



Google Cloud ユーザー ガイド向け Cisco Cloud Network Controller、リリース 25.0(5)

初版：2022 年 8 月 15 日

最終更新：2023 年 1 月 24 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



Trademarks

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

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at:

<http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at

<http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here

<http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

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

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

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

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

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



目次

はじめに :	Trademarks iii
--------	-----------------------

第 1 章	新機能と変更情報 1
	新規および変更情報 1

第 2 章	Cisco Cloud Network Controller について 3
	概要 3
	注意事項と制約事項 4
	Cisco Cloud Network Controller GUI について 4

第 3 章	Cisco Cloud Network Controller および Google Cloud について 7
	重要な Google Cloud プロジェクト情報の検索 7
	Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する 8
	クラウドネイティブ ルータを使用した外部ネットワーク接続 10
	BGP-EVPN を使用したサイト間接続 15
	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 17
	ルーティング ポリシーの設定 18
	セキュリティ ポリシーの設定 19
	GCP の VPC とサブネット、Google Cloud および Cisco Cloud Network Controller のクラウド コンテキスト プロファイルの理解 23
	Google Cloud を持つ Cisco Cloud Network Controller を構成する場合の注意事項と制限事項 27

第 4 章	Cisco Cloud Network Controller ポリシー モデル 31
	ACI ポリシー モデルの概要 31

ポリシー モデルの主な特性	31
論理コンストラクト	32
Cisco ACI ポリシー管理情報モデル	33
テナント	35
クラウド コンテキスト プロファイル	36
VRF	37
クラウド アプリケーション プロファイル	38
クラウド エンドポイント グループ	39
コントラクト	41
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	42
クラウド テンプレートの概要	44
管理対象オブジェクトの関係とポリシー解決	47
デフォルト ポリシー	48

第 5 章

Cisco Cloud Network Controller コンポーネントの構成	51
Cisco Cloud Network Controller の設定について	51
GUI を使用した Cisco Cloud Cisco Network Controller の構成	51
テナントの作成	51
ユーザー テナントの Google Cloud プロジェクトのセットアップ	51
管理対象テナントの作成	54
アンマネージド テナントの作成	57
Cisco Cloud Network Controller GUI を使用したアプリケーション プロファイルの作成	60
Cisco Cloud Network Controller GUI を使用した VRF の作成	61
Cisco Cloud Network Controller GUI を使用したクラウド ネイティブ ルータによる外部ネットワークの作成	64
BGP-EVPN を使用したサイト間ネットワークの構成	68
Cisco Cloud Network Controller GUI を使用した VRF 間ルート リークの構成	72
Google Cloud と外部デバイス間の接続の有効化	75
外部デバイス構成ファイルのダウンロード	75
Google Cloud と外部デバイス間の接続の有効化	76
Cisco Cloud Network Controller GUI を使用した EPG の作成	80

Cisco Cloud Network Controller GUI を使用したアプリケーション EPG の作成	80
Cisco Cloud Network Controller GUI を使用した外部 EPG の作成	86
Cisco Cloud Network Controller GUI を使用したフィルタの作成	90
Cisco Cloud Network Controller GUI を使用したコントラクトの作成	92
Cisco Cloud Network Controller GUI を使用したテナント間契約の作成	94
Cisco Cloud Network Controller を使用したコンシューマおよびプロバイダー EPG の指定	98
Cisco Cloud Network Controller GUI を使用したクラウド コンテキスト プロファイルの作成	99
Google Cloud の仮想マシン セキュリティの設定	103
Cisco Cloud Network Controller GUI を使用したバックアップ構成の作成	104
Cisco Cloud Network Controller GUI を使用したテクニカル サポート ポリシーの作成	109
Cisco Cloud Network Controller GUI を使用したスケジューラの作成	110
Cisco Cloud Network Controller GUI を使用してリモートの場所を作成する	114
Cisco Cloud Network Controller GUI を使用したログイン ドメインの作成	116
Cisco Cloud Network Controller GUI を使用したセキュリティ ドメインの作成	120
Cisco Cloud Network Controller GUI を使用したロールの作成	121
Cisco Cloud Network Controller GUI を使用した認証局の作成	124
Cisco Cloud Network Controller GUI を使用したキー リングの作成	126
Cisco Cloud Network Controller GUI を使用したローカル ユーザーの作成	128
Cisco Cloud Network Controller GUI を使用したリージョンの管理 (クラウド テンプレートの構成)	133
REST API を使用した Cisco Cloud Network Controller の構成	135
REST API を使用したテナントの作成	135
REST API を使用して VRF 間のルート リークの構成	137
REST API を使用したフィルタの作成	138
REST API を使用したコントラクトの作成	138
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	139
REST API を使用したアプリケーション プロファイルの作成	140
REST API を使用した EPG の作成	141
REST API を使用したクラウド EPG の作成	141
REST API を使用した外部クラウド EPG の作成	142

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 143

第 6 章

システムの詳細の表示 147

VM ホスト メトリックのモニタリング 147

GUI を使用した VM ホストメトリックのモニタリング 147

REST API を使用した VM ホストメトリックスの監視 149

アプリケーション管理詳細の表示 150

クラウドリソースの詳細の表示 152

操作の詳細の表示 153

インフラストラクチャの詳細の表示 156

管理の詳細の表示 156

Cisco Cloud Network Controller GUI を使用したヘルス詳細の表示 159

第 7 章

Cisco Cloud Network Controller 統計情報 163

Google Cloud 統計について 163

Guidelines and Limitations For Configuring Google Cloud Statistics 164

Viewing Router Statistics 164

Enabling Flow Log Statistics 167

フロー ログ統計の表示 168

REST API を使用した VPC フロー ログの有効化 170

第 8 章

Cisco Cloud Network Controller のセキュリティ 173

アクセス、認証、およびアカウントティング 173

設定 173

TACACS+、RADIUS、LDAP、および SAML アクセスの構成 174

概要 174

TACACS+ アクセス用の Cisco Cloud Network Controller の構成 174

RADIUS アクセス用の Cisco Cloud Network Controller の構成 176

Cisco Cloud Network Controller への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の構成 177

LDAP Access の構成 178

Cisco AVPair を使用した APIC アクセス用の Windows Server 2008 LDAP の設定	178
LDAP アクセスのための Cisco Cloud Network Controller の構成	178
SAML アクセス用の Cisco Cloud Network Controller の構成	180
SAML について	181
SAML アクセス用の Cisco Cloud Network Controller の構成	181
Okta で SAML アプリケーションの設定	183
AD FS で Relying Party Trust の設定	183
HTTPS Access の構成	183
HTTPSアクセスについて	183
カスタム証明書の構成のガイドライン	184
GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定	184



第 1 章

新機能と変更情報

この章は、次の項で構成されています。

- [新規および変更情報 \(1 ページ\)](#)

新規および変更情報

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

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

機能または変更	説明	参照先
Cisco Cloud APIC の名称変更	リリース 25.0(5) 以降、Cisco Cloud APIC は Cisco Cloud Network Controller に名前が変更されました。	ドキュメント全体



第 2 章

Cisco Cloud Network Controller について

- [概要 \(3 ページ\)](#)
- [注意事項と制約事項 \(4 ページ\)](#)
- [Cisco Cloud Network Controller GUI について \(4 ページ\)](#)

概要

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

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

Cisco Cloud Network Controller とは

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

- 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。
- クラウド接続の展開と設定を自動化します。
- クラウドルータコントロールプレーンを設定します。
- Cisco ACI ポリシーをクラウドネイティブポリシーに変換します。
- エンドポイントを検出します。

注意事項と制約事項

ここでは、Cisco Cloud Network Controller 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 Network Controller 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 Network Controller 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 Network Controller 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 Network Controller GUI について

Cisco Cloud Network Controller 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。

Cisco Cloud Network Controller コンポーネントの構成の詳細については、[Cisco Cloud Network Controller コンポーネントの構成 \(51 ページ\)](#) を参照してください。



第 3 章

Cisco Cloud Network Controller および Google Cloud について

この章の次のトピックでは、Cisco Cloud Network Controller 展開がどのように Google Cloud で動作するかの詳細を説明します。

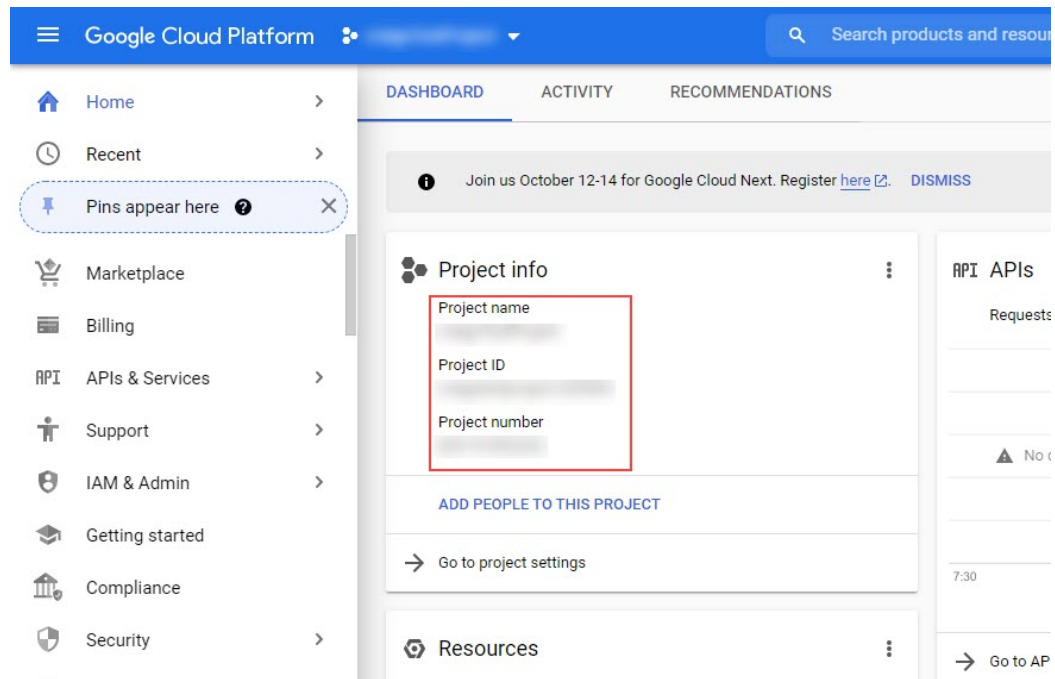
- [重要な Google Cloud プロジェクト情報の検索 \(7 ページ\)](#)
- [Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する \(8 ページ\)](#)
- [クラウド ネイティブ ルータを使用した外部ネットワーク接続 \(10 ページ\)](#)
- [BGP-EVPN を使用したサイト間接続 \(15 ページ\)](#)
- [ルーティング ポリシーとセキュリティ ポリシーの個別の構成 \(17 ページ\)](#)
- [GCP の VPC とサブネット、Google Cloud および Cisco Cloud Network Controller のクラウド コンテキスト プロファイルの理解 \(23 ページ\)](#)
- [Google Cloud を持つ Cisco Cloud Network Controller を構成する場合の注意事項と制限事項 \(27 ページ\)](#)

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 Network Controller の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。



Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する

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。

Google Cloud の観点から理解するのに有用な領域は、組織とフォルダのレベルですが、Cisco Cloud Network Controller の観点から最も関連性があるのは、プロジェクトのレベルです。

各 Cisco Cloud Network Controller 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。

- Cisco Cloud Network Controller 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 プロジェクト内に複数の Cisco Cloud Network Controller テナントを存在させることはできません。

Cisco Cloud Network Controller 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、Cisco Cloud Network Controller と他のテナントのポリシーを実行、展開し、また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クレデンシャル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クレデンシャルが必要です。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（Cisco Cloud Network Controller 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 Cisco Cloud Network Controller テナントを構成するさまざまな方法について詳しく説明します。

- [管理対象クレデンシャルを持つユーザ テナント](#) (9 ページ)
- [管理対象外クレデンシャルを持つユーザ テナント](#) (9 ページ)

管理対象クレデンシャルを持つユーザ テナント

このタイプのユーザ 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 Network Controller によって管理されます。
- このタイプのユーザ 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 Network Controller GUI で **[マネージド ID (Managed Identity)]** を選択します。
- Cisco Cloud Network Controller 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。Cisco Cloud Network Controller 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 ネットワーク管理者
 - コンピューティング セキュリティ管理者
 - 管理者のログイン
 - パブ/サブ管理者
 - 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、[Cisco Cloud Network Controller GUI を使用した管理対象テナントの作成](#) (54 ページ) を参照してください。

管理対象外クレデンシャルを持つユーザ テナント

このタイプのユーザ 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 Network Controller によって管理されていません。

- このタイプのテナントの Cisco Cloud Network Controller 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。
- 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 Network Controller GUIで[アンマネージド ID (Unmanaged Identity)]を選択します。Cisco Cloud Network Controller 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 プライベート キー
 - クライアントID
 - E メール

このようなテナントの作成手順については、[Cisco Cloud Network Controller GUI を使用したアンマネージドテナントの作成 \(58 ページ\)](#) を参照してください。

クラウドネイティブルータを使用した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、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 \(10 ページ\)](#)
- [クラウドネイティブルータ \(11 ページ\)](#)
- [VPN 通信 \(11 ページ\)](#)
- [ハブ ネットワーク構成 \(12 ページ\)](#)

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 Network Controller 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 にルートを一括したり、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

Google Cloud を使用して Cisco Cloud Network Controller を構成すると、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 Network Controller 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 Network Controller 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

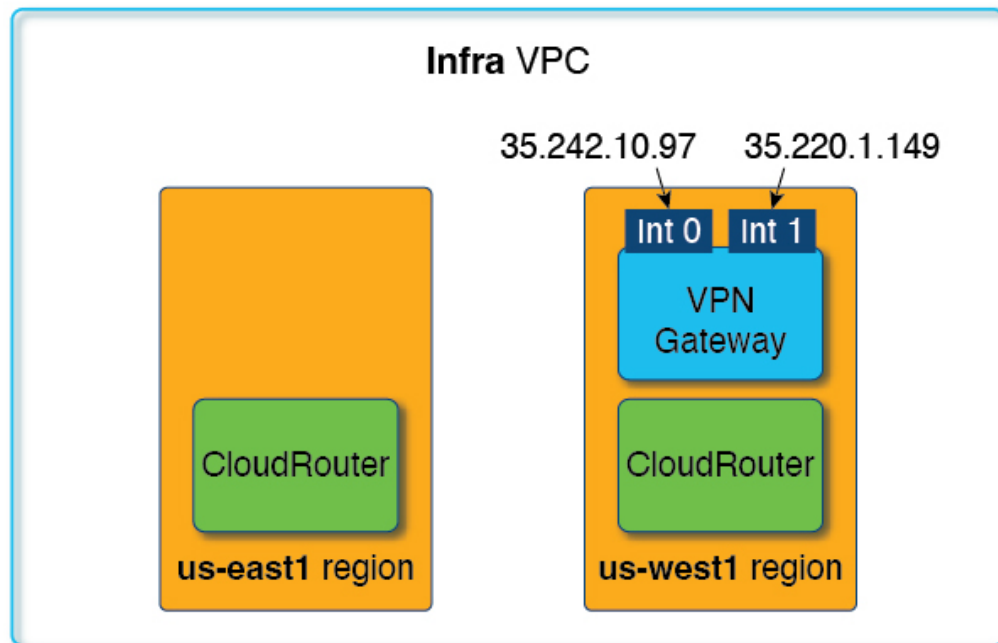
Cisco Cloud Network Controller を Google Cloud で構成する場合、インフラ VPC を使用して Cisco Cloud Network Controller をホストし、外部デバイスおよびサイトへの VPN 接続をホストします。ただし、インフラ VPC は、スポーク間通信を実装するための中継として使用されません。代わりに、Cisco Cloud Network Controller を Google Cloud を使用して構成すると、スポーク間通信はスポーク間 VPC ピアリングによって行われます。

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 Network Controller 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

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。Cisco Cloud Network Controller には、cloudtemplateHubNetworkName が 1 つだけという制限があります。

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。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。例えば、us-central1 および us-east1 でハブ ネットワークを展開することを選択できます。Cisco Cloud Network Controller は、これらのリージョンに 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 Network Controller 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。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。

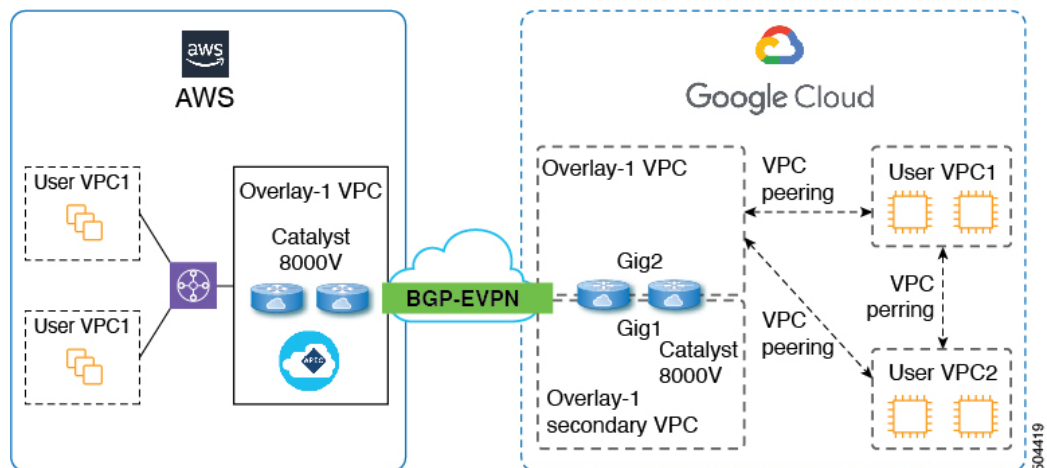
- 外部デバイスへの ikev1 と ikev2 の両方。
- 複数の cloudtemplateIpSecTunnelSubnetPool サブネットプール。
cloudtemplateIpSecTunnelSubnetPool サブネットプールで許可される IP 範囲は、クラウドプロバイダーと使用例によって異なります。たとえば、169.254.0.0 / 16 以下のサブネットが Google Cloud VPN 接続でサポートされます。

BGP-EVPN を使用したサイト間接続

リリース 25.0(5)以降、サイト間ユースケースでは、次のシナリオでサイト間接続用の BGP-EVPN 接続を構成するためのサポートも利用できます。

- クラウド サイト間サイト :
 - Google Cloud サイト ~ Google Cloud サイト
 - Google Cloud サイトから AWS サイトへ
 - Google Cloud サイトから Azure サイトへ
- Google Cloud サイトから ACI オンプレミス サイト

これらの各シナリオでは、BGP-EVPN 接続に Cisco Catalyst 8000V が使用されます。



次のセクションでは、BGP-EVPN を使用したサイト間接続を可能にするコンポーネントについて詳しく説明します。

- [BGP-EVPN を使用したサイト間接続の特性 \(15 ページ\)](#)
- [VPC ピアリング \(16 ページ\)](#)

BGP-EVPN を使用したサイト間接続の特性

Google Cloud 動作に基づいて、VM またはインスタンスの各ネットワーク インターフェイスは、異なる VPC に関連付ける必要があります。Cisco Catalyst 8000V も VM であるため、これは、特定の Cisco Catalyst 8000V の各ネットワーク インターフェイスを異なる VPC に関連付ける必要があることを意味します。したがって、Cisco Catalyst 8000V の 2 つのギガビット ネットワーク インターフェイスは、次のように使用されます。

- gig1 インターフェイスは、overlay-1 セカンダリ VPC に関連付けられています。また、gig1 インターフェイスは管理インターフェイスとして使用されます。

- gig2 インターフェイスは、overlay-1 VPC に関連付けられています。また、ルーティング インターフェイスとして gig2 インターフェイスを使用しています。

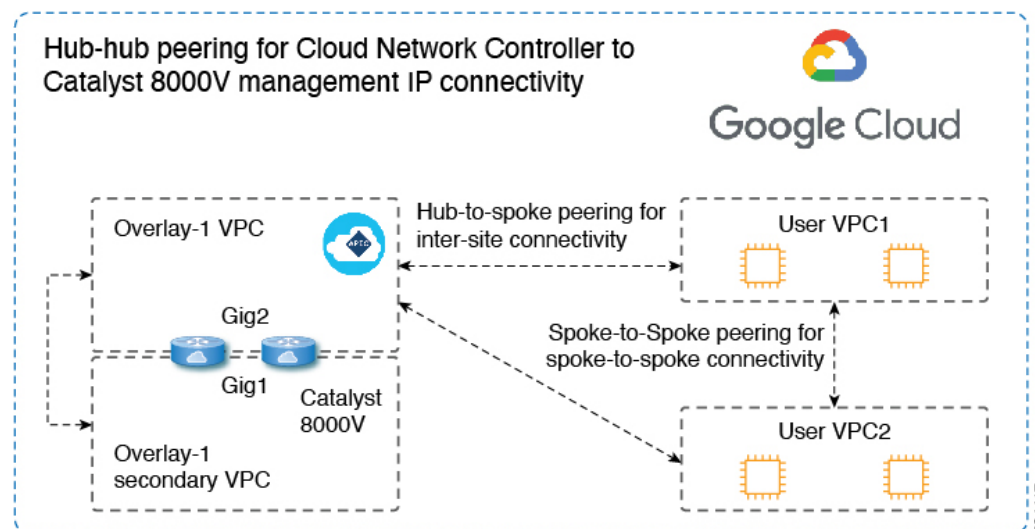
VPC ピアリング

スポーク VPC からオンプレミス ネットワーク への通信を行うには、スポーク VPC でハブ VPC へのピアリングが有効になっている必要があります。ピアリングは、Cisco Cloud Network Controller からのインテントによって自動化されます。次の図に示すように、Google Cloud を使用する Cisco Cloud Network Controller の VPC ピアリングはハブスポーク トポロジを採用しています。

Google Cloud を使用する Cisco Cloud Network Controller は、次の 3 種類の VPC ピアリングを使用します。

- スポーク間 VPC ピアリング：これは、スポーク間のサイト内通信に使用されます。
- ハブツースポーク VPC ピアリング：これは、BGP-EVPN を使用して Cisco Catalyst 8000V ルーターを経由するサイト間通信に使用されます。
- ハブツーハブ VPC ピアリング：これは、overlay-1 VPC の Cisco Cloud Network Controller と overlay-1 セカンダリ VPC の Cisco Catalyst 8000V ルーター管理インターフェイスとの通信に使用されます。

オーバーレイ 1 セカンダリ VPC は、スポーク間またはサイト間トラフィックのデータパスに 関与しないことに注意してください。

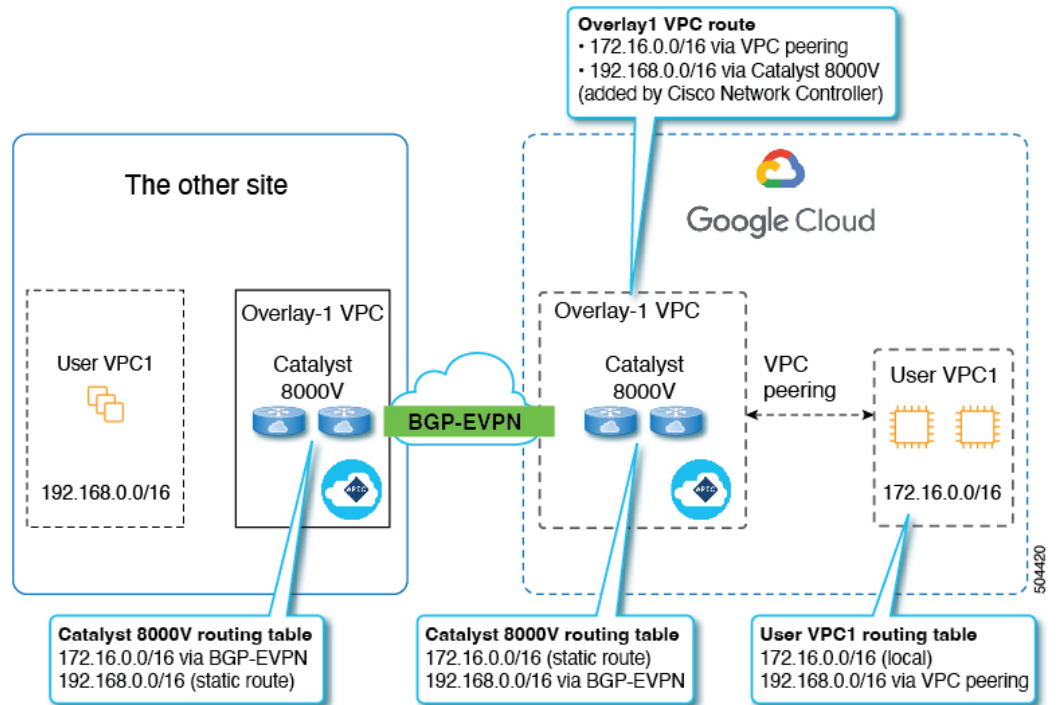


Cisco Cloud Network Controller は、次の状況でクラウド サイト間でルートを交換するための構成を自動化します。

- 同じサイト内の接続先へのオーバーレイ 1 VPC：オーバーレイ 1 VPC には、VPC ピアリングを介した同じサイト内のスポーク VPC へのルートがあります。
- 別のサイトの接続先への VPC のスポーク：他のサイトのサブネットのルートは、Cisco Cloud Network Controller によってオーバーレイ 1 VPC に追加され、ルートはスポーク VPC

にエクスポートされます。このようにして、スポーク VPC には、他のサイトの接続先サブネットに到達するためのルートがあります。

- 異なるサイトの Cisco Catalyst 8000V 間：スポーク VPC CIDR の静的ルートは、同じサイトの Cisco Catalyst 8000V ルーターに追加されます。静的ルートは、BGP EVPN を介して他のサイトの Catalyst 8000V ルータに再配布されます。このようにして、Catalyst 8000V には、次の図に示すように、他のサイトの接続先サブネットに到達するためのルートがあります。



このシナリオでは、リモート CIDR への静的ルートがハブ VPC で、ネクストホップが Cisco Catalyst 8000V としてプログラムされています。これらのルートは、ピアリングを使用してスポーク VPC によって学習されます。

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に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 (t_1 と t_2) と 2 つの対応する VRF (v_1 と v_2) があるとします。VRF $t_2:v_2$ のすべてのルートリークエントリ $t_1:v_1$ に対して、VRF $t_1:v_1$ の対応するルートリークエントリ $t_2:v_2$ 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 Network Controller 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）。

Google Cloud による Cisco Cloud Network Controller ファイアウォール ルールの実装方法

次のリストは、Cisco Cloud Network Controller 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 Network Controller 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カールールとネットワーク タグ** : ファイアウォール出カールールは、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カー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カールールには、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 Network Controller は VPC の作成時に、低プライオリティの deny-all 入カールールと出カールールのペアを構成します。その後、Cisco Cloud Network Controller は EPG の優先度の高い契約に従ってトラフィックを開くルールを構成します。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 Network Controller で、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収集です。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 Network Controller 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 : サブネットセクタはエンドポイントセクタのタイプで、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、サブネットセクタをエンドポイントセ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 Network Controller エンドポイントセ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 Network Controller のカスタムエンドポイントセクタは、Google Cloud の VM に割り当てられたラベルを認識します。

Cisco Cloud Network Controller 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クタに一致すると、Cisco Cloud Network Controller 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>
```

次の構成の VPC に 3 つのエンドポイントがあると仮定すると、Cisco Cloud Network Controller は次のネットワーク タグを構成します。Cisco Cloud Network Controller 構成済みネットワーク 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	Cisco Cloud Network Controller で構成さ 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

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	Cisco Cloud Network Controller で構成さ れたネットワーク タグ
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 Network Controller 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 Network Controller 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 タグを構成し、その後で Cisco Cloud Network Controller に適切なエンドポイントセレクタ構成を指定できます。

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 Network Controller 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。

GCP の VPC とサブネット、Google Cloud および Cisco Cloud Network Controller のクラウド コンテキスト プロファイルの理解

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 Network Controller 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 から VPC から Cisco Cloud Network Controller VRF への 1 対 1 のマッピング** : Google Cloud VPC は、Cisco Cloud Network Controller VRF (`fvCtx` オブジェクト) ごとに展開されます。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 Network Controller は Cisco Cloud Network Controller CIDR 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 Network Controller 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 Network Controller 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 Network Controller 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 Network Controller 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 Network Controller 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 Network Controller 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。

1つの Cisco Cloud Network Controller VRF 内で1つの Google Cloud 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 Network Controller 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 Network Controller 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 Network Controller 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。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 グループに一意的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 Network Controller 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/cloudcomp/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 を持つ Cisco Cloud Network Controller を構成する場合の注意事項と制限事項

Google Cloud で Cisco Cloud Network Controller を構成する場合のガイドラインと制限事項は次のとおりです。

- リリース 25.0(5) より前のリリースでは、Google Cloud は契約に基づくルーティングをサポートしていません。詳細については、[BGP-EVPN を使用したサイト間接続 \(15 ページ\)](#) を参照してください。
- 2 つの Google Cloud サイト間の外部接続はサポートされていません。
- 外部 VRF は Cisco Cloud Network Controller のインフラ テナントでのみ構成可能です。
- Cisco Cloud Network Controller のテナント common は、Google Cloud プロジェクトに関連付けることはできません。
- 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
- 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構成するには、外部デバイス構成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 デバイスを手動で構成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。
- リージョンあたり 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 Network Controller 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 Network Controller は、内部ポリシーに次の命名スキームを使用します。

```
{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 Network Controller コンポーネントを構成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 Network Controller 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。

$62 - 4 (\text{ハイフンの数}) - 2 (\text{in または eg 文字数}) = 56 \text{ 文字}$

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 Network Controller ポリシー モデル

- [ACI ポリシー モデルの概要 \(31 ページ\)](#)
- [ポリシー モデルの主な特性 \(31 ページ\)](#)
- [論理コンストラクト \(32 ページ\)](#)
- [Cisco ACI ポリシー管理情報モデル \(33 ページ\)](#)
- [テナント \(35 ページ\)](#)
- [クラウド コンテキスト プロファイル \(36 ページ\)](#)
- [VRF \(37 ページ\)](#)
- [クラウド アプリケーション プロファイル \(38 ページ\)](#)
- [クラウド エンドポイント グループ \(39 ページ\)](#)
- [コントラクト \(41 ページ\)](#)
- [クラウド テンプレートの概要 \(44 ページ\)](#)
- [管理対象オブジェクトの関係とポリシー解決 \(47 ページ\)](#)
- [デフォルト ポリシー \(48 ページ\)](#)

ACI ポリシー モデルの概要

ACI ポリシー モデルにより、アプリケーション要件のポリシーの指定を有効化します。Cisco Cloud Network Controller 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 Network Controller は最初にポリシー モデルにその変更を適用します。このポリシー モデルの変更により、実際の管理対象項目への変更がトリガーされます。この方法を、モデル方式フレームワークといいます。

ポリシー モデルの主な特性

ポリシー モデルの主な特性には次のものがあります。

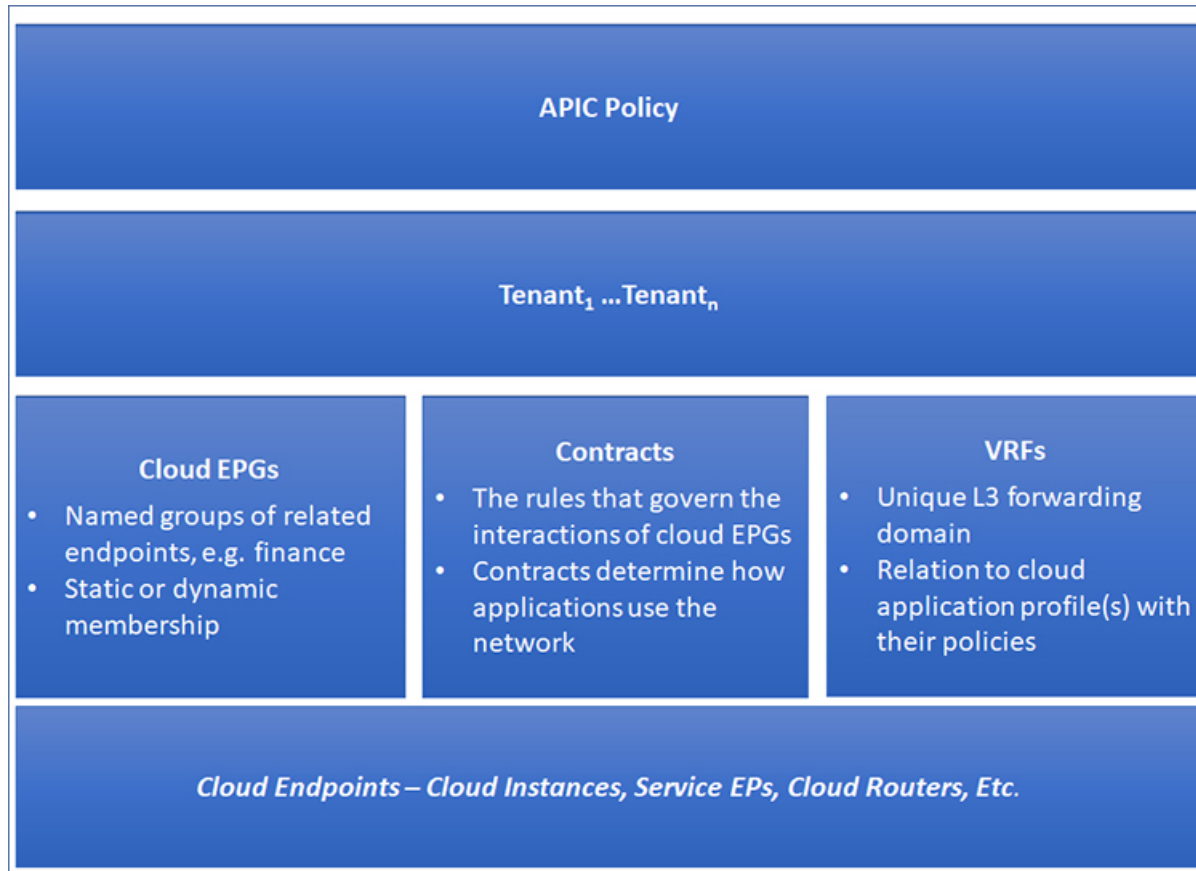
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

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

論理コンストラクト

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 1: 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、ネットワークの動作を誘導する必要があり、その逆ではありません。

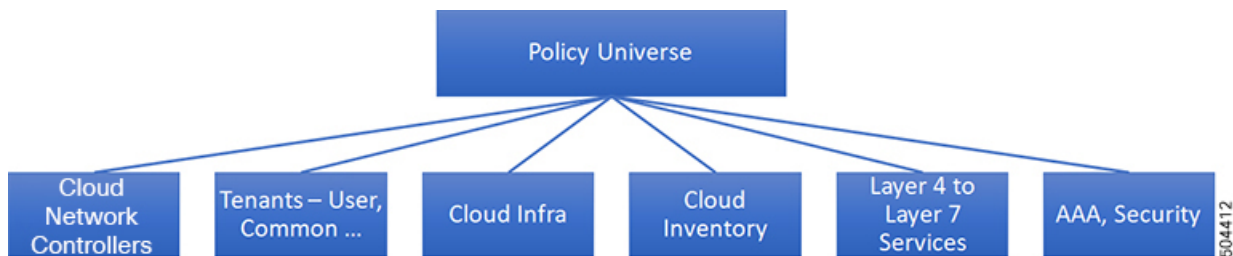
Cisco ACI ポリシー管理情報モデル

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 Network Controller 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 バリエーションと同様に、Cisco Cloud Network Controller 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 2: Cisco ACI ポリシー管理情報モデルの概要



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

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

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



(注) Cisco Cloud Network Controller は、レイヤ4からレイヤ7のサービスとしてロードバランサのみをサポートします。

- 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 Network Controller 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 Network Controller インストールガイド (Cisco Cloud Network Controller Installation Guide)] を参照してください。

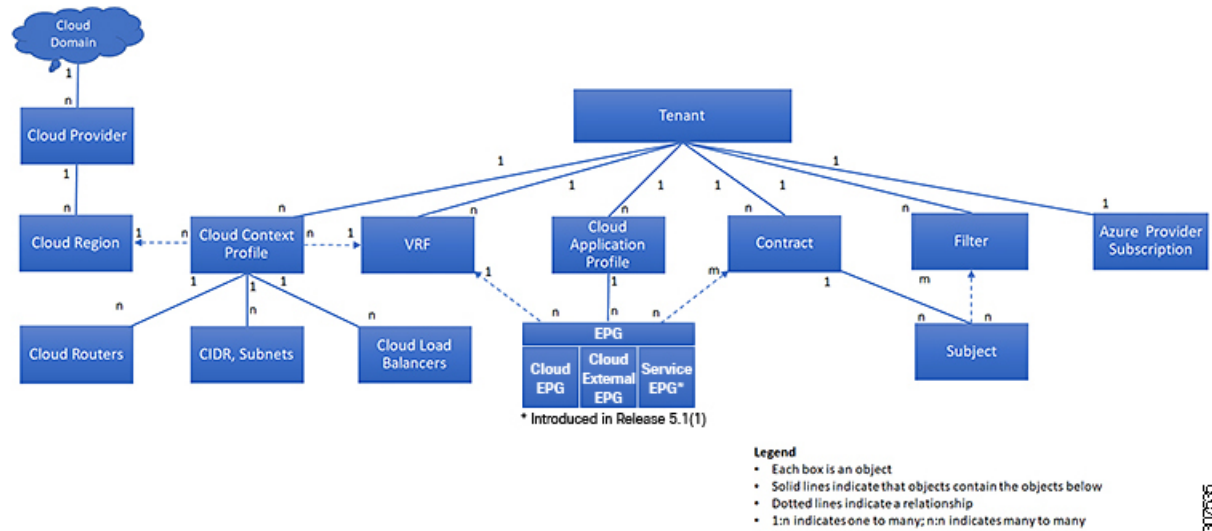
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ4～レイヤ7のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、[レイヤ4からレイヤ7サービスの展開](#)を参照してください。
- アクセス、認証、およびアカウントिंग（AAA）ポリシーは、Cisco Cloud Network Controller 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 Network Controller のセキュリティ \(173 ページ\)](#)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 3: テナント



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

テナントはアプリケーションポリシーの論理コンテナです。クラウドインフラストラクチャには、複数のテナントを含めることができます。レイヤ 4～7 のサービスを展開する前に、テナントを設定する必要があります。ACI クラウドインフラストラクチャは、テナントネットワークに対して IPv4 およびデュアルスタック構成をサポートします。

クラウドコンテキストプロフィール

クラウドコンテキストプロフィールには、以下の Cisco Cloud Network Controller コンポーネントに関する詳細が含まれます：

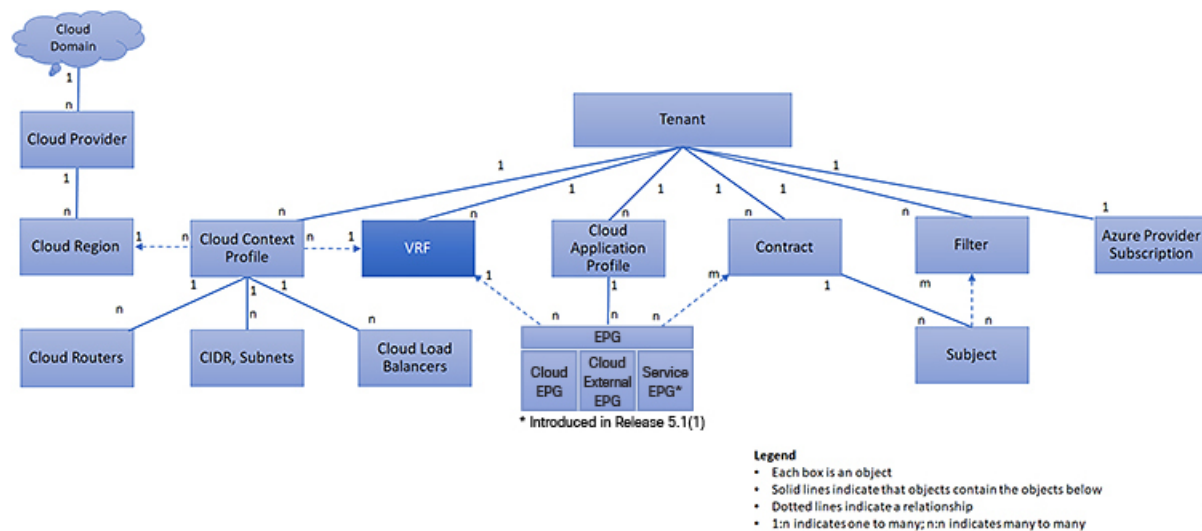
- CIDR
- VRF
- EPG
- [Regions]
- 仮想ネットワーク
- ルータ

- エンドポイント

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 Network Controller 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 4: 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 が含まれる場合があります。管理者が論理デバイスを作成した後、管理者はデバイスクラスタの選択基準ポリシーを提供する論理デバイスの VRF を作成できます。論理デバイスは、コントラクト名、グラフ名、またはグラフ内の関数ノード名に基づいて選択できます。

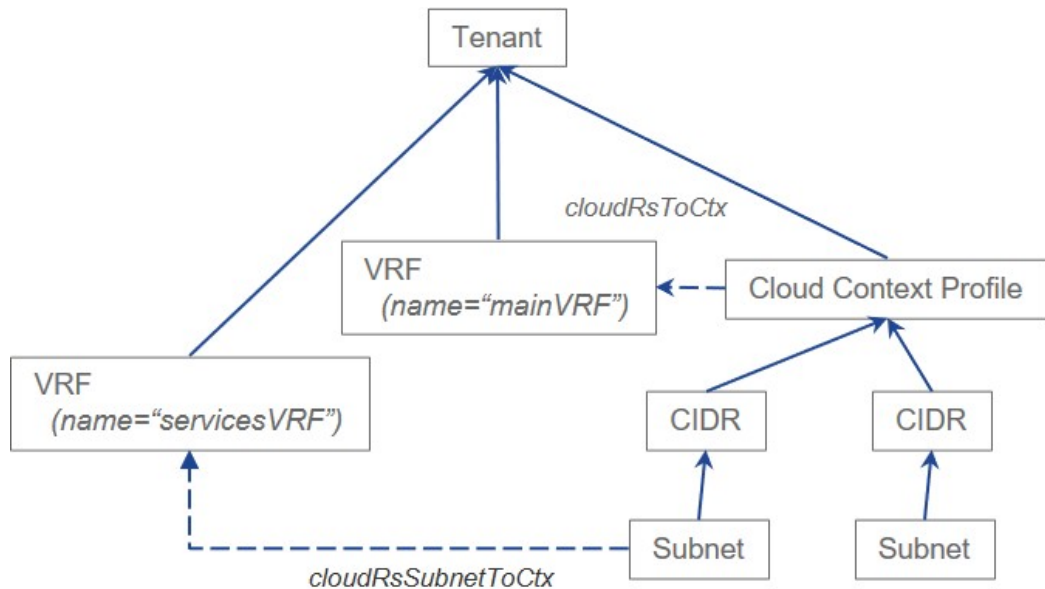
単一 VNet での複数の VRF のサポート

単一 VNet の下で複数の VRF がサポートされるようになりました。

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

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

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



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

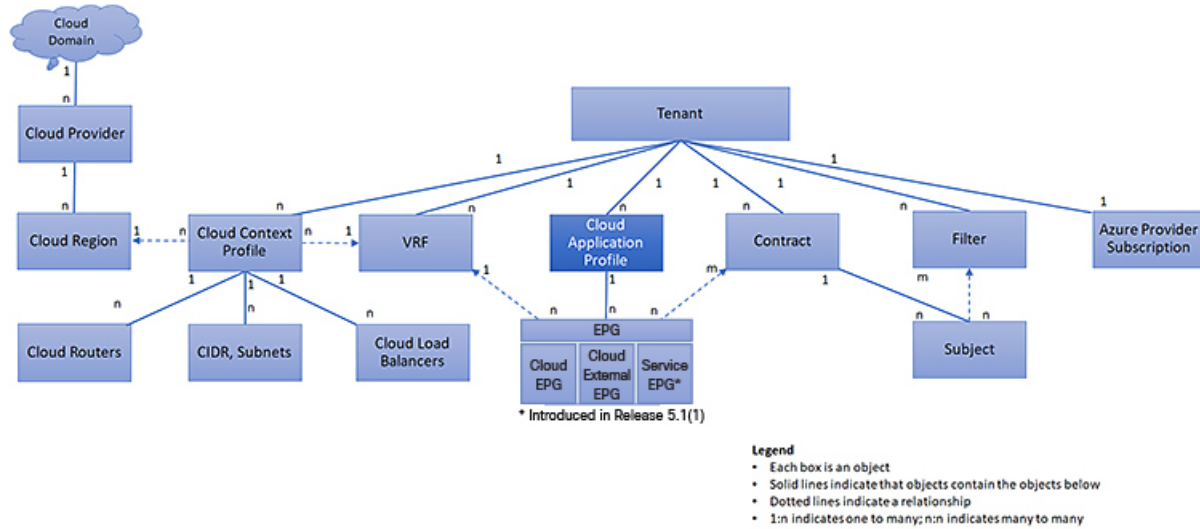
- mainVRF という名前のプライマリ VRF
- 名前が servicesVRF のセカンダリ VRF

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

クラウドアプリケーション プロファイル

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

図 5: 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。

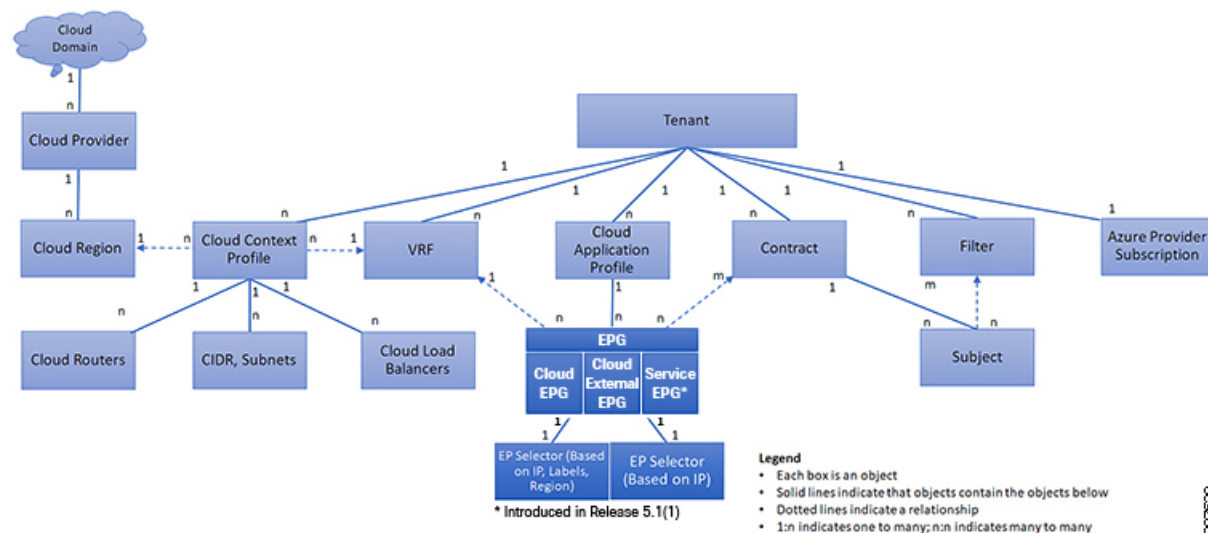
クラウド EPG は次のいずれかに従って組織化できます。

- 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 6: 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、他のすべての ID の詳細にアクセスすることもできます。クラウド EPG は、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ストレージサービス、またはクライアントが含まれます。クラウド EPG 内のエンドポイントメンバシップは、ダイナミックまたはスタティックにできます。

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

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

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

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

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

クラウドインフラストラクチャへの WAN ルータ接続は、スタティッククラウド EPG を使用する設定の1つの例です。クラウドインフラストラクチャへの WAN ルータ接続を設定するに

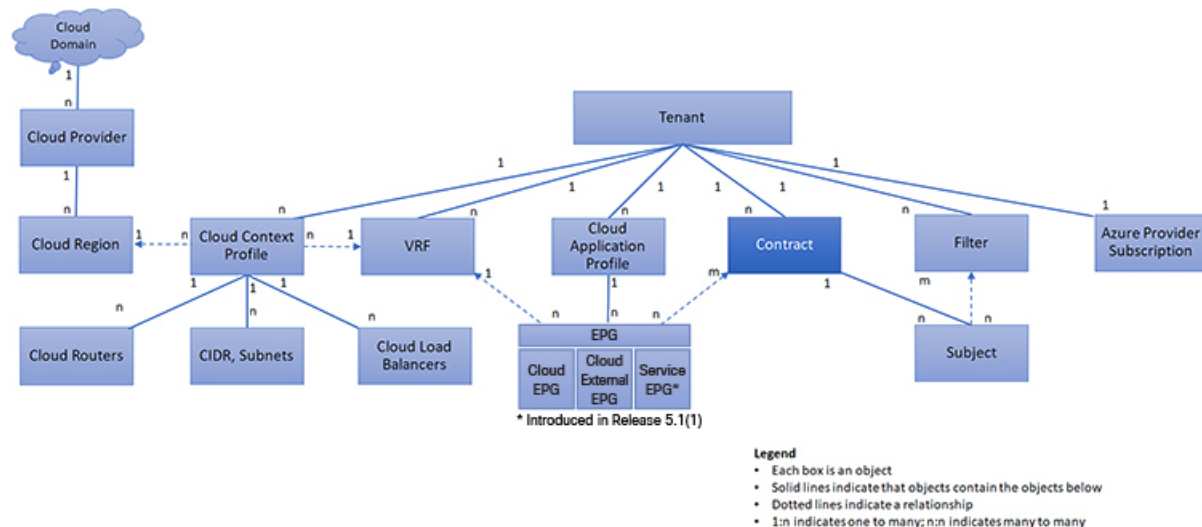
は、関連付けられている WAN サブネット内のエンドポイントを含む cloudExtEPg クラウド EPG を管理者が設定します。クラウドインフラストラクチャは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通してクラウド EPG のエンドポイントについて学習します。エンドポイントを学習すると、クラウドインフラストラクチャは、それに基づいて cloudExtEPg クラウド EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション (cloudEPg) クラウド EPG 内でサーバとの TCP セッションを開始すると、cloudExtEPg クラウド EPG は、cloudEPg クラウド EPG Web サーバとの通信が始まる前に、そのクライアントエンドポイントにポリシーを適用します。クライアントサーバ TCP セッションが終わり、クライアントとサーバ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 Network Controller はエンドポイントセクタを使用して、エンドポイントをクラウド EPG に割り当てます。エンドポイントセクタは、基本的に言って、Cisco ACI によって管理される Azure VNET に割り当てられたクラウドインスタンスに対して実行される一連のルールです。エンドポイントインスタンスに一致するエンドポイントセクタルールは、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 7: 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。コントラクトがない場合、EPG間通

信はデフォルトで無効になります。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。

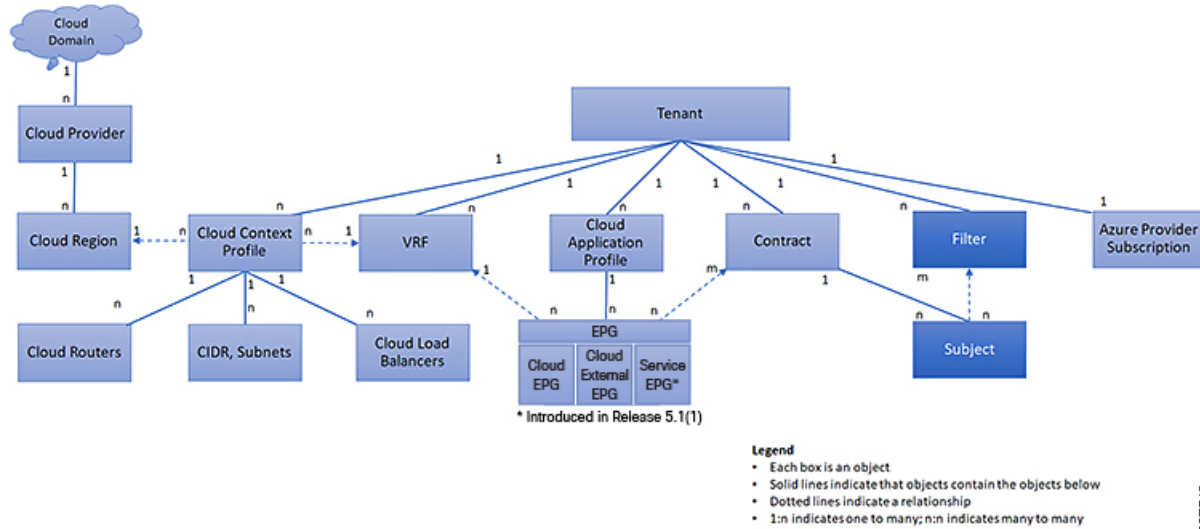


(注) 1 つのクラウド EPG で同じコントラクトを指定および使用できます。クラウド EPG は複数のコントラクトを同時に指定および使用することもできます。

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 8: サブジェクトおよびフィルタ



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



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

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

- フィルタは、レイヤ 3 ~ レイヤ 4 フィールド、レイヤ 3 プロトコルタイプなどの TCP/IP ヘッダーフィールド、レイヤ 4 ポートなどです。関連するコントラクトに従って、クラウド EPG プロバイダーは、IN および OUT 両方の方向でプロトコルおよびポートを決定します。コントラクトのサブジェクトは、コントラクトを提供する側と消費する側のクラウド EPG の間に適用されるフィルタ（およびその方向）への関連付けが含まれています。
- サブジェクトはコントラクトに含まれています。コントラクト内のサブジェクトがフィルタを使用して、通信できるトラフィックのタイプと発生の仕方を指定します。たとえば、HTTPS メッセージの場合、サブジェクトはその方向と許可される IP アドレスタイプ（たとえば IPv4）、HTTP プロトコル、およびポートを指定するフィルタを指定します。サブジェクトは、フィルタを単方向にするか双方向にするかを決定します。単方向フィルタは 1 方向で使用されます。単方向フィルタは、IN または OUT の通信を定義しますが、両方に対して同じではありません。双方向フィルタは両方に対して同じで、IN および OUT の通信を定義します。
- Azure 構造体でレンダリングされる ACI 契約は常にステートフルであり、リターントラフィックを許可します。

クラウドテンプレートの概要

クラウドテンプレートは、Cisco Cloud Network Controller 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 Network Controller 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、テンプレート入力要素を追加、変更、または削除できます。クラウドテンプレートは、それに応じて結果の設定を更新します。

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

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

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

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

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

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

インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。すべてのクラウド EPG とクラウド外部 EPG は、インフラ テナントのセカンダリ VRF に関連付けられます。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外

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

詳細については、[Cisco Cloud Network Controller GUI を使用したアプリケーション EPG の作成 \(80 ページ\)](#) 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 2: クラウドテンプレート MO

月	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。

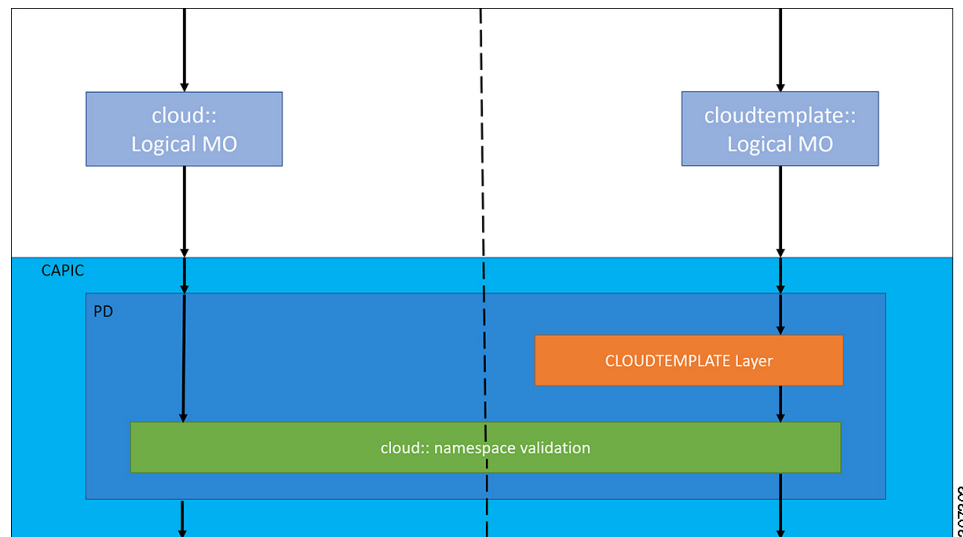
月	目的
cloudtemplateProfile	<p>すべてのクラウドルータの設定プロファイル。次の属性が含まれます。</p> <ul style="list-style-type: none"> routerUsername <p>(注)</p> <ul style="list-style-type: none"> ユーザ名を「admin」にすることはできません。 Azure からのユーザー名の制限が適用されます。 <ul style="list-style-type: none"> routerPassword routerThroughput routerLicenseToken routeDataInterfacePublicIP routerMgmtInterfacePublicIP
cloudtemplateIntNetwork	<p>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。</p>
cloudtemplateExtNetwork	<p>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。</p> <p>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。</p> <p>各リージョンは、cloudRegionName 子 MO を介してキャプチャされます。</p>
cloudtemplateVpnNetwork	<p>ACI オンプレミス サイトまたは別の Cisco Cloud Network Controller サイトで VPN を設定するための情報が含まれています。</p>
cloudtemplateIpSecTunnel	<p>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。</p>
cloudtemplateOspf	<p>VPN 接続に使用する OSPF エリアをキャプチャします。</p>
cloudtemplateBgpEvpn	<p>オンプレミス サイトとの BGP セッションを設定するために、ピア IP アドレス、ASN などをキャプチャします。</p>

Cisco Cloud Network Controller 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 Network Controller 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 9: 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 Network Controller コンポーネントの構成 \(51 ページ\)](#) を参照してください。

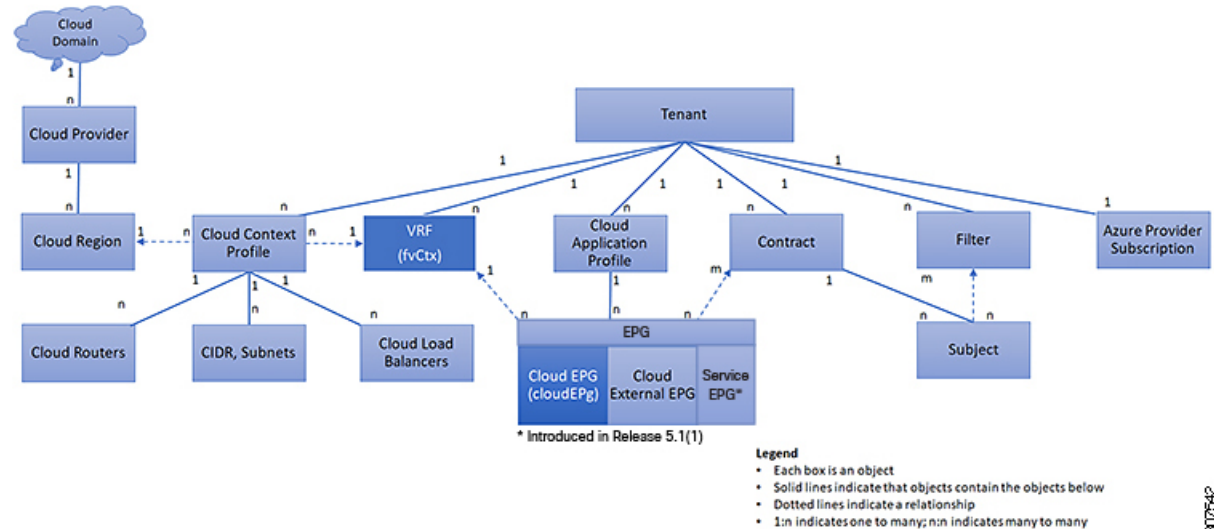
管理対象オブジェクトの関係とポリシー解決

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 10: MO の関係



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

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

デフォルト ポリシー



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

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

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



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

デフォルト ポリシーは、次の複数の目的に使用されます。

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

次のシナリオでは、一般的なポリシー解決の動作について説明します。

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



(注) 上記のシナリオは、テナントの VRF には適用されません。

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

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 Network Controller コンポーネントの構成

- [Cisco Cloud Network Controller の設定について](#) (51 ページ)
- [GUI を使用した Cisco Cloud Cisco Network Controller の構成](#) (51 ページ)
- [REST API を使用した Cisco Cloud Network Controller の構成](#) (135 ページ)

Cisco Cloud Network Controller の設定について

Cisco Cloud Network Controller GUI または REST API を使用して Cisco Cloud Network Controller 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 Network Controller GUI について](#) (4 ページ) を参照してください。

GUI を使用した Cisco Cloud Cisco Network Controller の構成

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アンマネージドテナントを作成する方法。

ユーザー テナントの Google Cloud プロジェクトのセットアップ

このセクションの手順を実行して、ユーザー テナントの Google Cloud プロジェクトをセットアップします。そのユーザー テナントは、管理対象または管理対象外のテナントです。

ステップ 1 必要に応じて、ユーザー テナントの Google Cloud プロジェクトを作成します。

各ユーザー 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。ユーザー 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。

- a) Google アカウントにログインします。
- b) **[IAM & Admin] > [Manage resources]** に移動します。
- c) 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。
- d) **[+プロジェクトの作成 (+ CREATE PROJECT)]** をクリックします。
- e) 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、4–30 文字にする必要があります。

- f) **[場所 (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。
- g) **[作成 (CREATE)]** をクリックします。

ステップ 2 Google Cloud で、この管理対象テナントに関連付けられたサービス アカウントで適切なサービス API を有効にします。

- a) Google Cloud GUIで、このユーザー 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。
プロジェクトの **ダッシュボード** が表示されます。
- b) **ダッシュボード** の上部にある検索バーで、「**API & Services**」を検索し、その検索結果をクリックして「**API & Services**」ウィンドウにアクセスします。
- c) 「**API & Services**」ウィンドウで、**[+ ENABLE APIS AND SERVICES]** タブをクリックします。

[API ライブラリ (API Library)] ウィンドウが表示されます。

- d) **[Search for APIs & Services]** フィールドで、必要なサービスを検索して有効にします。

次のリストの各サービスについて、

1. **[API とサービスの検索 (Search for APIs & Services)]** フィールドで API またはサービスを検索します。
2. 検索結果をクリックすると、その API またはサービスのページが表示されます。
3. その API またはサービス ページで **[ENABLE]** ボタンをクリックします。

次に、検索して有効にする必要がある API とサービスを示します。

- コンピューティング エンジン
- Cloud Deployment Manager V2 API

- Cloud Pub / Sub API
- クラウドリソース マネージャ API
- Service Usage API
- Cloud Logging API

各APIまたはサービスを有効にするには数分かかります。各APIまたはサービスを有効にした後、**[API とサービス (APIs & Services)]** ウィンドウに戻る必要があります。

上記のすべての API とサービスを有効にすると、次の追加の API とサービスが自動的に有効になります。

- Identity and Access Management (IAM) API
- IAM サービス アカウントの資格情報
- クラウド OS ログイン API
- クラウド DNS API
- レコメンダAPI

自動的に有効になっていない場合は、手動で有効にします。

ステップ 3 Google Cloud のこの管理対象テナントに必要な権限を設定します。

- a) Google Cloud GUIで、このユーザー 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。
プロジェクトの **ダッシュボード** が表示されます。
- b) 左側のナビゲーションバーで、**[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) 適切なサービス アカウントを見つけます。
- d) 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**[エディタ (Editor)]** 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。

- エディタ (Editor)
- ロール管理者

- プロジェクト IAM 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。

管理対象テナントの作成

次のセクションでは、管理対象テナントを作成するために必要な情報を提供します。

- Cisco Cloud Network Controller で管理対象テナントを作成する
- Google Cloud の管理対象テナントに必要な権限を設定します。

Cisco Cloud Network Controller 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 Network Controller で管理す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 ユーザーテナントの Google Cloud プロジェクトをセットアップします。

これらの手順については、[ユーザーテナントの Google Cloud プロジェクトのセットアップ \(51 ページ\)](#) を参照してください。

ステップ 2 Cisco Cloud Network Controller GUI で、[アプリケーション管理 (Application Management)] > [VRF] に移動します。

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 3: テナント ダイアログボックス フィールドの作成

[プロパティ (Properties)]	説明
名前 (Name)	テナント名を入力します。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。

[プロパティ (Properties)]	説明
説明	テナントの説明を入力します。
[設定 (Settings)]	
セキュリティドメインの追加 (Add Security Domain)	<p>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。</p> <ol style="list-style-type: none"> 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 Project	
Google Cloud Project ID	この Cisco Cloud Network Controller テナントに関連付けられる Google Cloud プロジェクト ID を入力します。
アクセスタイプ	<p>Cisco Cloud Network Controller で管理する予定のテナントの場合は、アクセスタイプとして [管理対象 ID (Managed Identity)] を選択します。</p> <p>詳細については、Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する (8 ページ) を参照してください。</p>
Google Cloud Project のセキュリティドメインを追加	<p>(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。</p> <p>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。</p> <ol style="list-style-type: none"> 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 [Save] をクリックします。

次のタスク

Google Cloud で管理対象テナントに必要な構成を完了します。これらの手順については、[管理対象テナント用に Google Cloud で必要な権限を設定する \(56 ページ\)](#) にアクセスしてください。

管理対象テナント用に Google Cloud で必要な権限を設定する

マネージドテナントを作成している場合は、Google Cloud で必要なアクセス許可を設定する必要があります。



(注) アンマネージドテナントを作成している場合は、この手順に従う必要はありません。

ステップ 1 Google Cloud GUI で、このマネージドテナントに関連付けられる Google Cloud プロジェクトにログインします。

プロジェクトの **ダッシュボード** が表示されます。

ステップ 2 左側のナビゲーションバーで、**[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。

ステップ 3 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作成されたサービスアカウントを見つけます。

ステップ 4 サービス アカウント名をコピーします。

ステップ 5 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。

ステップ 6 このサービス アカウントの権限を設定します。

a) 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。

b) **[+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。

c) **[+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 ネットワーク管理者
- コンピューティング セキュリティ管理者

- 管理者のログイン
- パブ/サブ管理者
- ストレージ管理者

d) 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。

アンマネージドテナントの作成

次のセクションでは、アンマネージドテナントを作成するために必要な情報を提供します。

- Google Cloud からアンマネージドテナントに必要な秘密鍵情報を生成してダウンロードします
- Cisco Cloud Network Controller にアンマネージドテナントを作成する

アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード

アンマネージドテナントを作成する場合は、最初に Google Cloud から必要な秘密キー情報を生成してダウンロードする必要があります。



(注) マネージドテナントを作成している場合は、この手順の手順に従う必要はありません。

ステップ 1 Google Cloud で、まだ選択されていない場合、アンマネージドテナントに関連付けられる Google Cloud プロジェクトを選択します。

ステップ 2 左側のナビゲーションバーで、[IAM & Admin] をクリックし、サービス アカウント 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 3 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 4 [キー (KEYS)] タブをクリックします。

ステップ 5 [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 6 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。

Cisco Cloud Network Controller GUI を使用したアンマネージドテナントの作成

- ステップ 7** 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。

```
{
  "type": "service_account",
  "project_id": " ",
  "private_key_id": " ",
  "private_key": "-----BEGIN PRIVATE
KEY-----
",
  "client_id": " ",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": " "
}
```

Cisco Cloud Network Controller GUI を使用したアンマネージドテナントの作成

このセクションでは、GUI を使用して Cisco Cloud Network Controller GUI で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。

始める前に

このセクションの手順を使って続行する前に、[アンマネージドテナントの Google Cloud から秘密キー情報の生成とダウンロード \(57 ページ\)](#) で説明されている手順を完了します。

- ステップ 1** ユーザーテナントの Google Cloud プロジェクトをセットアップします。
- これらの手順については、[ユーザーテナントの Google Cloud プロジェクトのセットアップ \(51 ページ\)](#) を参照してください。
- ステップ 2** Cisco Cloud Network Controller GUI で、[アプリケーション管理 (Application Management)] > [VRF] に移動します。
- 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

[プロパティ (Properties)]	説明
名前 (Name)	テナント名を入力します。正規表現の一致: <code>[az]([-a-z0-9]*[a-z0-9])?</code> 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。
[設定 (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。 <ol style="list-style-type: none"> 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 Project	
Google Cloud Project ID	この Cisco Cloud Network Controller テナントに関連付けられる Google Cloud プロジェクト ID を入力します。
アクセスタイプ	Cisco Cloud Network Controller で管理されていないテナントの場合は、アクセスタイプとして[アンマネージド ID (Unmanaged Identity)]を選択します。 詳細については、 Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する (8 ページ) を参照してください。
キーID	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード (57 ページ) でダウンロードした JSON ファイルの <code>private_key_id</code> フィールドの情報を入力します。

[プロパティ (Properties)]	説明
RSA プライベート キー	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード (57 ページ) でダウンロードした JSON ファイルの <code>private_key</code> フィールドの情報を入力します。
クライアントID	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード (57 ページ) でダウンロードした JSON ファイルの <code>client_id</code> フィールドの情報を入力します。
電子メール	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	<p>(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。</p> <p>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。</p> <ol style="list-style-type: none"> 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 [Save] をクリックします。

Cisco Cloud Network Controller 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 Network Controller GUI 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 [名前 (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:

```
[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 ルール名を作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、[Google Cloud ファイアウォール ルールによる命名の長さの制限 \(28 ページ\)](#) 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 [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用した VRF の作成

このセクションでは、Cisco Cloud Network Controller 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 Network Controller GUI を使用したクラウドネイティブルータによる外部ネットワークの作成 \(64 ページ\)](#) 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 5: [VRF の作成 (Create VRF)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	

[プロパティ (Properties)]	説明
名前	<p>[Name] フィールドに、VRF の表示名を入力します。</p> <p>次の制約事項に注意してください。</p> <ul style="list-style-type: none"> 正規表現の一致: <code>[az] ([-a-z0-9] * [a-z0-9]) ?</code> 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 ルール名を作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、Google Cloud ファイアウォールルールによる命名の長さの制限 (28 ページ) を参照してください。 <p>すべての VRF に <i>vrfEncoded</i> 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 <i>vrfEncoded</i> 値を使用してクラウドルータで識別されます。<i>vrfEncoded</i> 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。</p>
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [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。 [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。 <p>[VRF の作成 (Create VRF)] ダイアログボックスに戻ります。</p>
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 Network Controller GUI を使用したクラウドネイティブルータによる外部ネットワークの作成

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

始める前に

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

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

構成された外部ネットワークが表示されます。Cisco Cloud Network Controller 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 [Cisco Cloud Network Controller 設定 (Cisco Cloud Network Controller Setup)] リンクをクリックし、ハブネットワークを作成して、ここに戻ります。ハブネットワークの作成に関する詳細は、リリース 25.0(x)以降の『Google Cloud インストールガイドの Cisco Cloud Network Controller』にある「セットアップ ウィザードの Cisco Cloud Network Controller の構成」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 6: [外部ネットワークの作成 (Create External Network)] ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
VRF	<p>この外部 VRF は、オンプレミス CCR 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。</p> <p>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 として識別されません。</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <p>外部 VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [VRF の選択 (Select VRF)] をクリックします。 [VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 2. [VRF の選択 (Select VRF)] ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成 (+ Create VRF)] オプションを使用して VRF を作成することもできます。 3. [選択 (Select)] をクリックします。 [外部ネットワークの作成 (Create External Network)] ダイアログボックスに戻ります。
ハブ ネットワーク	<p>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。</p> <p>(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に関する詳細は、Cisco Cloud Network Controller for Google Cloud インストールガイド、リリース 25.0(x)以降の、「セットアップウィザードを使用した Cisco Cloud Network Controller の構成」の章を参照してください。</p>
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。
[設定 (Settings)]	

[プロパティ (Properties)]	説明
地域	<p>リージョンを選択するには:</p> <ol style="list-style-type: none">1. [地域の追加 (Add Region)] をクリックします。 [地域の選択 (Select Regions)] ダイアログボックスが表示されます。<ul style="list-style-type: none">• 初回セットアップの一部として選択した地域がここに表示されます。• 複数の地域を選択して、複数の地域でクラウドルータを起動できます。2. [地域の選択 (Select Regions)] ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)] をクリックします。 [外部ネットワークの作成 (Create External Network)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
VPN ネットワーク	<p>VPN ネットワークエントリーは、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。</p> <p>VPN ネットワークを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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 エントリーごとに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。 <ul style="list-style-type: none"> • IPsec トンネル ピアの パブリック IP • 事前共有キー • IKE Version : IPsec トンネル接続用に ikev1 または ikev2 を選択します。 • BGP ピア ASN • Subnet Pool Name : [サブネット プール名の選択 (Select Subnet Pool Name)] をクリックします。 [サブネット プール名の選択 (Select Subnet Pool Name)] ダイアログボックスが表示されます。リストされている使用可能なサブネットプールのいずれかを選択し、[選択 (Select)] をクリックします。 <p>(注) 必要に応じて、追加の IPsec トンネルサブネットプールを [外部ネットワーク] ページに追加するか、クラウドネットワークコントローラーの初回セットアップを介して追加できます。For more information on adding additional subnet pools through the Cloud Network Controller First Time Set Up, see the chapter "Configuring Cisco Cloud Network Controller Using the Setup Wizard" in the <i>Cisco Cloud Network Controller for GCP Installation Guide, Release 25.0(5)</i>. サブネットプールのサイズは、作成される IPsec トンネルの数に対応できる十分な大きさにする必要があります。</p> 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、[Hybrid Connectivity] > [VPN] > [Cloud VPN Tunnels] に移動します。

BGP-EVPN を使用したサイト間ネットワークの構成

リリース 25.0(5)以降、サイト間ユースケースでは、次のシナリオでサイト間接続用の BGP-EVPN 接続を構成するためのサポートが利用できます。

- クラウドサイト間サイト：
 - Google Cloud サイト～ Google Cloud サイト
 - Google Cloud サイトから AWS サイトへ
 - Google Cloud サイトから Azure サイトへ
- Google Cloud サイトから ACI オンプレミス サイト

これらの各シナリオでは、BGP-EVPN 接続に Cisco Catalyst 8000V が使用されます。詳細については、「[BGP-EVPN を使用したサイト間接続 \(15 ページ\)](#)」を参照してください。

ステップ 1 Cisco Cloud Network Controller GUI で、インテントアイコン (🔍) をクリックし、[Cloud Network Controller セットアップ (Cloud Network Controller Setup)] を選択します。

ステップ 2 [リージョン管理 (Region Management)] エリアで、[設定の編集 (Edit Configuration)] をクリックします。

[地域管理 (Region Management)] ページが表示されます。

ステップ 3 サイト間接続に Cisco Catalyst 8000V ルータを使用する地域を見つけ、それらの地域の **Catalyst 8000V** 列のボックスをクリックします。

これはリリース 25.0(5) で導入された機能であり、Cisco Catalyst 8000V ルーターを使用して、Google Cloud サイトと他のクラウドサイトまたは ACI オンプレミス サイトとの間のサイト間接続用に BGP-EVPN 接続を構成できるようにします。詳細については、「[BGP-EVPN を使用したサイト間接続 \(15 ページ\)](#)」を参照してください。

ステップ 4 ページの下部にある [次へ (Next)] をクリックします。

[General Connectivity] ページが表示されます。

ステップ 5 [クラウド ルータのサブネット プール (Subnet Pools for Cloud Routers)] 領域の必要な情報を入力します。

最初のサブネットプールが自動的に入力されます (System Internal として表示)。このサブネットプールのアドレスは、Cisco Cloud Network Controller で管理する必要がある追加のリージョンのリージョン間接続に使用されます。このフィールドに追加するサブネットプールは、マスク/24の有効なIPv4サブネットである必要があります。

前のページで Catalyst 8000V を展開する追加のリージョンを選択した場合は、2 ~ 4 台の Catalyst 8000V を展開するリージョンごとに 1 つのサブネットプールを追加します (6.c (70 ページ) の [リージョンあたりのルータ数 (Number of Routers Per Region)] で 2、3、4 を入力する場合)。

ステップ 6 リリース 25.0(5) 以降では、Catalyst 8000V 領域に必要な情報を入力します。

a) [C8kVs の BGP 自律システム番号 (BGP Autonomous System Number for C8kVs)] フィールドで、固有の BGP 自立システム番号 (ASN) を入力します。

BGP 自律システム番号は 1 ~ 65535 の範囲で指定できます。

b) [パブリック IP を C8kV インスタンスに割り当てる (Assign Public IP to C8kV Interface)] フィールドで、パブリック IP アドレスを Catalyst 8000V インターフェイスに割り当てるかどうかを決定します。

プライベート IP アドレスは、デフォルトで Catalyst 8000V インターフェイスに割り当てられます。[パブリック IP を C8kV インスタンスに割り当てる (Assign Public IP to C8kV Interface)] オプションは、パブリック IP アドレスを Catalyst 8000V インターフェイスにも割り当てるかどうかを決定します。

Catalyst 8000V インターフェイス IP アドレスは次の目的で使用されます。

- Catalyst 8000V を管理すること、または Catalyst 8000V に直接 SSH で接続することができます。
- マルチクラウドおよびハイブリッドクラウド接続のために、サイト全体のインターフェイスをクロスプログラムできます。Cisco Nexus Dashboard Orchestrator
- コントロールプレーントラフィックとデータプレーントラフィックの両方の Catalyst 8000V の場合

デフォルトでは、この [有効] チェックボックスはオンになっています。これは、Catalyst 8000V にパブリック IP アドレスを割り当てられることを意味します。

- [パブリック (public)] IP アドレスを Catalyst 8000V に割り当てる場合は、[有効 (Enabled)] の横にあるチェックボックスをオンのままにします。
- プライベート IP アドレスのみを Catalyst 8000V に割り当てるには、オプションを無効化するために [有効 (Enabled)] の横にあるチェックボックスをオフにします。

Catalyst 8000V 接続をプライベートからパブリック、またはその逆に変更すると、ネットワークが中断する可能性があることに注意してください。さらに、パブリック IP アドレスが Catalyst 8000V から削除された場合、Google Cloud サイトは Google Cloud 相互接続を介してプライベート IP アドレスを使用してオンプレミスの ACI サイトに接続します。Nexus Dashboard Orchestrator から Google Cloud

サイトのプライベート サイト間接続を構成し、Google Cloud ポータルから Google Cloud 相互接続を構成する必要があります。

(注) Catalyst 8000V に割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、[クラウドリソース (Cloud Resources)] 領域にルータの他の詳細とともに表示されます。Catalyst 8000V にパブリック IP アドレスが割り当てられていない場合は、プライベート IP アドレスだけが表示されます。

- c) [リージョンあたりのルータの数 (Number of Routers Per Region)] フィールドで、各リージョンで使用される Catalyst 8000Vs の数を選択します。
- d) [ユーザー名 (Username)] に、Catalyst 8000V のユーザー名を入力します。
- e) [パスワード (Password)] フィールドに、Catalyst 8000V のパスワードを入力します。
[Confirm Password] フィールドに、もう一度パスワードを入力します。
- f) [ルータのスループット (Throughput of the routers)] フィールドで、Catalyst 8000V のスループットを選択します。

このフィールドの値を変更すると、展開されている Catalyst 8000V インスタンスのサイズが変更されます。スループットの値を高くすると、導入される VM のサイズが大きくなります。

次の点に注意してください。

- Catalyst 8000V のライセンスは、この設定に基づいています。準拠するには、Smart アカウントに同等以上のライセンスが必要です。詳細については、『[Google Cloud インストールガイドの Cisco Cloud Network Controller](#)』の「Google Cloud の Cisco Cloud Network Controller 展開で使用するリソース」を参照してください。
- クラウドルータは、ルータのスループットまたはログインクレデンシャルを変更する前に、すべてのリージョンから展開解除する必要があります。

将来のある時点でこの値を変更することが必要になった場合は、Catalyst 8000V を削除してから、この章のプロセスを再度繰り返し、同じ[ルータのスループット (Throughput of the routers)] フィールドで新しい値を選択する必要があります。

- g) 必要に応じて、[TCP MSS] フィールドに必要な情報を入力します。

[TCP MSS] オプションを使用すれば TCP 最大セグメントサイズ (MSS) を構成できます。この値は、データギガビットイーサネットインターフェイス、クラウドルータのIPSecトンネルインターフェイス、およびクラウド、オンプレミス、またはその他のクラウドサイトに対するVPNトンネルインターフェイスを含む、すべてのクラウドルータインターフェイスに適用されます。クラウドへのVPNトンネルの場合、クラウドプロバイダーのMSS値がこのフィールドに入力した値よりも小さい場合は、低い方の値が使用されます。それ以外の場合は、このフィールドに入力した値が使用されます。

MSS値はTCPトラフィックにのみ影響し、pingトラフィックなどの他のタイプのトラフィックには影響しません。

- h) [ライセンス トークン (License Token)] フィールドに、Catalyst 8000V のライセンス トークンを入力します。

これは、シスコスマートソフトウェアライセンスアカウントからの製品インスタンス登録トークンです。このライセンストークンを取得するには、に移動し、[Smart Software Licensing Inventory Virtual Account]に移動して、製品インスタンス登録トークンを見つけます。<http://software.cisco.com>>> 詳細については、『[Google Cloud インストールガイドの Cisco Cloud Network Controller](#)』の「Cisco Cloud Network Controller ライセンシング」を参照してください。

(注) プライベート IP アドレスを [6.b \(69 ページ\)](#) の Catalyst 8000V に割り当てた場合、プライベート IP アドレスを使用して Catalyst 8000V のスマートライセンスを登録するときにサポートされる唯一のオプションは、[Cisco Smart Software Manager (CSSM) に直接接続 (Direct connect to Cisco Smart Software Manager (CSSM))] です。この場合、エクスプレスルート経由で CSSM に到達可能性を提供する必要があります。

ステップ 7 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。

ステップ 8 [詳細設定 (Advanced Settings)] 領域で、[構成の編集 (Edit Configuration)] をクリックします。

ステップ 9 [コントラクトベースのルーティング (Contract Based Routing)] フィールドで、[はい (yes)] の横のボックスをクリックしてコントラクトベースのルーティングを有効にし、[保存して続行 (Save and Continue)] をクリックします。

(注) Nexus Dashboard Orchestrator で Google Cloud サイトに移動し、[サイト間接続 (Inter-Site Connectivity)] 領域の [契約ベースのルーティング (Contract Based Routing)] オプションをクリックして、Nexus ダッシュボードオーケストレータを介して契約ベースのルーティングを有効にすることもできます。

ステップ 10 [基本を構成しましょう (Let's Configure the Basics)] ウィンドウの下部にある [完了 (Done)] をクリックします。

ステップ 11 Google Cloud サイドの VM インスタンスの数が、Cisco Cloud Network Controller で設定した Catalyst 8000V の数と一致することを確認します。

- インフラテナントに関連付けられた Google Cloud プロジェクトにログインします。
- Google Cloud の [コンピューティングエンジン (Compute Engine)] > [VM インスタンス (VM instances)] に移動します。
- [インスタンス (Instances)] タブに表示される VM インスタンスの数が、サイト間接続用の BGP-EVPN 接続に使用している Catalyst 8000V の総数と一致することを確認します。

たとえば、2つのリージョンと各リージョンに2つの Catalyst 8000V を選択した場合、[インスタンス (Instances)] タブに4つの VM インスタンスが表示されます。

ステップ 12 Google Cloud のオーバーレイ 1 VPC およびオーバーレイ 1 セカンダリ VPC 用に VPC ネットワークが設定されていることを確認します。

詳細については、「[BGP-EVPN を使用したサイト間接続 \(15 ページ\)](#)」を参照してください。

- Google Cloud の [VPC ネットワーク (VPC network)] > [VPC ネットワーク (VPC networks)] に移動します。
- [VPC ネットワーク (VPC networks)] 画面に、overlay-1 VPC および overlay-1 セカンダリ VPC 用に設定された VPC ネットワークが表示されていることを確認します。

ステップ 13 Cisco Cloud Network Controller で設定した Catalyst 8000V が、適切な Cisco Cloud Network Controller GUI 画面に正しく表示されていることを確認します。

- [ダッシュボード (Dashboard)] ページで、[接続 (Connectivity)] ペインを見つけて、Cisco Cloud Network Controller で設定した Catalyst 8000V がこの画面に正しく表示されることを確認します。
- [インフラストラクチャ (Infrastructure)] > [サイト間接続 (Inter-Site Connectivity)] に移動し、Cisco Cloud Network Controller で設定した Catalyst 8000V がこの画面に正しく表示されることを確認します。
- [クラウド リソース (Cloud Resources)] > [ルータ (Routers)] に移動し、Cisco Cloud Network Controller で設定した Catalyst 8000V がこの画面に正しく表示されることを確認します。

ステップ 14 BGP-EVPN を使用してサイト間接続の VPC ピアリングを構成します。

Cisco Catalyst 8000V ルータを使用してサイト間接続用に BGP-EVPN 接続を構成する場合、Google Cloud サイト内のユーザー VPC が他のクラウドサイトまたは ACI オンプレミス サイト内の VPC と通信できるように追加の構成を行う必要があります。

通常、VRF を作成してから、その VRF のハブ ピアリングを確認する Nexus ダッシュボード オーケストレータを介して BGP-EVPN を使用して、サイト間接続用に VPC ピアリングを構成します。これらの手順については、該当する [Nexus Dashboard Orchestrator のドキュメント](#) を参照してください。

Cisco Cloud Network Controller 側でこの構成を変更するには、次の手順を実行します。

- a) Cisco Cloud Network Controller GUI で、[アプリケーション管理 (Application Management)] > [クラウド コンテキスト プロファイル (Cloud Context Profiles)] に移動します。
- b) [名前 (Name)] 列で、オーバーレイ 1 VPC とピアリングする VPC に関連付けられているクラウド コンテキスト プロファイルの名前をダブルクリックします。

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

- c) [アクション (Actions)] > [編集 (Edit)] をクリックします。
- d) [VPC ハブ ピアリング (VPC Hub Peering)] 領域で、[有効化 (Enable)] の横にあるボックスをクリックして、この VPC の VPC ピアリングを有効にし、[保存 (Save)] をクリックします。
- e) Google Cloud で、[VPC ネットワーク (VPC network)] > [VPC ネットワーク ピアリング (VPC network peering)] に移動します。
- f) Google Cloud サイトのユーザー VPC がオーバーレイ 1 VPC とピアリングしていることを確認します。

Cisco Cloud Network Controller GUI を使用した VRF 間ルート リークの構成

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 \(17ページ\)](#) 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 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 7: 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 Dialog Box Fields)

[プロパティ (Properties)]	説明
送信元 VRF	<p>送信元 VRF を選択するには：</p> <ol style="list-style-type: none"> [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。 [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します。 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。 [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。

[プロパティ (Properties)]	説明
宛先 VRF	<p>宛先 VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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います。 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。
タイプ	<p>構成するリーク ルートのタイプを選択します。</p> <ul style="list-style-type: none"> • [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 \(73 ページ\)](#) – [ステップ 5 \(74 ページ\)](#) 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 \(73 ページ\)](#) – [ステップ 5 \(74 ページ\)](#) 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 \(73 ページ\)](#) 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 \(73 ページ\)](#) 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 Network Controller GUI で、[ダッシュボード (Dashboard)] をクリックします。Cisco Cloud Network Controller の [ダッシュボード (Dashboard)] ビューが表示されます。

- ステップ 2 [接続 (Connectivity)] 領域の [外部接続ステータス (External Connectivity Status)] で、[クラウドルーター (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 \(75 ページ\)](#) 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 と外部デバイス間の接続を有効にするために必要な情報を収集します。
- ステップ 2 外部デバイスにログインします。
- ステップ 3 外部ネットワークング 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 \(75 ページ\)](#) 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
hostname inf-act-[infra]/region-[us-west1]/site-[1]-id-[0]/ext-[extwfo-us-west1]/vpn-[vpwfo]/itr-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-abc-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 Network Controller 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 Network Controller 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 Network Controller GUI を使用してアプリケーション EPG を作成する方法を説明します。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 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 8: [EPG の作成 (Create EPG)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	

[プロパティ (Properties)]	説明
名前	<p>EPG の名前を入力します。</p> <p>次の制約事項に注意してください。</p> <ul style="list-style-type: none"> 正規表現の一致: [az] ([-a-z0-9] * [a-z0-9]) ? <p>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。</p> <ul style="list-style-type: none"> 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作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、Google Cloud ファイアウォールルールによる命名の長さの制限 (28 ページ) を参照してください。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [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。 [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。 [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	<p>アプリケーションプロファイルを選択します。</p> <ol style="list-style-type: none"> [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。 [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。 [選択 (Select)] をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
説明	EPG の説明を入力します。
[設定 (Settings)]	
タイプ	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。 <ol style="list-style-type: none">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。

[プロパティ (Properties)]	説明
エンドポイントセクタ	

[プロパティ (Properties)]	説明
	<p>(注) エンドポイントセ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 (103 ページ) を参照してください。</p> <p>エンドポイント セクタを追加するには：</p> <ol style="list-style-type: none"> 1. [エンドポイント セクタの追加 (Add Endpoint Selector)] をクリックして、[エンドポイント セクタの追加] ダイアログを開きます。 2. [エンドポイント セクタの追加 (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。 <ul style="list-style-type: none"> • エンドポイント セクタに 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。 <p>(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) 。</p> 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。 <ul style="list-style-type: none"> • [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

[プロパティ (Properties)]	説明
	<p>します。入力する値は、[キー (Key)]フィールドと[演算子 (Operator)]フィールドで選択した内容によって異なります。たとえば、[キー (Key)]フィールドが [IP] に設定され、[演算子 (Operator)]フィールドが [等しい (equals)] に設定されている場合、[値 (Value)]フィールドは IP アドレスまたはサブネットでなければなりません。ただし、[演算子 (Operator)]フィールドが [キー (keys)] に設定されている場合、[値 (Value)]フィールドは無効になります。</p> <p>7. 完了したら、チェックマークをクリックしてセクタ式を検証します。</p> <p>8. エンドポイントセクタに追加のエンドポイントセ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。</p> <p>たとえば、1つのエンドポイントセクタで2つの式セットを作成したとします。</p> <ul style="list-style-type: none"> • エンドポイントセクタ 1、式 1: <ul style="list-style-type: none"> • [キー (Key):] Region • 演算子 (Operator) : equals • 値 : us-west1 • エンドポイントセクタ1、式 2: <ul style="list-style-type: none"> • [キー (Key):] IP • 演算子 (Operator) : equals • [値 (Value):] 192.0.2.1/24 <p>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。</p>

[プロパティ (Properties)]	説明
	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • エンドポイントセレクタ 2、式 1: <ul style="list-style-type: none"> • [キー (Key):] Region • 演算子 : in • 値 : us-east1、us-central1 <p>その場合、次のようになります。</p> <ul style="list-style-type: none"> • 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 <p>または</p> <ul style="list-style-type: none"> • 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 <p>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。</p>

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用した外部 EPG の作成

このセクションでは、Cisco Cloud Network Controller GUI を使用して外部 EPG を作成する方法を説明します。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 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 9: [EPG の作成 (Create EPG)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	<p>EPG の名前を入力します。</p> <p>次の制約事項に注意してください。</p> <ul style="list-style-type: none"> 正規表現の一致: [az] ([-a-z0-9] * [a-z0-9]) ? <p>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。</p> <ul style="list-style-type: none"> 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作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、Google Cloud ファイアウォールルールによる命名の長さの制限 (28 ページ) を参照してください。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [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。 [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。 [選択 (Select)] をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
アプリケーションプロファイル	<p>アプリケーションプロファイルを選択します。</p> <ol style="list-style-type: none"> [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。 [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。 [選択 (Select)]をクリックします。[EPG の作成 (Create EPG)]ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定 (Settings)]	
タイプ	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	<p>VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [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。 [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。 [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) 。

[プロパティ (Properties)]	説明
エンドポイントセクタ	<p>(注) エンドポイントセ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 (103 ページ) を参照してください。</p> <p>エンドポイント セクタを追加するには：</p> <ol style="list-style-type: none"> 1. [エンドポイントセクタの追加 (Add Endpoint Selector)] をクリックして、エンドポイントセクタを追加します。 2. [名前 (Name)] フィールドに名前を入力します。 3. サブネット にサブネットを入力します。 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 セクタを検証します。 5. 追加のエンドポイント セクタを作成するかどうかを決定します。 <p>EPG の下で複数のエンドポイント セクタを作成した場合は、それらのエンドポイントセクタの間には論理 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クタを作成したとします。</p> <ul style="list-style-type: none"> • エンドポイントセクタ 1： <ul style="list-style-type: none"> • 名前：EP_Sel_1 • サブネット：192.1.1.1/24 • エンドポイント セクタ 2： <ul style="list-style-type: none"> • 名前：EP_Sel_2 • サブネット：192.2.2.2/24 <p>その場合、次のようになります。</p> <ul style="list-style-type: none"> • IP アドレスが 192.1.1.1/24 サブネット (エンドポイント セクタ 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 セクタ 2) に属する場合 <p>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。</p>

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したフィルタの作成

このセクションでは、Cisco Cloud Network Controller 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 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 10: フィルタの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	[名前 (Name)]フィールドにハードウェアフィルタの名前を入力します。
テナント	テナントを選択します。 <ol style="list-style-type: none"> [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。 [テナントの選択 (Select Tenant)]ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)]をクリックします。[フィルタの作成 (Create)]ダイアログボックスに戻ります。
説明	フィルタの説明を入力します。

[プロパティ (Properties)]	説明
フィルタの追加	<p>フィルタを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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。 <ul style="list-style-type: none"> • IP • [Unspecified] <p>(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。</p> 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。 <ul style="list-style-type: none"> • ICMP • [TCP] • UDP • [Unspecified] <p>(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。</p> 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 Network Controller 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 Network Controller 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 11: [コントラクトの作成 (Create Contract)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	<p>契約の名前を入力します。</p> <p>次の制約事項に注意してください。</p> <ul style="list-style-type: none"> 正規表現の一致: [az] ([-a-z0-9] * [a-z0-9]) ? <p>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。</p> <ul style="list-style-type: none"> 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 ルール名を作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、Google Cloud ファイアウォール ルールによる命名の長さの制限 (28 ページ) を参照してください。

[プロパティ (Properties)]	説明
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 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。
[設定 (Settings)]	
スコープ	<p>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。</p> <p>(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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • アプリケーション プロファイル • VRF • グローバル • テナント

[プロパティ (Properties)]	説明
フィルタの追加	<p>フィルタを選択します。</p> <ol style="list-style-type: none"> [フィルタの追加 (Add Filter)] をクリックします。フィルタ行が表示され、[フィルタの選択 (Select Filter)] オプションが表示されます。 [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。 [フィルタの選択 (Select Filter)] ダイアログで、左側の列のフィルタをクリックして選択し、[選択 (Select)] をクリックします。[コントラクトの作成 (Create Contract)] ダイアログボックスに戻ります。

ステップ5 設定が終わったら [Save] をクリックします。

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

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

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

[プロパティ (Properties)]	説明
名前 (Name)	<p>契約の名前を入力します。</p> <p>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]) ?</p> <p>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。</p>
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 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	<p>コントラクトの説明を入力してください。</p>
[設定 (Settings)]	
スコープ	<p>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。</p> <p>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。</p> <p>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。</p>

[プロパティ (Properties)]	説明
フィルタの追加	<p>フィルタを選択します。</p> <ol style="list-style-type: none"> [フィルタの追加 (Add Filter)] をクリックします。フィルタ行が表示され、[フィルタの選択 (Select Filter)] オプションが表示されます。 [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。 [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 ([ア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 Network Controller 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 通信 (EPG Communication)**] をクリックします。[**EPG 通信 (EPG Communication)**] ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

ステップ 4 コントラクトを選択します。

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

ステップ 5 コンシューマ EPG を追加するには、次の手順を実行します。

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

(注) テナント内 (契約が作成される) の EPG が表示されます。

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

ステップ 6 プロバイダー EPG を追加するには、次の手順を実行します。

- a) [プロバイダー EPG の追加 (Add Provider EPGs)] をクリックします。[プロバイダー EPG の選択 (Select Provider EPGs)] ダイアログが表示されます。
(注) テナント内 (契約が作成される) の EPG が表示されます。
- b) [プロバイダー EPG の選択 (Select Provider EPGs)] ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダー EPG を選択します。
(注) 選択したコントラクトがインポート済みコントラクトの場合、プロバイダー EPG の選択は無効になります。
- c) 完了したら、[選択 (Select)] をクリックします。[プロバイダー EPG の選択 (Select Provider EPGs)] ダイアログボックスが閉じ、[EPS コミュニケーション構成 (EPG Communication Configuration)] ウィンドウに戻ります。
- d) [保存 (Save)] をクリックします。

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

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

始める前に

VRF を作成します。

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

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

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

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

ステップ 4 次の [クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド (Create Cloud Context Profile 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 13:クラウドコントラクト プロファイルの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	クラウド コンテキスト プロファイルの名前を入力します。正規表現の一致: <code>[az]([-a-z0-9] * [a-z0-9]) ?</code> 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。 <ol style="list-style-type: none"> [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。 [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: <ol style="list-style-type: none"> [リージョンの選択 (Select Region)]をクリックします。[リージョンの選択 (Select Region)]ダイアログボックスが表示されます。 [リージョンの選択 (Select Region)]ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)]をクリックします。[クラウド コンテキスト プロファイルの作成 (Create Cloud Context Profile)]ダイアログボックスで、次の手順を実行します。
VRF	VRF を選択するには、次の手順を実行します。 <ol style="list-style-type: none"> [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。 [VRF の選択 (Select VRF)]ダイアログで、左側の列の VRF をクリックして選択し、[選択 (Select)]をクリックします。[クラウド コンテキスト プロファイルの作成 (Create Cloud Context Profile)]ダイアログボックスに戻ります。

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

[プロパティ (Properties)]	説明
	<p>(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、GCP の VPC とサブネット、Google Cloud および Cisco Cloud Network Controller のクラウドコンテキストプロファイルの理解 (23 ページ) を参照してください。</p> <p>CIDR を追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [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。 [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。 [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。 <ul style="list-style-type: none"> 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。 [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。 <ul style="list-style-type: none"> [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。 <ul style="list-style-type: none"> 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。 [VRF] フィールド で、必要に応じて選択します。 <ul style="list-style-type: none"> [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できなかった場合は、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。

[プロパティ (Properties)]	説明
	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 [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 Network Controller のためのエンドポイント セレクタを構成するとき Cisco Cloud Network Controller を構成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構成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 Network Controller のエンドポイント セレクタを構成する前に、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 \(20 ページ\)](#) を参照) 。

- Google Cloud のアカウントに移動し、最初に Google Cloud でカスタム タグまたはラベルを作成し、後で Cisco Cloud Network Controller 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 セレクタを作成できます。
- または、Cisco Cloud Network Controller 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 以降のカスタム 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 Network Controller 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 Google Cloud ユーザー テナントの Cisco Cloud Network Controller 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構成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 Network Controller 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 14: バックアップ構成の作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	バックアップ構成の名前を入力します。
説明	バックアップ構成の説明を入力します。
[設定 (Settings)]	
Backup Destination	バックアップ接続先を選択します。 <ul style="list-style-type: none">• ローカル• リモート

[プロパティ (Properties)]	説明
バックアップ オブジェクト	

[プロパティ (Properties)]	説明
	<p>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</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>2. Select <object_name> をクリックします。 Select <object_name> ダイアログが表示され</p>

[プロパティ (Properties)]	説明
	<p>ます。</p> <p>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。</p> <p>(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。</p> <p>• 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。</p> <p>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。</p>
スケジューラ	<p>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。</p> <p>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。</p>
作成後のバックアップのトリガー	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> • はい (Yes) : (デフォルト) バックアップ設定の作成後にバックアップをトリガーします。 • いいえ (No) : バックアップ設定の作成後にバックアップをトリガーしません。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller 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 15: テクニカル サポートの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	テクニカルサポートポリシーの名前を入力します。
説明	テクニカル サポートの説明を入力します。
[設定 (Settings)]	

[プロパティ (Properties)]	説明
エクスポート先	<p>エクスポート先を選択します。</p> <ul style="list-style-type: none"> • 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。 <ol style="list-style-type: none"> 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	<p>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。</p>

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用した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 Network Controller 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 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 16: スケジューラの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	トリガー スケジューラ ポリシーの名前を入力します。
説明	トリガーの説明を入力します。
[設定 (Settings)]	

[プロパティ (Properties)]	説明
繰り返しウィンドウ	

[プロパティ (Properties)]	説明
	<p>[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。</p> <ol style="list-style-type: none"> [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。 <ul style="list-style-type: none"> 毎日 (Every Day) 偶数日 (Even Days) 奇数日 (Odd Days) 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日 日曜日 [開始時間 (Start Time)] フィールドに、時間を入力します。 [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。 <ul style="list-style-type: none"> 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。 [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。 <ul style="list-style-type: none"> 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

[プロパティ (Properties)]	説明
	<p>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。</p> <p>5. 終了したら、[Add] をクリックします。</p>
ワンタイム ウィンドウの追加	<p>[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。</p> <ol style="list-style-type: none"> 1. [開始時間 (Start Time)] フィールドに、時間を入力します。 2. [最大同時タスク数 (Maximum Concurrent Tasks)] フィールドに数値を入力するか、フィールドを空白のままにして無制限を指定します。 3. [最大実行時間 (Maximum Running Time)] で、[無制限 (Unlimited)] または [カスタム (Custom)] をクリックして選択します。 4. 終了したら、[Add] をクリックします。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用してリモートの場所を作成する

このセクションでは、Cisco Cloud Network Controller を使用してリモートの場所を作成する方法を示します。

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 17: リモート ロケーションの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	リモート ロケーション ポリシーの名前を入力します。
説明	リモート ロケーション ポリシーの説明を入力します。
[設定 (Settings)]	
[ホスト名/IP アドレス (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
プロトコル	プロトコルを選択します。 <ul style="list-style-type: none"> • FTP • SFTP • SCP
パス	リモート ロケーションのパスを入力します。
[ポート (Port)]	リモート ロケーションのポートを入力します。
ユーザ名 (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 (Authentication Type)	SFTP または SCP を使用する場合は、認証タイプを選択します。 <ul style="list-style-type: none"> • [Password] • SSH キー (SSH Key)
SSH キー コンテンツ	SSH キーのコンテンツを入力します。
SSH キー パスフレーズ	SSH キー パスフレーズ
Password	リモート ロケーションにアクセスするためのパスワードを入力します。
Confirm Password	リモート ロケーションにアクセスするためのパスワードを再入力します。

ステップ5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したログイン ドメインの作成

このセクションでは、Cisco Cloud Network Controller 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 18: ログインドメインダイアログボックスの作成のフィールド

[プロパティ (Properties)]	説明
名前 (Name)	ログインドメインの名前を入力します。
説明	ログインドメインの説明を入力します。
レルム	レルムを選択します。 <ul style="list-style-type: none"> ローカル LDAP : プロバイダーを追加し、認証タイプを選択する必要があります。 RADIUS : プロバイダーを追加する必要があります。 TACACS+ : プロバイダーの追加が必要です。 SAML : プロバイダーの追加が必要です。

[プロパティ (Properties)]	説明
プロバイダ	<p>プロバイダーを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none">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 グループマッピングルール (LDAP Group Map Rules)] フィールドを表示します。
認証タイプ (Authentication Type)	<p>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。</p> <ul style="list-style-type: none">• Cisco AV ペア : (デフォルト)• LDAP グループマッピングルール : LDAP グループマッピングルールを追加する必要があります。

[プロパティ (Properties)]	説明
LDAP グループ マップ ルール	

[プロパティ (Properties)]	説明
	<p>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。</p> <ol style="list-style-type: none"> 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 : <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 1. [セキュリティ ドメインの追加 (Add Security Domain)] ダイアログボックスで、[ロールの選択 (Select Role)] をクリックします。[ロールの選択 (Select Role)] ダイアログボックスが表示され、左側のペインにロールのリストが表

[プロパティ (Properties)]	説明
	<p>示されます。</p> <ol style="list-style-type: none"> 2. クリックしてロールを選択します。 3. [選択 (Select)] をクリックしてロールを追加します。 [セキュリティ ドメインの追加 (Add Security Domain)] ダイアログボックスに戻ります。 4. [セキュリティ ドメインの追加 (Add Security Domain)] ダイアログボックスから、 [権限タイプ (Privilege Type)] ドロップダウンリストをクリックして、 [読み取り権限 (Read Privilege)] または [書き込み権限 (Write Privilege)] を選択します。 5. [権限タイプ (Privilege Type)] ドロップダウンリストの右側のチェックマークをクリックして、確認します。 6. 終了したら、 [Add] をクリックします。 [LDAP グループ マップ ルールの追加 (Add LDAP Group Map Rule)] ダイアログボックスに戻り、別のセキュリティ ドメインを追加できます。

ステップ 5 設定が終わったら **[Save]** をクリックします。

Cisco Cloud Network Controller 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 [Intent (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 [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したロールの作成

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

ステップ 1 Intent アイコンをクリックします。[Intent (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 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 19: ロールの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	[Name] フィールドにロール名を入力します。
説明	ロールの説明を入力します。
[設定 (Settings)]	

[プロパティ (Properties)]	説明
特権	

[プロパティ (Properties)]	説明
	<p>をクリックして、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。</p> <ul style="list-style-type: none"> • aaa : 認証、許可、アカウントティング、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 1~3 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 1~3 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 1~3 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 1~3 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。

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • 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 1-3 の接続変更で使用されます。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 1-3 プロトコルの管理、および traceroute、ping、oam、eprtk などのデバッグ/モニタリング/オブザーバ ポリシーに使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。 • tenant-network-profile : ネットワーク プロファイルの削除および作成、エンドポイントグループの削除および作成など、テナント設定の管理に使用されます。 • tenant-protocol : テナント下のレイヤ 1-3 プロトコルの設定、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 [Save] をクリックします。

Cisco Cloud Network Controller 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 20: 証明書認証局の作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	証明書認証局の名前を入力してください。
説明	証明書認証局の説明を入力してください。
コントローラ	次のオプションから選択します。 <ul style="list-style-type: none"> • 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。 <ol style="list-style-type: none"> 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。

[プロパティ (Properties)]	説明
[証明書チェーン (Certificate Chain)]	<p>[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。</p> <p>(注) チェーンの証明書を次の順序で追加します。</p> <ol style="list-style-type: none"> 1. CA 2. Sub-CA 3. サブサブCA 4. サーバ

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したキーリングの作成

このセクションでは、Cisco Cloud Network Controller 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 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 21: キーリングの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
説明	キー リングの説明を入力します。
コントローラ	<ul style="list-style-type: none"> • 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	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 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。
[設定 (Settings)]	
認証局	<p>認証局を選択するには :</p> <ol style="list-style-type: none"> 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	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> • [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。

[プロパティ (Properties)]	説明
秘密キー	[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)。
モジュール	[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。 <ul style="list-style-type: none"> • MOD 512 • MOD 1024 • MOD 1536 • MOD 2048 : デフォルト
認証	[証明書 (Certificate)] テキスト ボックスに証明書情報を入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller 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、Cisco Cloud Network Controller GUI を使用してローカル ユーザーを作成する例を示します。

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 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 22: ローカルユーザーの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
ユーザー名 (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。

[プロパティ (Properties)]	説明
説明	ローカル ユーザーの説明を入力します。
[設定 (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。 <ul style="list-style-type: none">• 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	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	ローカル ユーザーの E メール アドレスを入力します。
電話番号 (Phone Number)	ローカル ユーザーの 電話番号を入力します。

[プロパティ (Properties)]	説明
セキュリティドメイン	

[プロパティ (Properties)]	説明
	<p>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。</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 1. [セキュリティドメインの追加 (Add Security Domain)]ダイアログボックスで、[ロールの選択 (Select Role)]をクリックします。[ロールの選択 (Select Role)]ダイアログボックスが表示され、左側のペインにロールのリストが表示されます。 2. クリックしてロールを選択します。 3. [選択 (Select)]をクリックしてロールを追加します。[セキュリティドメインの追加 (Add Security Domain)]ダイアログボックスに戻ります。 4. [セキュリティドメインの追加 (Add Security Domain)]ダイアログボックスから、[権限タイプ (Privilege Type)]ドロップダウンリストをクリックして、[読み取り権限 (Read Privilege)]または[書き込み権限 (Write Privilege)]を選択します。 5. [権限タイプ (Privilege Type)] ドロップダウンリストの右側のチェックマークをクリッ

[プロパティ (Properties)]	説明
	<p>クして、確認します。</p> <p>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。</p>

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 Dialog 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 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：高度な設定

プロパティ	説明
アカウント期限切れ	[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	<p>ユーザー証明書を追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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. [名前 (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. [追加 (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	<p>SSH キーを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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. [名前 (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. [追加 (Add)] をクリックします。[SSH キーの追加 (Add SSG Key)] ダイアログボックスが閉じます。[ローカル ユーザー] ダイアログボックスに戻ります。

ステップ 6 設定が終わったら **[Save]** をクリックします。

Cisco Cloud Network Controller 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構成）

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は Google Cloud で管理され、リージョン間接続が存在します。Cisco Cloud Network Controller 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、**[Cisco Cloud Network Controller の設定 (Cisco Cloud Network Controller 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]** のオプションが表示されます。

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 外部接続を設定するかどうかを決定します。

[有効 (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、Cisco Cloud Network Controller 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 でハブ 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 で 1 つのクラウドルータのみが作成されます。
- a) **[ハブ ネットワーク (Hub Network)]** 領域で、**[ハブ ネットワークの追加 (Add Hub Network)]** をクリックします。
- [ハブ ネットワークの追加 (Add Hub Network)]** ウィンドウが表示されます。
- b) **[名前 (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 は秘密 ASN である必要があります。各ハブ ネットワークに 64512~65534 または 4200000000~4294967294 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 ツールの追加 (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を入力したら、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 Network Controller GUI を使用したクラウドネイティブルータによる外部ネットワークの作成 \(64 ページ\)](#) にアクセスしてください。

REST API を使用した Cisco Cloud Network Controller 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、[Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する \(8 ページ\)](#) 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-network-controller-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="cnc-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="cnc-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
  </fvTenant>

```

ステップ 2 Cisco Cloud Network Controller が Google Cloud 外部で実行されているユーザー テナント（資格情報を持つインフラ 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-network-controller-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="cnc-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-network-controller-ip-address>/api/mo/uni.xml

```

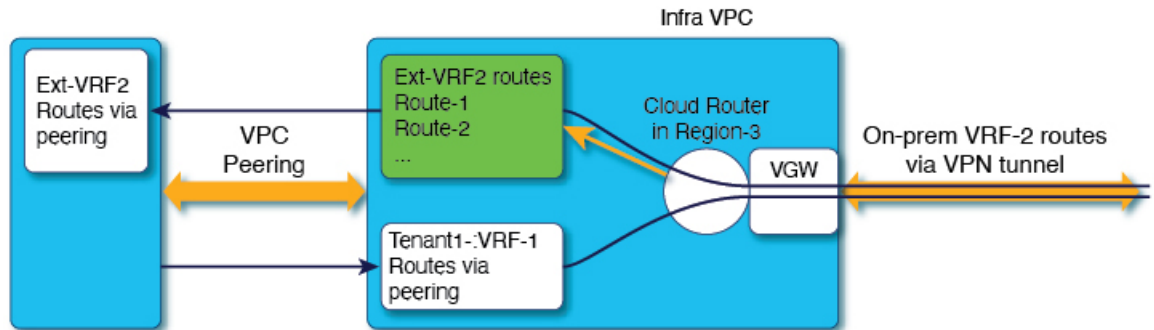
  <fvTenant name="infra">
    <cloudAccount id="project1" vendor="gcp" accessType="managed" />
    <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
  </fvTenant>

  <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 Cisco Cloud Network Controller のルート リーク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。



Subnet1 (Region-1) Route-Table

CIDR1 (Region-1) - 100.100.0.0/16
Subnet1 - 100.100.100.0/24

100.100.0.0/16 -> Local
50.50.0.0/16 -> Infra-VPC

Leak-All-routes to
Tenant-Infra:Ext-RF-2

503863

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=""/>
        </leakExternalPrefix>
      </leakRoutes>
    </fvCtx>
  </fvTenant>
```

```

        </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 Network Controller 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:

```
[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 ルール名を作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、[Google Cloud ファイアウォール ルールによる命名の長さの制限 \(28 ページ\)](#) 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>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>
```

```

    </cloudSubnet>
    <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
      <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
    </cloudSubnet>
    <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="vpcl" status="">
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-centrall" 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-centrall/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-centrall/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:

```
[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 ルール名を作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、[Google Cloud ファイアウォール ルールによる命名の長さの制限 \(28 ページ\)](#) 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:

```
[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作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、[Google Cloud ファイアウォールルールによる命名の長さの制限 \(28 ページ\)](#) 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:

```
[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作成する各 Cisco Cloud Network Controller コンポーネントに許可されている制限と合計文字数をより理解するには、[Google Cloud ファイアウォールルールによる命名の長さの制限 \(28 ページ\)](#) 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" />

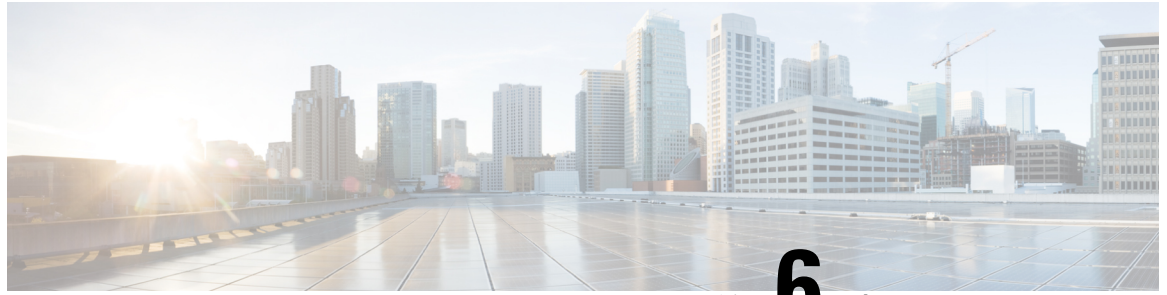
      <cloudtemplateHubNetwork name="default" status="" >
        <cloudtemplateHubNetworkName name="fool" asn="64514" status="">
          <cloudRegionName provider="gcp" region="us-west4" status="" />
          <cloudRegionName provider="gcp" region="us-west2" status="" />
          <cloudRegionName provider="gcp" 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="extnwfool" vrfName="extv1" hubNetworkName="fool"
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="fool"
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="fool"
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 (147 ページ)
- アプリケーション管理詳細の表示 (150 ページ)
- クラウドリソースの詳細の表示 (152 ページ)
- 操作の詳細の表示 (153 ページ)
- インフラストラクチャの詳細の表示 (156 ページ)
- 管理の詳細の表示 (156 ページ)
- Cisco Cloud Network Controller GUI を使用したヘルス詳細の表示 (159 ページ)

VM ホスト メトリックのモニタリング

Prometheus Node Exporter を使用して Cisco Cloud ネットワーク コントローラが展開されている場所で 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 ノードエクスポートの概要については、以下を参照してください。

<https://prometheus.io/docs/introduction/overview/>

Cisco Cloud ネットワーク コントローラがリリース 25.0(1)以降で実行されている場合、Prometheus Node Exporter はデフォルトで自動的に使用可能になります。

ガイドラインと制約事項

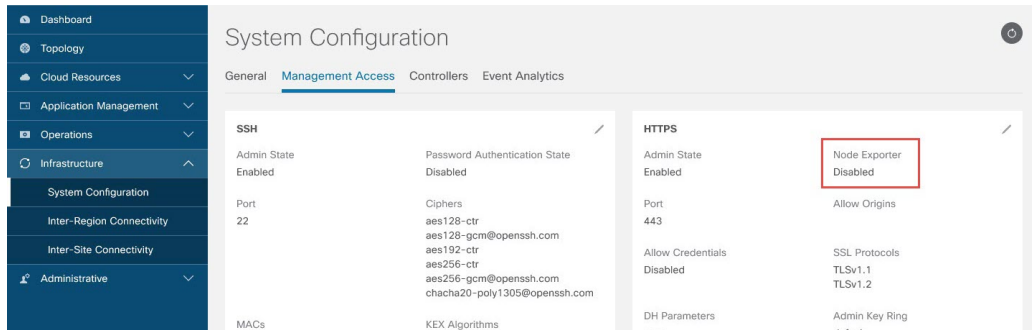
HTTP は、Prometheus Node Exporter を使用したモニタリングメトリックではサポートされていません。Prometheus Node Exporter を使用したメトリックのモニタリングでは、HTTPS のみがサポートされます。

GUI を使用した VM ホストメトリックのモニタリング

次の手順では、GUI を使用して Prometheus Node Exporter で VM ホストメトリックをモニタできるようにする方法について説明します。

ステップ 1 Cisco Cloud Network Controller GUI で、[インフラストラクチャ (Infrastructure)] > [システム構成 (System Configuration)] に移動し、[管理アクセス (Management Access)] タブをクリックします。

ステップ 2 ウィンドウの右側の [HTTPS] 領域で、[ノード エクスポート (Node Exporter)] フィールドのエントリを確認します。

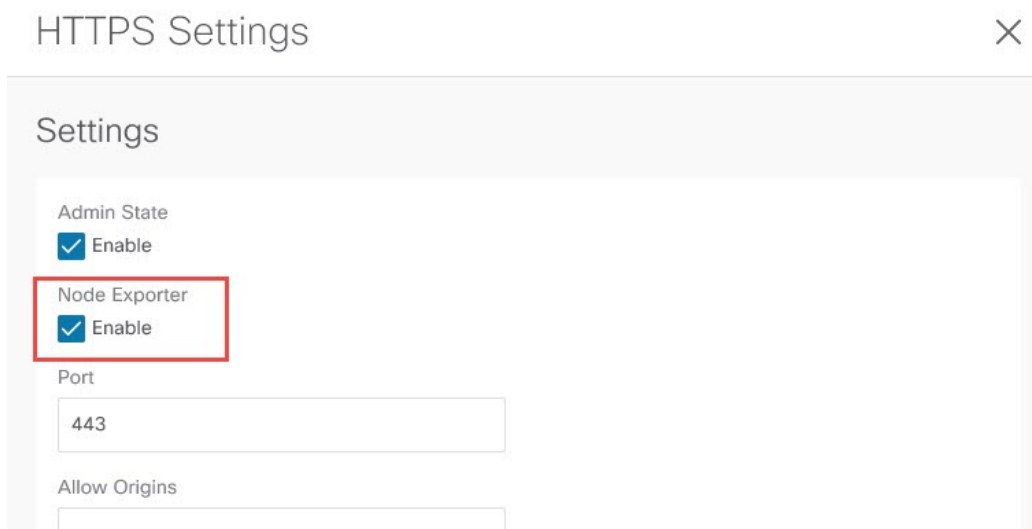


- **有効化 (Enabled)** : Prometheus Node Exporter はすでに有効になっています。この場合、これらの手順を続行する必要はありません。
- **無効化 (Disabled)** : Prometheus Node Exporter はまだ有効になっていません。Prometheus Node Exporter を有効にするには、次の手順に従います。

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 エクスポート (Node Exporter)] フィールドを見つけ、[有効化 (Enable)] をクリックします。



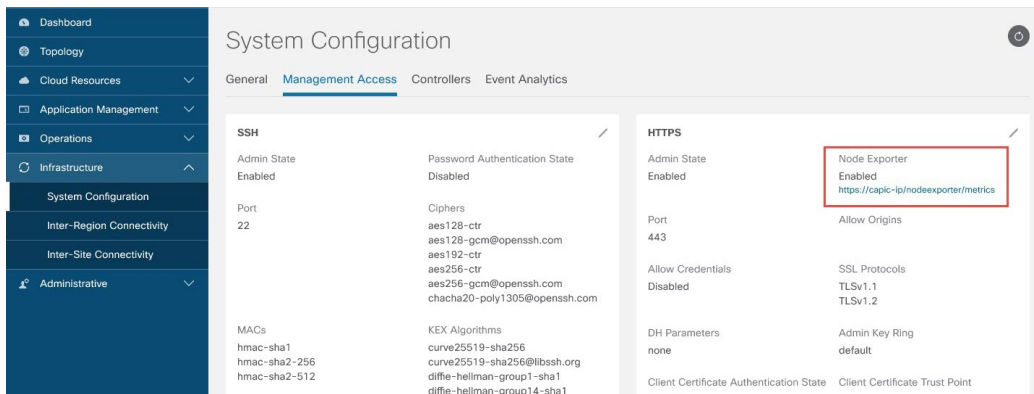
これらの設定を保存すると Web サービスが再起動され、要求への応答が再開されるまで少し時間がかかることを示す警告メッセージが表示されます。[OK] をクリックして、変更内容を確定します。

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 エクスポート (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 エクスポート (Node Exporter)] 領域の [有効化 (Enabled)] テキストの下にあるリンクをクリックします。

ブラウザに別のタブが表示され、Cisco Cloud Network Controller が展開されている VM ホストのメトリックが表示されます。

REST API を使用した VM ホストメトリックスの監視

これらの手順では、REST API を使用して VM ホストメトリックを監視するように Prometheus Node Exporter を有効にする方法について説明します。

ステップ 1 Prometheus Node Exporter が有効になっているかどうかを確認するには、次の GET コールを送信します。

```
GET https://<cloud-network-controller-ip-address>/api/mo/uni/fabric/comm-default/https.xml
```

nodeExporter フィールドを見つけて、有効または無効に設定されているかどうかを確認します。

ステップ 2 VM ホストメトリックを監視するには、次の投稿を送信して、Prometheus ノードエクスポートを有効にします。

```
POST https://<cloud-network-controller-ip-address>/api/mo/uni/fabric/comm-default/https.xml
```

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

メトリックスは、Cisco Cloud Network Controller が展開されている VM ホストに表示されます。

ステップ3 REST API を使用してメトリックを表示するには、次の GET コールを送信します。

```
GET https://<cloud-network-controller-ip-address>/nodeexporter/metrics
```

ステップ4 Prometheus ノード エクスポートを無効にするには、次の投稿を送信します。

```
POST https://<cloud-network-controller-ip-address>/api/mo/uni/fabric/comm-default/https.xml
<commHttps nodeExporter="disabled" />
```

アプリケーション管理詳細の表示

ここでは、Cisco Cloud Network Controller GUI を使用してアプリケーション管理の詳細を表示する方法について説明します。アプリケーション管理の詳細には、特定のテナント、アプリケーションプロファイル、EPG、コントラクト、フィルタ、VRF、サービス、またはクラウドコンテキストプロファイルの情報が含まれます。

ステップ1 [ナビゲーション (Navigation)] メニューで、[アプリケーション管理 (Application Management)] タブを選択します。

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。詳細については、「アプリケーション管理オプション」のテーブルを参照してください。

表 24: アプリケーション管理サブタブ

サブタブ名	説明
テナント	テナントをサマリー テーブルの行として表示します。
アプリケーション プロファイル	サマリー テーブルの行としてアプリケーション プロファイルを表示します。
EPG	EPG をサマリー テーブルの行として表示します。
契約	コントラクトをサマリー テーブルの行として表示します。
フィルタ (Filters)	サマリー テーブルの行としてフィルタを表示します。
VRF	サマリー テーブルの行として VRF を表示します。

サブタブ名	説明
Services	次の 2 つのサブタブと情報が含まれています。 <ul style="list-style-type: none"> • デバイス : サマリーテーブルの行としてデバイスを表示します。 • サービス グラフ : サービス グラフをサマリーテーブルの行として表示します。
クラウド コンテキスト プロファイル	クラウド コンテキスト プロファイルをサマリーテーブルの行として表示します。

ステップ 2 表示する詳細のコンポーネントを表すタブをクリックします。

サマリーテーブルには、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。

属性によるフィルタ処理バーをクリックすることにより、行をフィルタ処理できます。属性、演算子、およびフィルタ値を選択します。たとえば、テナントに基づくフィルタリングの場合は、[Name] == T1 (T1 はテナントの名前) を選択します。

ステップ 3 サマリー ペインを表示するには、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。
- **統計 (Statistics)** : 選択したサンプリング間隔と統計情報タイプに基づいて統計情報を表示できます。**[統計 (Statistics)]** タブには、表示しているコンポーネントに応じてサブタブが表示されます。
- **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 Network Controller GUI を使用してクラウドリソースの詳細を表示する方法について説明します。クラウドリソースの詳細には、特定のリージョン、VNET、ルータ、セキュリティグループ（アプリケーションセキュリティグループ/ネットワークセキュリティグループ）、エンドポイント、VM、およびクラウドサービスに関する情報が含まれます。

[クラウドタグ（Cloud Tag）] 属性に基づく検索が[エンドポイント（Endpoints）]のサブタブをサポートしています。

ステップ 1 [ナビゲーション（Navigation）]メニューから[クラウドリソース（Cloud Resources）]タブを選択します。

[クラウドリソース（Cloud Resources）]タブが展開すると、サブオプションオプションのリストが表示されます。詳細については、「*Cloud Resource Options*」の表を参照してください。

表 25:クラウドリソースサブタブ

サブタブ名	説明
地域	リージョンをサマリーテーブルの行として表示します。
仮想ネットワーク	サマリーテーブルの行として VNET を表示します。
ルータ	ルータをサマリーテーブルの行として表示します。
セキュリティグループ	サマリーテーブルの行としてセキュリティを表示します。
エンドポイント	エンドポイントをサマリーテーブルの行として表示します。
仮想マシン	VM をサマリーテーブルの行として表示します。
クラウドサービス	次のサブタブを含みます。 <ul style="list-style-type: none"> • [クラウドサービス（Cloud Service）] タブ：クラウドサービスをサマリーテーブルの行として表示します。 • [ターゲットグループ] タブ：ターゲットグループをサマリーテーブルの行として表示します。

ステップ 2 表示する詳細のコンポーネントを表すタブをクリックします。

サマリーテーブルには、項目が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。 [エンドポイントに関連付けられたクラウドタグも表示されます。 (The cloud tags associated with endpoints are also displayed.)]
- **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。
- **統計 (Statistics)** : 選択したサンプリング間隔と統計情報タイプに基づいて統計情報を表示できます。 [統計 (Statistics)]タブには、表示しているコンポーネントに応じてサブタブが表示されます。
- **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。

操作の詳細の表示

ここでは、Cisco Cloud Network Controller 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 26: [操作 (Operations)] サブタブ

サブタブ名	説明
イベント分析	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [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。 • [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。
アクティブなセッション	Cisco Cloud Network Controller にログインしているアクティブ ユーザーのリストを表示します。
バックアップと復元	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [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。 <ul style="list-style-type: none"> • [障害 (Faults)] タブ: サマリー テーブルの行として障害を表示します。 • [イベント (Events)] タブ: イベントをサマリー テーブルの行として表示します。 • [監査ログ (Audit Logs)] タブ: 監査ログをサマリー テーブルの行として表示します。

サブタブ名	説明
テクニカル サポート	次のサブタブを含みます。 <ul style="list-style-type: none"> • [Tech Support] タブ：テクニカルサポート ポリシーをサマリー テーブルの行として表示します。 • [コア ログ (Core Logs)] タブ：コア ログをサマリー テーブルの行として表示します。
Firmware Management	次のサブタブを含みます。 <ul style="list-style-type: none"> • [全般 (General)] タブ：現在のファームウェアバージョン、アップグレードステータスなどの一般的なファームウェア管理情報が表示されます。 • [イメージ (Images)] タブ：イメージのリストを表示します。 • [イベント分析 (Event Analytics)] タブ：次のサブタブが含まれます。 <ul style="list-style-type: none"> • [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 Cisco Cloud Network Controller 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 Network Controller 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せん。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 27: インフラストラクチャ サブタブ

サブタブ名	説明
システム設定	[全般 (General)] システム構成情報、[管理アクセス (Management Access)] 情報、[コントローラ (Controllers)]、[クラウドリソース名前付けルール (Cloud Resource Naming Rules)]、[イベント分析 (Event Analytics)] を表示します。
リージョン間接続	リージョン間接続ビューおよび各リージョンの追加ペインを含むマップを1つのペインに表示します。
サイト間接続	サイト間接続ビューおよび各サイトの追加ペインを含むマップを1つのペインに表示します。

ステップ 2 表示する詳細を含むコンポーネントを表すタブをクリックします。

管理の詳細の表示

ここでは、Cisco Cloud Network Controller 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 28: 管理サブタブ

サブタブ名	説明
認証	<p>[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。</p> <ul style="list-style-type: none"> • [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	<p>次のサブタブのリストが含まれます。</p> <ul style="list-style-type: none"> • [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。
ユーザー数	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [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	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [一般 (General)] タブ : ライセンスをサマリー テーブルの行として表示します。 • [CCR] タブ : CCR をサマリー テーブルの行として表示します。 • [障害 (Faults)] タブ : 障害をサマリー テーブルの行として表示します。

ステップ 2 表示するコンポーネントを表すタブをクリックします。

一部のオプションでは、サマリーテーブルに項目がテーブル内の行として表示されます (たとえば、[ユーザー (Users)] タブを選択した場合、ユーザーのリストはサマリー テーブルに行として表示されます)。

サマリーペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。詳細を表示するには、表示する特定の項目を表すサマリーテーブルの行をダブルクリックします。作業ウィンドウに新しいダイアログボックスが表示され、サマリーテーブルから選択した項目に関する追加情報が表示されます。

属性によるフィルタ処理バーをクリックすることにより、行をフィルタ処理できます。属性、演算子、およびフィルタ値を選択します。たとえば、ユーザーに基づいてフィルタリングする場合は、[User ID == admin] を選択します (admin はユーザー ID です)。

Cisco Cloud Network Controller GUI を使用したヘルス詳細の表示

ここでは、Cisco Cloud Network Controller GUI を使用して正常性の詳細を表示する方法について説明します。Cisco Cloud Network Controller GUI のクラウドリソース エリアで確認できるオブジェクトの正常性の詳細は、次のように表示できます。

- 地域
- アベイラビリティゾーン (AWS クラウド サイトの場合)
- VPC (AWS クラウド サイト用)
- VNET (Azure クラウド サイト用)
- ルータ
- セキュリティグループ
- エンドポイント
- Instances
- クラウド サービス

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

Cisco Cloud Network Controller の [ダッシュボード (Dashboard)] ビューを表示します。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。

Cisco Cloud Network Controller GUI を使用したヘルス詳細の表示

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。

Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
<input type="checkbox"/>	Critical	F0104	topology/pod-1/node-1/sys/caggr-[po1]	Bond Interface po1 on node 1 of fabric mininet with hostname capic1 is now down	raised	Sep 11 2019 05:22:33pm
<input type="checkbox"/>	Critical	F0104	topology/pod-1/node-1/sys/caggr-[po1]	Bond Interface po1 on node 1 of fabric mininet with hostname capic1 is now down	raised	Sep 11 2019 05:22:33pm

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。

Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
No	Critical	F0104	topology/pod-1/node-1/phys/agg-[po1.1]	Bond interface po1 on node 1 of fabric mininet with hostname capic1 is now down	raised	Sep 11 2019 05:22:33pm
No	Critical	F0104	topology/pod-1/node-1/phys/agg-[po1.1]	Bond interface po1 on node 1 of fabric mininet with hostname capic1 is now down	raised	Sep 11 2019 05:22:33pm
No	Major	F3442	acct-[infra]region-[eastus]context-[overly-1]-addr-[10.10.0.128/25]csr-[ct_routers_eastus_1_0]/nsdoper	Operational State of the hcloudInstanceOper is down with [compute.VirtualMachineClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceNotFound" Message="Resource group 'CAPIC-infra-mininet-kchazel-centralus' could not be found. "]	raised	Sep 11 2019 07:38:27pm
No	Major	F3442	acct-[infra]region-[centralus]context-[overly-1]-addr-[10.10.0.0/25]csr-[ct_routers_centralus_1_0]/nsdoper	Operational State of the hcloudInstanceOper is down with [compute.VirtualMachineClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceNotFound" Message="Resource group 'CAPIC-infra-mininet-kchazel-centralus' could not be found. "]	raised	Sep 11 2019 07:38:27pm
No	Major	F3442	acct-[infra]region-[eastus]context-[overly-1]-addr-[10.10.0.128/25]csr-[ct_routers_eastus_1_0]/nsdoper	Operational State of the hcloudInstanceOper is down with [compute.VirtualMachineClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceNotFound" Message="Resource group 'CAPIC-infra-mininet-kchazel-centralus' could not be found. "]	raised	Sep 11 2019 07:38:27pm
No	Major	F3442	acct-[infra]region-[centralus]context-[overly-1]-addr-[10.10.0.0/25]csr-[ct_routers_centralus_1_0]/nsdoper	Operational State of the hcloudInstanceOper is down with [compute.VirtualMachineClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceNotFound" Message="Resource group 'CAPIC-infra-mininet-kchazel-centralus' could not be found. "]	raised	Sep 11 2019 07:45:10pm
No	Major	F3527	acct-[infra]region-[eastus]context-[overly-1]-addr-[10.10.0.128/25]csr-[ct_routers_eastus_0_0]/license/oper	Operational State of the HcpPlatformLicense is down with administrative-down	raised	Sep 11 2019 05:21:24pm
No	Major	F3527	acct-[infra]region-[centralus]context-[overly-1]-addr-[10.10.0.0/25]csr-[ct_routers_centralus_1_0]/license/oper	Operational State of the HcpPlatformLicense is down with administrative-down	raised	Sep 11 2019 05:21:35pm
No	Major	F0101	topology/pod-1/node-1/phys/ctrl-[1]dev/vdb	Storage unit (dev/vdb) on node 1 with hostname capic1 has failed.	raised	Sep 11 2019 05:22:33pm

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

[クラウドリソース (Cloud Resources)]タブが展開すると、サブオプションオプションのリストが表示されます。詳細については「Administrative Options」の表を参照してください。

ステップ 5 [クラウドリソース (Cloud Resources)]タブで任意の項目を選択すると、そのコンポーネントのヘルス情報が表示されます。

たとえば、次の図は、[クラウドリソース (Cloud Resources)]>[リージョン (Regions)]をクリックしたときに表示される可能性のあるヘルス情報を示しているため、特定のリージョンを選択します。

Name	Admin State	Tenants	EPGs	AZs	Virtual Networks
eastus	managed	N/A	N/A	N/A	N/A
eastus2	managed	N/A	N/A	N/A	N/A
westus	managed	N/A	N/A	N/A	N/A
centralus	managed	N/A	N/A	N/A	N/A
koreasouth	unmanaged	N/A	N/A	N/A	N/A
francecentral	unmanaged	N/A	N/A	N/A	N/A
eastasia	unmanaged	N/A	N/A	N/A	N/A
canadeseast	unmanaged	N/A	N/A	N/A	N/A
brazilsouth	unmanaged	N/A	N/A	N/A	N/A
australiaeast	unmanaged	N/A	N/A	N/A	N/A
australiascentral2	unmanaged	N/A	N/A	N/A	N/A
koreacentral	unmanaged	N/A	N/A	N/A	N/A
ukwest	unmanaged	N/A	N/A	N/A	N/A
southindia	unmanaged	N/A	N/A	N/A	N/A
southeastasia	unmanaged	N/A	N/A	N/A	N/A

Cloud Provider's Region: eastus

Critical	Major	Minor	Warning
0	0	0	0

General

Region: region-eastus

Usage

0 Total

Settings

Admin State: Managed

Oper State: In use

Account: infra

Cloud Provider ID: ct_ctxprofile_eastus



第 7 章

Cisco Cloud Network Controller 統計情報

- [Google Cloud 統計について](#) (163 ページ)
- [Guidelines and Limitations For Configuring Google Cloud Statistics](#) (164 ページ)
- [Viewing Router Statistics](#) (164 ページ)
- [Enabling Flow Log Statistics](#) (167 ページ)
- [フロー ログ統計の表示](#) (168 ページ)
- [REST API を使用した VPC フロー ログの有効化](#) (170 ページ)

Google Cloud 統計について

Cisco Cloud Network Controller リリース 25.0(4) 以降、Google Cloud フロー ログを処理することによって得られた統計を表示できます。

Cisco Cloud Network Controller リリース 25.0(5) 以降、Cisco Catalyst 8000V ルータから収集された統計を表示できます。

Router Statistics

Cisco Cloud Network Controller を使用すると、テナント内の個々のクラウド コンテキスト プロファイルのルータ統計を表示できます。クラウド コンテキスト プロファイル内の Cisco Catalyst 8000V ルータの統計が表示されます。

各ルーター インスタンスは、物理インターフェースとトンネルインターフェースごとに、入力および出力のバイトとパケットの統計をキャプチャして保存します。The Cisco Cloud Network Controller queries the routers for these statistics and maps the response to router statistics on the Cisco Cloud Network Controller. 統計クエリは、トンネルが稼働している限り、5 分ごとに繰り返されます。Cisco Cloud Network Controller GUI には、ルータについて収集された統計が表示されます。

Flow Log Statistics

Cisco Cloud Network Controller を使用すると、テナント内の個々のクラウド コンテキスト プロファイルのフロー ログ統計を有効にすることができます。クラウド コンテキスト プロファイルの統計が有効になっている場合、対応する VPC 内のすべての IP アドレスの統計が収集され

まず、使用可能な統計には、VPC、リージョン、およびエンドポイントの、内部および外部の入力および出力のバイトとパケットが含まれます。

収集された統計は、次の階層を介して集計されます。

- IP 統計は、エンドポイント統計を決定するために集約されます。
- エンドポイント統計は、ゾーン統計を決定するために集約されます。
- ゾーンの統計は、サブネットの統計を決定するために集約されます。
- サブネット統計は、リージョン統計を決定するために集約されます。
- リージョン統計は、VPC 統計を決定するために集約されます。

Cisco Cloud Network Controller GUI には、VPC、リージョン、およびエンドポイントの収集された統計が表示されます。

For more information about Google Cloud flow logs, see "VPC Flow Logs" on the Google Cloud website.

Guidelines and Limitations For Configuring Google Cloud Statistics

Following are the guidelines and limitations when configuring Cisco Cloud Network Controller to collect Google Cloud statistics:

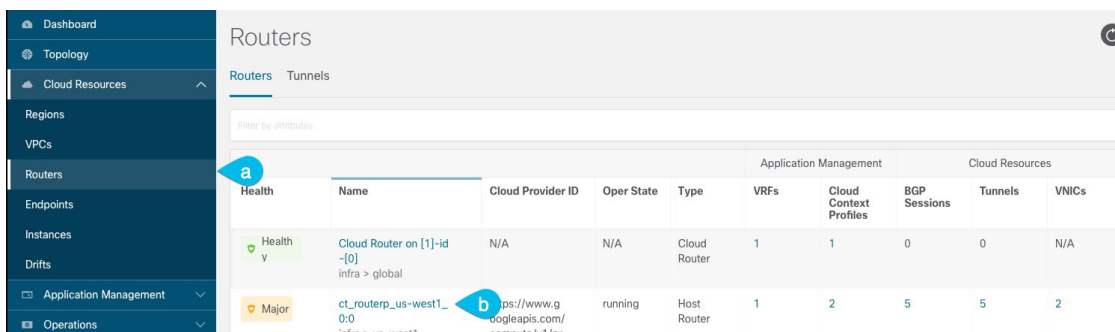
- ルータ統計は、Cisco Catalyst 8000V ルータが Cisco Cloud Network Controller で起動されると、デフォルトで有効になります。
- フロー ログ統計機能は、デフォルトでは有効になっていません。
- フロー ログ統計は、テナント内の個々のコンテキスト プロファイルに対して有効にすることができます。この場合、対応する VPC に属するすべてのサブネットでフロー ログが有効になります。
- フロー ログは 1 分間隔で集計されます。集計間隔とサンプル レートは構成できません。
- ドロップされたトラフィックの統計は、フロー ログではサポートされていません。
- 統計フィルターはサポートされていません。
- ゾーンとサブネットの統計は表示されません。

Viewing Router Statistics

Cisco Cloud Network Controller GUI では、Cisco Catalyst 8000V ルータのグラフ化された統計を表示できます。各ルーターで利用可能な統計には、イングレスとエグレスのバイトとパケットが含まれます。各カウンターのピーク値は、ピーク値がいつ発生したかを示すタイムスタンプとともに表示されます。

この手順例は、Cisco Cloud Network Controller GUI でルータの統計を表示する方法を示しています。

ステップ 1 統計を表示する Cisco Catalyst 8000V ルータを選択します。



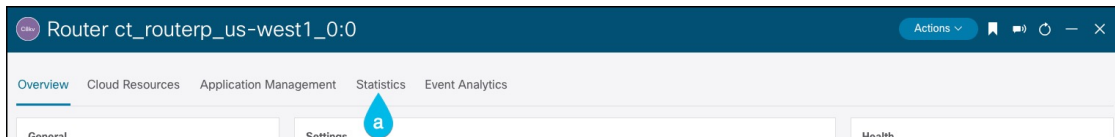
a) ナビゲーションメニューから [Cloud Resources Routers] を選択します。 >

Routers サマリーテーブルが作業ペインに表示されます。

b) サマリーテーブルで、ルーターの名前をダブルクリックします。

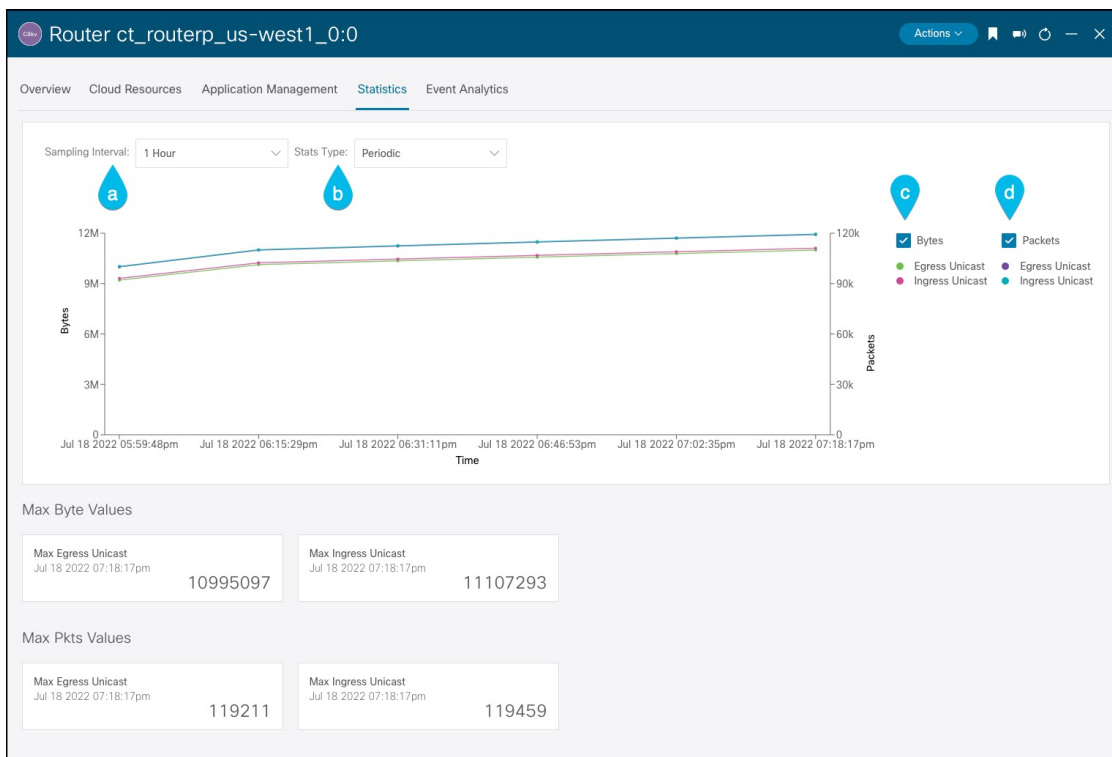
The router dialog box appears over the work pane. The router dialog box displays the **Overview**, **Cloud Resources**, **Application Management**, **Statistics**, and **Event Analytics** tabs.

ステップ 2 [Statistics] タブをクリックします。



最大値の表とともに、ルータ統計のグラフィカルビューが表示されます。

Viewing Router Statistics



ステップ 3 統計の表示を構成します。

表示される統計のパラメータを構成するには、次の設定を変更します。

【プロパティ (Properties)】	説明
サンプリング間隔	間隔を選択してください: <ul style="list-style-type: none"> • 1 時間 • 12時間 • 1日 • 週 1 回 • 1ヵ月
Stats Type	表示タイプを選択します。 <ul style="list-style-type: none"> • 定期 • 累計 • パフォーマンスの • 利率

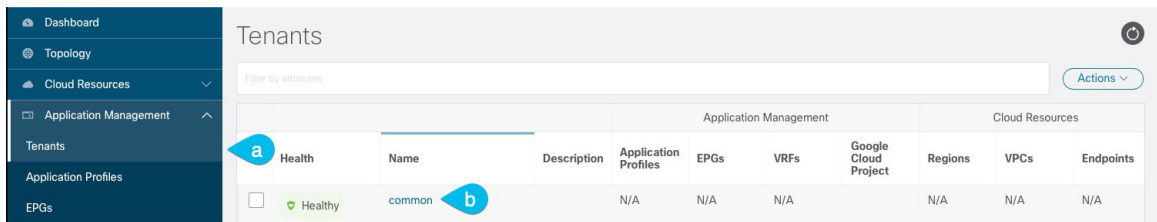
[プロパティ (Properties)]	説明
Bytes	チェックボックスを選択すると、バイトカウンターのグラフが表示されます。グラフの左側の縦軸はバイト数を示しています。
Packets	チェックボックスを選択すると、パケットカウンターのグラフが表示されます。グラフ右側の縦軸はパケット数を示しています。

Enabling Flow Log Statistics

テナント内の個々のコンテキスト プロファイルの Google Cloud フロー ログ統計の収集を有効にすることができます。その後、それぞれのクラウドリソース GUI メニューで VPC、リージョン、およびエンドポイントの統計を表示できます。

To enable flow log statistics using the Cisco Cloud Network Controller GUI:

ステップ 1 フロー ログ統計を有効にするリソースを含むテナントを選択します。



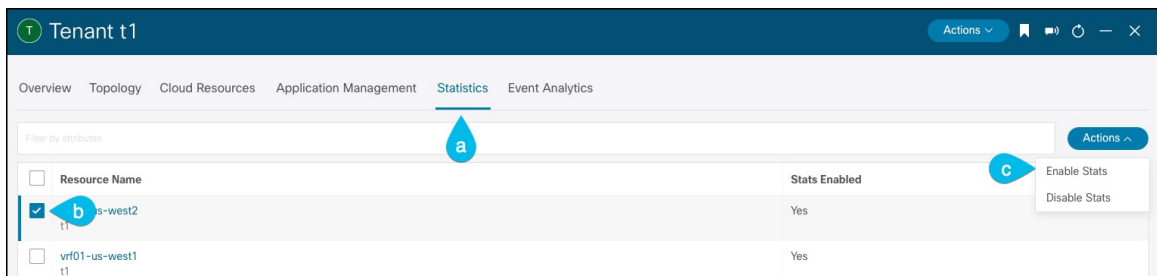
a) From the navigation menu, select **Application Management > Tenants**.

作業ウィンドウにテナント サマリー テーブルが表示されます。

b) サマリー テーブルで、テナントの名前をダブルクリックします。

The tenant dialog box appears over the work pane. The tenant dialog box displays the **Overview**, **Topology**, **Cloud Resources**, **Application Management**, **Statistics**, and **Event Analytics** tabs.

ステップ 2 目的のリソースでフロー ログ統計収集を有効にします。



a) テナント ダイアログ ボックスで、[統計] タブを選択します。

リソース名テーブルが表示され、コンテキスト プロファイルがテーブルの行としてリストされます。Stats Enabled 列は、各リソースに対してフロー ログ統計が有効になっているかどうかを示します。

- b) Check the checkbox next to the desired resource.
- c) テナント ダイアログ ボックスの右上で、[アクション] メニューをクリックし、[統計を有効にする] を選択します。

フロー ログ統計の表示

Cisco Cloud Network Controller GUI では、VPC、リージョン、およびエンドポイントのグラフ化された統計を表示できます。それぞれの利用可能な統計には、入力と出力のバイトとパケットが含まれます。VPC とリージョンの場合、統計はさらに次のカテゴリに分類されます。

- 統計: フロー ログ レコードから抽出されたすべてのトラフィック カウンター。
- リージョン間統計: 特定のリージョンについて、VPC 内の他のリージョンとの間のすべてのインGRESSおよびエグレス トラフィック。
- 外部統計: VPC の外部にあるソースまたは宛先を持つすべてのインGRESSおよびエグレス トラフィック。
- ゾーン間統計: 特定のゾーンについて、同じリージョンおよびVPC内の他のゾーンとの間のすべてのインGRESSおよびエグレス トラフィック。これらの集計された統計は、リージョン ページと VPC ページで利用できます。

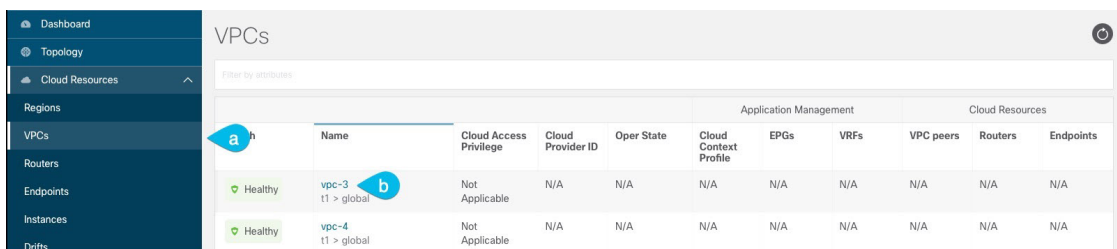
Peak values for each counter are displayed with a timestamp that shows when the peak value occurred.

この手順例は、Cisco Cloud Network Controller GUI で VPC のフロー ログ統計を表示する方法を示しています。次の手順で VPC の代わりにリージョンまたはエンドポイントを選択することで、同じ方法でリージョンまたはエンドポイントの統計を表示することもできます。

始める前に

この手順を使用して、目的のクラウド コンテキスト プロファイルの Google Cloud フロー ログ統計を有効にします。 [Enabling Flow Log Statistics \(167 ページ\)](#)

ステップ 1 統計を表示したいリソースを選択します。



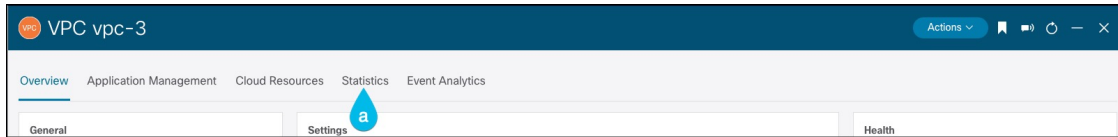
- a) From the navigation menu, select **Cloud Resources > VPCs**.

作業ペインに VPC の概要テーブルが表示されます。

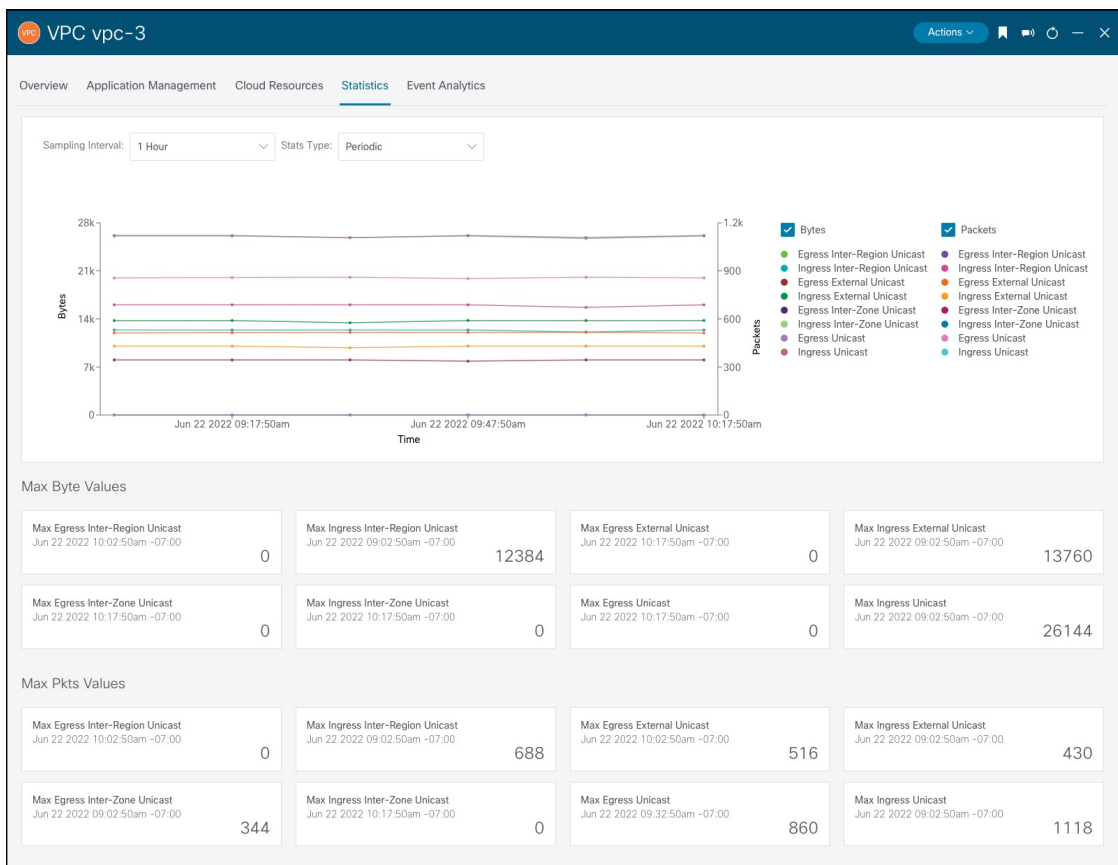
- b) 概要テーブルで、VPC の名前をダブルクリックします。

The VPC dialog box appears over the work pane. The VPC dialog box displays the **Overview**, **Application Management**, **Cloud Resources**, **Statistics**, and **Event Analytics** tabs.

ステップ 2 [Statistics] タブをクリックします。



VPC 統計のグラフィカル ビューが、最大値のテーブルとともに表示されます。



ステップ 3 Configure the display of the statistics.

To configure the parameters of the displayed statistics, you can modify the following settings:

[プロパティ (Properties)]	説明
サンプリング間隔	Choose the interval: <ul style="list-style-type: none"> • 1 時間 • 12時間 • 1日 • 週 1 回 • 1ヵ月
Stats Type	Choose the display type: <ul style="list-style-type: none"> • 定期 • 累計 • パフォーマンスの • 利率
Bytes	チェックを入れるとバイトカウンターグラフが表示されます。The vertical axis on the left side of the graph indicates the byte count.
Packets	チェックボックスをオンにすると、パケットカウンターのグラフが表示されます。The vertical axis on the right side of the graph indicates the packet count.

REST API を使用した VPC フロー ログの有効化

Google Cloud フロー ログ統計は、テナント内の個々のコンテキストプロファイルに対して有効にすることができます。

ステップ 1 テナントの下にフロー ログ ポリシー (cloudGcpFlowLogPol) を定義します。

名前以外の構成設定は必要ありません。

(注) For the name of the flow log policy, note the following restrictions:

- 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。

- 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。

例 :

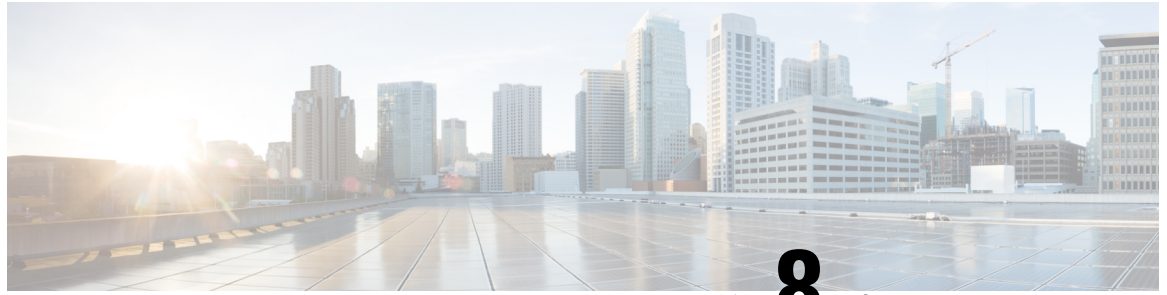
```
<polUni>
  <fvTenant name="tenant1" status="">
    <cloudGcpFlowLogPol name="myFlowLogPol1" status="">
    </cloudGcpFlowLogPol>
    <cloudCtxProfile name="ctxProfile2" status="" vpcGroup="vpc-4">
    .
    .
    .
```

ステップ 2 クラウド コンテキスト プロファイル内で、フロー ログ ポリシーへの参照を追加します。

クラウド コンテキスト プロファイルのフロー ログ統計は、参照オブジェクト (`cloudRsCtxToGcpFlowLog`) の存在によって有効になります。クラウド コンテキスト プロファイルのフロー ログ統計を無効にするには、参照オブジェクトを削除します。

例 :

```
.
.
.
    <cloudRsCtxToGcpFlowLog tnCloudGcpFlowLogPolName="myFlowLogPol1" status=""/>
  </cloudCtxProfile>
</fvTenant>
</polUni>
```

第 8 章

Cisco Cloud Network Controller のセキュリティ

この章は、次の内容で構成されています。

- [アクセス、認証、およびアカウントティング](#) (173 ページ)
- [TACACS+、RADIUS、LDAP、および SAML アクセスの構成](#) (174 ページ)
- [HTTPS Access の構成](#) (183 ページ)

アクセス、認証、およびアカウントティング

Cisco Cloud Network Controller ポリシーは、認証、認可、アカウントティング (AAA) 機能を管理します。管理者は、ユーザ権限、ロール、ドメインとアクセス権限の継承機能を組み合わせることで、管理対象オブジェクトレベルで細かく AAA 機能を設定できます。これらの設定は、REST API または GUI を使用して実行できます。



- (注) ログインドメイン名に 32 文字を超えることはできないという既知の制限があります。また、ログインドメイン名とユーザ名を合わせた文字数は 64 文字を超えることはできません。

アクセス、認証、およびアカウント構成情報の詳細については、[Cisco Cloud Network Controller Security Configuration Guide](#) 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となります。

ローカル ユーザの設定

[Cisco Cloud Network Controller GUI を使用したローカル ユーザーの作成 \(128 ページ\)](#) を参照して、ローカル ユーザーを設定し、Cisco Cloud Network Controller GUI を使用して OTP、SSH 公開キー、および X.509 ユーザー証明書に関連付けます。

TACACS+、RADIUS、LDAP、および SAML アクセスの構成

次のトピックは、Cisco Cloud Network Controller の TACACS+、RADIUS、LDAP および SAML アクセスを構成する方法を説明します。

概要

このトピックでは、RADIUS、TACACS+、LDAP、および SAML ユーザー (ADFS、Okta、PingID など) の Cisco Cloud Network Controller 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、[\[Cisco Cloud Network Controller セキュリティ構成ガイド \(Cisco Cloud Network Controller Security Configuration Guide\)\]](#) を参照してください。

。

TACACS+ アクセス用の Cisco Cloud Network Controller の構成

始める前に

- Cisco Cloud Network Controller はオンラインです。
- 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。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。

ステップ 1 Cisco Cloud Network Controller で、**[TACACS+ プロバイダ (TACACS+ Provider)]** を作成します。

- a) メニューバーで、**[管理 (Administrative)]** > **[認証 (Authentication)]** を選択します。
- b) 作業ペインで、**[プロバイダー (Providers)]** タブをクリックして、**[アクション (Actions)]** ドロップダウンをクリックして、**[プロバイダーの作成 (Create Provider)]** を選択します。

[プロバイダーの作成 (Create Provider)] ダイアログボックスが表示されます。

- c) **[ホスト名/IP アドレス (Host name/IP Address)]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- d) **[説明 (Description)]** フィールドに、プロバイダーの説明を入力します。
- e) **[タイプ (Type)]** ドロップダウンリストをクリックし、**[TACACS+]** を選択します。

- f) [設定 (Settings)] セクションで、[キー (Key)]、[ポート (Port)]、[認証プロトコル (Authentication Protocol)]、[タイムアウト (Timeout)]、[再試行 (Retries)]、[管理 EPG (Management EPG)] を指定します。有効化 (Enabled) または 無効化 (Disabled) のいずれかを [サーバー監視 (Server Monitoring)] に対して選択します。

ステップ 2 TACACS+ の [Login Domain] を作成します。

- a) インテント アイコンをクリックします。
[インテント (Intent)] メニューが表示されます。
- b) [Intent] 検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative] を選択します。
[Intent] メニューに管理オプションのリストが表示されます。
- c) [インテント (Intent)] メニューの [管理 (Administrative)] リストで、[ログインドメインの作成 (Create Login Domain)] をクリックします。
[ログインドメインの作成 (Create Login Domains)] ダイアログボックスが表示されます。
- d) 次の [ログインドメインダイアログボックスの作成のフィールド (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。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
[設定 (Settings)]	
レルム	ドロップダウンメニューから TACACS+ を選択します。
プロバイダー	<p>プロバイダーを選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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。

- e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

これで、APIC TACACS+ 構成手順は完了です。次に、RADIUS サーバーも使用する場合は、RADIUS の APIC を設定します。

RADIUS アクセス用の Cisco Cloud Network Controller の構成

始める前に

- Cisco Cloud Network Controller はオンラインです。
- 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。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。

ステップ 1 Cisco Cloud Network Controller で、[RADIUS プロバイダ (LDAP Provider)] を作成します。

- メニューバーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- 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。
- [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。
- [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- [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。
- [設定 (Settings)] セクションで、[キー (Key)]、[ポート (Port)]、[認証プロトコル (Authentication Protocol)]、[タイムアウト (Timeout)]、[再試行 (Retries)]、[管理 EPG (Management EPG)] を指定します。有効化 (Enabled) または無効化 (Disabled) のいずれかを [サーバー監視 (Server Monitoring)] に対して選択します。

ステップ 2 RADIUS の [ログイン ドメイン] を作成します。

- intent アイコンをクリックします。
[intent (Intent)] メニューが表示されます。
- [intent (Intent)] 検索ボックスの下にあるドロップダウン矢印をクリックし、[管理 (Administrative)] を選択します。
[Intent] メニューに管理オプションのリストが表示されます。
- [intent (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。
- 次の [ログイン ドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
[設定 (Settings)]	
レルム	ドロップダウンメニューから RADIUS を選択します。
プロバイダー	<p>プロバイダーを選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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。

e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

これで、Cisco Cloud Network Controller RADIUS 構成手順は完了です。次に、RADIUS サーバを設定します。

Cisco Cloud Network Controller への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の構成

[\[Cisco Cloud Network Controller セキュリティ構成ガイド \(Cisco Cloud Network Controller Security Configuration Guide\) \]](#)にある [\[APIC への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の構成 \(Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the APIC\) \]](#) セクションを参照します。

LDAP Access の構成

LDAP 設定には 2 つのオプションがあります。

- Cisco AVPair の設定
- Cisco Cloud ネットワーク コントローラで LDAP グループ マップを構成する

次のセクションには、両方の構成オプションの手順が含まれています。

Cisco AVPair を使用した APIC アクセス用の Windows Server 2008 LDAP の設定

[Cisco Cloud Network Controller Security Configuration Guide](#)の[Cisco AVPair を使用した APIC アクセスのための Windows Server 2008 LDAP の設定 (Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair)]セクションを参照してください。

LDAP アクセスのための Cisco Cloud Network Controller の構成

始める前に

- Cisco Cloud Network Controller はオンラインです。
- LDAP サーバのホスト名または IP アドレス、ポート、バインド DN、ベース DN、およびパスワードを使用できること。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。

ステップ 1 Cisco Cloud Network Controller で、[LDAP プロバイダ (LDAP Provider)]を作成します。

- a) メニュー バーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- b) 作業ペインで、[プロバイダー (Providers)] タブをクリックして、[アクション (Actions)] ドロップダウンをクリックして、[プロバイダーの作成 (Create Provider)] を選択します。

[プロバイダーの作成 (Create Provider)] ダイアログボックスが表示されます。

- c) [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- d) [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- e) [タイプ (Type)] ドロップダウンリストをクリックし、[LDAP] を選択します。
- f) バインド DN、ベース DN、パスワード、ポート、属性、フィルタ タイプ、および管理 EPG を指定します。

- (注)
- バインド DN は、Cisco Cloud Network Controller が LDAP サーバにログインするために使用する文字列です。Cisco Cloud Network Controller は、ログインしようとするリモートユーザーの検証にこのアカウントを使用します。ベース DN は、Cisco Cloud Network Controller がリモートユーザー アカウントを検索する LDAP サーバのコンテナ名とパスです。これはパスワードが検証される場所です。フィルタを使用して、Cisco Cloud Network Controller が *cisco-av-pair* に使用するために要求している属性を見つけます。これには、Cisco Cloud Network Controller で使用するユーザー承認と割り当て済み RBAC ロールが含まれます。Cisco Cloud Network Controller は、この属性を LDAP サーバから要求します。
 - [属性] フィールド：次のうちいずれかを入力します。
 - LDAPサーバの設定では、Cisco AVPair、入力 **CiscoAVPair**。
 - LDAP グループ マップ LDAPサーバ設定、入力 **memberOf**。

ステップ 2 LDAP の ログイン ドメイン を作成します。

- a) メニュー バーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- b) [Work] ペインで、[Login Domains] タブをクリックし、[Actions] ドロップダウンをクリックして [Create Login Domain] を選択します。
- c) 次の [ログイン ドメイン ダイアログボックスの作成のフィールド (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。

[プロパティ (Properties)]	説明
全般	
名前	ログイン ドメインの名前を入力します
説明	ログイン ドメインの説明を入力します。
[設定 (Settings)]	
レルム	ドロップダウンメニューから [LDAP] 選択します。
プロバイダー	<p>プロバイダーを選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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。

[プロパティ (Properties)]	説明
認証タイプ (Authentication Type)	<ol style="list-style-type: none"> 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。 <ol style="list-style-type: none"> 1. [LDAP グループ マップ ルールの追加 (Add LDAP Group Map Rule)] をクリックします。ダイアログボックスが表示されます。 2. マップの名前と説明 (オプション) およびグループ DN を指定します。 3. [セキュリティ ドメインの追加 (Add Security Domain)] の横にある [+] をクリックします。ダイアログボックスが表示されます。 4. [+] をクリックして、[ロール (Role)] の名前およびロールの [権限 (Privilege)] タイプ (Read または Write) フィールドにアクセスします。チェックマークをクリックします。 5. さらにロールを追加するには、手順 4 を繰り返します。次に、[追加 (Add)] をクリックします。 6. 手順 3 を繰り返して、さらにセキュリティ ドメインを追加します。次に、[追加 (Add)] をクリックします。

- d) [ログイン ドメインの作成 (Create Login Domain)] ダイアログボックスで [保存 (Save)] をクリックします。

SAML アクセス用の Cisco Cloud Network Controller の構成

次のセクションでは、SAML Access 用の Cisco Cloud Network Controller の設定について詳しく説明します。

SAML について

[Cisco Cloud Network Controller Security Configuration Guide](#)の[SAML について (About SAML)]セクションを参照してください。

SAML の基本要素

[Cisco Cloud Network Controller Security Configuration Guide](#)の[SAML のベーシック エlement (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

[Cisco Cloud Network Controller Security Configuration Guide](#)の[サポートされている IdPs and SAML コンポーネント (Supported IdPs and SAML Components)]セクションを参照してください。

SAML アクセス用の Cisco Cloud Network Controller の構成



(注) SAML ベースの認証は Rest に対するものではなく、Cisco Cloud Network Controller 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。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。
- 次のように設定を行います。
 - 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 Cisco Cloud Network Controller で、[SAML プロバイダ (LDAP Provider)] を作成します。

- a) メニューバーで、[管理 (Administrative)] > > [認証 (Authentication)] を選択します。
- b) [作業 (Work)] ペインで、[プロバイダー (Providers)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [プロバイダーの作成 (Create Provider)] を選択します。
- c) [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- d) [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- e) [タイプ (Type)] ドロップダウンリストをクリックし、[SAML] を選択します。
- f) [設定 (Settings)] ペインで、次の手順を実行します。

- IdP メタデータ URL を指定します。

- AD FS の場合、IdP メタデータ URL は `https://<FQDN ofADFS>/FederationMetadata/2007-06/FederationMetadata.xml` という形式になります。
 - Okta の場合、IdP メタデータの URL を取得するには、Okta サーバから該当 SAML アプリケーションの [Sign On] セクションに、**アイデンティティ プロバイダー メタデータ** のリンクをコピーします。
- SAML ベースのサービスの **エンティティ ID** を指定します。
 - IdP メタデータの URL にアクセスする必要がある場合は、**メタデータ URL の HTTPS プロキシ (HTTPS Proxy for Metadata URL)** を構成します。
 - IdP はプライベート CA によって署名された場合は、**[認証局 (Certificate Authority)]** を選択します。
 - ドロップダウンリストから、**[署名アルゴリズム認証ユーザー要求 (Signature Algorithm Authentication User Requests)]** を選択します。
 - **SAML 認証要求の署名、SAML 応答メッセージの署名、SAML 応答の署名アサーション、SAML アサーションの暗号化**を有効にするには、チェックボックスをオンにします。
- g) **[保存 (Save)]** をクリックして、設定を保存します。

ステップ 2 SAML のログイン ドメインを作成します。

- a) メニュー バーで、**[管理 (Administrative)]** > **[認証 (Authentication)]** を選択します。
- b) 作業ペインで、**[ログインドメイン (Login Domains)]** タブをクリックして、**[アクション (Actions)]** ドロップダウンをクリックして、**[ログインドメインの作成 (Create Login Domains)]** を選択します。
- c) 次の **[ログインドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)]** のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
[設定 (Settings)]	
レルム	ドロップダウンメニューから SAML を選択します。

[プロパティ (Properties)]	説明
プロバイダー	<p>プロバイダーを選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 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

[Cisco Cloud Network Controller Security Configuration Guide](#) の [Okta の SAML アプリケーションの設定 (Setting Up a SAML Application in Okta)] セクションを参照してください。

AD FS で Relying Party Trust の設定

[Cisco Cloud Network Controller Security Configuration Guide](#) の [AD FS での証明書利用者信頼の設定 (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、の『[Cisco Cloud Network Controller Security Configuration Guide](#)』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 Network Controller ではサポートされません。これは、Cisco Cloud Network Controller 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 Network Controller 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 Network Controller で公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
 - 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキーリングを削除しないでください。キーリングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。
- ポッドあたり 1 つの証明書ベースのルートのみをアクティブにすることができます。
- このリリースでは、クライアント証明書認証はサポートされていません。

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

始める前に

注意：ダウンタイムの可能性があるので、メンテナンス時間中のみこのタスクを実行してください。この操作中に Cisco Cloud Network Controller 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)] フィールドで、Cisco Cloud Network Controller 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、Cisco Cloud Network Controller 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、Cisco Cloud Network Controller 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。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。