更新（Refresh）]をクリックする必要があります）。

IPSec セッションを表示するには、**[ハイブリッド接続（Hybrid Connectivity）]** > **[VPN]** > **[クラウド VPN トンネル（Cloud VPN Tunnels）]** に移動します。

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

VRF 間ルートリークを使用すると、独立したルーティング ポリシーを設定して、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、VRF のペア間でリークするルートを指定できます。

- 2 つのクラウド サイト
- クラウド サイトと非 ACI オンプレミス サイト

（注） 詳細については、ルーティング ポリシーとセキュリティ ポリシーの個別の構成 （21 ページ）を参照してください。

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 *8*：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*）

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（トランスポート）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。

Properties	説明
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。 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。 • **[すべてリーク（Leak All）]**：VRF 間でリークするすべてのルートを設定する場合に選択します。 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**：VRF 間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。 VRF 間のリークのルートとして複数のサブネット IP アドレスを設定するには、異なるサブネットの追加エントリを入力します。

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 **[別のルートの追加（Add Another 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 （63 ページ）ーステップ 5 （64 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 ルートの追加（Add Reverse 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 （63 ページ）ーステップ 5 （64 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 （63 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 （63 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。

Google Cloud と外部デバイス間の接続の有効化

Google Cloud ルータと外部デバイス間の接続を手動で有効にするには、次の手順に従います。

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**が表示されます。

ステップ 2 **[接続（Connectivity）]** 領域の **[外部接続ステータス（External Connectivity Status）]** で、**[クラウド ルータ（Cloud Routers）]** エントリの上にある番号をクリックします。
[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、Google Cloud ルーターと外部デバイス間の接続を有効にするため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。

Google Cloud と外部デバイスの間の接続の有効化

始める前に

外部デバイス構成ファイルのダウンロード （65 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ます。

ステップ 1 Google Cloud と外部デバイスの間の接続を有効にするために必要な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 デバイスをクラウド ACI ファブリックに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 （65 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。

次に、vpn-connectivity 設定ページから **PRESHARED-KEY** を取得した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 54.215.245.58 5.500 for
hcextnwTunIf.acct-[infra]/region-[us-west1]/hubCtx-[1]-id-[0]/ext-[extnwfoo_us-west1]/vpn-[vpnwfoo]/rtr-default-peer-54.215.245.58/src-1-dest-[54.215.245.58]
! USER-DEFINED: please define rd: RD
! USER-DEFINED: please provide preshared-key: PRESHARED-KEY
! USER-DEFINED: please define router-id: ROUTER-ID
! USER-DEFINED: please define gig-number: GIG-NUMBER
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! ikev: ikev2
! vrf-name: extv1
! user name: root
! tunnel counter: 5
! IPV4 address: 35.220.50.132
! tunnel interface destination: 54.215.245.58
! tunne id: 500
! BGP peer address: 169.254.10.6
! BGP peer neighbor address: 169.254.10.5
```

```
! BGP peer ASN: 64513
! hcloudHubCtx ASN: 64512

vrf definition extv1
    rd RD:1
    address-family ipv4
    exit-address-family
exit

interface Loopback0
    vrf forwarding extv1
    ip address 41.41.41.41 255.255.255.255
exit


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
exit

crypto ikev2 policy ikev2-1
    proposal ikev2-1
exit

crypto ikev2 keyring keyring-root-5
    peer peer-ikev2-keyring
        address 35.220.50.132
        pre-shared-key PRESHARED-KEY
    exit
exit

crypto ikev2 profile ikev-profile-root-5
    match address local interface GIG-NUMBER
    match identity remote address 35.220.50.132 255.255.255.255
    identity local address 54.215.245.58
    authentication remote pre-share
    authentication local pre-share
    keyring local keyring-root-5
    lifetime 3600
    dpd 10 5 periodic
exit

crypto ipsec transform-set ikev-transport-root-5 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile ikev-profile-root-5
    set transform-set ikev-transport-root-5
    set pfs group14
    set ikev2-profile ikev-profile-root-5
exit

interface Tunnel500
    vrf forwarding extv1
    ip address 169.254.10.6 255.255.255.252
    ip mtu 1400
    ip tcp adjust-mss 1400
    tunnel source GIG-NUMBER
    tunnel mode ipsec ipv4
    tunnel destination 35.220.50.132
    tunnel protection ipsec profile ikev-profile-root-5
exit
```

```
ip route 35.220.50.132 255.255.255.255 GIG-NUMBER GIG-GATEWAY

router bgp 64513
    bgp router-id ROUTER-ID
    bgp log-neighbor-changes

    address-family ipv4 vrf extv1
        network 41.41.41.41 mask 255.255.255.255
        neighbor 169.254.10.5 remote-as 64512
        neighbor 169.254.10.5 ebgp-multihop 255
        neighbor 169.254.10.5 activate
    exit-address-family
exit
```

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

```
vrf definition Ext-V1
rd 1:10
!
address-family ipv4
  route-target export 64550:10
  route-target import 64550:10
!
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
lifetime 28800
!
crypto isakmp keepalive 10 10 periodic
crypto isakmp aggressive-mode disable
!
```

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

Cisco Cloud APIC GUI を使用した EPG の作成

アプリケーション EPG または外部 EPG を作成するには、このセクションの手順を使用します。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。

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

Properties	説明
General	

Properties	説明
Name	EPG の名前を入力します。 次の制約事項に注意してください。 • 正規表現の一致: `[a-z]([-a-z0-9]*[a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 • 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。
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 EPG を作成している場合、オーバーレイ-1 VRF でそのアプリケーション プロファイルがしようされているため、`cloud-infra` アプリケーション プロファイルを選択しないことをお薦めします。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。

Properties	説明
Settings	
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。
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。

Properties	説明
エンドポイントセレクタ	

Properties	説明
	（注） エンドポイント セレクタ構成プロセスの一部として、Google Cloud の仮想マシンを構成する方法については、Google Cloud の仮想マシン セキュリティの設定（92 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。 • エンドポイント セレクタに Google Cloud 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）]**：キーを含まない式に使用されます。 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

Properties	説明
	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**：us-west1 • 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 us-west1 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。

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**：us-east1、us-central1 その場合、次のようになります。 • リージョンが us-west1 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) 場合 または • リージョンが us-east1 または us-central1 (エンドポイント セレクタ 2 の式) のいずれかである場合 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 **[保存（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。

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

Properties	説明
General	
Name	EPG の名前を入力します。 次の制約事項に注意してください。 • 正規表現の一致: `[a-z]([-a-z0-9]*[a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 • 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。
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。

Properties	説明
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。
Settings	
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。
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。
ルート到達可能性	外部 EPG のルート到達可能性のタイプが自動的に選択されます（**Internet** または **外部サイト** のいずれか）。

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 Google Cloud で仮想マシンを設定する手順については、Google Cloud の仮想マシン セキュリティの設定 （92 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. [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。 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 **[保存（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 *11* : フィルタの作成ダイアログボックスのフィールド

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。
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。

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。 • **ICMP** • **[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 *12 : [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

Properties	説明
[名前（Name）]	契約の名前を入力します。 次の制約事項に注意してください。 • 正規表現の一致: `[a-z]([-a-z0-9]*[a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 • Google Cloud ファイアウォール ルールによる制限のため、この名前には 14 文字以下を使用することをお勧めします。ファイアウォールルール名を構成する各 Cisco Cloud APIC コンポーネントに使用できる制限と文字数の合計については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ）を参照してください。

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。 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。
Settings	
スコープ	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 グループに契約を制限します。 （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。 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**
Add Filter	フィルタを選択します。 1. [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 **[保存（Save）]** をクリックします。

Cisco Cloud APIC GUI を使用したテナント間コントラクトの作成

このセクションでは、Cisco Cloud APIC GUI を使用したテナント間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 *13 : [*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

Properties	説明
[名前（Name）]	契約の名前を入力します。 これは Google Cloud のコントラクトの名前です。正規表現の一致: `[az]([-a-z0-9] * [a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。
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。**[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。

Properties	説明
説明	コントラクトの説明を入力してください。
Settings	
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。
Add Filter	フィルタを選択します。 **1.** [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 **[保存（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。

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 APIC 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 APIC 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 *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

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。正規表現の一致: `[a-z]([-a-z0-9]*[a-z0-9])?` このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。
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。

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、**[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。

Properties	説明
CIDR の追加（Add CIDR）	（注） プライマリおよびセカンダリ CIDR とサブネット グループラベルの詳細については、Google Cloud の下の VPC とサブネット、およびクラウド APIC でのクラウドコンテキストプロファイルについて （26 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。 • クラウド コンテキスト プロファイルごとに少なくとも 1 つのプライマリ CIDR を追加する必要があります。 • VPC のセカンダリ CIDR とサブネットを追加する場合は、**[プライマリ（Primary）]** ボックスをオフのままにします。 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。 • **[サブネット グループ ラベル（Subnet Group 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）**：**[サブネット グループ ラベルの選択（Select Subnet Group Label）]** をクリックし、このサブネットに関連付ける既存のサブネット グループ 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サブネットグループ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。

ステップ 5 設定が終わったら **[保存（Save）]** をクリックします。

Google Cloud の仮想マシン セキュリティの設定

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を設定するエンドポイントセレクタに対応するGoogle Cloudで必要なインスタンスについても設定することが必要になります。

このトピックでは、Google Cloud 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 Google Cloud のインスタンスを設定することができます。

たとえば、エンドポイントセレクタのタイプとして **[カスタム（Custom）]** を使用するとします（エンドポイントおよびエンドポイント セレクタ （23 ページ）を参照）。

- Google Cloud のアカウントに移動し、 Google Cloud でカスタムタグまたはラベルを使用してしてから、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もできます。
- または、Cisco Cloud APIC でカスタムタグまたはラベルを使用してエンドポイント セレクタを作成してから、Google Cloud のアカウントに移動し、Google Cloud のカスタム タグまたはラベルを作成することもできます。

始める前に

Google Cloud 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、Google Cloud 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
- Google Cloud プロジェクト 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 Google Cloud 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。Google Cloud 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 Cisco Cloud APIC ユーザー テナントの Google Cloud 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 Google Cloud VM の作成を開始します。

（注） Google Cloud ポータルで VM を作成する方法の詳細については、Google Cloud 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 *15 :* 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

Properties	説明
General	
Name	バックアップ構成の名前を入力します。

Properties	説明
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）]**

Properties	説明
バックアップ オブジェクト	

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。 • **[クラウド コンテキスト プロファイル（Cloud Context Profile）]**：これを選択すると、**[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

Properties	説明
	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 **[保存（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 *16* : 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

Properties	説明
General	
Name	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	

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。

ステップ 5 設定が終わったら [保存（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 *17 :* スケジューラの作成ダイアログボックスのフィールド

Properties	説明
General	
Name	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	

Properties	説明
繰り返しウィンドウ	

Properties	説明
	[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（Every Day）** • **偶数日（Even Days）** • **奇数日（Odd Days）** • **[Monday]** • **[Tuesday]** • **[Wednesday]** • **[Thursday]** • **[Friday]** • **[Saturday]** • **[Sunday]** 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）]** フィールドで、次のいずれかを選択します。 • **無制限（Unlimited）**：スケジューラ ウィンドウに適用できる同時タスクの最大数はありません。 • **カスタム（Custom）**：2番目の **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドに、同時に処理できるタスクの最大数を入力します。このフィールドに許容される最大値は 65535 レコードです。 4. **[最大実行時間（Maximum Running Time）]** フィールドで、次のいずれかを選択します。 • **無制限（Unlimited）**：スケジューラ ウィンドウに適用される時間制限はありません。 • **カスタム（Custom）**：2番目の**[最大実行時**

Properties	説明
	間（**Maximum Running Time**）**]** フィールドに、ウィンドウの最大継続時間を入力します。このフィールドで使用できる形式は `dd:hh:mm:ss` です。 **5.** 終了したら、[Add] をクリックします。
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 **[保存（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 *18* : 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

Properties	説明
General	
Name	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 **[保存（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作成のフィールド（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 *19 :* 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

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。

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。

Properties	説明
LDAP グループ マップ ルール	

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 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。 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から、**[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で、左側のペインにロールのリストが表示されま

Properties	説明
	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 **[保存（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 **[タイプ（Type）]** フィールドで、セキュリティ ドメインのタイプを選択します。

- **制限なし（Unrestricted）**：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。
- **制限あり（Restricted）**：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せん。

ステップ 7 設定が終わったら **[保存（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 *20 :* ロールの作成ダイアログボックスのフィールド

Properties	説明
General	
Name	**[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	

Properties	説明
特権	

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**：インフラでのレイヤ 1ー3 の設定、テナントの L3Out でのスタティック ルート設定、管理インフラポリシー、およびテナント 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**：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ー3 のプロトコル設定に使用されます。 • **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。 • **admin**：すべてへのアクセス（すべてのロールの組み合わせ） • **config-manager** • **custom-port-privilege** • **custom-privilege-1 ～ custom-privilege-22** • 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ー3の設定に使用します。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ー3 のプロトコル設定、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 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。 • **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。

Properties	説明
	• **site-admin** • **site-policy** • **tenant-connectivity**：ブリッジ ドメイン、サブネット、および VRF を含むレイヤ 1ー3 の接続変更に使用されます。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設定。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。 • **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ー3 プロトコルの管理、および traceroute、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ー3 プロトコルの設定、テナント traceroute 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**：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-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。

ステップ 5 設定が終わったら **[保存（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 *21 :* 証明書認証局の作成ダイアログボックスのフィールド

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。

Properties	説明
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 **[保存（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 *22*：キー リングの作成ダイアログボックスのフィールド

Properties	説明
[名前（Name）]	キー リングの名前を入力します。

Properties	説明
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。
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。

Properties	説明
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）。
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 **[保存（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 *23 :* 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

Properties	説明
Username	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。

Properties	説明
説明	ローカル ユーザーの説明を入力します。
Settings	
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。 • **Blocked**：ローカルユーザーアカウントをブロックします。 • **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。

Properties	説明
セキュリティ ドメイン	

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

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 *24 :* 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。
ユーザー証明書属性	ユーザー証明書の属性。
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 **[保存（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）

Google Cloud では、VPC リソースはすべての Google Cloud リージョンにまたがるグローバル リソースです。デフォルトでは、すべてのリージョンがGoogle Cloudによって管理され、リージョン間接続が存在します。Cloud APIC は、25 の Google Cloud リージョンすべてを管理します。

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 **[ワークフロー（Workflows）]** 領域で、**[Cloud APIC の設定（Cloud APIC 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 3 **[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。
[リージョン管理（Region Management）] ウィンドウが表示されます。

ステップ 4 外部接続を構成するかどうかを決定します。

[有効化（Enable）] の横にあるボックスをクリックして、外部接続を有効にします。

ステップ 5 ページ内のすべてのリージョンが選択されていることを確認します。

このページには、Google Cloud でサポートされているすべてのリージョンが表示されます。すべてのリージョンは Cloud APIC によって管理されます。

ステップ 6 ページの下部にある **[次へ（Next）]** をクリックします。

外部接続を有効にした場合は、**[一般接続（General Connectivity）]** ページが表示されます。

ステップ 7 **[ハブ ネットワーク（Hub Network）]** 領域に必要な情報を入力します。

ハブ ネットワーク管理は、特定の管理対象リージョンにクラウドルータを展開するために使用されます。クラウド サイトのファブリック インフラ接続を設定し、このエリアのクラウド サイトのクラウド ルータに使用する構成テンプレートを定義します。

次の制約事項に注意してください。

- Google Cloud のハブ ネットワークは 1 つだけ作成できます。
- ハブ ネットワークでは、Google Cloud に1 つのクラウドルータのみが作成されます。

a) [Hub Network] 領域で、[Add Hub Network] をクリックします。

[Add Hub Network] ウィンドウが表示されます。

b) **[Name]** フィールドにハブ ネットワークの名前を入力します。

c) **[BGP 自律システム番号（BGP Autonomous System Number）]** フィールドに値を入力します。

BGP 自律システム番号（ASN）は、クラウドサイト内の BGP ピアリングと、他のサイトへの MP-BGP IPv4 ピアリングに使用されます。

ASN はプライベート ASN である必要があります。各ハブ ネットワークに 64512ー65534 または 4200000000ー4294967294 の値を入力し、フィールドの横にあるチェックマークをクリックします。

d) **[リージョン（Region）]** フィールドで、適切なリージョンを選択します。

このエリアには、最大 4 つのリージョンを追加してハブ ネットワークを展開できます。ハブ ネットワークは、選択した各リージョンに 1 つのクラウド ルータを作成します。

e) **[VPN ルータ（VPN Router）]** フィールドに VPN ルータの名前を入力します。

インフラ VPC は、クラウド ルータと VPN ゲートウェイを使用して、オンプレミス サイトまたはその他のクラウド サイトへの IPSec トンネルと BGP セッションを作成します。 スポーク VPC は、インフラ VPC とピアリングして、外部サイトへの VPN 接続を共有します。

ステップ 8 **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** 領域に必要な情報を入力します。

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** 領域で、**[IPSec トンネル サブネット プールの追加（Add IPSec Tunnel Subnet Pools）]** をクリックします。

[IPSec トンネル サブネット ツールの追加（Add IPSec Tunnel Subnet Pools）] ウィンドウが表示されます。

b) 必要に応じて、IPSec トンネルに使用するサブネット プールを入力します。

デフォルトでは、`169.254.0.0/16`のサブネットプールが設定され、IPsec トンネルが作成されます。必要に応じて、既存のサブネット プールを削除し、サブネット プールを追加できます。

IPSec トンネル サブネット プール エントリに使用されるサブネットは、169.254.0.0/16 ブロックの共通 /30 CIDR である必要があります。たとえば、169.254.7.0/24 と 169.254.8.0/24 は、このフィールドのサブネット プールの許容エントリです。

適切なサブネット プールに入力したら、チェック マークをクリックします。

ステップ 9 このページに必要な情報をすべて入力したら、ページの下部にある [保存して続行（Save and Continue）] をクリックします。

必要に応じて、外部ネットワークを作成し、外部接続設定を完了するオプションが表示されます。これらの手順については、Cisco Cloud APIC GUI を使用した外部ネットワークの作成 （58 ページ） にアクセスしてください。

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

始める前に

このセクションの手順を実行する前に、Cloud APIC での Google Cloud の展開について （14 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 複数のテナント間で同じログイン情報を共有するには、次の POST を入力します。各テナントで cloudCredentials オブジェクトを複製し、同じ Google Cloud サービス アカウントを指定します。

次の点に注意してください。

- テナント T1 は、サービス アカウントの秘密キーを保持する cloudCredentials オブジェクトを定義します。
- テナント T1 と T2 は両方とも、cloudRsCredentials リレーションを介してこの cloudCredentials オブジェクトを参照します。
- テナント T1 によって定義されたサービス アカウントは、このシナリオの Google Cloud プロジェクト project1 および project2 のメンバーである必要があります。
- テナント T2 の POST で強調表示された領域は、最初のユーザー テナントと共有されるログイン情報を示します。

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="T1">
    <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-T1/credentials-creds1" />
    </cloudAccount>
    <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
```

```
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T1/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-T2/credentials-creds1" />
    </cloudAccount>
   <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

ステップ 2 Cloud APIC が Google Cloud（ログイン情報を持つインフラ テナント）の外部で実行されるユーザー テナントを作成するには、次の手順を実行します。

Google Cloudに追加された新しいプロパティは、以下で強調表示されていることに注意してください。

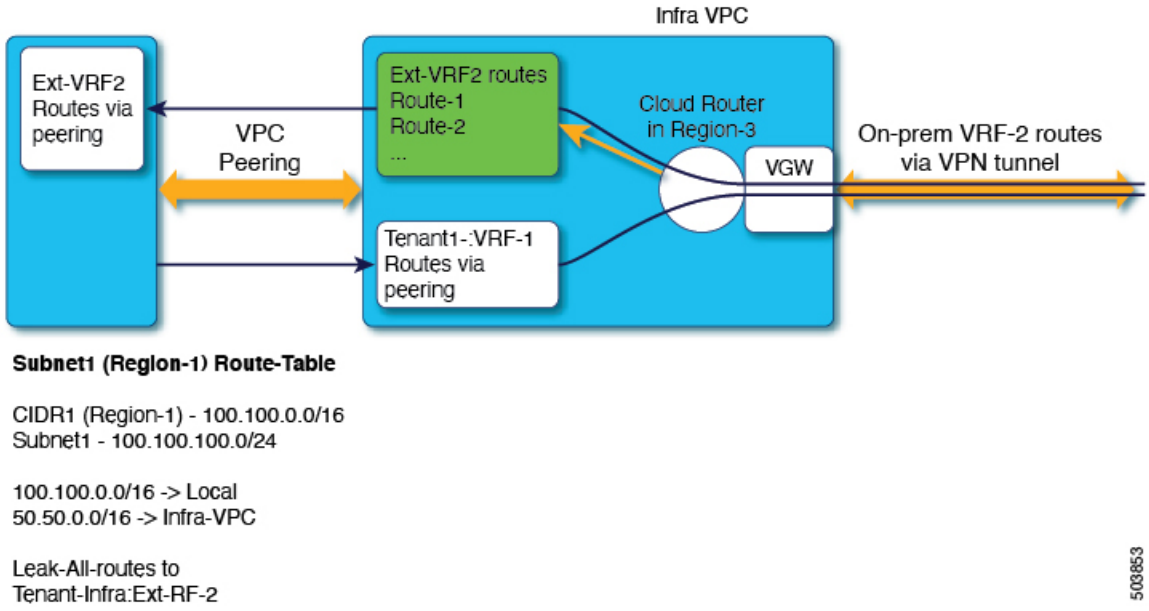
```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="infra">
    <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
    </cloudAccount>
    <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
    </cloudAccount>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

ステップ 3 ユーザーが複数の Google Cloud プロジェクトでインフラサービス アカウントを共有する管理対象ユーザー テナントを作成するには、次の手順を実行します。

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="infra">
    <cloudAccount id="project1" vendor="gcp" accessType="managed" />
    <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="managed" />
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

REST API を使用して VRF 間のルート リークの構成

この例では、REST API を使用した Cloud APIC のリーク ルートを構成する方法を示します。この例では、次の図に示すように、外部 VRF とクラウド VRF 間の VRF 間ルート リークを設定する方法を示します。



この例では、VRF 間ルート リークを設定します。

例：

```
<polUni>
    <fvTenant name="t1">
        <fvCtx name="VRF1">
            <leakRoutes>
                <leakInternalPrefix ip="0.0.0.0/0" status="">
                    <leakTo tenantName="infra" ctxName="Ext-VRF2" scope="public" status=""/>
                </leakInternalPrefix>
            </leakRoutes>
        </fvCtx>
        <cloudCtxProfile name="v1-us-west1" type="regular" vpcGroup="one" status="">
            <cloudRsToCtx tnFvCtxName="VRF1"/>
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
            <cloudCidr addr="100.100.0.0/16" primary="yes">
                <cloudSubnet ip="100.100.100.0/20" scope="public,shared" subnetGroup="one">
                   <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>

                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
    <fvTenant name="infra" status="">
        <fvCtx name="Ext-VRF2">
            <leakRoutes>
                <leakExternalPrefix ip="0.0.0.0/0" status="">
                    <leakTo tenantName="t1" ctxName="VRF1" scope="public" status=""/>
```

```
            </leakInternalPrefix>
          </leakRoutes>
        </fvCtx>
    </fvTenant>
</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：

```
<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>
```

コントラクトの名前（`vzBrCP` エントリ）には次の制限があることに注意してください。

- 正規表現の一致:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。

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="cProfilewest1151">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
      <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-gcp/region-us-west1/zone-default"/>
```

```
        </cloudSubnet>
        <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
          <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/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-gcp/region-us-central1" 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-gcp/region-us-central1/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-gcp/region-us-central1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </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-[<gcp-id>]-vendor-gcp" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">

    </cloudApp>

  </fvTenant>
</polUni>
```

アプリケーション プロファイル名については、次の制約事項に注意してください。

- 正規表現の一致:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。

REST API を使用した EPG の作成

REST API を使用してアプリケーション EPG または外部 EPG を作成するには、このセクションの手順を使用します。

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。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
```

```
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<gcp-id>]-vendor-gcp" />


        <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>
```

次の制約事項に注意してください。

- 正規表現の一致:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。

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。

外部 EPG の名前については、次の制約事項に注意してください。

- 正規表現の一致:

  ```
  [a-z]([-a-z0-9]*[a-z0-9])?
  ```

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 （31 ページ） を参照してください。

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-[<gcp-id>]-vendor-gcp" />
        <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** の外部クラウド EPG、またはインフラ L3Out 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="infra">
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="site-ext" name="extEpg-1">
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="ctx152"/>
            <cloudExtEPSelector name="extSelector1" subnet="10.100.0.0/16"/>
       </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

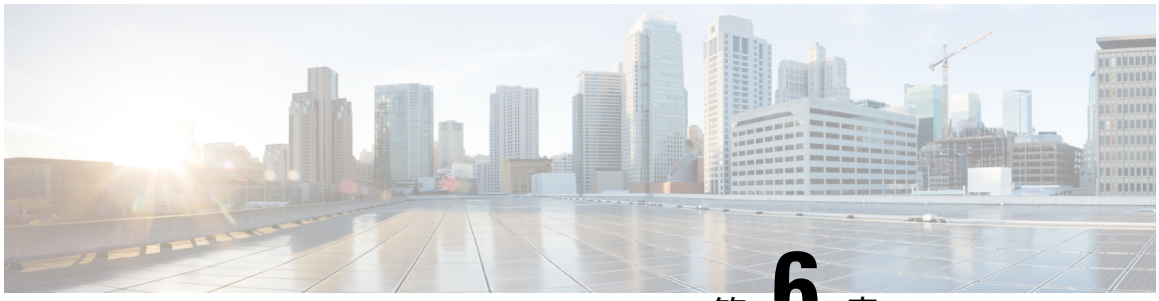
REST API を使用したクラウド ルータ、外部ネットワーク、および外部 VRF の作成

このセクションでは、REST API を使用してクラウド ルータ、外部ネットワーク、および外部 VRF を作成する方法を示します。

次の POST の例では、4 つのリージョンでクラウド ルータを起動し、各リージョンで外部 VRF を使用して外部ネットワークを追加する方法を示します。

```
<polUni>
    <fvTenant name="infra" status="">
        <fvCtx name="extv1" pcEnfPref="enforced" status=""/>
         <fvCtx name="extv2" pcEnfPref="enforced" status=""/>
          <fvCtx name="extv3" pcEnfPref="enforced" status=""/>

           <cloudtemplateInfraNetwork name="default" vrfName="overlay-1" hostRouterMode="manual"
status="">
            <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.7.0/24" poolname="pool1" />
             <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.8.0/24" poolname="pool2" />
              <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.10.0/24" poolname="pool3" />


            <cloudtemplateHubNetwork name="default" status="" >
                <cloudtemplateHubNetworkName name="foo1" asn="64514" status="">
                    <cloudRegionName provider="gcp" region="us-west4" status="" />
                    <cloudRegionName provider="gcp" region="us-west2" status="" />
                    <cloudRegionName provider="gcp" region="us-east1" status="" />
                      <cloudRegionName provider="gcp" region="us-west1" status=""/>
                </cloudtemplateHubNetworkName>
            </cloudtemplateHubNetwork>

            <cloudtemplateIntNetwork name="default">
                <cloudRegionName provider="gcp" region="us-west1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-west2">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-east1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                  </cloudRegionName>
                    <cloudRegionName provider="gcp" region="us-west4">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
            </cloudtemplateIntNetwork>

            <cloudtemplateExtNetwork name="default">
         </cloudtemplateExtNetwork>
                <cloudtemplateExtNetwork name="extnwfoo1" vrfName="extv1" hubNetworkName="foo1"
vpnRouterName="default" status="">
                    <cloudRegionName provider="gcp" region="us-west1" status=""/>
                       <cloudtemplateVpnNetwork name="onprem01" remoteSiteId="1" status="">
                 <cloudtemplateIpSecTunnel peeraddr="128.1.1.1" preSharedKey="abcd" poolname="pool1"
 status="">
                      <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
            <cloudtemplateExtNetwork name="extnwfoo2" vrfName="extv2" hubNetworkName="foo1"
vpnRouterName="default" status="">
             <cloudRegionName provider="gcp" region="us-west2" status=""/>
                <cloudtemplateVpnNetwork name="onprem02" remoteSiteId="2" status="">
                       <cloudtemplateIpSecTunnel peeraddr="128.1.1.2" preSharedKey="def"
poolname="pool2" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
             <cloudtemplateExtNetwork name="extnwfoo3" vrfName="extv3" hubNetworkName="foo1"
vpnRouterName="default" status="">
                <cloudRegionName provider="gcp" region="us-east1" status=""/>
                   <cloudtemplateVpnNetwork name="onprem03" remoteSiteId="3" status="">
```

```
                        <cloudtemplateIpSecTunnel peeraddr="128.1.1.3" preSharedKey="abc"
poolname="pool3" status="">
                         <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                      </cloudtemplateIpSecTunnel>
                  </cloudtemplateVpnNetwork>
                    </cloudtemplateExtNetwork>
        </cloudtemplateInfraNetwork>
    </fvTenant>
</polUni>
```



第 6 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 APIC が導入されている 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 APIC 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

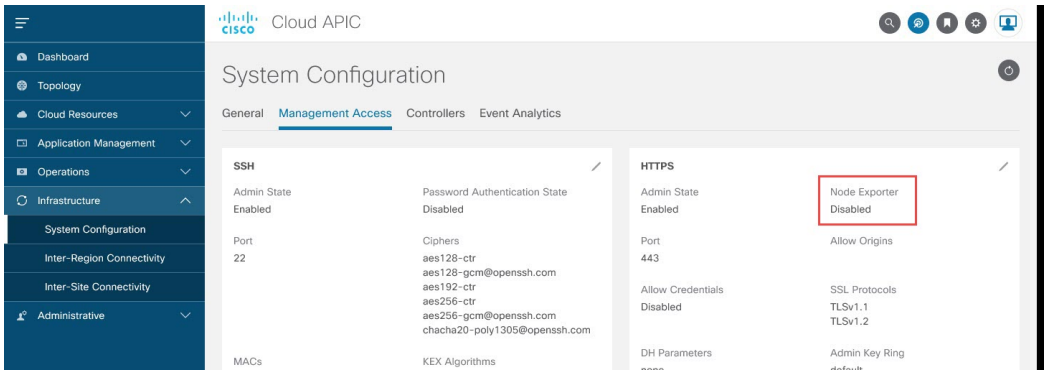
HTTP は、Prometheus Node Exporter を使用したモニタリング メトリックではサポートされていません。Prometheus Node Exporter を使用したメトリックのモニタリングでは、HTTPS のみがサポートされます。

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 APIC 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。

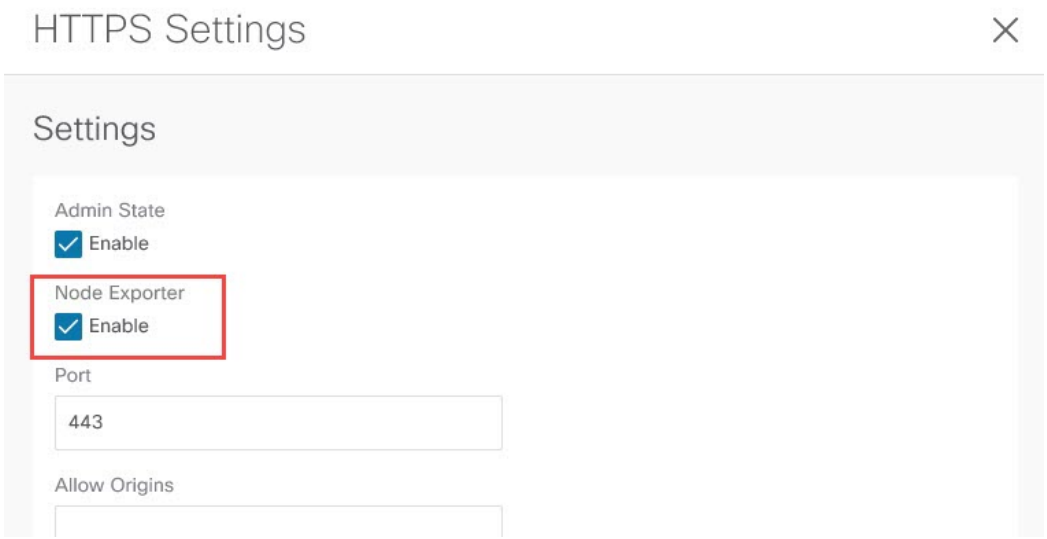


- **有効化（Enabled）**：Prometheus Node Exporter はすでに有効になっています。この場合、これらの手順を続行する必要はありません。
- **無効化（Disabled）**：Prometheus Node Exporter はまだ有効になっていません。Prometheus Node Exporter を有効にするには、次の手順に従います。

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。



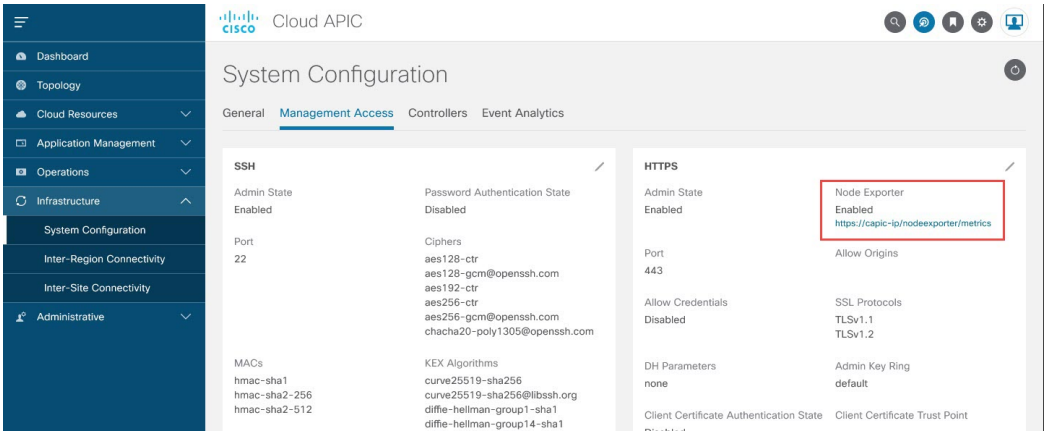
これらの設定を保存すると Web サービスが再起動され、要求への応答が再開されるまで少し時間がかかることを示す警告メッセージが表示されます。**[OK]** をクリックして、変更内容を確定します。

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 APIC 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-apic-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-apic-ip-address>/api/mo/uni/fabric/comm-default/https.xml
```

```
<commHttps nodeExporter="enabled" />
```

Cisco Cloud APIC が展開されている VM ホストのメトリックが表示されます。

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-apic-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-apic-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、クラウド コンテキスト プロファイル、または外部ネットワーク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 *25* : 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。

サブタブ名	説明
VRF	サマリー テーブルの行として VRF を表示します。
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。
外部ネットワーク	サマリーテーブルの行として外部ネットワークを表示します。

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。

サマリーテーブルには、項目が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。

*[*属性でフィルタ（*Filter by Attributes*）*]* バーをクリックすると、行をフィルタリングできます。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 ペインを表示するには、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。

次のいずれかのタブを含む新しいダイアログボックスが**作業**ウィンドウに表示されます。

（注） 表示されるタブは、コンポーネントと設定によって異なります。

- **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（Cloud Resources）**：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が含まれます。
- **アプリケーション管理（Application Management）**：コンポーネントに関連する ACI 関係情報を表示するサブタブのリストが含まれます。
- **イベント分析**：障害、イベント、および監査ログを表示するサブタブのリストが含まれます。

（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、VPC、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。

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 *26 :* 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。
VPC	サマリー テーブルの行としてVPC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。
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。
Instances	インスタンスをサマリー 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）]**：エンドポイントに関連付けられたクラウドタグを含む、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提供します。
- **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。
- **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 27 : [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。

サブタブ名	説明

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 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。

[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。

サブタブ名	説明
Firmware Management	次のサブタブを含みます。 • **[コントローラ（Controllers）]** 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 *28*：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	**一般的な**システム設定情報、**管理アクセス**情報、**コントローラ**、および**イベント分析**を表示します。
外部接続	リージョン間接続ビューを含むマップを 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 *29* : 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。 • **[CSR]** タブ：CSR 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）。

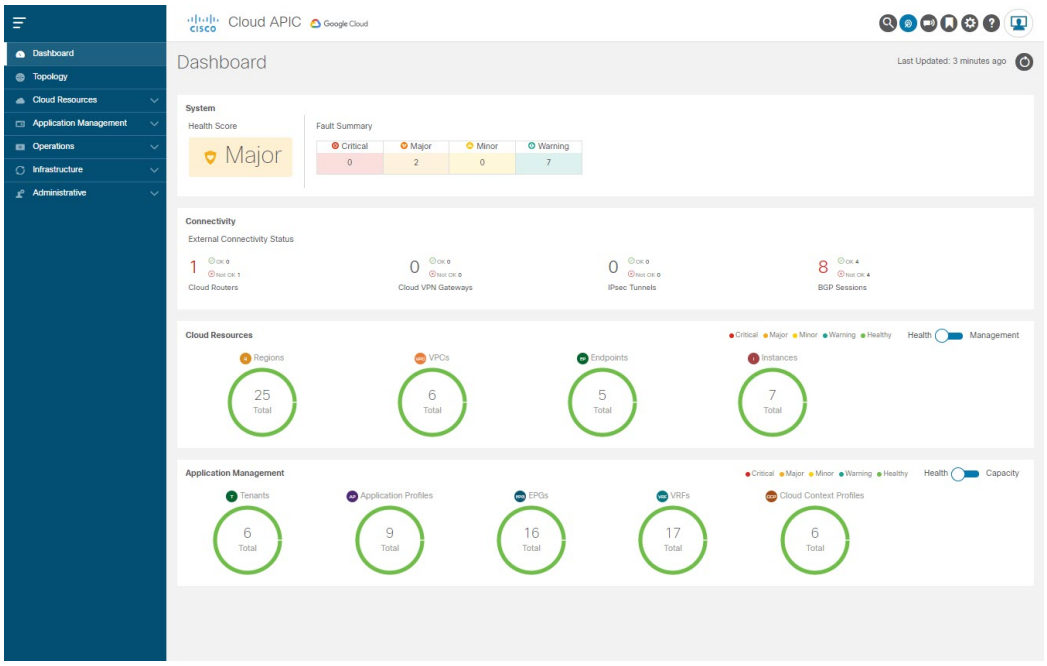
Cisco Cloud APIC GUI を使用したヘルスの詳細の表示

ここでは、Cisco Cloud APIC GUI を使用してヘルス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]
- VPC
- エンドポイント
- Instances

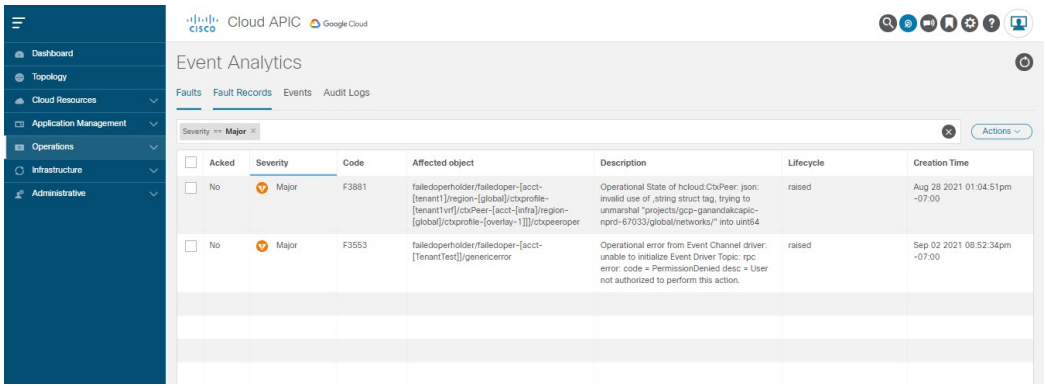
ステップ 1 **[ナビゲーション（Navigation）]** メニューから **[ダッシュボード（Dashboard）]** タブを選択します。

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。



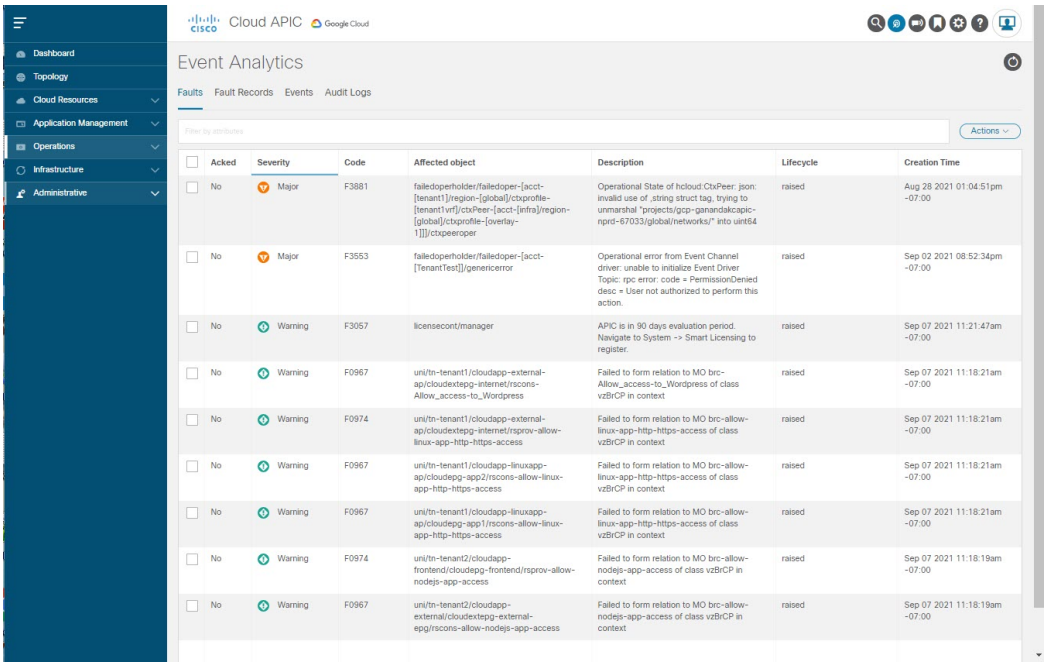
ステップ 2 **[ダッシュボード（Dashboard）]** ウィンドウの [障害サマリー] 領域内をクリックします。

[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。

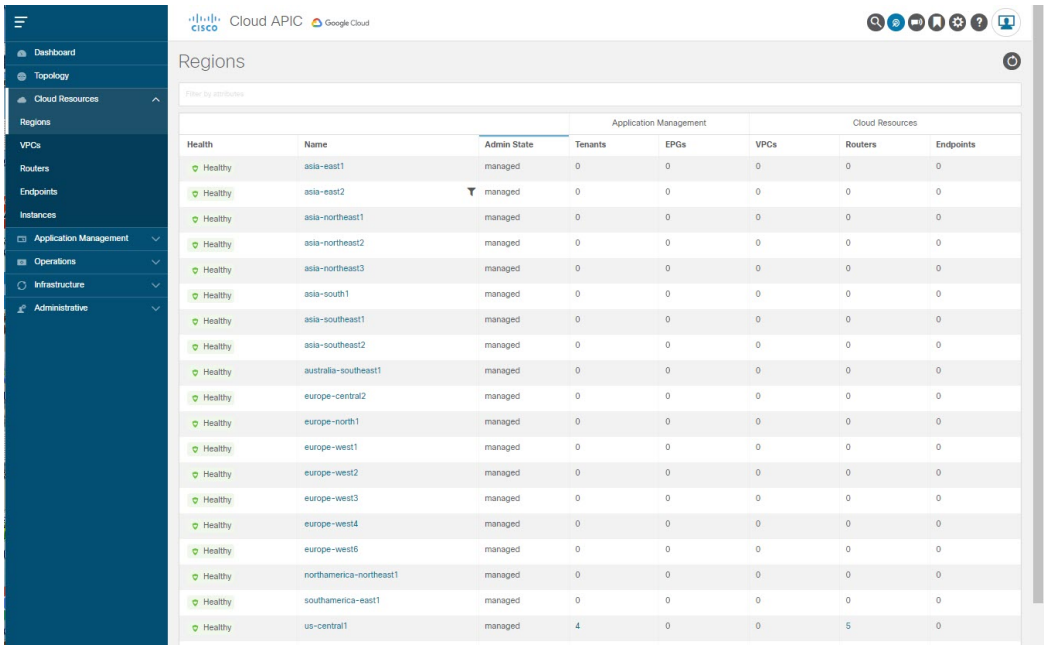


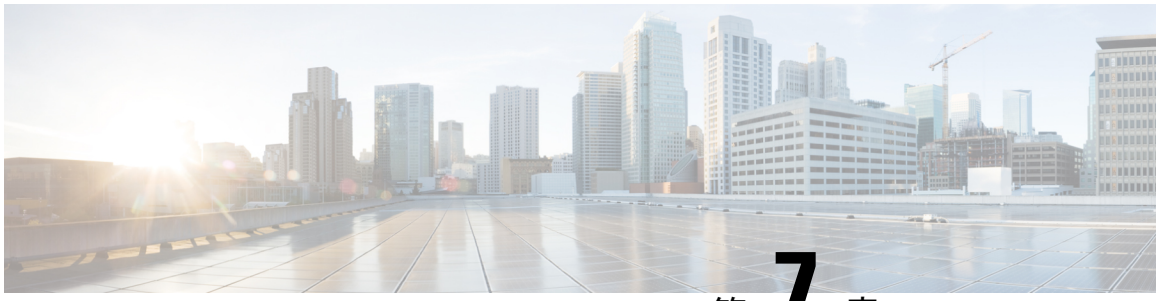
ステップ 4 **[ナビゲーション（Navigation）]** メニューから **[クラウド リソース（Cloud Resources）]** タブを選択します。

[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ます。 各リージョンのヘルスは、**[リージョン（Regions）]** ウィンドウのテーブルの左側の列に表示されます。


Cloud APIC
Google Cloud
Dashboard
Topology
Cloud Resources
Regions
VPCs
Routers
Endpoints
Instances
Application Management
Operations
Infrastructure
Administrative
Regions
Application Management
Cloud Resources
Health
Name
Admin State
Tenants
EPGs
VPCs
Routers
Endpoints
Healthy asia-east1 managed 0 0 0 0 0
Healthy asia-east2 managed 0 0 0 0 0
Healthy asia-northeast1 managed 0 0 0 0 0
Healthy asia-northeast2 managed 0 0 0 0 0
Healthy asia-northeast3 managed 0 0 0 0 0
Healthy asia-south1 managed 0 0 0 0 0
Healthy asia-southeast1 managed 0 0 0 0 0
Healthy asia-southeast2 managed 0 0 0 0 0
Healthy australia-southeast1 managed 0 0 0 0 0
Healthy europe-central2 managed 0 0 0 0 0
Healthy europe-north1 managed 0 0 0 0 0
Healthy europe-west1 managed 0 0 0 0 0
Healthy europe-west2 managed 0 0 0 0 0
Healthy europe-west3 managed 0 0 0 0 0
Healthy europe-west4 managed 0 0 0 0 0
Healthy europe-west6 managed 0 0 0 0 0
Healthy northamerica-northeast1 managed 0 0 0 0 0
Healthy southamerica-east1 managed 0 0 0 0 0
Healthy us-central1 managed 4 0 0 5 0



第 7 章

Cisco Cloud APIC セキュリティ

この章の内容は、次のとおりです。

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ー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。

設定

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 （117 ページ） を参照して、ローカルユーザーを設定し、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

次のトピックでは、Cloud APIC の TACACS+、RADIUS、LDAP、および SAML アクセスを設定する方法について説明します。

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 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）]** と **[キーの確認（Confirm 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) 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。

[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。

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。

Properties	説明
General	
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。
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。

d) [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、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 Cloud 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）]** と **[キーの確認（Confirm 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) 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。

[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。

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。

Properties	**説明**
General	
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。
Settings	
Realm	ドロップダウン メニューから **RADIUS** を選択します。

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。

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
- クラウド APIC での LDAP グループ マップの設定

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。

Cloud APIC for LDAP 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。
- 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。
- 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、**LDAP 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、**[LDAP]** を選択します。

f) バインドDN、ベースDN、パスワード、パスワードの確認、ポート、タイムアウト、再試行、SSL、SSL証明書検証レベル、属性、フィルタタイプ、管理EPG、およびサーバモニタリングを指定します。

[SSL 証明書検証レベル（SSL Certificate Validation Level）] フィールドには、次のオプションがあります。

- **Permissive**：DUO LDAP SSL証明書の問題の診断に役立つデバッグノブ。
- **Strict**：実稼働環境で使用するレベル。

（注）
- バインド DN は、Cloud APIC が LDAP サーバーにログインするために使用する文字列です。Cloud APIC 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、Cloud APIC がリモートユーザーアカウントを検索する LDAP サーバー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、Cloud APIC 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、Cloud APIC 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。Cloud APIC 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。

Properties	**説明**
General	
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。
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。

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. **[セキュリティ ドメインの選択（Select Security Domain）]** オプションを使用してセキュリティ ドメインを選択します。 5. [+] 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。 6. 必要に応じて、前の手順を繰り返してさらにロールを追加します。次に、[追加（Add）] をクリックします。 7. セキュリティ ドメインをさらに追加する場合は、**[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、それらの手順を再度実行します。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。

SAML Access 用の APIC の設定

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。

- **[IDプロバイダー（Identity Provider）]** オプション（**[ADFS]**、**[OKTA]**、または **[PING IDENTITY]**）を選択します。
- 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、場合に、IdP メタデータの URL を取得するには、Okta サーバーから対応する SAML アプリケーションの **[サインオン]** セクションで、**アイデンティティ プロバイダー メタデータ URL** 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。
- **[GUI リダイレクト バナー メッセージ（GUI Redirect Banner Message（URL））]** フィールドに値を入力します。
- 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。
- **[再試行時間（秒）（Retry Period (sec)）]** フィールドに値を入力します。
- **[再試行回数（Retries）]** フィールドに値を入力します。
- 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。

Properties	説明
General	

Properties	説明
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。
Settings	
Realm	ドロップダウン メニューから **SAML** 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、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ます。 2. 左側の列でプロバイダーをクリックして選択します。 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 Cloud ACIC HTTPS Access 用カスタム証明書の構成

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（Cloud 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。

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。