



Cisco Cloud APIC for AWS ユーザーガイド、リリース 25.0(1)-25.0(4)

初版：2021年9月20日

最終更新：2022年12月30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

新機能と更新情報 1

新規および変更情報 1

第 2 章

Cisco Cloud APIC の概要 5

概要 5

外部ネットワーク接続 6

サポートされているルーティングとセキュリティ ポリシーの概要 7

ルーティングおよびセキュリティ ポリシー: 25.0(1) より前のリリース 7

ルーティングおよびセキュリティ ポリシー: リリース 25.0(1) 8

ルーティング ポリシー: リリース 25.0(2) 10

トンネルのソース インターフェイスの選択 13

Cisco Cloud APIC の一般的な注意事項と制限事項 13

Cisco Cloud APIC GUI の概要 17

Cisco Cloud APIC GUI アイコンについて 18

第 3 章

Cisco Cloud APIC ポリシー モデル 23

ACI ポリシー モデルの概要 23

ポリシー モデルの主な特性 23

論理構造 24

Cisco ACI ポリシー管理情報モデル 25

テナント 27

クラウド コンテキスト プロファイル 28

CCR	29
Cisco Catalyst 8000V について	29
Cisco Cloud APIC および AWS の CCR 向けプライベート IP アドレス サポート	32
CCR なしのリージョンからの外部サイトへのコミュニケーション	33
CCR のリモートサイトからの ECMP 転送のサポート	37
ローカル CIDR によるリージョンの CCR へのルートの基本設定	37
可用性ゾーン	37
仮想アベイラビリティゾーンからクラウドアベイラビリティゾーンへの移行	38
注意事項と制約事項	40
VRF	40
クラウドアプリケーションプロファイル	41
クラウドエンドポイントグループ	42
コントラクト	43
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	45
クラウドテンプレートの概要	46
管理対象オブジェクトの関係とポリシー解決	49
デフォルトポリシー	50
共有サービス	51
第 4 章	Cisco Cloud APIC コンポーネントの設定
	53
Cisco クラウド APIC の設定について	53
GUI を使用した Cisco Cloud Cisco APIC の設定	53
Cisco Cloud APIC GUI、リリース 4.2(2) 以前を使用したテナントの作成	53
Cisco Cloud APIC GUI、リリース 4.2(3) 以降を使用したテナントの作成	54
リリース 4.2(2) 以前のテナント AWS プロバイダーを設定する	56
リリース 4.2(3) 以降のテナント AWS プロバイダーの設定	59
Cisco Cloud APIC GUI を使用したアプリケーションプロファイルの作成	65
Cisco Cloud APIC GUI を使用した VRF の作成	65
Cisco Cloud APIC GUI を使用した外部ネットワークの作成	67
グローバル VRF 間ルートリークポリシーの構成	72
Cisco Cloud APIC GUI を使用したリークルートの構成	74

Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定	74
Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成	77
AWS サイトと外部デバイスの間の接続の有効化	80
外部デバイス構成ファイルのダウンロード	80
AWS サイトと外部デバイスの間の接続の有効化	81
Cisco Cloud APIC GUI を使用した EPG の作成	84
Cisco Cloud APIC GUI を使用したコントラクトの作成	91
Cisco Cloud APIC を使用したコンシューマおよびプロバイダー EPG の指定	94
Cisco Cloud APIC GUI を使用したフィルタの作成	95
Cisco Cloud APIC GUI を使用したクラウド コンテキスト プロファイルの作成	99
AWS でのインスタンスの設定	102
Cisco Cloud APIC GUI を使用したバックアップ構成の作成	104
Cisco Cloud APIC GUI を使用したテクニカル サポート ポリシーの作成	108
Cisco Cloud APIC GUI を使用したトリガー スケジューラの作成	109
Cisco Cloud APIC GUI を使用したリモート ロケーションの作成	112
Cisco Cloud APIC GUI を使用したローカル ドメインの作成	114
Cisco Cloud APIC GUI を使用したプロバイダーの作成	118
Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成	124
Cisco Cloud APIC GUI を使用したロールの作成	124
Cisco Cloud APIC GUI を使用した RBAC ルールの作成	131
Cisco Cloud APIC GUI を使用した認証局の作成	132
Cisco Cloud APIC GUI を使用したキー リングの作成	133
Cisco Cloud APIC GUI を使用したローカル ユーザーの作成	136
Cisco Cloud APIC GUI を使用したリージョンの管理 (クラウド テンプレートの設定)	140
REST API を使用した Cisco Cloud APIC の構成	143
REST API を使用したテナントの作成	143
REST API を使用したコントラクトの作成	143
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	144
REST API を使用したクラウド リージョンの管理	146
REST API を使用したフィルタの作成	146
REST API を使用したアプリケーション プロファイルの作成	147

REST API を使用したクラウド EPG の作成	148
REST API を使用した外部クラウド EPG の作成	148
REST API を使用したクラウドテンプレートの作成	149
REST API を使用して VRF リーク ルートの構成	151
REST API を使用したトンネルのソース インターフェイス選択の構成	153

第 5 章**システムの詳細の表示 155**

VM ホスト メトリックのモニタリング	155
GUI を使用した VM ホストメトリックのモニタリング	155
REST API を使用した VM ホストメトリックスの監視	157
アプリケーション管理詳細の表示	158
クラウドリソースの詳細の表示	160
操作の詳細の表示	161
インフラストラクチャの詳細の表示	164
管理の詳細の表示	164
Cisco Cloud APIC GUI を使用したヘルスの詳細の表示	166

第 6 章**レイヤ 4 から レイヤ 7 サービスの展開 169**

概要	169
アプリケーション ロード バランサの概要	169
サーバー プールへのダイナミック サーバーのアタッチ	171
サービス グラフについて	172
機能ノードについて	173
端末ノードについて	173
サービス グラフの展開	173
Cloud APIC GUI を使用したサービス グラフの展開	174
Cisco Cloud APIC GUI を使用したロード バランサの作成	174
Cisco Cloud APIC GUI を使用したサービス グラフ テンプレートの作成	175
Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開	177
REST API を使用したサービス グラフの展開	182
REST API を使用したインターネット向けロード バランサの作成	182

REST API を使用したインターネット向けロードバランサの構成	183
REST API を使用したサービス グラフの作成	183
REST API を使用してサービス グラフを添付する	184
REST API を使用した HTTPS サービス ポリシーの構成	184
REST API を使用したキー リングの設定	185
REST API を使用した HTTPS サービス ポリシーの作成	187

第 7 章

Cisco Cloud APIC 統計 189

Cisco Cloud APIC 統計の概要	189
AWS ネットワーク インターフェイス統計コレクション	190
Cisco Cloud APIC エンドポイントと cloudEPg 統計処理	190
Cisco Cloud APIC 統計フィルタ	191
AWS Transit ゲートウェイ統計	191
VPC フロー ログの有効化	192
Cisco Cloud APIC GUI を使用した VPC フロー ログの有効化	193
REST API を使用した VPC フロー ログの有効化	195
クラウドルータ統計	196

第 8 章

Cisco Cloud APIC セキュリティ 199

アクセス、認証およびアカウントティング	199
構成	199
TACACS+、RADIUS、LDAP、および SAML アクセスの構成	200
概要	200
Cloud APIC for TACACS+ Access の構成	200
Cloud APIC for RADIUS Access の構成	202
Cloud APIC への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の設定	203
LDAP Access の構成	204
Cisco AVPair を使用した APIC アクセス用の Windows Server 2008 LDAP の設定	204
Cloud APIC for LDAP Access の構成	204
Cloud APIC for SAML Access の構成	206

SAML について	207
Cloud APIC for SAML Access の構成	207
Okta で SAML アプリケーションの設定	209
AD FS で Relying Party Trust の設定	209
HTTPS Access の構成	209
HTTPSアクセスについて	209
カスタム証明書の構成のガイドライン	210
GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定	210

第 9 章**設定のばらつき 213**

構成のばらつき通知と障害	213
構成ドリフトのメインページにアクセスする	215
欠落しているコントラクト構成の確認	217
欠落している EPG 構成の確認	219
欠落している VRF 構成の確認	221
構成のばらつきのトラブルシューティング	223

第 10 章**Cisco Cloud APIC の AWS Transit Gateway 225**

Cisco Cloud APIC の AWS Transit Gateway	225
--	-----

付録 A :**Cisco Cloud APIC エラーコード 227**

Cisco Cloud APIC エラーコード	227
-------------------------	-----



第 1 章

新機能と更新情報

- [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: リリース 25.0(4) の *Cisco Cloud APIC* での新機能と動作変更

機能または変更	説明	参照先
Cisco Cloud APIC の Cisco Catalyst 8000V での PAYG ライセンス モデルのサポート	Cisco Cloud APIC は Cisco Catalyst 8000V でのペイアズユーゴー (PAYG) ライセンスモデルをサポートしています。これにより、ユーザは VM サイズに基づいてクラウドに Catalyst 8000V インスタンスを展開し、時間単位で使用料を購入できます。	

表 2: リリース 25.0(3) の *Cisco Cloud APIC* での新機能と動作変更

機能または変更	説明	参照先
Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V への移行	Cisco Cloud APIC は、リリース 25.0(3) 以降、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。	

機能または変更	説明	参照先
Cisco Cloud Services Router 1000v および Cisco Catalyst 8000V で使用される用語	<p>上記の2種類のルータには、次の用語が使用されます。</p> <ul style="list-style-type: none"> • CSR : クラウドサービスルータの省略語です。シスコクラウドサービスルータ 1000v を指し、リリース 25.0(3) より前のリリースで使用されました。 • CCR : Cisco Cloud ルータの略。リリース 25.0(3) 以降で使用される Cisco Catalyst 8000V を指します。 <p>さらに、このドキュメント全体で、CCR は、リリースに応じて、上記のいずれかのルータの総称として使用されます。</p>	
マルチサイト オーケストレータの名前の変更	<p>Cisco ACI マルチサイト Orchestrator (MSO) は、2021年8月15日のMSOリリース3.4.1から Cisco Nexus Dashboard Orchestrator (NDO) に変更されました。この Cisco Cloud APIC ドキュメントでは、MSO のすべてのインスタンスが NDO になりました。</p>	

表 3: リリース 25.0(2) の Cisco Cloud APIC での新機能と動作変更

機能または変更	説明	参照先
Cisco Cloud APIC の AWS での複数 (2 つ以上) のアベイラビリティゾーンをサポート	<p>Cisco Cloud APIC の AWS の複数 (2 つ以上) のアベイラビリティゾーンをサポートが提供されるようになりました。</p>	<p>Cisco Cloud APIC ポリシーモデル (23 ページ)</p>

機能または変更	説明	参照先
AWSでルーティングとセキュリティポリシーを個別に構成するためのサポート	<p>リリース 25.0(2) 以降、ルーティングポリシーに対して次の更新を利用できます。</p> <ul style="list-style-type: none"> 内部 VRF ペア間のルートマップベースのルートリークをサポート 内部 VRF ルートリークポリシーのサポート。これにより、内部 VRF のペア間で契約ベースのルーティングまたはマップベースのルーティングを使用するかどうかを選択できます。 	<ul style="list-style-type: none"> • Cisco Cloud APIC の概要 (5 ページ) • Cisco Cloud APIC コンポーネントの設定 (53 ページ)
CCRIPsec トンネルは、外部ブランチ接続に使用可能な 3 つのデータ インターフェイスのいずれかを使用できるようになりました。	<p>リリース 25.0(2) より前では、外部ネットワークへのすべてのトンネルは、CCR ルータの 1 つの特定のインターフェイス (GigabitEthernet3 インターフェイス、または cloudHostIfp-2) から発信されてきました。</p> <p>リリース 25.0(2) 以降、サポートが拡張され、同じ宛先へのトンネルを GigabitEthernet2、GigabitEthernet3、および GigabitEthernet4 インターフェイスから形成できるようになりました。これは、IKEv2 構成のトンネルでのみサポートされます。</p>	<ul style="list-style-type: none"> • Cisco Cloud APIC の概要 (5 ページ) • Cisco Cloud APIC コンポーネントの設定 (53 ページ)
ワークロードデプロイ用のクラウドリージョン数の増加のサポート	<p>リリース 25.0(2) より前では、サイトごとに最大 4 つのリージョンを持つことができます。リリース 25.0(2) 以降、サイトごとに最大 16 のリージョンを持つことができます。</p>	

表 4: リリース 25.0(2) の Cisco Cloud APIC での新機能と動作変更

機能または変更	説明	参照先
Cisco Cloud APIC のリリース番号の変更	リリース 25.0(1) 以降では、Cisco Cloud APIC のリリース番号が変更されています。Cisco Cloud APIC のリリース順序は次のとおりです。 <ul style="list-style-type: none"> • 4.1(x) (AWS のみのサポート) • 4.2(x) • 5.0(x) • 5.1(x) • 5.2(x) • 25.0(x) 	
Cisco Cloud APIC での Prometheus Node Exporter のサポート	Prometheus ノードエクスポータは、リリース 25.0(1) 以降から Cisco Cloud APIC でサポートされています。	システムの詳細の表示 (155 ページ)
インフラ VPC CCR から IPSec/BGP を使用した外部デバイスへの IPv4 接続のサポート。	インフラ VPC CCR から IPSec/BGP を使用する任意の外部デバイスへの IPv4 接続がサポートされるようになりました。	外部ネットワーク接続 (6 ページ)
外部接続の設定時に、セキュリティ ポリシーに関係なく、内部 VRF と外部 VRF の間でルーティング ポリシーを個別に設定するためのサポート。	外部接続の設定時に、セキュリティ ポリシーに関係なく、内部 VRF と外部 VRF の間でルーティング ポリシーを個別に設定するためのサポートが利用できるようになりました。	サポートされているルーティングとセキュリティ ポリシーの概要 (7 ページ)



第 2 章

Cisco Cloud APIC の概要

- [概要 \(5 ページ\)](#)
- [外部ネットワーク接続 \(6 ページ\)](#)
- [サポートされているルーティングとセキュリティ ポリシーの概要 \(7 ページ\)](#)
- [トンネルのソース インターフェイスの選択 \(13 ページ\)](#)
- [Cisco Cloud APIC の一般的な注意事項と制限事項 \(13 ページ\)](#)
- [Cisco Cloud APIC GUI の概要 \(17 ページ\)](#)

概要

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1(1) では、クラウドベースの仮想マシン (VM) に展開する Cisco APIC のソフトウェア展開である Cisco Cloud APIC が導入されています。展開されると、Cisco Cloud APIC は次のことを行います。

- AWS パブリッククラウドと対話するための既存の Cisco APIC と同様のインターフェイスを提供します
- クラウド構成の展開と構成を自動化します
- クラウド ルータ コントロール プレーンを設定します
- オンプレミス Cisco ACI ファブリックとクラウドサイト間のデータ パスを設定します
- Cisco ACI ポリシーをクラウド ネイティブ コンストラクトに変換します
- エンドポイントを検出します
- オンプレミスのデータセンターまたはパブリッククラウドの両方またはいずれかに展開されたワークロードに対して一貫したポリシー、セキュリティ、および分析を提供します



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

- オンプレミスのデータセンターとパブリッククラウド間の自動接続を提供し、プロビジョニングとモニタリングを容易にします。
- ポリシーは Cisco Nexus Dashboard Orchestrator によってオンプレミスおよびクラウドサイトにプッシュされ、Cisco Cloud APIC はポリシーをクラウドに変換して、ポリシーをオンプレミスサイトと一致させます。

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

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

外部ネットワーク接続

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

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

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

外部VRF

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

外部VRFは、他のクラウドサイトまたはオンプレミスサイトに接続されている外部ネットワークを表します。複数のクラウド VRF は、外部VRF にルートを一括したり、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。

非 ACI 外部デバイスへの接続

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

このタイプの接続に関する注意事項と制限事項を次に示します。

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

注意事項と制約事項

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

サポートされているルーティングとセキュリティ ポリシーの概要

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

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

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

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

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

ルーティングおよびセキュリティ ポリシー: リリース 25.0(1)

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



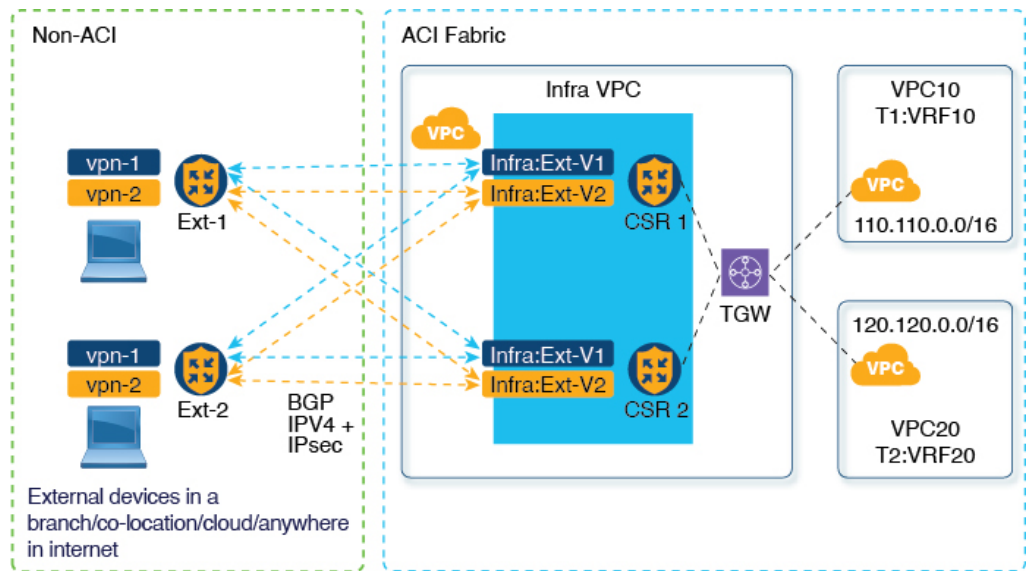
- (注) このセクションで説明するルーティングおよびセキュリティ ポリシーは、25.0(1) リリース専用であり、内部と外部VRFの間でのみ適用されます。25.0(2) リリースでのルーティングポリシーとセキュリティポリシーの変更については、[ルーティングポリシー: リリース 25.0\(2\) \(10 ページ\)](#) を参照してください。

ルーティングおよびセキュリティ ポリシーを構成する手順は次のとおりです。

- **ルーティング ポリシー:** リリース 25.0(1) で導入された VRF 間ルーティング機能を使用して、ルーティング ポリシーを個別に設定します。これらの手順については、[Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 \(74 ページ\)](#) を参照してください。
- **セキュリティ ポリシー:** ルーティング ポリシーを構成した後、セキュリティ ポリシーを個別に構成するために以前に行ったように、引き続きコントラクトを使用します。
 - まず、外部 EPG を作成します。これらの手順については、[Cisco Cloud APIC GUI を使用した EPG の作成 \(84 ページ\)](#) を参照してください。
 - 次に、外部 EPG とクラウド EPG の間のコントラクトを作成します。これらの手順については、[Cisco Cloud APIC GUI を使用したコントラクトの作成 \(91 ページ\)](#) を参照してください。

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

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



この例では、infra:Ext-V1 はインフラ VPC の CCR 上の外部 VRF にあり、リモートデバイスへの IPsec トンネルを介した BGP IPv4 セッションがあります。リモートエンドポイントルートは、これらのセッションを介して infra:Ext-V1 VRF で受信され、図の右側に表示されている内部 VRF (たとえば、VPC10 の T1:VRF10) にリークされます。逆リークルートも設定されています。

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

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

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

リリース 25.0(1) のセキュリティおよびルーティング ポリシーの注意事項と制約事項

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

- ルートは常に、内部 VRF と外部 VRF の間で双方向にリークされます。
たとえば、内部 VRF (V1) と外部 VRF (Ext-V1) を持つユーザー テナント (t1) があるとし
ます。ルート リークは、これらの VRF の両方に対して双方向に設定する必要があります。
- 「より大きな」プレフィックスがすでにリークされている間に、「より小さな」プレフィッ
クスをリークするように設定することはできません。たとえば、10.10.0.0/16 プレフィッ
クスがすでにリークされるように設定されている場合、10.10.10.0/24 プレフィックスの設
定は拒否されます。同様に、0.0.0.0/0 (すべてリーク) プレフィックスを設定した場合、
他のプレフィックスは設定できません。
- クラウド外部 EPG (cloudExtEpgs) 間の契約は許可されていません。
- 外部VRF は、クラウド EPG の作成には使用できません。
- 外部VRF は常にインフラ テナントに属します。
- 外部VRF 間のリーク ルーティングはサポートされていません。

ルーティング ポリシー: リリース 25.0(2)



- (注) このセクションで説明するルーティングおよびセキュリティ ポリシーは、25.0(2) リリース専用です。以前のリリースでのルーティング ポリシーとセキュリティ ポリシーの変更については、[ルーティングおよびセキュリティ ポリシー: リリース 25.0\(1\) \(8 ページ\)](#) を参照してください。

リリース 25.0(2) では、ルーティング ポリシーとセキュリティ ポリシーは、[ルーティングおよびセキュリティ ポリシー: リリース 25.0\(1\) \(8 ページ\)](#) で説明されているように引き続き分割されますが、特にルーティング ポリシーに次の変更が追加されています。

- [内部 VRF 間のルート リーク \(10 ページ\)](#)
- [グローバルな Inter-VRF ルート リーク ポリシー \(11 ページ\)](#)
- [注意事項と制約事項 \(12 ページ\)](#)

内部 VRF 間のルート リーク

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

[およびセキュリティポリシー: リリース 25.0\(1\) \(8 ページ\)](#) で説明されているように、その状況ではコントラクトベースのルーティングのみを使用できます。

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

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

グローバルな Inter-VRF ルート リーク ポリシー

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

このポリシーには、次の特性があります。

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

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

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

この Boolean フラグを前後に切り替えることができます。次に、このグローバル VRF ルートリーク ポリシーを切り替えるための一般的な推奨手順を示します。詳細な手順は、[Cisco Cloud APIC GUI を使用した内部 VRF のルートリークの構成 \(77 ページ\)](#) で提供されています。

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

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

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

その時点で、ルーティング ポリシーをルート マップ ベースのルーティングに変更できます。その後、新しいルート マップ ベースのルーティングで必要な粒度を反映するようにルーティングを変更できます。

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

注意事項と制約事項

次の注意事項および制約事項は、リリース 25.0(2) に適用されます。

- 外部 VRF と内部 VRF 間のルーティングでは、引き続きルート マップ ベースのルーティングのみが使用されます。
- `leakExternalPrefix` は、インターネットゲートウェイ (SSH を実行する外部 EPG 用に構成された外部エンドポイントセレクタ) へのルートと重複してはなりません。そうしないと、SSH が壊れます。

トンネルのソース インターフェイスの選択

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

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

```
<cloudtemplateIpsecTunnel peeraddr="173.36.19.2" preSharedKey="def" poolname="pool1">  
  <cloudtemplateIpsecTunnelSourceInterface sourceInterfaceId="3" />  
</cloudtemplateIpsecTunnel>
```

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

```
<cloudtemplateIpsecTunnel peeraddr="173.36.19.2" preSharedKey="def" poolname="pool1">  
  <cloudtemplateIpsecTunnelSourceInterface sourceInterfaceId="2" />  
  <cloudtemplateIpsecTunnelSourceInterface sourceInterfaceId="3" />  
</cloudtemplateIpsecTunnel>
```

注意事項と制約事項

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

Cisco Cloud APIC の一般的な注意事項と制限事項

この項では、Cisco Cloud APIC のガイドラインと制限事項について説明します。

- VRF の 1 つが別の VRF グループ (ハブ ネットワーク) の接続として存在する場合、サイト間 (VRF から VRF) トラフィックはサポートされません。たとえば、次のシナリオを考えてください。
 - VRF-1 は、さまざまなサイト (Azure と AWS) にまたがっています。AWS サイトでは、VRF-1 は VRF グループ 1 にあります。
 - VRF-2 は、別の VRF グループ (VRF グループ 2) に存在します。

このシナリオでは、VRF 間のコントラクトにより異なる VRF グループ間のトラフィックも暗黙的に許可されるため、サイト間の VRF-2 から VRF-1 へのトラフィックはサポートされません。異なる VRF グループ (ハブ ネットワーク) 間のトラフィックはサポートされていません。

- CCR (クラウドルータ) で VRF 間ルートリークを使用しているときに、オンプレミスとクラウドの間で複数の VRF をストレッチすることはできません。たとえば、EPG1 を持つ VRF1 が拡張され、EPG2 を持つ VRF2 も拡張される状況では、EPG1 は EPG2 とコントラクトできません。ただし、クラウド内に複数の VRF を設定して、1 つのオンプレミス VRF と 1 つ以上のコントラクトを共有することができます。
- クラウド上の CSR にアダプタイズするために、外部でアダプタイズされたオンプレミスサイトのブリッジドメインサブネットを設定します。
- デフォルトの AWS セキュリティグループ (SG) ルールでは、リージョンごとに 2 つの CCR のみが許可され、2 つのリージョンのみが CCR を展開できます (合計で最大 4 つの CCR)。より多くの CCR を展開するには、AWS SG ルールの制限を 120 以上に増やします。ルールの制限を 500 に増やすことをお勧めします。
- テナントのオブジェクトを設定するときに、AWS の古いクラウドリソースを確認します。古い構成は、アカウントを管理していた以前の Cisco Cloud APIC から適切に消去されなかった場合に存在する可能性があります。



- (注) テナントアカウント ID の追加後、Cisco Cloud APIC が古いクラウドリソースを検出するまでに時間がかかります。

古いクラウドリソースを確認し、クリーンアップするには、次の手順を実行します。

1. [ナビゲーション (Navigation)] メニュー > [アプリケーション管理 (Application Management)] > [テナント (Tenants)] の順にクリックします。[テナント (Tenants)] サマリーテーブルは、テナントのリストとともに、サマリーテーブルの行として作業ペインに表示されます。
2. オブジェクトを作成するテナントをダブルクリックします。[概要 (Overview)]、[クラウドリソース (Cloud Resources)]、[アプリケーション管理 (Application Management)]、[統計 (Statistics)]、および [イベント分析 (Event Analytics)] タブが表示されます。
3. [クラウドリソース (Cloud Resources)] > [アクション (Actions)] > [古いクラウドリソースの表示 (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。
4. 古いオブジェクトが見つかった場合は、[古いクラウドオブジェクトを自動的にクリーンアップする] チェックボックスをクリックしてチェックマークを付けます。
5. [保存 (Save)] をクリックします。Cisco Cloud APIC は、古いクラウドオブジェクトを自動的にクリーンアップします。



(注) 自動クリーンアップを無効にするには、手順 1 ~ 4 に従って、**[古いクラウドオブジェクトを自動的にクリーンアップする]**チェックボックスをクリックしてチェックマークを外します。

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

- AciDnTag
- AciOwnerTag

Cisco Cloud APIC は EC2、またはその他のリソースを作成、削除、または更新する権限を持つ AWS IAM ユーザーが Cisco Cloud APIC によって作成および管理されるリソースへアクセスすることや変更することを防止する必要があります。このような制限は、インフラとその他のユーザのテナントアカウントの両方に適用する必要があります。AWS アカウント管理者は、上記の 2 つのタグを使用して、意図しないアクセスや変更を防ぐ必要があります。たとえば、次のようなアクセス ポリシーがある場合、Cloud APIC によって管理されているリソースへのアクセスを防止することができます。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {"ec2:ResourceTag/AciDnTag": "*"}
  }
}
```

- 共有 L3Out を構成する場合:
 - オンプレミスの L3Out とクラウド EPG をテナント共通にすることはできません。
 - オンプレミスの L3Out とクラウド EPG が異なるテナントにある場合は、テナント共通でコントラクトを定義します。オンプレミス サイトまたはクラウドテナントでコントラクトすることはできません。
 - オンプレミスの L3Out 外部 EPG (l3extInstP) でクラウド EPG の CIDR を指定します。
 - オンプレミスの L3Out が別の VRF のクラウド EPG とコントラクトしている場合、クラウド EPG が存在する VRF をオンプレミス サイトに拡張することはできず、オンプレミス サイトの他の VRF とコントラクトすることはできません。
 - オンプレミスの外部 EPG で外部サブネットを構成する場合:

- 外部サブネットをゼロ以外のサブネットとして指定します。
- 外部サブネットは、別の外部サブネットと重複できません。
- クラウド EPG とコントラクトするには、共有ルート制御フラグを使用して外部サブネットをマークします。
- オンプレミスの外部 EPG でマークされている外部サブネットは、L3Out のルーティングプロトコルを介して学習されているか、静的ルートとして作成されている必要があります。
- アベイラビリティーゾーンをマッピングするときは、Cisco Cloud APIC で a または b のみを選択します。内部的には、ゾーンマッピング機能により、これが AWS の実際のアベイラビリティーゾーンにマッピングされます。



(注) マッピングがアルファベット順になっていない可能性があります。アベイラビリティーゾーンはアルファベット順に並べ替えられ、関数は最初の2つを選択し、それらを Cisco Cloud APIC のゾーン a と b に関連付けます。

- クラウドルーターに ASN 64512 を設定すると、クラウドルーターと AWS 仮想プライベートゲートウェイの間で BGP セッションが機能しなくなります。
- サポートされているスケールの合計については、次のサポートされているスケールの表を参照してください。



(注) サポートされているスケールの表で指定されているスケールを使用する場合:

- 合計で4つの管理対象リージョンのみを持つことができます。
- 2つのリージョン、2 * 2 CCR でのみ CCR を持つことができます。これは、AWS SG ルールの制限に関係ありません。

表 5: サポートされるスケール

コンポーネント	サポートされている数
テナント	20
アプリケーション	500
EPG	500

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

Cisco Cloud APIC GUI の概要

Cisco Cloud APIC GUI は、関連するウィンドウのグループに分類されます。各ウィンドウでは、特定のコンポーネントにアクセスして管理できます。GUIの左側にある **[ナビゲーション (Navigation)]** メニューを使用して、ウィンドウ間を移動します。メニューのいずれかの部分にマウスを移動すると、**[ダッシュボード (Dashboard)]**、**[トポロジ (Topology)]**、**[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、テナント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)]** > **[テナント (Tenants)]** 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、**[クラウドリソース (Cloud Resources)]** **[アベイラビリティゾーン (Availability Zones)]** をクリックすると、**[テナント (Tenants)]** から**[アベイラビリティゾーン (Availability Zones)]** 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、**[アベイラビリティゾーン (Availability Zones)]** ウィンドウの表示中にテナントを作成するには、**[インテント (Intent)]** アイコンをクリックします。検索ボックスとドロップダウンリストを含むダイアログが表示されます。ドロップダウンリストをクリックして**[アプリケーション管理 (Application Management)]** を選択すると、**[テナント (Tenant)]** オプションを含むオプションのリストが表示されます。**[テナント (Tenant)]** オプションをクリックすると、テナントの作成に必要なフィールドのグループを示す**[テナントの作成 (Create Tenant)]** ダイアログが表示されます。

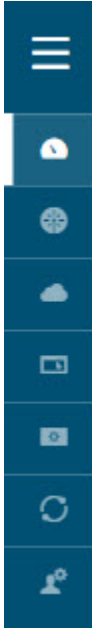
GUI アイコンの詳細については、[Cisco Cloud APIC GUI アイコンについて \(18 ページ\)](#) を参照してください。

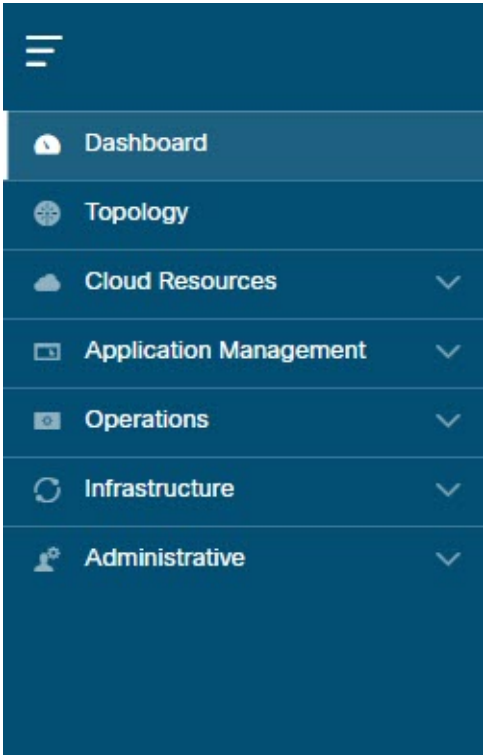

Cisco Cloud APIC コンポーネントの構成の詳細については、[Cisco Cloud APIC コンポーネントの設定 \(53 ページ\)](#) を参照してください。




Cisco Cloud APIC GUI アイコンについて



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

表 6: Cisco Cloud APIC GUI アイコン

アイコン	説明
<p data-bbox="100 487 505 516">図 1: ナビゲーション ペイン (折りたたみ)</p> 	<p data-bbox="771 487 1481 810">GUI の左側には ナビゲーション ウィンドウがあり、折りたたんだり展開したりします。ペインを展開するには、マウスアイコンをマウスオーバーするか、上部のメニューアイコンをクリックします。メニューアイコンをクリックすると、ナビゲーション ペインが開いた位置でロックされます。折りたたむには、メニューアイコンをもう一度クリックします。メニューアイコンの上にマウスのアイコンを重ねてナビゲーション ウィンドウを展開すると、ナビゲーション ウィンドウはマウスアイコンから移動して折りたたまれます。</p> <p data-bbox="771 831 1481 970">展開すると、ナビゲーション ウィンドウにタブのリストが表示されます。各タブをクリックすると、Cisco Cloud APIC コンポーネント ウィンドウ間を移動できる一連のサブタブが表示されます。</p>

アイコン	説明
<p>図 2: ナビゲーション ウィンドウ (展開)</p> 	<p>Cisco Cloud APIC コンポーネント ウィンドウは、ナビゲーション ウィンドウで次のように構成されています。</p> <ul style="list-style-type: none"> • [ダッシュボード (Dashboard)] タブ : Cisco Cloud APIC コンポーネントに関する概要情報を表示します。 • [トポロジ] タブ - 管理対象リージョンの地形図を表示します。 • [クラウド リソース] タブ : リージョン、アベイラビリティゾーン、VPC、ルーター、セキュリティグループ、エンドポイント、インスタンス、クラウドサービス (およびターゲットグループ) に関する情報を表示します。 • [アプリケーション管理 (Application Management)] タブ : テナント、アプリケーションプロファイル、EPG、コントラクト、フィルタ、VRF、サービス グラフ、デバイス、およびクラウド コンテキストプロファイルに関する情報を表示します。 • [操作 (Operations)] タブ : イベント分析、アクティブセッション、バックアップおよび復元ポリシー、テクニカル サポート ポリシー、ファームウェア管理、スケジューラ、およびリモート ロケーションに関する情報が表示されます。 • [インフラストラクチャ (Infrastructure)] タブ : システム設定、リージョン間接続、およびオンプレミス接続に関する情報が表示されます。 • [管理 (Administrative)] タブ : 認証、イベント分析、セキュリティ、ローカルおよびリモート ユーザー、およびスマートライセンスに関する情報が表示されます。 <p>(注) これらのタブの内容の詳細については、システムの詳細の表示 (155 ページ) を参照してください。</p>
<p>図 3: 検索メニューバー アイコン</p> 	<p>[検索 (Search)] メニューバー アイコンは、検索フィールドを表示します。このフィールドを使用すると、名前またはその他の特徴的なフィールドでオブジェクトを検索できます。</p>

アイコン	説明
<p>図 4: インテント メニューバー アイコン</p> 	<p>メニュー アイコンの 検索 アイコンとフィードバック アイコンの間に、[インテント (Intent)] アイコンが表示されます。</p> <p>クリックすると、[インテント (Intent)] ダイアログが表示されます (以下を参照)。[インテント (Intent)] ダイアログでは、Cisco Cloud APIC GUI の任意のウィンドウからコンポーネントを作成できます。コンポーネントを作成または表示すると、ダイアログボックスが開き、[インテント (Intent)] アイコンが非表示になります。[インテント (Intent)] アイコンに再度アクセスするには、ダイアログボックスを閉じます。</p> <p>コンポーネントの作成の詳細については、Cisco Cloud APIC コンポーネントの設定 (53 ページ) を参照してください。</p>
<p>図 5: インテント (何をしたいか?) ダイアログボックス</p> 	<p>[インテント (Intent)] (何をしたいか?) ダイアログボックスには、検索 ボックスとドロップダウン リストがあります。ドロップダウン リストを使用すると、特定のオプションを表示するためのフィルタを適用できます。検索ボックスでは、フィルタリングされたリストを検索するためのテキストを入力できます。</p>
<p>図 6: フィードバック アイコン</p> 	<p>フィードバック アイコンは、メニューバーのインテント アイコンとブックマーク アイコンの間に表示されます。</p> <p>クリックすると、フィードバック パネルが表示されます。</p>
<p>図 7: ブックマーク アイコン</p> 	<p>ブックマーク アイコンは、フィードバック とシステム ツール アイコンの間にあるメニューバーに表示されます。</p> <p>クリックすると、現在のページがシステム上でブックマークされます。</p>
<p>図 8: システム ツール メニューバー アイコン</p> 	<p>システム ツール のメニューバー アイコンには、次のオプションがあります。</p> <ul style="list-style-type: none"> • 概要 (About) : Cisco Cloud APIC のバージョンを表示します。 • オブジェクトストア ブラウザ — 管理対象オブジェクト ブラウザ (バイザー) を開きます。これは Cisco Cloud APIC に組み込まれているユーティリティで、管理対象オブジェクトを (MO) をブラウザによりグラフィカルに表示します。

アイコン	説明
図 9: ヘルプメニューバーアイコン 	<p>[ヘルプ (Help)]メニューバーアイコンには、[クラウド APIC について (About Cloud APIC)]メニュー オプションが表示され、クラウド APIC のバージョン情報が提供されます。[ヘルプ (Help)]メニューバーアイコンには、[ヘルプセンター (Help Center)]および[ようこそ画面 (Welcome Screen)]メニュー オプションも表示されます。</p>
図 10: [ユーザー プロファイル (User Profile)]メニューバーアイコン 	<p>ユーザー プロファイルのメニューバーアイコンには、次のオプションがあります。</p> <ul style="list-style-type: none"> • [ユーザー設定 (User Preferences)] : 時刻形式 (ローカルまたは UTC) を設定し、ログイン時にウェルカム画面を有効または無効にすることができます。 • [パスワードの変更 (Change Password)] : パスワードを変更できます。 • [SSH キーの変更 (Change SSH Key)] : SSH キーを変更できます。 • [ユーザー証明書の変更 (Change User Certificate)] : ユーザー証明書を変更できます。 • [ログアウト (Logout)] : GUI からログアウトできます。



第 3 章

Cisco Cloud APIC ポリシー モデル

- [ACI ポリシー モデルの概要 \(23 ページ\)](#)
- [ポリシー モデルの主な特性 \(23 ページ\)](#)
- [論理構造 \(24 ページ\)](#)
- [Cisco ACI ポリシー管理情報モデル \(25 ページ\)](#)
- [テナント \(27 ページ\)](#)
- [クラウド コンテキスト プロファイル \(28 ページ\)](#)
- [VRF \(40 ページ\)](#)
- [クラウド アプリケーション プロファイル \(41 ページ\)](#)
- [クラウド エンドポイント グループ \(42 ページ\)](#)
- [コントラクト \(43 ページ\)](#)
- [クラウド テンプレートの概要 \(46 ページ\)](#)
- [管理対象オブジェクトの関係とポリシー解決 \(49 ページ\)](#)
- [デフォルト ポリシー \(50 ページ\)](#)
- [共有サービス \(51 ページ\)](#)

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

ポリシー モデルの主な特性

ポリシー モデルの主な特性には次のものがあります。

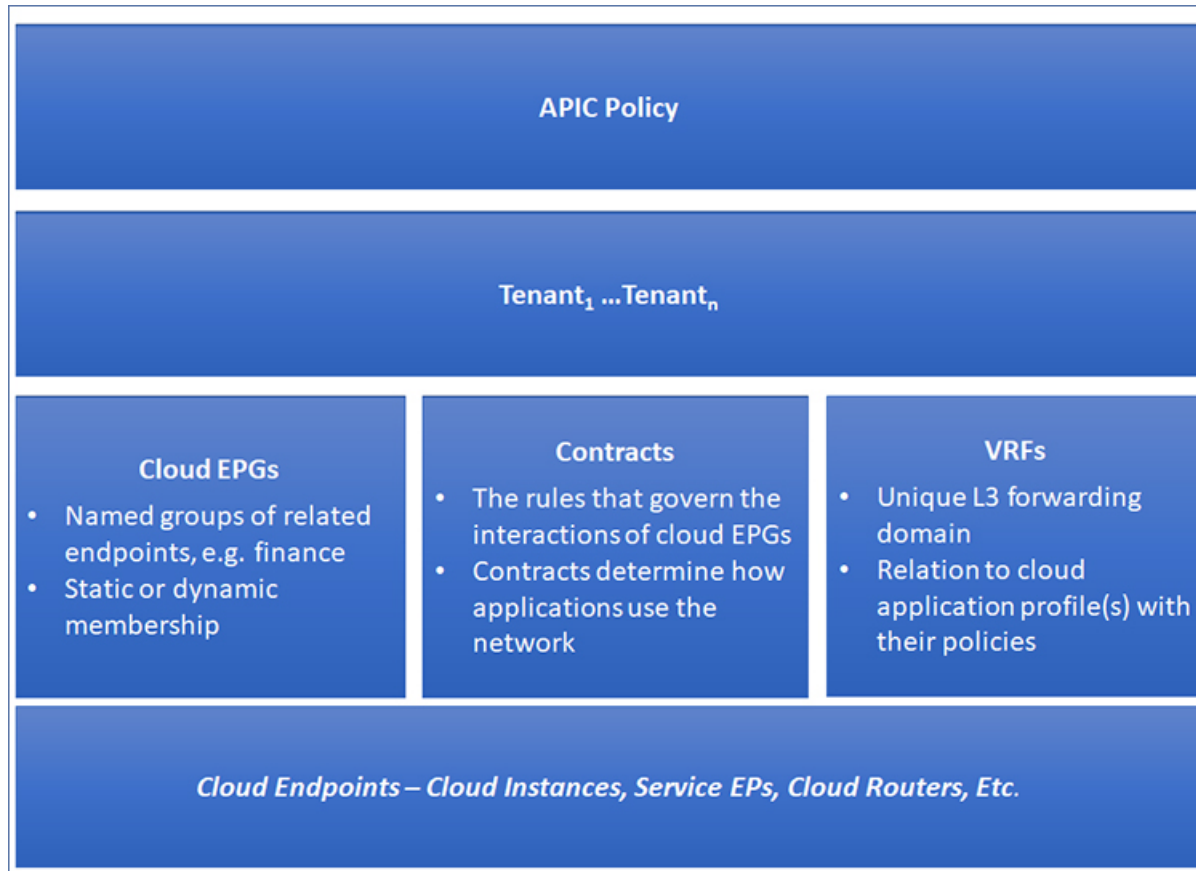
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

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

論理構造

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

図 11: ACI ポリシー モデルの論理構造の概要



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

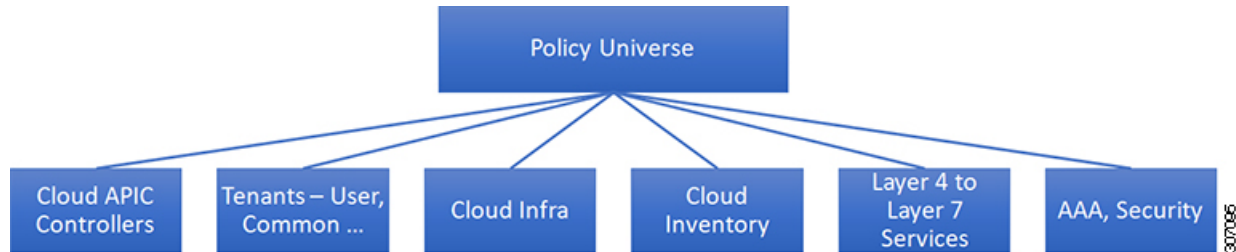
Cisco ACI ポリシー管理情報モデル

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 APIC は、情報モデルを保存および管理するプロセスを実行します。OSI 共通管理情報プロトコル (CMIP) および他の X.500 バリエーションと同様に、Cisco Cloud APIC によって、MIT の階層構造内のオブジェクトの場所に応じて継承できるオブジェクトのプロパティとして管理可能な特性を示すことにより、管理対象リソースの制御が可能になります。

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

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

図 12: Cisco ACI ポリシー管理情報モデルの概要



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

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

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



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

- インフラストラクチャテナントは、システムによって提供されますが、クラウドインフラストラクチャの管理者が設定できます。インフラストラクチャリソースの動作を管理するポリシーが含まれます。また、ファブリックプロバイダーはリソースを1つ以上のユーザテナントに選択的に展開できます。インフラストラクチャテナントポリシーは、クラウドインフラストラクチャ管理者によって構成可能です。
- クラウドインフラポリシーを使用すると、Cisco Cloud APICを設定するときに、オンプレミスおよびリージョン間接続を管理できます。詳細については、『Cisco Cloud APIC Installation Guide』を参照してください。

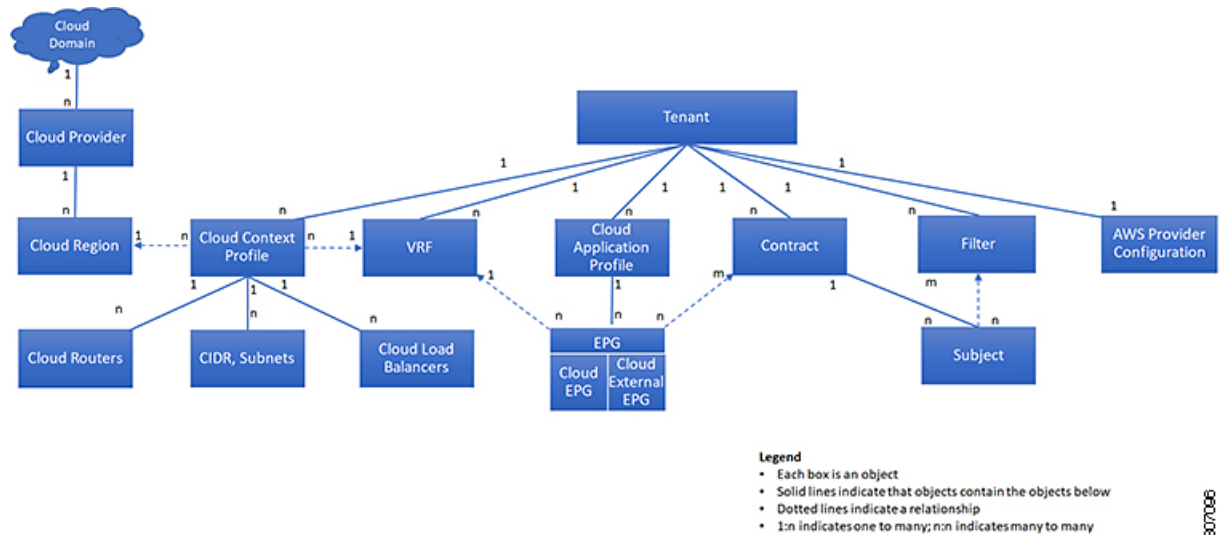
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ4～レイヤ7のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、[レイヤ4からレイヤ7サービスの展開 \(169 ページ\)](#) を参照してください。
- アクセス、認証、およびアカウントिंग (AAA) ポリシーは、Cisco Cloud ACI クラウドインフラストラクチャのユーザー権限、ロール、およびセキュリティ ドメインを管理します。詳細については、[Cisco Cloud APIC セキュリティ \(199 ページ\)](#) を参照してください。

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

テナント

テナント (`fvTenant`) は、アプリケーションポリシーの論理コンテナで、管理者はドメインベースのアクセスコントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。次の図は、管理情報ツリー (MIT) のテナント部分の概要を示します。

図 13: テナント



テナントは相互に分離することも、リソースを共有することもできます。テナントに、フィルタ、コントラクト、Virtual Routing and Forwarding (VRF) インスタンス、クラウドコンテキストプロフィール、AWS プロバイダー構成、およびエンドポイントグループ (EPG) を含む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。VRFおよびリージョンと組み合わせたクラウドコンテキストプロフィールは、そのリージョンのAWS VPCを表します。

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、次のCisco Cloud APICコンポーネントに関する情報が含まれています。

- アベイラビリティゾーンおよびリージョン
- CIDR
- CCR
- エンドポイント
- EPG
- 仮想ネットワーク
- VRF

次のセクションでは、クラウド コンテキスト プロファイルの一部である一部のコンポーネントに関する追加情報を提供します。

CCR

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

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

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

Cisco Catalyst 8000V について

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

- [ライセンス \(29 ページ\)](#)
- [Throughput \(30 ページ\)](#)

ライセンス

リリース 25.0(4) 以降、Cisco Cloud APIC 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

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



(注) 25.0(4) より前のリリースの場合、Cisco Cloud APIC 上の Cisco Catalyst 8000V は、**所有ライセンス持ち込み (BYOL) ライセンス モデルのみ**をサポートします。

BYOL ライセンス モデル

Cisco Catalyst 8000V の BYOL ライセンス モデルでは、Cisco から Catalyst 8000V Cisco DNA ライセンスを購入し、クラウドに展開する必要があります。

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクリプションする手順については、[Cisco Catalyst 8000V Edge ソフトウェア](#)を参照してください。

- 層に基づくさまざまなスループットの詳細については、[Throughput \(30 ページ\)](#) を参照してください。

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

PAYGライセンス モデル

25.0(4) リリース以降、Cisco Cloud APIC は Cisco Catalyst 8000V でのペイアズユーゴー (PAYG) ライセンス モデルをサポートしています。これにより、ユーザは VM サイズに基づいてクラウドに Catalyst 8000V インスタンスを展開し、時間単位で使用料を購入できます。

スループットを得るために VM サイズに完全に依存しているため、PAYG ライセンス モデルを有効にするには、まず現在の Cisco Catalyst 8000V の展開を解除してから、新しい VM サイズでの初回セットアップを使用して再度展開します。詳細については、『[Cisco Cloud APIC for AWS 設置ガイド](#)』の「セットアップウィザードを使用した Cisco Cloud APIC の構成」の章を参照してください。



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



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

Throughput

リリース 25.0(4) 以降、Cisco Cloud APIC 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

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



-
- (注) 25.0(4) より前のリリースの場合、Cisco Cloud APIC 上の Cisco Catalyst 8000V は、**所有ライセンス持ち込み (BYOL) ライセンス モデルのみ**をサポートします。
-

1. 所有ライセンス持ち込み (BYOL)

このモデルでは、Cisco Catalyst 8000V は、ティアベース（T0/T1/T2/T3）のスループットオプションをサポートしています。次の表に、Cisco Catalyst 8000V 向けのさまざまなルータ スループット設定に使用される AWS EC2 インスタンスを示します。

CCR スループット	AWS EC2 インスタンス
T0（最大 15M のスループット）	c5.xlarge
T1（最大 100M のスループット）	c5.xlarge
T2（最大 1G のスループット）	c5.xlarge
T3（最大 10G のスループット）	c5.9xlarge

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

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

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

2. ペイアズユーゴー（PAYG）ライセンス モデル

このモデル向けに、Cisco Cloud APIC は Cisco Catalyst 8000V 仮想ルータを使用し、クラウド ネットワーキングのニーズに合わせて AWS EC2 インスタンスの範囲をサポートします。

以下の表は、AWS 上の Cisco Cloud APIC でサポートされているクラウドインスタンス タイプを示しています。

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
c5.xlarge	最大 5 ギガビット スループット	4	8 GiB
c5.2xlarge	最大 10 ギガビット スループット	8	16 GiB
c5.4xlarge	最大 10 ギガビット スループット	16	32 GiB
c5.9xlarge	最大 10 ギガビット スループット	36	72 GiB
c5n.xlarge	最大 25 ギガビット スループット	4	10.5 GiB
c5n.2xlarge	最大 25 ギガビット スループット	8	21 GiB
c5n.4xlarge	最大 25 ギガビット スループット	16	42 GiB
c5n.9xlarge	最大 50 ギガビット スループット	36	96 GiB

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



- (注) Azure の場合、Cisco Cloud APIC および CCR のプライベート IP アドレスのサポートは、リリース 5.1(2) で利用可能になりました。AWS の場合、このサポートはリリース 5.2(1) 以降で利用できます。

AWS の場合、リリース 5.2(1) より前のリリースでは、Cisco Cloud Router (CCR) インターフェイスには Cisco Cloud APIC により、パブリックとプライベートの両方の IP アドレスが割り当てられていました。リリース 5.2(1) 以降、CCR インターフェイスはプライベート IP アドレスのみが割り当てられ、パブリック IP アドレスを CCR インターフェイスに割り当てることはオプションとなりました。プライベート IP アドレスは、常に CCR のすべてのインターフェイスに割り当てられます。CCR の GigabitEthernet1 のプライベート IP アドレスは、BGP および OSPF ルーター ID として使用されます。

CCR インターフェイスのパブリック IP アドレスを無効にするサイト間接続の CCR プライベート IP アドレスを有効にするには、[Cisco Cloud APIC GUI を使用したリージョンの管理 \(クラウド テンプレートの設定\)](#) (140 ページ) の手順を参照してください。

AWS の場合、リリース 5.2 (1) より前は、Cisco Cloud APIC の管理インターフェイスにパブリック IP アドレスとプライベート IP アドレスが割り当てられていました。リリース 5.2 (1) 以降、プライベート IP アドレスはの管理インターフェイスに割り当てられ、パブリック IP アド

レスの割り当てはオプションです。Cisco Cloud APIC Cisco Cloud APIC へのパブリック IP を無効にして、プライベート IP アドレスが接続に使用されるようにするには、*Cisco Cloud APIC for AWS Installation Guide*、Release 5.2(1) 以降の「AWS での Cisco Cloud APIC」手順を参照してください。

プライベート IP アドレスを使用した CCR の制限

パブリック IP が無効になっている場合、パブリック インターネットにはパブリック IP アドレスが必要なため、アンダーレイのサイト間接続をパブリック インターネットにすることはできません。アンダーレイのサイト間接続は、次のいずれかになります。

- AWS Direct Connect または Azure Express Route を介した、オンプレミスの ACI サイトに接続するためのプライベート接続
- AWS VPC ピアリングまたは Azure Vnet ピアリングを介して、同じクラウドプロバイダーの Cisco Cloud APIC サイトに接続するためのクラウドバックボーン

CCR なしのリージョンからの外部サイトへのコミュニケーション

リリース 5.2(1) より前では、トラフィックが外部サイトに通過するには、トラフィックが通過するリージョンに CCR が展開されている必要があります。CCR は、そのリージョンにローカルな CIDR をアドバタイズします。リージョン内の EPG が外部サイトと契約している場合、そのリージョンには、その外部サイトと通信するために CCR が展開されている必要があります。

リリース 5.2(1) 以降、CCR のないリージョンから外部サイトと通信できるようになりました。これは、Cisco Cloud APIC リリース 5.0(1) で利用可能になった AWS Transit Gateway 機能を利用することによって実現されます。Cisco Cloud APIC で AWS Transit Gateway 機能を有効にすると、AWS のすべてのマネージドリージョン間のピアリングも有効になります。このようにして、Cisco Cloud APIC は AWS Transit Gateway のピアリング機能により、CCR なしでリージョンから外部サイトと通信する問題に対処できます。この問題は、トラフィックを CCR のあるリージョンに再ルーティングすることで解決します。

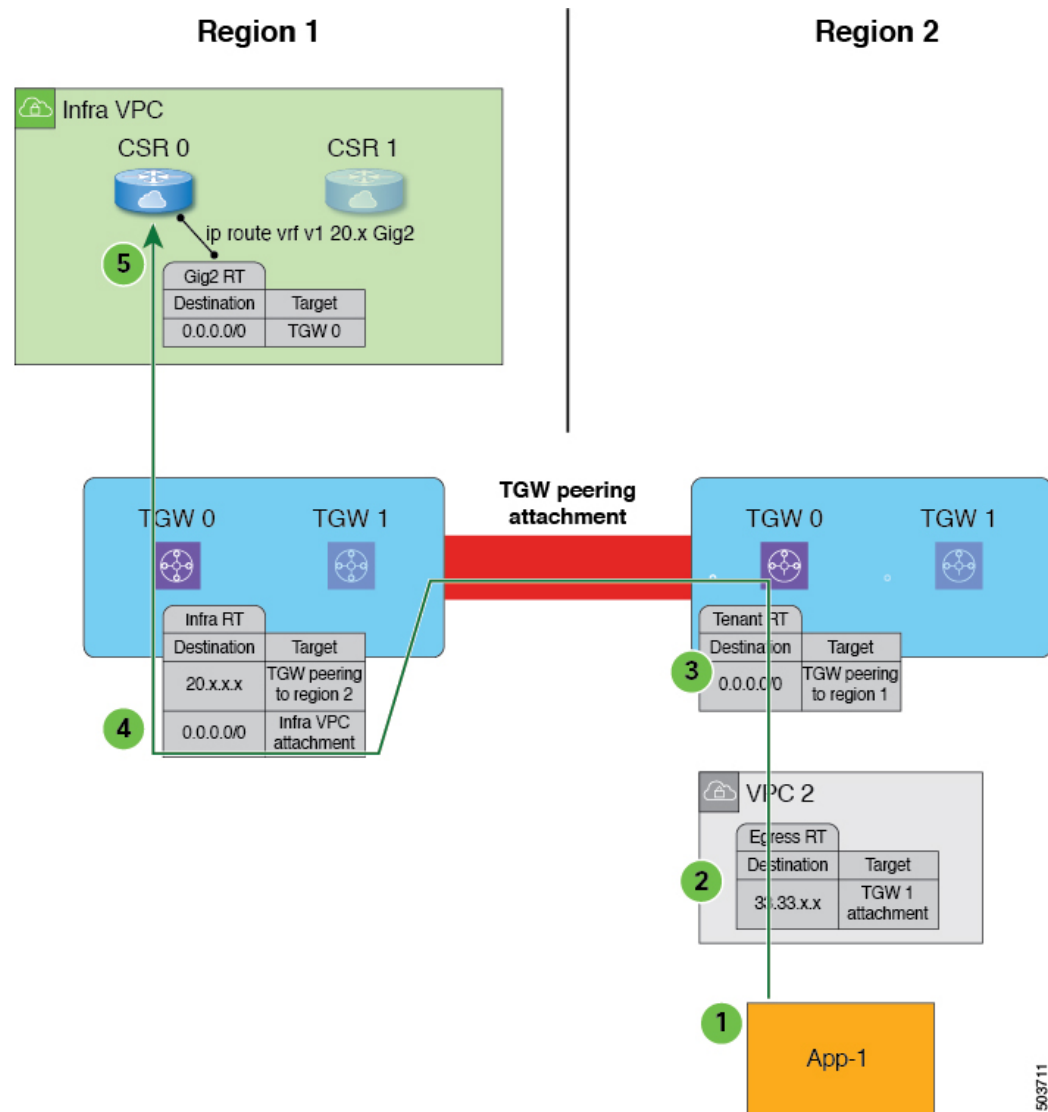
AWS Transit Gateway 機能を使用して、CCR のないリージョンからのトラフィックがサイトから出ようとする、このトラフィックは CCR のある最も近いリージョンのインフラ VPC にルーティングされます。トラフィックがそのリージョンのインフラ VPC に再ルーティングされた後、その CCR はパケットの送信に使用されます。入力トラフィックの場合、外部サイトからのパケットは任意のリージョンの CCR に到達し、入力データパスの AWS Transit Gateway ピアリングを使用して接続先リージョンにルーティングできます。

このような状況では、外部トラフィックが CCR のない領域を出入りしていることをシステムが認識すると、トラフィックは自動的に再ルーティングされます。ただし、システムがこの再ルーティング タスクを自動的に実行するには、次のコンポーネントを構成する必要があります。

- AWS Transit Gateway を設定する必要があります。詳細については、ドキュメント「[AWS Transit Gateway を使用した VPC 間の帯域幅の増加](#)」を参照してください。

- CCR は、少なくとも1つのリージョンに展開する必要があります。この拡張機能により、CCR を含まないリージョンから外部サイトと通信できるようになりますが、トラフィックが CCR のないリージョンから CCR のあるリージョンに再ルートできる CCR を含む別のリージョンが必要です。

次の図は、CCR のないリージョンから外部トラフィックが送信されていることをシステムが認識したときに、トラフィックが自動的に再ルーティングされるシナリオの例を示しています。



Cisco Cloud APIC がリージョン 2 に CCR がいないことを認識しているが、トラフィックが外部サイトに出力されている場合、次のことが発生します（緑色の矢印と円で示されています）。

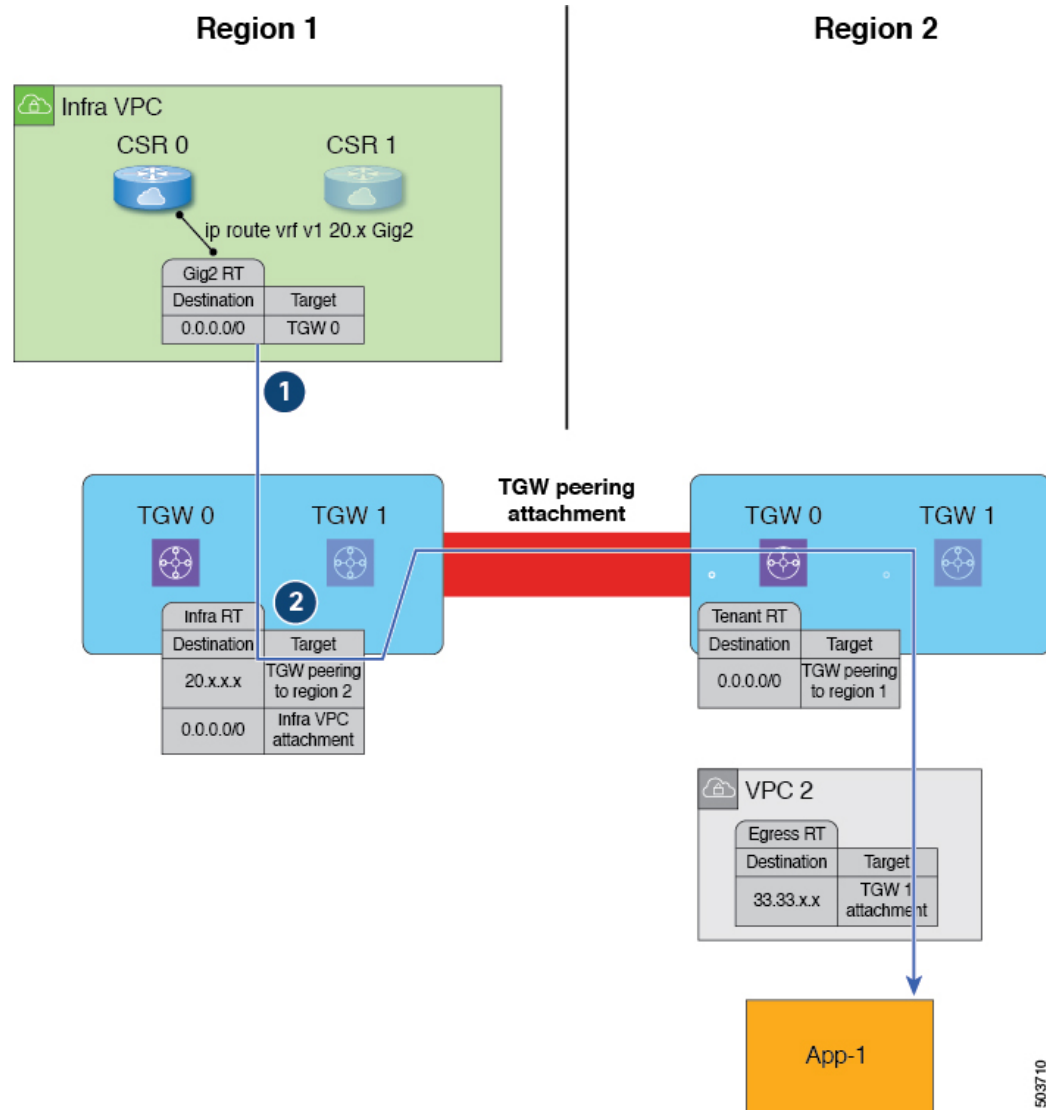
1. トラフィックフローは、リージョン 2 の App-1 の CIDR からリモートサイトへの出力を開始します。エンドポイントは、リモートサイトの CIDR を許可する適切なアウトバウンドルールで構成されていることに注意してください。

2. VPC2 出力ルートテーブルにはリモートサイト CIDR があり、次ホップとして AWS Transit Gateway があります。AWS Transit Gateway 情報は、設定されたコントラクトに基づいて自動的にプログラムされます。
3. 0.0.0.0/0 ルートが AWS Transit Gateway ルートテーブルに挿入されます。これは、基本的に、トラフィックが外部サイトに送信されているが、このリージョンに CCR がない場合に、AWS Transit Gateway ピアリング アタッチメントを取得するようにシステムに指示します。この状況では、AWS Transit Gateway ピアリングのアタッチメントは、CCR がある別のリージョン（例のシナリオではリージョン1）に移動します。使用される CCR のあるリージョンは、CCR がないリージョンへの地理的な近さに基づいて選択されます。
4. パケットは、最初に CCR を持つリージョン（リージョン1）のインフラ VPC に転送され、次に適切な VRF グループに関連付けられている CCR 上のギガビットイーサネットネットワーク インターフェイスに転送されます。
5. リージョン1の CCR のギガビット2 インバウンドセキュリティグループは、リモートリージョン VPC からのトラフィックを許可するように構成されています。

上記の出力の例では、次の点に注意してください。

- 手順1と2については、プレリリース 5.2(1) の動作から変更はありません。
- ステップ3は、リリース 5.2(1) のこの機能に固有の新しい動作であり、CCR のないリージョンから CCR のあるリージョンへの TGW ピアリング接続にリダイレクトが発生します。さらに、ステップ3は AWS クラウドで発生します。
- ステップ4と5は、通常、リリース 5.2(1) より前のリージョン2で発生しますが、リージョン2に CCR がある場合のみです。ただし、リージョン2には CCR がないため、リリース 5.2(1) のこの機能により、これらの手順は CCR が存在するリージョン1で実行されます。

次の図は、CCR のない領域に外部トラフィックが入っていることをシステムが認識したときに、トラフィックが自動的に再ルーティングされるシナリオの例を示しています。



503710

Cisco Cloud APIC が、リージョン 2 に CCR がないことを認識しているが、トラフィックが外部サイトからリージョン 2 の App-1 の CIDR に進入している場合、以下が発生します（青い矢印と円で示されています）。

- 通常、リージョン 1 の CCR は、そのリージョンにローカルな CIDR のみをアドバタイズします。ただし、リリース 5.2(1) の一部であるこの機能強化により、すべてのリージョンのすべての CCR がすべてのリモートリージョンからの CIDR をアドバタイズするようになりました。したがって、この例では、リージョン 1 の CCR は、リージョン 2 にある CIDR もアドバタイズします（AWS Transit Gateway ピアリングが両方のリージョン間で構成され、コントラクトが正しく構成されていると仮定します）。この状況では、トラフィックは外部サイトからリージョン 1 の CCR に進入し、リージョン 1 の CCR はリモートリージョン VPC CIDR の静的ルートをアドバタイズします。

2. インフラ ルート テーブル (リージョン 1 の AWS Transit Gateway ルート テーブル) には、リージョン 2 への AWS Transit Gateway ピアリング アタッチメントへのネクスト ホップがあります。

上記の入力の例では、次の点に注意してください。

- 上記の入力例の両方のステップ (ステップ 1 と 2) は、リリース 5.2(1) のこの機能に固有の新機能です。
- 入力例のステップ 1 は、CCR でプログラムされた構成を示しています。
- 入力例のステップ 2 は、AWS クラウドで発生します。

CCR のリモートサイトからの ECMP 転送のサポート

クラウド内の CCR は、通常、プレフィックスに対して複数のパスを受け取ります。リリース 5.2(1) より前は、CCR が複数のパスを受信する場合でも、均等コスト マルチパス (ECMP) を使用した CCR からのデータ転送はサポートされていませんでした。

リリース 5.2(1) 以降、CCR を使用した ECMP がサポートされるようになりました。CCR からのトラフィックは、接続先サイトから受信したすべての ECMP パスに転送されます。このサポートはリリース 5.2(1) で自動的に有効になり、このサポートを有効にするために手動で設定する必要はありません。

ローカル CIDR によるリージョンの CCR へのルートの基本設定

構成されているすべての CIDR は、特定のリージョンに対してローカルです。クラウド内に複数のリージョンがある場合、すべてのリージョンの CCR は冗長性のために CIDR をアドバタイズします。リリース 5.2(1) より前は、すべてのリージョンの CCR が同じ設定で CIDR がアドバタイズされました。これにより、リモートクラウドサイトまたはオンプレミスサイトが、CIDR がローカルではないリージョンを介して CIDR へのパスをインストールする可能性があります。これにより、パケットが必要以上に長い経路をたどる可能性があります。

リリース 5.2(1) 以降、複数のリージョンからの CCR は引き続き CIDR をアドバタイズしますが、CIDR がローカルであるリージョンからの CCR は、より高い優先度でアドバタイズします。これにより、オンプレミス サイトまたはリモートクラウドサイトは、CIDR がローカルであるリージョンにトラフィックを直接送信します。ローカルリージョンの CCR に障害が発生した場合、他のリージョンからのパスをデータ転送に使用できます。

可用性ゾーン

リリース 25.0(2) より前は、Cisco Cloud APIC は AWS のリージョンごとに 2 つのアベイラビリティゾーンのみをサポートします。その際に、Cisco Cloud APIC が <region-name>a と <region-name>b の形式を使用して、各リージョンに対して仮想アベイラビリティゾーンと呼ばれる 2 つのアベイラビリティゾーンを作成します。たとえば、us-west-1 リージョンの下に、Cisco Cloud APIC は 2 つの仮想アベイラビリティゾーン us-west-1a と us-west-1b を作成します。

仮想アベイラビリティゾーンからクラウドアベイラビリティゾーンへの移行

リリース 25.0(2) 以降、クラウドアベイラビリティゾーンがサポートされるようになり、各 AWS リージョンで Cisco Cloud APIC を使用して、複数のアベイラビリティゾーンが可能になりました。

- Cisco Cloud APIC の仮想アベイラビリティゾーンを表示するには、[クラウドリソース]>[アベイラビリティゾーン]に移動し、[仮想アベイラビリティゾーン]タブをクリックします。

The screenshot shows the 'Availability Zones' page in Cisco Cloud APIC. The 'Virtual Availability Zones' tab is selected. The table below lists three virtual availability zones.

Name	Cloud Availability Zone	Application Management			Cloud Resources		
		Tenants	App. Profiles	EPGs	VPCs	Routers	Endpoints
af-south-1-1a region-af-south-1		N/A	N/A	N/A	N/A	0	N/A
af-south-1-1b region-af-south-1		N/A	N/A	N/A	N/A	0	N/A
ap-east-1-1a region-ap-east-1		N/A	N/A	N/A	N/A	0	N/A

- Cisco Cloud APIC のクラウドアベイラビリティゾーンを表示するには、[クラウドリソース]>[アベイラビリティゾーン]に移動し、[クラウドアベイラビリティゾーン]タブをクリックします。

The screenshot shows the 'Availability Zones' page in Cisco Cloud APIC. The 'Cloud Availability Zones' tab is selected. The table below lists three cloud availability zones.

Name	Tenants	Application Management			Cloud Resources		
		App. Profiles	EPGs	VPCs	Routers	Endpoints	
us-east-1a AWS > infra > us-east-1	N/A	N/A	N/A	N/A	0	N/A	
us-east-1b AWS > infra > us-east-1	N/A	N/A	N/A	N/A	0	N/A	
us-east-1c AWS > infra > us-east-1	N/A	N/A	N/A	N/A	0	N/A	

仮想アベイラビリティゾーンからクラウドアベイラビリティゾーンへの移行

リリース 25.0(2) より前に構成したデプロイで、仮想アベイラビリティゾーンが構成されている場合、リリース 25.0(2) にアップグレードするときに、リリース 25.0(2) にアップグレードした後で、古い仮想アベイラビリティゾーンから新しいクラウドアベイラビリティゾーンに移行することをお勧めします。

- アベイラビリティゾーンの移行の一部として、CIDR ブロック範囲内の個々のサブネットまたはすべてのサブネットを移行できます。
- 古い仮想アベイラビリティゾーンから新しいクラウドアベイラビリティゾーンに移行しても、AWS のクラウドリソースでトラフィックのドロップなどの機能への影響はありません。



- (注) 次の手順では、クラウドコンテキストプロファイルを使用して仮想アベイラビリティゾーンからクラウドアベイラビリティゾーンに移行する方法について説明しますが、コンテンツアイコン (📄) をクリックし、**[アベイラビリティゾーン構成の移行]** を選択して、アベイラビリティゾーンを移行することもできます。

仮想アベイラビリティゾーンからクラウドアベイラビリティゾーンに移行するには:

1. 以前の仮想アベイラビリティゾーンで以前に構成されたクラウドコンテキストプロファイルに移動します。

左側のナビゲーションペインで、**[アプリケーション管理]>[クラウドコンテキストプロファイル]**に移動し、以前の仮想アベイラビリティゾーンで以前に構成されたクラウドコンテキストプロファイルを見つけます。

2. そのクラウドコンテキストプロファイルをダブルクリックします。

そのクラウドコンテキストプロファイルの詳細パネルが表示され、**[概要]** タブが自動的に選択されます。

[概要] タブの **[アベイラビリティゾーン]** 列のエントリを表示して、このクラウドコンテキストプロファイルに、クラウドアベイラビリティゾーンに移行できる仮想アベイラビリティゾーンがあるかどうかを判断します。

3. **[アクション]>[サブネット構成の移行]** の順にクリックします。

[アベイラビリティゾーン構成の移行 (Availability Zone Configuration Migration)] ウィンドウが表示されます。

4. クラウドアベイラビリティゾーンに移行する仮想アベイラビリティゾーンに関連付けられているサブネットを選択します。

- このウィンドウに一覧表示され、仮想アベイラビリティゾーンに関連付けられているすべてのサブネットがデフォルトで選択されます。クラウドアベイラビリティゾーンに移行したくない仮想アベイラビリティゾーンに関連付けられているサブネットを手動で選択解除します。
- クラウドアベイラビリティゾーンに移行される各仮想アベイラビリティゾーンについて、必要に応じて、**[クラウドアベイラビリティゾーン]** 列のエントリを書き留めて、そのサブネットの新しいアベイラビリティゾーン値を決定します。

5. **[サブネット構成の移行]** をクリックします。

選択した仮想アベイラビリティゾーンがクラウドアベイラビリティゾーンに移行されます。

注意事項と制約事項

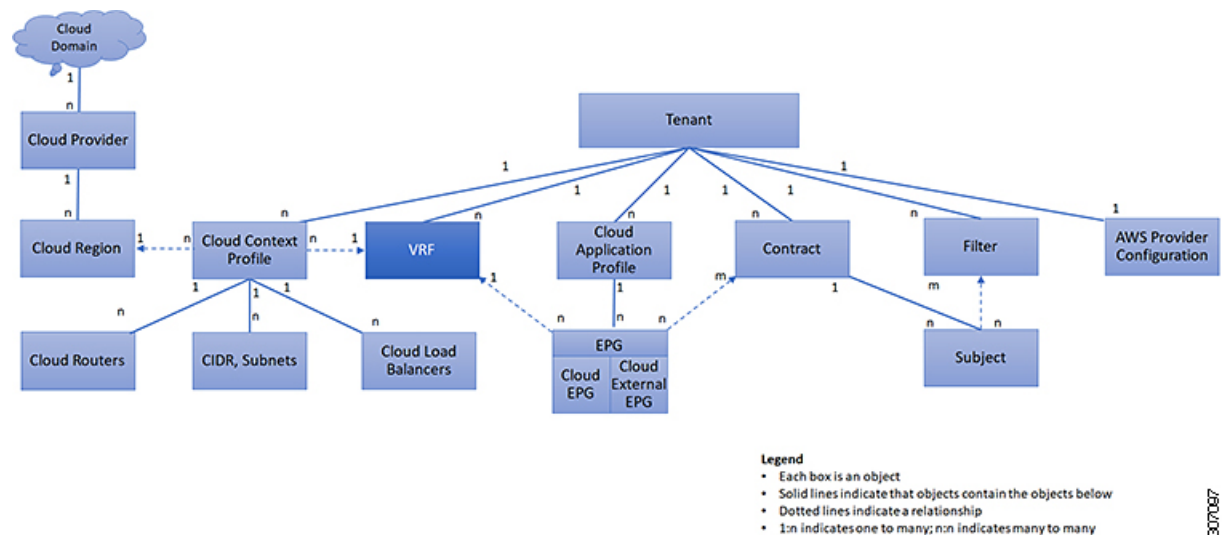
次に、複数のアベイラビリティ ゾーンをサポートに関するガイドラインと制限事項を示します。

- 3 つ以上のアベイラビリティ ゾーンを持つことができるクラウドアベイラビリティ ゾーンをサポートは、ユーザーテナントでのみ利用できます。インフラテナントは、2 つのアベイラビリティゾーンの制限がある仮想アベイラビリティゾーンを引き続き使用します。

VRF

仮想ルーティングおよび転送 (VRF) オブジェクト (fvCtx) またはコンテキストは、テナントネットワーク (Cisco Cloud APIC GUI のプライベート ネットワーク) と呼ばれます。テナントには、複数の VRF を含めることができます。VRF は、一意のレイヤ 3 フォワーディングおよびアプリケーションポリシードメインです。次の図は、管理情報ツリー (MIT) 内の VRF の場所とテナントの他のオブジェクトとの関係を示します。

図 14: VRF

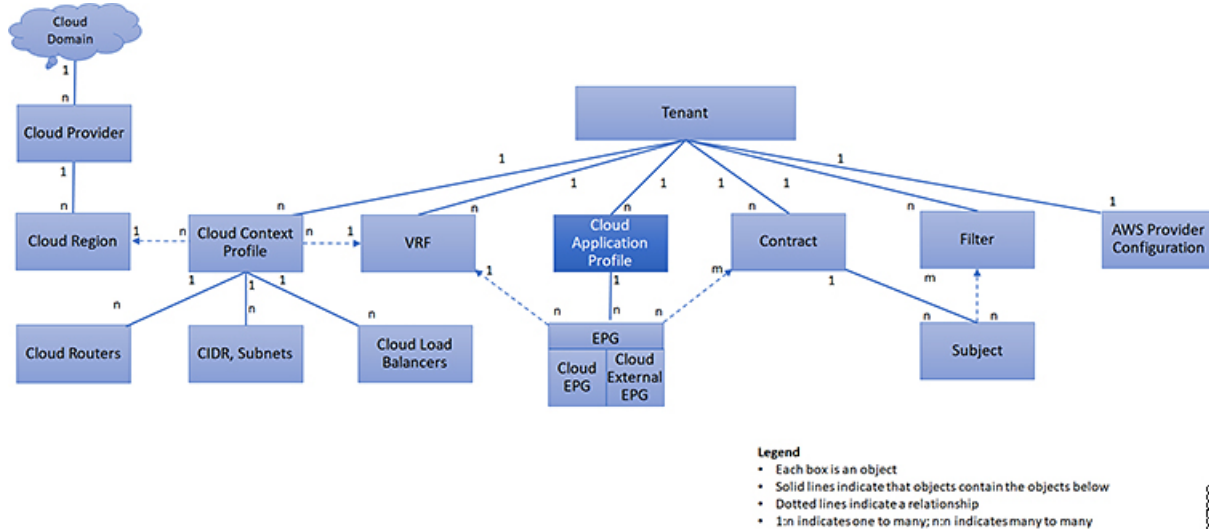


VRF は、レイヤ 3 のアドレス ドメインを定義します。1 つ以上のクラウド コンテキスト プロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウド コンテキスト プロファイルは 1 つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイスクラスタの選択基準ポリシーを提供する論理デバイスの VRF を作成できます。論理デバイスは、コントラクト名、グラフ名、またはグラフ内の関数ノード名に基づいて選択できます。

クラウドアプリケーション プロファイル

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

図 15: クラウドアプリケーション プロファイル



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

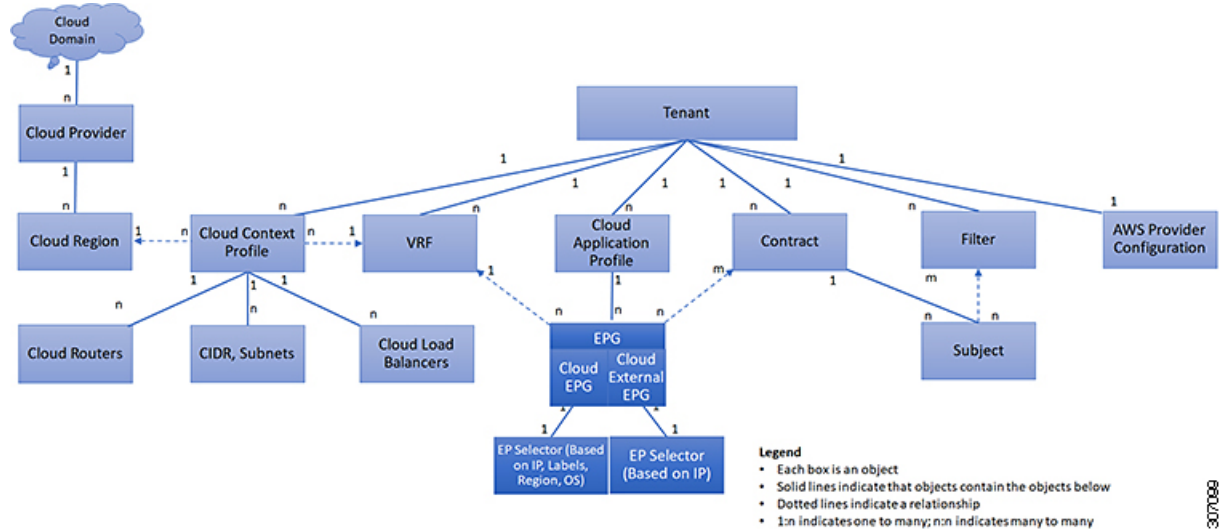
クラウド EPG は次のいずれかに従って組織化できます。

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

クラウドエンドポイントグループ

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

図 16: クラウドエンドポイントグループ



クラウド EPG は、エンドポイントの集合を含む名前付き論理エンティティである管理対象オブジェクトです。エンドポイントは、ネットワークに直接的または間接的に接続されるデバイスです。エンドポイントは、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 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。

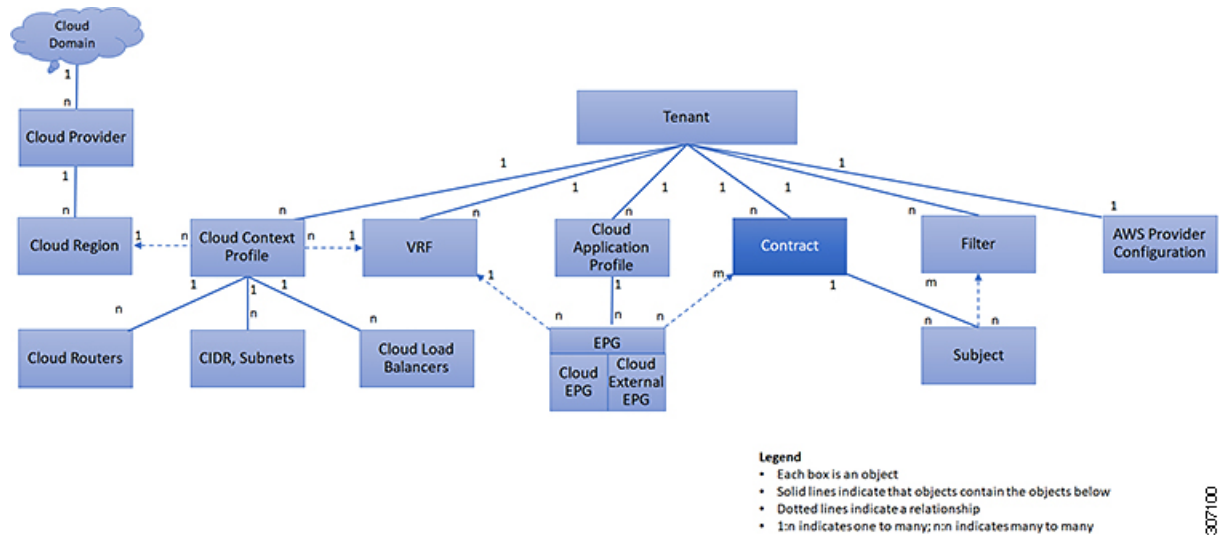
クラウド インフラストラクチャへの WAN ルータ接続は、スタティック クラウド EPG を使用する設定の 1 つの例です。クラウド インフラストラクチャへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む cloudExtEPg クラウド EPG を管理者が設定します。クラウド インフラストラクチャは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通してクラウド EPG のエンドポイントについて学習します。エンドポイントを学習すると、クラウド インフラストラクチャは、それに基づいて cloudExtEPg クラウド EPG 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

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

コントラクト

クラウド EPG に加えて、コントラクト (vzBrCP) はポリシー モデルのキー オブジェクトです。クラウド EPG が他のクラウド EPG と通信するには、コントラクトのルールに従う必要があります。次の図は、管理情報ツリー (MIT) 内のコントラクトの場所とテナントの他のオブジェクトとの関係を示します。

図 17: コントラクト



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

コントラクトは、次のタイプのクラウド EPG 通信を管理します。

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



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

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

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

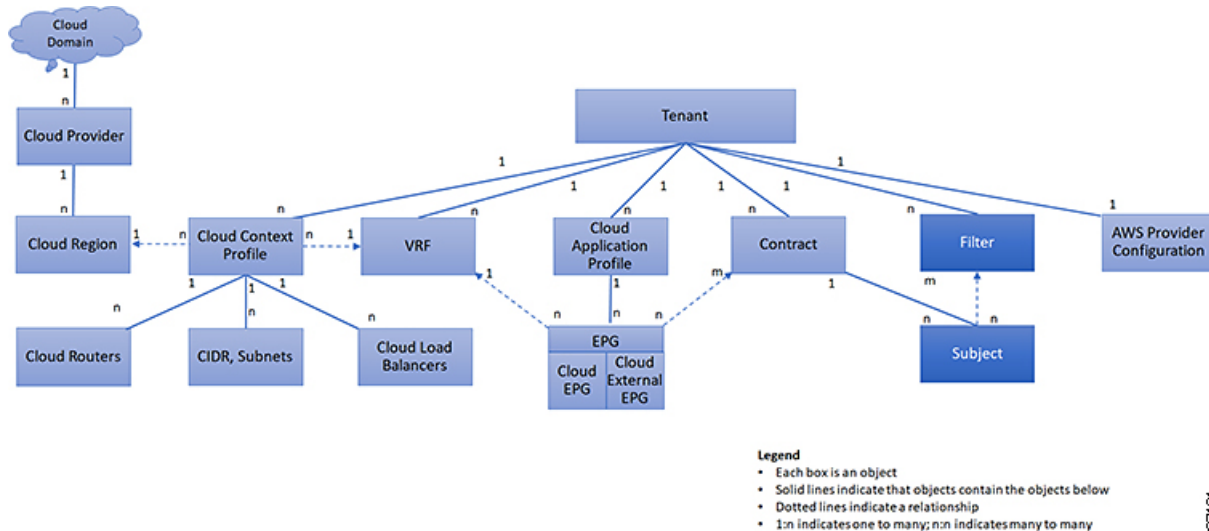


(注) 1つのクラウド EPG で同じコントラクトを指定および使用できます。クラウド EPG は複数のコントラクトを同時に指定および使用することもできます。

クラウド EPG 通信を制御するフィルタおよびサブジェクト

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

図 18: サブジェクトおよびフィルタ



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



- (注) サブジェクトは Cisco Cloud APIC で非表示になり、設定できません。AWS 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2～レイヤ4フィールド、レイヤ3プロトコルタイプ、レイヤ4ポートなどの TCP/IP ヘッダー フィールドなどです。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。



(注) コントラクトフィルタの一致タイプがすべて (All) の場合、ベストプラクティスは VRF 非強制モードを使用することです。特定の状況下では、これらのガイドラインに従わないと、コントラクトで VRF のクラウド EPG 間のトラフィックが許可されなくなります。

- 情報カテゴリはコントラクトに含まれています。コントラクト内の1つ以上の情報カテゴリ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。



(注) AWS 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。

- AWS 構造体でレンダリングされる ACI コントラクトは常にステートフルであり、リターントラフィックを許可します。

クラウドテンプレートの概要

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

AWS ネットワーク構成の中心的なものの1つは、仮想プライベートクラウド (VPC) です。AWS 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 VPC 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受け入れ、それらのリージョンのインフラ VPC の設定全体を生成します。これらはインフラ VPC です。AWS VPC に対応する Cisco Cloud APIC 管理対象オブジェクト (MO) は cloudCtxProfile です。クラウドテンプレートで指定されたすべてのリージョンに対して、cloudCtxProfile 設定が生成されます。cloudCtxProfile は、リージョンに対応するすべての設定の最上位 MO です。その下には、特定の設定をキャプチャするためのツリーとして編成された他の多くの MO があります。クラウドテンプレートによって生成された cloudCtxProfile MO には、ctxProfileOwner == SYSTEM が含まれます。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。

AWS VPC の主要なプロパティは CIDR です。すべてのリージョンには、一意の CIDR が必要です。Cisco Cloud APIC では、インフラ VPC の CIDR を提供できます。最初の 2 つのリージョンの CIDR は、AWS に Cisco Cloud APIC AMI をデプロイする Cloud Formation Template (CFT) から取得されます。cloudApicSubnetPool MO は、追加リージョンの CIDR を Cisco Cloud APIC に直接提供します。Cisco Cloud APIC 構成では、cloudCtxProfile の子である cloudCidr MO が CIDR をモデル化します。

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
- サブネットと AWS アベイラビリティーゾーンの関連付け
- 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 7:クラウドテンプレートMO

MO	目的
cloudtemplateInfraNetwork	クラウドテンプレート設定のルート。次の属性が含まれます。 numRoutersPerRegion : cloudtemplateIntNetwork で指定された各 cloudRegionName のクラウドルータの数。
cloudtemplateProfile	すべてのクラウドルータの設定プロファイル。次の属性が含まれます。 <ul style="list-style-type: none"> • routerUsername • routerPassword • routerThroughput • routerLicenseToken • routeDataInterfacePublicIP • routerMgmtInterfacePublicIP

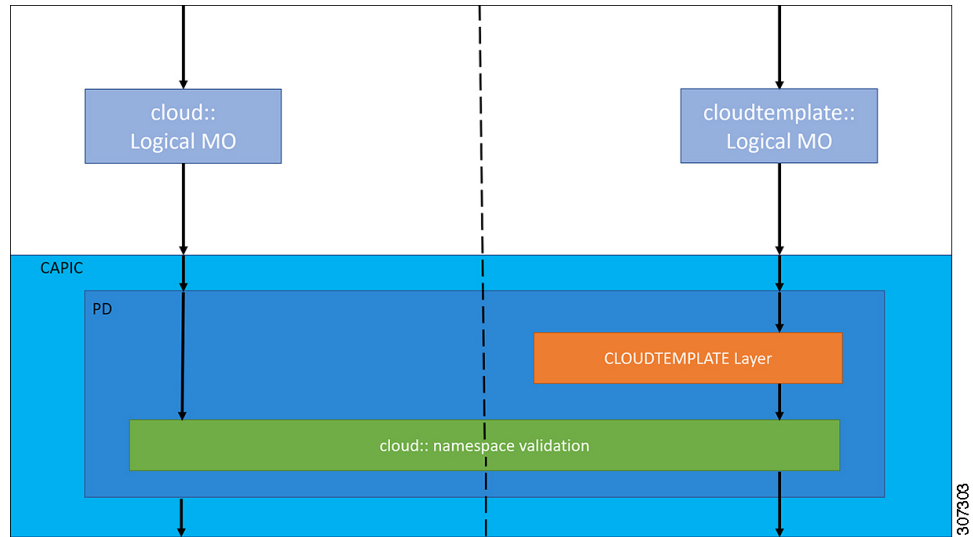
MO	目的
cloudtemplateIntNetwork	クラウドルータを展開する場所を指定するリージョンのリストが含まれます。各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateExtNetwork	クラウド外部のインフラ ネットワーク設定入力が含まれます。 クラウドルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。 各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateVpnNetwork	ACI オンプレミス サイトまたは別の Cisco Cloud APIC サイトで VPN を設定するための情報が含まれています。
cloudtemplateIpSecTunnel	ACI オンプレミス サイトの IPSec ピアの IP アドレスをキャプチャします。
cloudtemplateOspf	VPN 接続に使用する OSPF エリアをキャプチャします。
cloudtemplateBgpEvpn	オンプレミスサイトとの BGP セッションを設定するために、ピア IP アドレス、ASN などをキャプチャします。

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

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

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

図 19: クラウドおよびクラウドテンプレート MO 変換



(注) クラウドテンプレートの設定については、[Cisco Cloud APIC コンポーネントの設定 \(53 ページ\)](#) を参照してください。

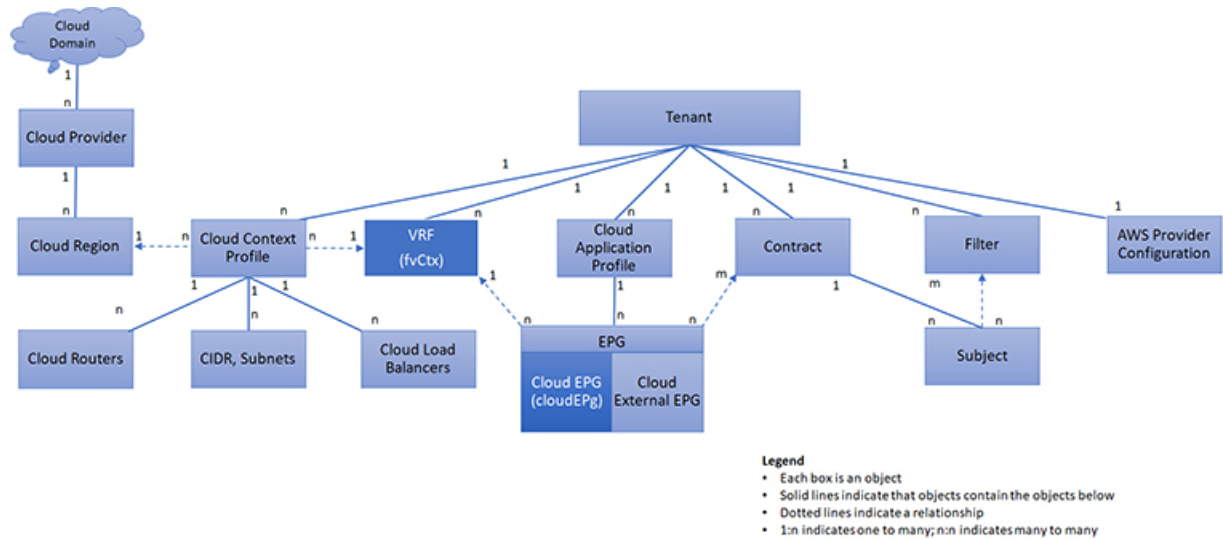
管理対象オブジェクトの関係とポリシー解決

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。

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

次の図の点線は、いくつかの一般的な MO の関係を示します。

図 20: MO の関係



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

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

- モニタリングと統計情報



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

デフォルト ポリシーは、次の複数の目的に使用されます。

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

次のシナリオでは、一般的なポリシー解決の動作について説明します。

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



- (注) 上記のシナリオは、テナントの VRF には適用されません。

- 構成はポリシー名を参照しません。現在のテナントにデフォルト ポリシーが存在する場合は、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。

共有サービス

あるテナントのクラウド EPG は、共有テナントに含まれるコントラクト インターフェイスを介して他のテナントのクラウド EPG を伝達できます。同じテナント内で、ある VRF のクラウド EPG は、テナントで定義された契約を通じて、別の VRF の別のクラウド EPG と通信できま

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

共有サービス コントラクトの設定時は、次のガイドラインに従ってください。

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



第 4 章

Cisco Cloud APIC コンポーネントの設定

- [Cisco クラウド APIC の設定について](#) (53 ページ)
- [GUI を使用した Cisco Cloud Cisco APIC の設定](#) (53 ページ)
- [REST API を使用した Cisco Cloud APIC の構成](#) (143 ページ)

Cisco クラウド APIC の設定について

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



- (注)
- ロードバランサとサービス グラフの設定については、[レイヤ 4 から レイヤ 7 サービスの展開](#) (169 ページ) を参照してください。
 - ナビゲーションや構成可能なコンポーネントのリストなどの GUI については、[Cisco Cloud APIC GUI の概要](#) (17 ページ) を参照してください。

GUI を使用した Cisco Cloud Cisco APIC の設定

Cisco Cloud APIC GUI、リリース 4.2(2) 以前を使用したテナントの作成

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

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

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

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

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

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

表 8: テナント ダイアログボックス フィールドの作成

[プロパティ (Properties)]	説明
名前 (Name)	テナント名を入力します。
説明	テナントの説明を入力します。
設定	
セキュリティドメインの追加	<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。
信頼できるテナント	[有効] チェックボックスをクリックしてオン(デフォルト)またはオフにします。オンにすると、 信頼できるテナント が有効になります。
クラウドアカウントID	クラウドアカウント ID を入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI、リリース 4.2(3) 以降を使用したテナントの作成

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

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

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

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

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

ステップ 4 次の [**テナントの作成 (Create Tenant)**] 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 9: テナント ダイアログボックス フィールドの作成

[プロパティ (Properties)]	説明
名前 (Name)	テナント名を入力します。
説明	テナントの説明を入力します。
設定	
セキュリティドメインの追加	<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"> [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。 セキュリティドメインをクリックして選択します。 [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。
AWSアカウントID	クラウドアカウント ID を入力します。
アクセスタイプ	<p>クリックしてテナントタイプを有効にします。</p> <ul style="list-style-type: none"> 信頼できない 信頼できる 組織

ステップ 5 設定が終わったら [Save] をクリックします。

リリース 4.2(2) 以前のテナント AWS プロバイダーを設定する

始める前に

- AWS プロバイダーは、インフラ テナント用に自動設定されます。インフラ テナント用に AWS プロバイダーを構成するために何もする必要はありません。
- すべての非インフラ テナントの場合、AWS プロバイダーは信頼できるテナントまたは信頼できないテナントとして設定されます。資格情報の管理は簡単ではないため、信頼できるテナントを使用することをお勧めします。また、各テナントは個別の AWS アカウントに属している必要があります。複数のテナントで同じ AWS アカウントを共有することは許可されていません。

信頼できるテナントの場合、最初に Cisco Cloud APIC が展開されているアカウント (インフラテナントのアカウント) との信頼関係を確立します。信頼関係を確立し、テナントアカウントにアクセスするために必要なすべての権限を Cisco Cloud APIC に付与するには、テナントアカウントでテナント ロール `cloud-formation` テンプレートを実行します。このテンプレートは、インフラテナントの AWS アカウントの `capic-common-[capicAccountId]-data` という名前の S3 バケットの `tenant-cft.json` オブジェクトとして使用できます。セキュリティ上の理由から、S3 バケットへのパブリック アクセスは許可されていないため、S3 バケット所有者はこのファイルをダウンロードしてテナントアカウントで使用する必要があります。

- 信頼されていないテナント：アカウントアクセスと秘密鍵を使用します。使用されるアクセス鍵と秘密鍵は、少なくともこれらのアクセス許可を持つ IAM ユーザーのものである必要があります。作成された IAM ロールは、`ApicTenantRole` という名前にする必要があります。



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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
```

```

    "Effect": "Allow"
  }, {
    "Action": [
      "events:*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": [
      "logs:*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": [
      "cloudtrail:*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": [
      "cloudwatch:*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": [
      "resource-groups:*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": [
      "sqs:*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": "elasticloadbalancing:*",
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": [
      "config:*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }, {
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::<account-id>:role/ApicTenantRole",
    "Effect": "Allow"
  }
]
}

```

• 信頼関係の追加:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com",

```

```

        "AWS": "arn:aws:iam::<account-d>:root"
    },
    "Action": "sts:AssumeRole"
}
]
}

```

- Cloud APIC は所有権チェックを適用して、意図的にまたは誤って行われた同じテナントとリージョンの組み合わせでポリシーが展開されないようにします。たとえば、リージョン R1 の AWS アカウント IA1 に Cloud APIC が展開されているとします。ここで、リージョン R2 にテナント TA1 を展開します。このテナント展開（TA1-R2 のアカウントとリージョンの組み合わせ）は、IA1-R1 によって所有されています。別の Cloud APIC が将来のある時点で同じテナントとリージョンの組み合わせを管理しようとした場合（たとえば、CAPIC2 がリージョン R3 の AWS アカウント IA2 に導入されている場合）、これは展開 TA1-R2 の所有者が現在、IA1-R1 であるため許可されません。つまり、1 つの Cloud APIC で管理できるのは 1 つのリージョン内の 1 つのアカウントのみです。以下の例は、いくつかの有効な展開の組み合わせと間違った展開の組み合わせを示しています。

```

Capic1:
IA1-R1: TA1-R1 - ok
        TA1-R2 - ok

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

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

```

- 所有権の強制は、AWS リソース グループを使用して行われます。リージョン R2 のアカウント TA1 の新しいテナントが Cloud APIC によって管理される場合、リソース グループ CAPIC_TA1_R2 (例: CAPIC_123456789012_us-east-2) がテナントアカウントに作成されます。このリソース グループには、値が IA1_R1_TA1_R2 のリソース タグ AciOwnerTag があります (アカウント IA1 の Cloud APIC によって管理され、リージョン R1 に展開されていると想定)。AciOwnerTag の不一致が発生した場合、テナントとリージョンの管理は中止されます。

AciOwnerTag の不一致ケースの概要は次のとおりです。

- 最初に Cloud APIC がアカウントにインストールされ、次に削除され、Cloud APIC が別のアカウントにインストールされます。既存のすべてのテナントリージョンの展開が失敗します。
- 別の TA1-R2 が同じテナントリージョンを管理しています。

所有権が一致しない場合、**再試行** (テナントリージョンの再セットアップ) は現在サポートされていません。回避策として、他の Cloud APIC が同じテナントとリージョンの組み合わせを管理していないことが確実な場合は、テナントの AWS アカウントにログオンし、影響を受けるリソース グループ (CAPIC_123456789012_us-east-2 など) を手動で削除します。次に、Cloud APIC をリロードするか、テナントを再度削除して追加します。

ステップ 1 Cloud APIC で、AWS プロバイダーを作成します。

- a) [インテント (Intent)]メニューで、ドロップダウンから [テナント (tenant)]> [tenant_name] を選択します。
- b) [インテント (Intent)]ペインで、[アプリケーション管理 (Application Management)]> [tenant_name] を選択します。

ステップ 2 次のアクションを実行します。

- a) [信頼された] テナント チェックボックスがオンになっていることを確認します。
AWS アカウントは、クラウドを使用するユーザーテナントの信頼できるアカウントである必要があります。
- b) [クラウド アカウント ID] フィールドで、クラウド アカウント ID を指定します。
- c) インフラ テナントの AWS アカウントの s3 バケットにある URL
[https://capic-common-*<infraAccountId>-data.s3.amazonaws.com/tenant-cft.json*](https://capic-common-<i><infraAccountId>-data.s3.amazonaws.com/tenant-cft.json) にあるテナント ロールの cloud-formation テンプレートを実行します。

(注) または、信頼済みフラグをオフのままにして、テナントに対して通常行われるようにアクセス鍵と秘密鍵を提供します。

ステップ 3 [保存 (Save)] をクリックします。

リリース 4.2(3) 以降のテナント AWS プロバイダーの設定

始める前に

- AWS プロバイダーは、インフラ テナント用に自動設定されます。インフラ テナント用に AWS プロバイダーを構成するために何もする必要はありません。
- すべての非インフラ テナントの場合、AWS プロバイダーは、信頼できるテナント、信頼できないテナント、または組織のテナントとして設定されます。資格情報の管理は簡単ではないため、信頼できるテナントを使用することをお勧めします。また、各テナントは個別の AWS アカウントに属する必要があります。複数のテナントで同じ AWS アカウントを共有することは許可されていません。

信頼できるテナントの場合、最初に Cisco Cloud APIC が展開されているアカウント (インフラテナントのアカウント) との信頼関係を確立します。信頼関係を確立し、テナントアカウントにアクセスするために必要なすべての権限を Cisco Cloud APIC に付与するには、最初にテナントを作成し、そのテナントにアクセスタイプとして信頼済みタグを割り当てます。次に、[テナント] ページでテナント名をクリックして、その新しい信頼できるテナントを再度表示し、テナント ウィンドウの [AWS アカウント] 領域で、[CloudFormation テンプレートの実行] リンクをクリックします。

- 組織テナントは、組織の一部であるテナントアカウントを追加するためのものです。これには、組織のマスターアカウントに Cisco Cloud APIC を展開する必要があります。

- 信頼されていないテナントは、アカウントアクセスと秘密鍵を使用します。使用されるアクセス鍵と秘密鍵は、少なくともこれらのアクセス許可を持つ IAM ユーザーのものである必要があります。作成された IAM ロールは、`ApicTenantRole` という名前にする必要があります。



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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "events:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "logs:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "cloudtrail:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "cloudwatch:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "resource-groups:*"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }, {
      "Action": [
        "sqs:*"
      ],

```

```

        "Resource": "*",
        "Effect": "Allow"
    }, {
        "Action": "elasticloadbalancing:*",
        "Resource": "*",
        "Effect": "Allow"
    }, {
        "Action": [
            "config:*"
        ],
        "Resource": "*",
        "Effect": "Allow"
    }, {
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::<account-id>:role/ApicTenantRole",
        "Effect": "Allow"
    }
]
}

```

- 信頼関係の追加:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com",
        "AWS": "arn:aws:iam::<infra-account-id>:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

- Cloud APIC は、AWS Organizations テナントのポリシーを管理するために、OrganizationAccountAccessRole IAM ロールを使用します。

- マスターアカウント内の既存の組織内で AWS アカウントを作成した場合は、その作成した AWS アカウントに組織の OrganizationAccountAccessRole IAM ロールが自動的に割り当てられます。この場合、AWS の OrganizationAccountAccessRole の IAM ロールを手動で設定する必要はありません。
- マスターアカウントが組織に参加するために既存の AWS アカウントを招待した場合は、AWS で OrganizationAccountAccessRole IAM ロールを手動で設定する必要があります。組織テナントの AWS で OrganizationAccountAccessRole IAM ロールを設定し、Cloud APIC に関連する権限があることを確認します。

OrganizationAccountAccessRole IAM ロールは、組織またはアカウントに使用される SCP (サービス制御ポリシー) とともに、組織またはアカウントに対して、組織またはアカウントに使用する SCP (サービス制御ポリシー) とともに、組織のポリシーを管理するために Cloud APIC に必要な最小限の権限が付与されている必要があります。アクセスポリシーの要件は、信頼できるテナントまたは信頼できないテナントの要件と同じです。

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```

{
  "Action": [
    "ec2:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "s3:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "events:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "logs:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "cloudtrail:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "cloudwatch:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "resource-groups:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "sqs:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": "elasticloadbalancing:*",
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": [
    "config:*"
  ],
  "Resource": "*",
  "Effect": "Allow"
}, {
  "Action": "iam:PassRole",
  "Resource": "*",
  "Effect": "Allow"
}
}

```



```
    ]
  }
}
```

組織テナントの信頼関係を追加するには:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com",
        "AWS": "arn:aws:iam::<infra-account-id>:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Cloud APIC は所有権チェックを適用して、意図的にまたは誤って行われた同じテナントとリージョンの組み合わせでポリシーが展開されないようにします。たとえば、リージョン R1 の AWS アカウント IA1 に Cloud APIC が展開されているとします。ここで、リージョン R2 にテナント TA1 を展開します。このテナント展開 (TA1-R2 のアカウントとリージョンの組み合わせ) は、IA1-R1 によって所有されています。別の Cloud APIC が将来のある時点で同じテナントとリージョンの組み合わせを管理しようとした場合 (たとえば、CAPIC2 がリージョン R3 の AWS アカウント IA2 に導入されている場合)、これは展開 TA1-R2 の所有者が現在、IA1-R1 であるため許可されません。つまり、1 つの Cloud APIC で管理できるのは 1 つのリージョン内の 1 つのアカウントのみです。以下の例は、いくつかの有効な展開の組み合わせと間違った展開の組み合わせを示しています。

```
Capic1:
IA1-R1: TA1-R1 - ok
        TA1-R2 - ok

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

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

- 所有権の強制は、AWS リソース グループを使用して行われます。リージョン R2 のアカウント TA1 の新しいテナントが Cloud APIC によって管理される場合、リソース グループ CAPIC_TA1_R2 (例: CAPIC_123456789012_us-east-2) がテナント アカウントに作成されます。このリソース グループには、値が IA1_R1_TA1_R2 のリソース タグ AciOwnerTag があります (アカウント IA1 の Cloud APIC によって管理され、リージョン R1 に展開されていると想定)。AciOwnerTag の不一致が発生した場合、テナントとリージョンの管理は中止されます。

AciOwnerTag の不一致ケースの概要は次のとおりです。

- 最初に Cloud APIC がアカウントにインストールされ、次に削除され、Cloud APIC が別のアカウントにインストールされます。既存のすべてのテナントリージョンの展開が失敗します。

- 別の TA1-R2 が同じテナントリージョンを管理しています。

所有権が一致しない場合、**再試行** (テナントリージョンの再セットアップ) は現在サポートされていません。回避策として、他の CloudAPIC が同じテナントとリージョンの組み合わせを管理していないことが確実な場合は、テナントの AWS アカウントにログオンし、影響を受けるリソースグループ (CAPIC_123456789012_us-east-2 など) を手動で削除します。次に、Cloud APIC をリロードするか、テナントを再度削除して追加します。

ステップ 1 Cloud APIC で、AWS プロバイダーを作成します。

- a) **[Intent (Intent)]** メニューで、ドロップダウンから **[テナント (tenant)]** > *[tenant_name]* を選択します。
- b) **[Intent (Intent)]** ペインで、**[アプリケーション管理 (Application Management)]** > *[tenant_name]* を選択します。

ステップ 2 次のアクションを実行します。

- a) **[AWS アカウント ID]** フィールドに、クラウドアカウント ID を指定します。
- b) **[アクセス タイプ]** 領域で、**[信頼済み]** を選択します。

AWS アカウントは、クラウドを使用しているユーザーテナントの信頼できるアカウントである必要があります。

- c) **[保存 (Save)]** をクリックします。
- d) **[テナント]** ページでテナント名をクリックして、新しい信頼できるテナントを再度表示します。

テナントの **[概要]** ページの **[AWS アカウント]** 領域に、次のメッセージが表示されます。「このテナントから設定をデプロイするには、AWS インフラアカウントとの信頼を確立する信頼できるロールをテナント AWS アカウントに作成する必要があります。これを行うには、以下のリンクを開いて CloudFormation テンプレートを実行してください」。

- e) **[CloudFormation テンプレートの実行]** リンクをクリックします。

これにより、AWS サインインページに戻ります。このページには、Cloud APIC GUI のこれらの手順で前に入力した必要な AWS アカウント情報が事前に入力されているはずですが。

- f) サインイン情報が正しいことを確認したら、AWS サインイン ページで **[次へ]** をクリックします。
- g) テナントアカウントでテナントロールの cloud-formation テンプレートを実行します。

(注) または、信頼済みフラグをオフのままにして、テナントに対して通常行われるようにアクセス鍵と秘密鍵を提供します。

ステップ 3 **[保存 (Save)]** をクリックします。

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

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

始める前に

テナントを作成します。

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

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

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

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

ステップ 4 [Name] フィールドに名前を入力します。

ステップ 5 テナントを選択します。

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

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

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

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

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

ステップ 7 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した VRF の作成

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

始める前に

テナントを作成します。

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

ステップ 2 [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、[Application Management (Application Management)] を選択します。

[Application Management (Application Management)] オプションのリストが [Intent (Intent)] メニューに表示されます。

ステップ 3 [Intent (Intent)] メニューの [Application Management (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 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 10: [VRF の作成 (Create VRF)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	[Name] フィールドに、VRF の表示名を入力します。すべての VRF に <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。
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。[VRF の作成 (Create VRF)] ダイアログボックスに戻ります。
説明	VRF の説明を入力します。
設定 > IPv4 ユニキャスト アドレス ファミリ BGP ターゲット	

[プロパティ (Properties)]	説明
フィルタの追加	<ol style="list-style-type: none"> 1. 構成するユニキャストアドレスファミリ BGP ターゲットの [ルート ターゲットの追加] オプションをクリックします。 2. [タイプ] フィールドで次のオプションをクリックして選択します。 <ul style="list-style-type: none"> • エクスポート : ルート ターゲットを他の VRF にエクスポートできます • インポート : ルート ターゲットは他の VRF からインポートされます • [ルート ターゲット] テキストボックスに、現在の VRF からエクスポートまたは現在の VRF にインポートできるルートターゲットを入力します。

ステップ 5 作業が完了したら、[保存 (Save)] をクリックします。

Cisco Cloud APIC GUI を使用した外部ネットワークの作成

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

始める前に

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

- ステップ 1** 左側のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [外部ネットワーク (External Networks)] に移動します。
構成された外部ネットワークが表示されます。
- ステップ 2** [アクション (Actions)] をクリックし、[外部ネットワークの作成 (Create External Network)] を選択します。
[外部ネットワークの作成 (Create External Network)] ウィンドウが表示されます。
- ステップ 3** 次の [外部ネットワークの作成ダイアログボックスのフィールド (Create External Network Dialog Box Fields)] の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 11: 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。
VRF	<p>この外部VRFは、外部の非 ACI デバイスとの外部接続に使用されます。この目的で複数の外部VRFを作成できます。</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 として識別されます。</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。外部VRFをクラウド コンテキスト プロファイルまたはサブネットに関連付けることはできません。</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。
ルータ タイプ	<p>ルータ タイプを選択します。</p> <ul style="list-style-type: none"> • CCR : <ul style="list-style-type: none"> • 25.0(3) よりも前のリリースでは、シスコクラウドサービス ルータ 1000V • リリース 25.0(3) 以降では、Cisco Catalyst 8000V • TGW: AWS トランジット ゲートウェイ ルーター
ホスト ルーター名	<p>このフィールドは、[ルータ タイプ (Router Type)] として CCR を選択した場合に表示されます。</p> <p>このフィールドは編集できません。デフォルトのホスト ルータが自動的に選択されます。</p>

[プロパティ (Properties)]	説明
ハブ ネットワーク	<p>このフィールドは、ルータ タイプとして TGW を選択した場合に表示されます。</p> <p>ハブ ネットワークを選択するには:</p> <ol style="list-style-type: none"> 1. [ハブ ネットワークの選択] をクリックします。 [ハブ ネットワークの選択] ダイアログボックスが表示されます。 2. [ハブ ネットワークの選択] ダイアログ ボックスで、リストから目的のハブ ネットワークをクリックし、[選択] をクリックします。 [外部ネットワークの作成 (Create External Network)] ページに戻ります。
設定	
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。 初回セットアップの一部として選択した地域がここに表示されます。 2. [地域の選択 (Select Regions)] ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)] をクリックします。 [外部ネットワークの作成 (Create External Network)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
VPN ネットワーク	

[プロパティ (Properties)]	説明
	<p>VPN ネットワーク エントリは、外部接続に使用されます。設定されたすべてのVPNネットワークが、選択したすべてのリージョンに適用されます。</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 トンネル接続先の追加 (Add IPsec Tunnel Destination)] ウィンドウが表示されます。 4. 追加する IPsec トンネル接続先の次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 バージョン: IPsec トンネル接続用に ikev1 または ikev2 を選択します。 • BGP ピア ASN • Subnet Pool Name : [サブネット プール名の選択 (Select Subnet Pool Name)] をクリックします。 [サブネット プール名の選択 (Select Subnet Pool Name)] ダイアログボックスが表示されます。リストされている使用可能なサブネット プールのいずれかを選択し、[選択 (Select)] をクリックします。 • IPsec トンネル ソース インターフェイス: このフィールドのエントリを使用して、Cisco Cloud APIC は、選択された各ソース インターフェイスから接続先 IP アドレスへの 1 つの IPsec トンネルを作成します。 (注) ikev2 は、このフィールドのデフォルト オプションです。IPsec トンネル ソース インターフェイス機能は、IKEv2 構成でのみサポートされます。 <p>gig3 は、デフォルトで選択されます。次の中から 1 つまたは複数のインターフェイスを選択します</p> <ul style="list-style-type: none"> • gig2: GigabitEthernet2 インターフェイス • gig3: GigabitEthernet3 インターフェイス • gig4: GigabitEthernet4 インターフェイス <p>(注) この外部ネットワークで IPsec トンネル ソース インターフェイスを構成した後、ルーティング ポリシー: リリース 25.0(2) (10 ページ) で説明されて</p>

[プロパティ (Properties)]	説明
	<p>いるように、同じ接続先へのトンネルを形成できる追加のネットワークで IPsec トンネル ソース インターフェイスを構成できます。</p> <p>5. [追加 (Add)] をクリックして、この IPsec 接続先を追加します。 [VPN ネットワークの追加] ウィンドウに戻ります。 別の IPsec トンネル接続先を追加する場合は、[+ IPsec ピアの追加 (+ Add IPsec Peer)] をクリックします。</p> <p>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。</p>

ステップ 4 外部ネットワークの作成が完了したら、**[保存 (Save)]** をクリックします。

[外部ネットワークの作成 (Create External Network)] ウィンドウで **[保存 (Save)]** をクリックすると、クラウドルータが AWS で構成されます。

グローバル VRF 間ルート リーク ポリシーの構成

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

始める前に

[クラウド APIC セットアップ (Cloud APIC Setup)] ウィンドウの **[コントラクト ベース ルーティング (Contract Based Routing)]** 領域で変更を行う前に、[グローバルな Inter-VRF ルート リーク ポリシー \(11 ページ\)](#) で提供された情報を確認してください。

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

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

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

ステップ 3 **[インテント (Intent)]** メニューの **[構成 (Configuration)]** リストで、**[クラウド APIC セットアップ (Cloud APIC Setup)]** をクリックします。

[セットアップ - 概要] ダイアログ ボックスが表示されます。

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

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

- **オフ**: デフォルト設定。ルートがコントラクトに基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。
- **オン (On)**: ルート マップが存在しない場合に、契約に基づいてルートが漏洩していることを示します。有効にすると、ルートマップが構成されていないときにコントラクトがルーティングを駆動します。ルートマップが存在する場合、ルートマップは常にルーティングを駆動します。

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

ある設定から別の設定に切り替える場合は、次の手順に従います。

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

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

1. 既存のコントラクトを持つ VRF のすべてのペア間で、ルート マップ ベースのルート リークを有効にします。

[Cisco Cloud APIC GUI を使用したリーク ルートの構成 \(74 ページ\)](#) の手順を実行します。

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

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

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

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

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

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

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

Cisco Cloud APIC GUI を使用したリーク ルートの構成

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

- 25.0(2) より前のリリースでは、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先の間ルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。これらの手順については、[Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 \(74 ページ\)](#) を参照してください。
- リリース 25.0(2) 以降では、内部 VRF のペア間のルート マップベースのルート リークがサポートされています。これらの手順については、[Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成 \(77 ページ\)](#) を参照してください。

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

リーク ルートの設定は、ルーティング ポリシーとセキュリティ ポリシーが別々に設定されるリリース 25.0(1) アップデートの一部です。VRF 間ルーティングを使用すると、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先との間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。詳細については、「[サポートされているルーティングとセキュリティポリシーの概要 \(7 ページ\)](#)」を参照してください。

外部宛先は、[AWS サイトと外部デバイスの間の接続の有効化 \(80 ページ\)](#) 手順を使用して手動で構成する必要があります。外部の接続先は、別のクラウド サイト、ACI オンプレミス サイト、または分散拠点である可能性があります。



- (注)
- これらの手順を使用して、リリース 25.0(1) で提供されたアップデートに基づいて、内部と外部VRFの間でのみセキュリティ ポリシーに依存しないルーティング ポリシーを設定します。
 - これらの手順を使用して、内部 VRF のペア間のルーティングを設定しないでください。その場合、リリース 25.0(1) より前の通常どおりにコントラクトを使用します。

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

設定された VRF が表示されます。

ステップ2 [リーク ルート (Leak Routes)] タブをクリックします。

すでに構成されているリーク ルートが表示されます。

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

ステップ4 次の [リーク ルートの作成ダイアログボックスのフィールド (Leak Routes 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 12: 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
Source 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います。 送信元 VRF は、内部または外部 VRF であることに注意してください。 [選択 (Select)] をクリックして、この送信元 VRF を選択します。 [リーク ルートの作成 (Create Leak Route)] ダイアログボックスに戻ります。
宛先 VRF	<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"> [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。 [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。 送信元 VRF も内部 VRF である場合、接続先 VRF を内部 VRF にすることはできないことに注意してください。 [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。

[プロパティ (Properties)]	説明
Type	<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"> • すべてをリーク: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを作成することを選択します。 この場合、デフォルトでは、エントリ 0.0.0.0/0 がサブネット IP エリアに自動的に入力されます。 • サブネット IP: 接続元 VRF から接続先 VRF までのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。[サブネット IP (Subnet IP)] ダイアログボックスが表示されます。 [サブネット IP (Subnet IP)] ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。

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

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

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

[リーク ルートの追加 (Add Leak Route)] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、[ステップ 4 \(75 ページ\)](#) ~ [ステップ 5 \(76 ページ\)](#) を繰り返します。

- リバース ルートを追加する場合は、次のようにします。
 - 以前の設定の宛先 VRF が送信元 VRF になり、
 - 以前の設定の送信元 VRF が宛先 VRF になります。

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

[リーク ルートの追加 (Add Leak Route)] ウィンドウに戻ります。[ステップ 4 \(75 ページ\)](#) ~ [ステップ 5 \(76 ページ\)](#) 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 \(75 ページ\)](#) の情報を使用して、必要な情報を入力します。送信元 VRF のエントリは事前を選択されており、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 \(75 ページ\)](#) の情報を使用して、必要な情報を入力します。宛先 VRF のエントリは事前を選択されており、この状況では変更できないことに注意してください。

次のタスク

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

- [Cisco Cloud APIC GUI を使用した EPG の作成 \(84 ページ\)](#) : 次の手順を使用して、外部 EPG を作成します。
- [Cisco Cloud APIC GUI を使用したコントラクトの作成 \(91 ページ\)](#) : これらの手順を使用して、外部 EPG とクラウド EPG 間のコントラクトを作成します。

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

リリース 25.0(2) 以降、[内部 VRF 間のルート リーク \(10 ページ\)](#) で説明されているように、内部 VRF のペア間のルート マップベースのルート リークがサポートされます。この機能は、リリース 25.0(1) で提供されたルーティングとセキュリティの分割更新を拡張したもので、ルーティングとセキュリティ ポリシーが別々に設定されています。

- ステップ 1** 左側のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [VRF] に移動します。設定された VRF が表示されます。
- ステップ 2** [リーク ルート (Leak Routes)] タブをクリックします。すでに構成されているリーク ルートが表示されます。

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

ステップ 4 次の [リーク ルートの作成ダイアログボックスのフィールド (Leak Routes 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: 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
Source 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います。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続元 VRF には内部 VRF を選択します。 [選択 (Select)] をクリックして、この送信元 VRF を選択します。 [リーク ルートの作成 (Create Leak Route)] ダイアログボックスに戻ります。
宛先 VRF	<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"> [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。 [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。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続先 VRF には内部 VRF を選択します。 [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。

[プロパティ (Properties)]	説明
Type	<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"> • すべてをリーク: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを構成することを選択します。 この場合、デフォルトでは、エン트리 0.0.0.0/0 がサブネット IP エリアに自動的に入力されます。 • サブネット IP: 接続元 VRF から 接続先 VRF までのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。[サブネット IP (Subnet IP)] ダイアログボックスが表示されます。 [サブネット IP (Subnet IP)] ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。

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

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

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

[リーク ルートの追加 (Add Leak Route)] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、[ステップ 4 \(78 ページ\)](#) – [ステップ 5 \(79 ページ\)](#) を繰り返します。

- リバースルートを追加する場合は、次のようにします。
 - 以前の設定の宛先 VRF が送信元 VRF になり、
 - 以前の設定の送信元 VRF が宛先 VRF になります。

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

[リーク ルートの追加 (Add Leak Route)] ウィンドウに戻ります。[ステップ 4 \(78 ページ\)](#) – [ステップ 5 \(79 ページ\)](#) 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 \(78 ページ\)](#) の情報を使用して、必要な情報を入力します。送信元 VRF のエントリーは事前に選択されており、この状況では変更できないことに注意してください。
 - この VRF にリークルートを追加するには、[アクション (Actions)] をクリックし、[<VRF_name> にリーク ルートを追加 (Add Leak Route to <VRF_name>)] を選択します。
[リーク ルートの追加 (Add Leak Router)] ウィンドウが表示されます。 [ステップ 4 \(78 ページ\)](#) の情報を使用して、必要な情報を入力します。宛先 VRF のエントリーは事前に選択されており、この状況では変更できないことに注意してください。

AWS サイトと外部デバイス間の接続の有効化

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

外部デバイス構成ファイルのダウンロード

- ステップ 1** Cisco Cloud APIC GUI で、[ダッシュボード (Dashboard)] をクリックします。Cisco Cloud APIC のダッシュボードが表示されます。
- ステップ 2** [インフラストラクチャ]>[外部接続]に移動します。[外部接続 (External Connectivity)] ウィンドウが表示されます。
- ステップ 3** [アクション (Actions)]>[外部デバイス構成ファイルのダウンロード (Download External Device Configuration Files)] をクリックします。[外部デバイス構成ファイルのダウンロード (Download External Device Configuration Files)] ポップアップが表示されます。
- ステップ 4** ダウンロードする外部デバイス構成ファイルを選択し、[ダウンロード (Download)] をクリックします。このアクションにより、CCR への IPv4 接続のための外部デバイスの手動構成に使用する構成情報を含む zip ファイルがダウンロードされます。

AWS サイトと外部デバイスの間の接続の有効化

- ステップ 1** インフラ VPC CCR から EVPN を使用しない外部デバイスへの IPv4 接続を手動で有効にするために必要な情報を収集します。
- ステップ 2** 外部デバイスにログインします。
- ステップ 3** 外部ネットワークング デバイスを接続するための構成情報を入力します。

[外部デバイス構成ファイルのダウンロード \(80 ページ\)](#) の手順を使用して外部デバイス構成ファイルをダウンロードした場合、最初のトンネルの構成情報を見つけて、その構成情報を入力します。

最初のトンネルの外部デバイス設定ファイルの例を示します。

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

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

vrf definition infra:externalvrf1
  rd 1:1

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

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

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

crypto ikev2 keyring keyring-ikev2-100
```

```

peer peer-ikev2-keyring
  address 13.88.168.176
  pre-shared-key devicelazure
exit
exit

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

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

crypto ipsec profile ikev2-100
  set transform-set ikev2-100
  set pfs group14
  set ikev2-profile ikev2-100
exit

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

ip route 13.88.168.176 255.255.255.255 GigabitEthernet2 GIG-GATEWAY

router bgp 65015

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

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

  distance bgp 20 200 20
exit-address-family

```

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

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

```

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 <abdefgl2345>
!
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

Cisco Cloud APIC GUI を使用した EPG の作成

```

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

```

Ikev2 Global Configurations

IPSec and Ikev2
Per Tunnel Configurations

ステップ 4 前の手順を繰り返して、追加のトンネルを構成します。

Cisco Cloud APIC GUI を使用した EPG の作成

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

始める前に

アプリケーションプロファイルと VRF を作成します。

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

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

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

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

ステップ 4 次の [EPG 作成ダイアログボックスのフィールド (Create EPG 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: [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
名前 (Name)	EPG の名前を入力します。
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、[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"> 1. [アプリケーション プロファイルの選択 (Select Application Profile)] をクリックします。[アプリケーション プロファイルの選択 (Select Application Profile)] ダイアログボックスが表示されます。 2. [アプリケーション プロファイルの選択 (Select Application Profile)] ダイアログで、左側の列のアプリケーション プロファイルをクリックして、[選択] をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定 (Settings)]	
タイプ (Type)	<p>EPG タイプを選択します。</p> <ul style="list-style-type: none"> • クラウド - クリックして、クラウドに EPG を作成します。 • 外部 - クリックして外部 EPG を作成します。

[プロパティ (Properties)]	説明
ルート到達可能性	<p>(外部 EPG の作成時に表示されます) [ルート到達性 (Route Reachability)] ドロップダウンリストをクリックして、次を選択します。</p> <ul style="list-style-type: none"> • オンプレミス • インターネット • [Unspecified]
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"> 1. [VRF の選択 (Select VRF)] をクリックします。 [VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 2. [VRF の選択 (Select VRF)] ダイアログで、左側の列の VRF をクリックして選択し、[選択 (Select)] をクリックします。 [EPG の作成 (Create EPG)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
エンドポイントセレクタ	

[プロパティ (Properties)]	説明
	<p>(注) エンドポイントセレクタ構成プロセスの一部として AWS で仮想マシンを設定する手順については、AWS でのインスタンスの設定 (102 ページ) を参照してください。</p> <p>エンドポイントセレクタを追加するには：</p> <ol style="list-style-type: none"> 1. [エンドポイントセレクタの追加 (Add Endpoint Selector)]をクリックして、[エンドポイントセレクタの追加] ダイアログを開きます。 2. [エンドポイントセレクタの追加 (Add Endpoint Selector)]ダイアログの[Name (名前)]フィールドに名前を入力します。 3. [セレクタ式 (Selector Expression)]をクリックします。[キー (Key)]、[演算子 (Operator)]、および[値 (Value)]フィールドが有効になります。 4. [キー (Key)]ドロップダウンリストをクリックしてキーを選択します。次のオプションがあります。 <ul style="list-style-type: none"> • エンドポイントセレクタに IP アドレスまたはサブネットを使用する場合は、[IP]を選択します。 • エンドポイントセレクタにアベイラビリティゾーンを使用する場合は、[ゾーン]を選択します。 • エンドポイントセレクタに Amazon Web Services リージョンを使用する場合は、[リージョン (Region)]を選択します。 • エンドポイントセレクタのカスタムキーを作成する場合は、[カスタム (Custom)]を選択します。 <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>

[プロパティ (Properties)]	説明
	<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。</p> <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。 • [の中にある (Not In)]: 値フィールドに複数のカンマ区切り値がある場合に使用されます。 • [キーを持つ (Has Key)]: 式にキーのみが含まれている場合に使用されます。 • [キーを持たない (Does Not Have Key)]: 式にキーのみが含まれている場合に使用されます。 <p>6. [値 (Value)] フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。入力する値は、[キー (Key)] フィールドと [演算子 (Operator)] フィールドで選択した内容によって異なります。たとえば、[キー (Key)] フィールドが [IP] に設定され、[演算子 (Operator)] フィールドが [等しい (equals)] に設定されている場合、[値 (Value)] フィールドはIPアドレスまたはサブネットでなければなりません。ただし、[演算子 (Operator)] フィールドが [キー (keys)] に設定されている場合、[値 (Value)] フィールドは無効になります。</p> <p>7. 完了したら、チェックマークをクリックしてセレクト式を検証します。</p>

[プロパティ (Properties)]	説明
	<p>8. エンドポイントセレクタに追加のエンドポイントセレクタ式を作成するかどうかを決定します。単一のエンドポイントセレクタで複数の式を作成した場合、それらの式の間には論理ANDがあるものとみなされます。</p> <p>たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。</p> <ul style="list-style-type: none"> • エンドポイントセレクタ 1、式 1: <ul style="list-style-type: none"> • [キー (Key):] Zone • 演算子 (Operator) : equals • [値 (Value):] us-west-1a • エンドポイントセレクタ 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(アベイラビリティゾーンが us-west-1a 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、前のステップで説明したようにエンドポイントセクタ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2、式1: <ul style="list-style-type: none"> • [キー (Key):] Region • 演算子 : in • [値 (Value):] us-east-1a, us-east-2 <p>その場合、次のようになります。</p> <ul style="list-style-type: none"> • アベイラビリティゾーンが us-west-1a で、IPアドレスが 192.0.2.1/24 サブネットに属している (エンドポイントセクタ1の式) <p>または</p> <ul style="list-style-type: none"> • リージョンが us-east-1a または us-east-2 (エンドポイントセクタ2の式) のいずれかである <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 APIC GUI を使用したコントラクトの作成

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

始める前に

フィルタを作成します。

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

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

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

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

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

表 15: [**コントラクトの作成 (Create Contract)**] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	契約の名前を入力します。
テナント	テナントを選択します。 <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。[コントラクトの作成 (Create Contract)] ダイアログボックスに戻ります。
説明	コントラクトの説明を入力してください。
[設定 (Settings)]	

[プロパティ (Properties)]	説明
<p>スコープ</p>	<p>このスコープは、同じアプリケーションプロファイル内、同じVRFインスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイントグループにコントラクトを制限します。</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>共有サービスの詳細については、共有サービス (51 ページ) を参照してください。</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 • Global • テナント
<p>フィルタを両方向に適用</p>	<p>チェックボックスをオンにして、コンシューマーからプロバイダーおよびプロバイダーからコンシューマーへのトラフィックに同じフィルターを適用します。トラフィックの方向ごとに異なるフィルターを適用する場合は、ボックスにチェックを入れしないでください。</p> <p>デフォルトでチェックボックスはオンになっています。</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"> 1. [フィルタの追加 (Add Filter)]をクリックします。フィルタ行が表示され、[フィルタの選択 (Select Filter)]オプションが表示されます。 2. [フィルタの選択 (Select Filter)]をクリックします。[フィルタの選択 (Select Filter)]ダイアログボックスが表示されます。 3. [フィルタの選択 (Select Filter)]ダイアログで、左側の列のフィルタをクリックして選択し、[選択 (Select)]をクリックします。[コントラクトの作成 (Create Contract)]ダイアログボックスに戻ります。

ステップ 5 設定が終わったら [Save] をクリックします。

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

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

始める前に

- コントラクトを設定できます。
- EPG が設定済みです。

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

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

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

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

ステップ 4 コントラクトを選択します。

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

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

ステップ 5 コンシューマ EPG を追加するには、次の手順を実行します。

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

Cisco Cloud APIC GUI を使用したフィルタの作成

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

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

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

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

ステップ 3 [インテント (Intent)] メニューの [アプリケーション管理 (Application Management)] リストで、[フィルタの作成 (Create Filter)] 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 16: フィルタの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
テナント	テナントを選択します。 <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。[フィルタの作成 (Create)]ダイアログボックスに戻ります。
説明	フィルタの説明を入力します。

[プロパティ (Properties)]	説明
Add Filter	

[プロパティ (Properties)]	説明
	<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 エントリの作成 (Create Filter Entry)] 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. [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。 4. [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、残りのフィールドが無効になります。</p> 5. [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> 6. [送信元ポート (Origin Port)] の [開始] と [終了] フィールドに適切なポート情報を入力します。 7. [宛先ポート (Origin Port)] の [開始] と [終了]

[プロパティ (Properties)]	説明
	<p>フィールドに適切なポート情報を入力します。</p> <p>8. 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。</p>

ステップ 5 作業が完了したら、[保存 (Save)]をクリックします。

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

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

始める前に

VRF を作成します。

ステップ 1 [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。

構成されたクラウド コンテキスト プロファイルのリストが表示されます。

ステップ 2 [アクション (Actions)]>[クラウド コンテキスト プロファイル) Create Cloud Context Profile] を順に選択します。

[クラウド コンテキスト プロファイルの作成 (Create Cloud Context Profile)]ダイアログ ボックスが表示されます。

ステップ 3 次の [クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド (Create Cloud Context Profile 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 17: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。

[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、[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	(オプション) 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。
[設定 (Settings)]	
地域を選択	<p>リージョンを選択するには:</p> <ol style="list-style-type: none"> 1. [リージョンの選択 (Select Region)]をクリックします。[リージョンの選択 (Select Region)]ダイアログボックスが表示されます。 2. [リージョンの選択 (Select Region)]ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)]をクリックします。[クラウドコンテキストプロファイルの作成 (Create Cloud Context Profile)]ダイアログボックスで、次の手順を実行します。
VRFの選択(Select 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"> 1. [VRFの選択 (Select VRF)]をクリックします。[VRFの選択 (Select VRF)]ダイアログボックスが表示されます。 2. [VRFの選択 (Select VRF)]ダイアログで、左側の列のVRFをクリックして選択し、[選択 (Select)]をクリックします。[クラウドコンテキストプロファイルの作成 (Create Cloud Context Profile)]ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
CIDR の追加 (Add CIDR)	<p>(注) 次のサブネットは予約済みであり、この [CIDR の追加 (Add CIDR)] フィールドでは使用しないでください。</p> <ul style="list-style-type: none"> • 169.254.0.0/16 (トランジット ゲートウェイへの VPN トンネル用に予約済み) • 192.168.100.0/24 (ブリッジドメインインターフェイス用に CCR によって予約済み) <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"> 1. [CIDR の追加 (Add CIDR)] をクリックします。[CIDR の追加 (Add CIDR)] ダイアログボックスが表示されます。 2. [アドレス (Address)] フィールドに IP アドレスを入力します。 3. [サブネットの追加 (Add subnet)] をクリックして、サブネット アドレスを [アドレス (Address)] に入力します。 4. アベイラビリティゾーンを追加するには: <ol style="list-style-type: none"> 1. [アベイラビリティ ゾーン の 選択 (Select Availability Zone)] を選択します。[アベイラビリティ ゾーン の 選択 (Select Availability Zone)] ダイアログボックスが表示されます。 2. [アベイラビリティ ゾーン の 選択] ダイアログボックスで、左側の列でアベイラビリティゾーンをクリックして選択します。 リリース 25.0(2) 以降、このウィンドウに表示されるアベイラビリティゾーンのタイプは、このクラウドコンテキストプロファイルに選択したテナントのタイプによって異なります。 (注) ユーザー テナントでクラウドコンテキストプロファイルを作成している場合、このウィンドウでは クラウドアベイラビリティゾーン のみに制限されます。 詳細については、「可用性ゾーン (37 ページ)」を参照してください。 3. [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。 5. [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。 6. 完了したら、[追加 (Add)] をクリックします。

[プロパティ (Properties)]	説明
VPNゲートウェイルータ	(オプション) VPN ゲートウェイルータ のチェックボックスをクリックしてオン(有効)またはオフ(無効)にします。
TGW 添付ファイル	(オプション) TGW 添付ファイル のチェックボックスをクリックしてオン(有効)またはオフ(無効)にします。

ステップ4 設定が終わったら [Save] をクリックします。

AWS でのインスタンスの設定

Cisco Cloud APIC のためのエンドポイントセレクトアを設定するとき、Cisco Cloud APIC のために構成されたエンドポイントセレクトアに対応する AWS で必要になるインスタンスを構成するためにも必要です。

このトピックでは、AWS でインスタンスを設定する手順について説明します。Cisco Cloud APIC のためのエンドポイントセレクトアを設定する前に、または後で、これらの手順を使用して AWS のインスタンスを設定することができます。たとえば、先に AWS のアカウントに移動し、AWS のカスタム タグまたはラベルを作成してから、Cisco Cloud APIC のカスタム タグまたはラベルを使用して、エンドポイントセレクトアを作成することができます。または、Cisco Cloud APIC でカスタム タグまたはラベルを使用してエンドポイントセレクトアを作成してから、AWS のアカウントに移動し、AWS 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。

ステップ1 クラウドコンテキストプロファイルの設定を確認し、AWS インスタンスで使用する設定を決定します。

AWS インスタンスの構成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、後で AWS にプッシュされます。

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

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブオプションのリストが表示されます。

- b) **[クラウドコンテキストプロファイル (Cloud Context Profiles)]** サブタブ オプションを選択します。

Cisco Cloud APIC 用に作成したクラウドコンテキストプロファイルのリストが表示されます。

- c) この AWS 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。AWS インスタンスを設定するときには、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** まだログインしていない場合は、Cisco Cloud APIC ユーザテナントの Amazon Web Services アカウントにログインします。
- ステップ 3** [サービス (Services)] > [EC2] > [インスタンス (Instances)] > [インスタンスの起動 (Launch Instance)] に移動します。
- ステップ 4** [Amazon マシン イメージ (AMI) の選択 (Choose Amazon Machine Image (AMI))] ページで、Amazon マシン イメージ (AMI) を選択します。
- ステップ 5** [インスタンス タイプの選択 (Choose An Instance type)] ページで、インスタンス タイプを選択し、[インスタンスの詳細の設定 (Configure instance Detail)] をクリックします。
- ステップ 6** [インスタンスの詳細の設定 (Configure instance Detail)] ページで、該当するフィールドに必要な情報を入力します。

- [ネットワーク (Network)] フィールドで、Cisco Cloud APIC VRF を選択します。

これは、この AWS インスタンス設定プロセスの一部として使用しているクラウド コンテキスト プロファイルに関連付けられている VRF です。

- [サブネット (Subnet)] フィールドに、サブネットを入力します。

- パブリック IP を使用する場合は、[パブリック IP の自動割り当て (Auto Assign public IP)] フィールドで、スクロールダウンメニューから [有効 (Enable)] を選択します。

- ステップ 7** [インスタンスの詳細の設定 (Configure Instance Details)] ページに必要な情報を入力したら、[ストレージを追加 (Add Storage)] をクリックします。
- ステップ 8** [ストレージの追加 (Add Storage)] ページで、デフォルト値を受け入れるか、必要に応じてこのページでストレージを設定し、[タグの追加 (add Tags)] をクリックします。
- ステップ 9** [タグの追加 (Add Tags)] ページで、[タグの追加 (add Tag)] をクリックし、このページの該当するフィールドに必要な情報を入力します。

(注) これらの手順の後の部分で、エンドポイントセクタのタイプに対して IP アドレス、リージョン、またはゾーンを使用する場合は、このページに情報を入力する必要はありません。このような状況では、AWS でインスタンスを開始すると、Cisco Cloud APIC によって IP アドレス、リージョン、またはゾーンが検出され、エンドポイントが EPG に割り当てられます。

- [キー (Key):] これらの手順で後で追加するエンドポイントセクタのタイプのカスタム タグを作成するときに使用するキーを入力します。
- [値 (Value):] このキーで使用する値を入力します。
- [インスタンス (Instance):] このフィールドのチェックボックスをオンにします。
- [ボリューム (Volume):] このフィールドのチェックボックスをオンにします。

たとえば、これらの手順で後ほど、エンドポイントセクタの特定のビルディングのカスタム タグを作成する予定の場合 (building6 など) は、このページの次のフィールドに次の値を入力できます。

- [キー (Key):] ロケーション
- [値 (value):] building6

ステップ 10 [確認して起動する (Review and Launch)] をクリックします。

既存のキー ペアを選択するか、新しいキー ペアを作成します。キーペアの ページが表示されます。後ほどインスタンスに ssh 接続する場合は、このページの情報を使用します。

Cisco Cloud APIC GUI を使用したバックアップ構成の作成

ここでは、バックアップ構成を作成する方法を説明します。

始める前に

必要に応じて、リモート ロケーションとスケジューラを作成します。

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

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

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

ステップ 3 [インテント (Intent)] の [操作 (Operations)] リストから、[バックアップ構成の作成 (Create Backup Configuration)] をクリックします。[バックアップ構成の作成 (Create Backup Configuration)] ダイアログ ボックスが表示されます。

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

表 18: バックアップ構成の作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
バックアップオブジェクト	

[プロパティ (Properties)]	説明
	<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。 • デバイス : [SelectfvcloudLBCtx] プションが表示されます。 • サービス グラフ : 選択すると、[Select Service Graph] オプションが表示されます。 • [クラウド コンテキスト プロファイル (Cloud Context Profile)] : これを選

[プロパティ (Properties)]	説明
	<p>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> <ol style="list-style-type: none"> 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ます。 3. Select <object_name> ダイアログから左側の列のオプションからクリックして選んで、[選択 (Select)] をクリックします。[バックアップ構成の作成 (Create Backup Configuration)] ダイアログ ボックスに戻ります。 <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> <ul style="list-style-type: none"> • 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。 <ol style="list-style-type: none"> 1. [オブジェクトDN (Object DN)] フィールドに、バックアップするオブジェクトツリーのルートとして使用する特定のオブジェクトの DN を入力します。
スケジューラ	<ol style="list-style-type: none"> 1. [スケジューラの選択 (Select Scheduler)] をクリックして[スケジューラの選択 (Select Scheduler)] ダイアログを開き、左側の列からスケジューラを選択します。 2. 終了したら、右下隅にある[選択 (Select)] ボタンをクリックします。
作成後のバックアップのトリガー	<p>次のいずれかを選択します。</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 APIC GUI を使用したテクニカル サポート ポリシーの作成

このセクションでは、テクニカル サポート ポリシーを作成する方法について説明します。

始める前に

リモート ロケーションのテクニカル サポート ポリシーを作成する場合は、まずリモート ロケーションを作成する必要があります。

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

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

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

ステップ3 [**インテント (Intent)**] の [操作 (Operations)] リストから、[**テクニカル サポートの作成 (Create Tech Support)**] をクリックします。[**テクニカル サポートの作成 (Create Tech Support)**] ダイアログ ボックスが表示されます。

ステップ4 次の [テクニカル サポートの作成ダイアログボックスのフィールド (Create Tech Support Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

表 19: テクニカル サポートの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
エクスポート先	<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>
作成後のトリガー	<p>ポリシーの作成後にテクニカル サポート ポリシーを作成する場合は、[有効] (デフォルト) チェックボックスをクリックしてオンにします。無効にするには、チェックボックスをオフにします。</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 APIC GUI を使用したトリガー スケジューラの作成

このセクションでは、トリガー スケジューラの作成方法について説明します。

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

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

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

ステップ 3 [インテント (Intent)] 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。[トリガー スケジューラの作成 (Create Trigger Scheduler)] ダイアログボックスが表示されます。

ステップ 4 次の [トリガー 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 20: トリガー スケジューラの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
繰り返しウィンドウ	<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">1. [スケジュール (Schedule)] ドロップダウンリストから、次のいずれかを選択します。<ul style="list-style-type: none">• 毎日• 月曜日• 火曜日• 水曜日• 木曜日• 金曜日• 土曜日• 日曜日• 奇数日• 偶数日2. [開始時間 (Start Time)] フィールドに、時間を入力します。3. [最大同時タスク数 (Maximum Concurrent Tasks)] フィールドから数値を入力するか、フィールドを空白のままにして無制限を指定します。4. [最大実行時間 (Maximum Running Time)] で、[無制限 (Unlimited)] または [カスタム (Custom)] をクリックして選択します。5. 終了したら、[Add] をクリックします。

[プロパティ (Properties)]	説明
ワンタイム ウィンドウの追加	<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 APIC GUI を使用したリモート ロケーションの作成

このセクションでは、Cisco Cloud APIC を使用したリモート ロケーションの作成方法について説明します。

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

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

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

ステップ 3 [インテント (Intent)] メニューの [操作 (Operations)] リストで、[リモート ロケーションの作成 (Create Remote Location)] をクリックします。[リモート ロケーションの作成 (Create Remote Location)] ダイアログボックスが表示されます。

ステップ 4 次の [リモート ロケーションの作成ダイアログボックスのフィールド (Create Remote Location Box Fields)] テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 21: リモート ロケーションの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	

[プロパティ (Properties)]	説明
名前	リモート ロケーション ポリシーの名前を入力します。
説明	リモート ロケーション ポリシーの説明を入力します。
Settings	
Hostname/IP Address	リモート ロケーションのホスト名または IP アドレスを入力します
Protocol	プロトコルを選択します。 <ul style="list-style-type: none"> • FTP • SFTP • SCP
Path	リモート ロケーションのパスを入力します。
Port	リモート ロケーションのポートを入力します。
Username	リモート ロケーションのユーザー名を入力します。
認証タイプ	SFTP または SCP を使用する場合は、認証タイプを選択します。 <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。
管理EPG	<ol style="list-style-type: none"> 1. [管理 EPG の選択] をクリックします。[管理 EPG の選択] ダイアログが表示されます。 2. 左側の列で、 をクリックして管理 EPG を選択します。 3. [選択 (Select)] をクリックします。

ステップ5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したローカル ドメインの作成

このセクションでは、クラウド APIC GUI を使用したログイン ドメインの作成方法について説明します。

始める前に

非ローカルドメインを作成する前に、プロバイダーを作成します。

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

ステップ2 [Intent] 検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative] を選択します。

[Intent] メニューに管理オプションのリストが表示されます。

ステップ3 [インテント (Intent)] メニューの [管理 (Administrative)] リストで、[**ログインドメインの作成 (Create Login Domain)**] をクリックします。[**ログインドメインの作成 (Create Login Domains)**] ダイアログボックスが表示されます。

ステップ4 次の [ログインドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

表 22: 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"> • Local • LDAP : プロバイダーを追加し、認証タイプを選択する必要があります。 • RADIUS : プロバイダーを追加する必要があります。 • TACACS+ : プロバイダーの追加が必要です。 • SAML : プロバイダーの追加が必要です。

[プロパティ (Properties)]	説明
プロバイダ	<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	<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 APIC GUI を使用したプロバイダーの作成

このセクションでは、クラウド APIC GUI を使用したプロバイダーの作成方法について説明します。

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

ステップ 2 **[Intent]** 検索ボックスの下にあるドロップダウン矢印をクリックし、 **[Administrative]** を選択します。

[Intent] メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント (Intent)]** メニューの **[管理 (Administrative)]** リストで、 **[プロバイダーの作成 (Create Provider)]** をクリックします。 **[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。

ステップ 4 次の [プロバイダーの作成ダイアログボックスのフィールド (Create Provider 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 23: プロバイダ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
ホスト名/IP アドレス	プロバイダーのホスト名またはIPアドレスを入力します。
説明	プロバイダーの説明を入力します。
タイプ (Type)	<p>[タイプ (Type)] ドロップダウンリストから、次のいずれかのタイプを選択します。</p> <ul style="list-style-type: none"> • LDAP • RADIUS • TACACS+ • SAML <p>(注) 選択したタイプに基づいて一連のフィールドが表示されます。</p>
[LDAP] 設定	
[バインド DN (Bind DN)]	LDAP バインド DN を入力します。
[ベース DN (Base DN)]	LDAP ベース DN を入力します。
Password	LDAP 設定のパスワードを入力します。
Confirm Password	LDAP 設定のパスワードを再入力します。
[ポート (Port)]	プロバイダー タイプのポート番号を入力します。
詳細設定	プロバイダーダイアログボックスの [設定] セクションに追加フィールドを表示します。
タイムアウト(秒)	タイムアウトが発生するまでの許容秒数を入力します。デフォルトは 30 です。
リトライ (Retries)	許可された再試行数を設定します。デフォルトは 1 です。
[SSL]	SSL を有効にするには、[SSL] チェックボックスをクリックしてオンにします。SSL を無効にするには、[SSL] チェックボックスをクリックしてオフにします。デフォルトではイネーブルになっています。

[プロパティ (Properties)]	説明
SSL証明書の検証レベル	次のいずれかを実行します。 <ul style="list-style-type: none"> • 許可 • 厳格な設定(RFC2821準拠)
[Attribute]	[属性] テキスト ボックスに LDAP 属性を入力します。
フィルタタイプ	フィルタ タイプを選択します。 <ul style="list-style-type: none"> • Default • Microsoft AD • Custom
フィルタ (Filter)	テキストボックスにLDAPフィルタを入力します。このオプションは、 カスタム フィルタ タイプが選択されている場合にのみ表示されます。
[管理 EPG の選択 (Select Management EPG)]	管理 EPG を追加するには: <ol style="list-style-type: none"> 1. [管理 EPG の選択 (Select Management EPG)] 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 EPG を選択します。 3. [選択] をクリックして、管理 EPG を LDAP に追加します。
サーバーモニタリング	サーバーの監視を有効にするには、[有効] チェックボックスをクリックしてオンにします。サーバーの監視を無効にするには、[有効] チェックボックスをクリックしてオフにします。デフォルトではディセーブルになっています。
[RADIUS] 設定	
Key	RADIUS キーを入力します。
確認キー	RADIUS キーを再入力します。
詳細設定	プロバイダーダイアログボックスの[設定]セクションに追加フィールドを表示します。

[プロパティ (Properties)]	説明
[ポート (Port)]	RADIUS 設定のポート番号を入力します。デフォルトは 1812 です。
[認証プロトコル (Authentication Protocol)]	次の中から選択します。 <ul style="list-style-type: none"> • PAP : (デフォルト) • CHAP • MS-CHAP
タイムアウト(秒)	タイムアウトが発生するまでの許容秒数を入力します。デフォルトは 5 分です。
リトライ (Retries)	許可された再試行数を設定します。デフォルトは 1 です。
[管理 EPG の選択 (Select Management EPG)]	管理 EPG を追加するには: <ol style="list-style-type: none"> 1. [管理 EPG の選択 (Select Management EPG)] 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 EPG を選択します。 3. [選択] をクリックして、管理 EPG を RADIUS に追加します。
サーバーモニタリング	サーバーの監視を有効にするには、[有効] チェックボックスをクリックしてオンにします。サーバーの監視を無効にするには、[有効] チェックボックスをクリックしてオフにします。デフォルトではディセーブルになっています。
[TACACS+] 設定	
Key	TACACS+ キーを入力します。
確認キー	TACACS+ キーを再入力します。
詳細設定	プロバイダーダイアログボックスの [設定] セクションに追加フィールドを表示します。
[ポート (Port)]	TACACS+ 設定用のポート番号を入力します。デフォルトは 1812 です。

[プロパティ (Properties)]	説明
[認証プロトコル (Authentication Protocol)]	次の中から選択します。 <ul style="list-style-type: none"> • CHAP • MS-CHAP • PAP : (デフォルト)
タイムアウト(秒)	タイムアウトが発生するまでの許容秒数を入力します。デフォルトは5分です。
リトライ (Retries)	許可された再試行数を設定します。デフォルトは1です。
[管理 EPG の選択 (Select Management EPG)]	管理 EPG を追加するには: <ol style="list-style-type: none"> 1. [管理 EPG の選択 (Select Management EPG)] 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 EPG を選択します。 3. [選択] をクリックして、管理 EPG を TACACS+ に追加します。
サーバーモニタリング	サーバーの監視を有効にするには、[有効] チェックボックスをクリックしてオンにします。サーバーの監視を無効にするには、[有効] チェックボックスをクリックしてオフにします。デフォルトではディセーブルになっています。
[SAML] 設定	
ID プロバイダー	次のアイデンティティ プロバイダーから選択します。 <ul style="list-style-type: none"> • ADFS : (デフォルト) • OKTA • PING アイデンティティ
[IDプロバイダーのメタデータのURL (Identity Provider Metadata URL)]	アイデンティティプロバイダーから提供されたメタデータ URL を入力します。
Entity ID	SAML エンティティ識別子として一意の ID を入力します。

[プロパティ (Properties)]	説明
メタデータ URL の HTTPS プロキシ	ID プロバイダーのメタデータ URL にアクセスするために使用される HTTPS プロキシを入力します。
詳細設定	プロバイダーダイアログボックスの [設定] セクションに追加フィールドを表示します。
GUI リダイレクトバナー メッセージ (URL)	GUI リダイレクトバナーメッセージを入力します。
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、左側のペインに証明書リストが表示されます。 2. クリックして証明書を選択します。 3. [選択] をクリックして証明書を追加します。[プロバイダーの作成 (Create)] ダイアログボックスに戻ります。
タイムアウト(秒)	タイムアウトが発生するまでの許容秒数を入力します。デフォルトは5分です。
リトライ (Retries)	許可された再試行数を設定します。デフォルトは1です。
[署名アルゴリズム認証ユーザー要求 (Signature Algorithm Authentication User Requests)]	<p>[リクエストの署名アルゴリズム] ドロップダウンリストをクリックし、次のいずれかを選択します。</p> <ul style="list-style-type: none"> • RSA SHA1 • RSA SHA224 • RSA SHA256 (デフォルト) • RSA SHA384 • RSA SHA512
SAML 認証要求の署名	有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。

[プロパティ (Properties)]	説明
SAML応答メッセージの署名	有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。
SAML応答の署名アサーション	有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。
SAMLアサーションの暗号化	有効にするには、チェックボックスをクリックしてチェックを入れます。無効にするには、チェックボックスをクリックしてチェックを外します。デフォルトではイネーブルになっています。

ステップ5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したセキュリティドメインの作成

セキュリティドメインは、追加するセキュリティドメインにテナントを制限します。セキュリティドメインを追加しない場合、すべてのセキュリティドメインがこのテナントにアクセスできます。このセクションでは、GUI を使用してセキュリティドメインを作成する方法について説明します。

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

ステップ2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ3 [Intent]メニューの[Administrative]リストで、[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 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したロールの作成

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

- ステップ 1** インテント アイコンをクリックします。[**インテント (Intent)**] メニューが表示されます。
- ステップ 2** [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。
[Intent]メニューに管理オプションのリストが表示されます。
- ステップ 3** [Intent]メニューの [Administrative] リストで、[**セキュリティドメインの作成 (Create Security Domain)**] をクリックします。[**ロールの作成 (Create Role)**] ダイアログボックスが表示されます。
- ステップ 4** 次の [ロールの作成ダイアログボックスのフィールド (Create Role 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 24: ロールの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
特権	

[プロパティ (Properties)]	説明
	<p>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ینگ、インポート/エクスポート ポリシーの設定に使用されます。 • access-connectivity-l1 インフラの下のレイヤ1設定に使用されます。例: セクタとポートレイヤ1のポリシー設定。 • access-connectivity-l2 : インフラの下のレイヤ2設定に使用されます。例: セクタおよび接続可能なエンティティ設定をカプセル化します。 • access-connectivity : インフラでのレイヤ3の設定、テナントのL3Outでのスタティックルート設定に使用されます。 • access-connectivity-mgmt : 管理インフラ ポリシーに使用されます。 • access-connectivity-util : テナント ERSPAN ポリシーに使用されます。 • access-equipment : アクセスポートの設定に使用されます。 • access-protocol-l1 : インフラのレイヤ1プロトコル設定に使用されます。 • access-protocol-l2 : インフラのレイヤ2プロトコル設定に使用されます。 • access-protocol-l3 : インフラでのレイヤ3プロトコル設定に使用されます。 • access-protocol-mgmt : NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • access-protocol-ops : クラスタポリシーやファームウェアポリシーなどの操作関連のアクセスポリシーに使用されます。 • access-protocol-util : テナント ERSPAN ポリシーに使用されます。 • access-qos : CoPP および QoS に関連するポリシーの変更に使用されます。

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • admin : すべてへのアクセス (すべてのロールの組み合わせ) • fabric-connectivity-l1 : ファブリックの下のレイヤ 1 設定に使用されます。例: セレクタおよびポート レイヤ 1 のポリシーと vPC 保護。 • fabric-connectivity-l2 : ポリシー展開の影響を推定するための警告を生成するために、ファームウェアおよび展開ポリシーで使用されます。 • fabric-connectivity-l3 : ファブリックの下のレイヤ 3 設定に使用されます。例: ファブリック IPv4 および MAC 保護グループ。 • fabric-connectivity-mgmt : リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、および診断ポリシーに使用されます。 • fabric-connectivity-util : リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーに使用されます。 • fabric-equipment : リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーに使用されます。 • fabric-protocol-l1 : ファブリックの下のレイヤ 1 プロトコル設定に使用されます。 • fabric-protocol-l2 : ファブリックの下のレイヤ 2 プロトコル設定に使用されます。 • fabric-protocol-l3 : ファブリックの下のレイヤ 3 プロトコル設定に使用されます。 • fabric-protocol-mgmt : NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • fabric-protocol-ops : ERSPAN およびヘルス スコア ポリシーに使用されます。 • fabric-protocol-util : ファームウェア管理の traceroute およびエンドポイント トラッキング ポリシーに使用されます。 • none : 特権なし。

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • nw-svc-device : レイヤ 4 からレイヤ 7 のサービス デバイスを管理するために使用されます。 • nw-svc-devshare : 共有レイヤ 4 ~ レイヤ 7 サービス デバイスの管理に使用されます。 • nw-svc-params : レイヤ 4 ~ レイヤ 7 のサービス ポリシーの管理に使用されます。 • nw-svc-policy : レイヤ 4 ~ レイヤ 7 のネットワーク サービス オーケストレーションの管理に使用されます。 • ops : アトミック カウンタ、SPAN、TSW、技術サポート、トレースルート、分析、コア ポリシーなど、ポリシーのモニタリングとトラブルシューティングを含む動作ポリシーに使用されます。 • tenant-connectivity-11 : ブリッジドメインやサブネットなど、レイヤ 1 接続の変更に使用されます。 • tenant-connectivity-12 : ブリッジドメインやサブネットなど、レイヤ 2 接続の変更に使用されます。 • tenant-connectivity-13 : VRF を含むレイヤ 3 接続の変更に使用されます。 • tenant-connectivity-mgmt : テナントのインバンドおよびアウトオブバンドの管理接続構成、およびアトミック カウンターやヘルス スコアなどのポリシーのデバッグ/監視に使用されます。 • tenant-connectivity-util : リーフスイッチおよびスパインスイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • tenant-epg : エンドポイント グループ、VRF、ブリッジドメインの削除/作成など、テナント設定の管理に使用されます。 • tenant-ext-connectivity-12 : テナントの L2Out 構成を管理するために使用されます。 • tenant-ext-connectivity-13 : テナント L3Out 構成の管理に使用されます。

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • tenant-ext-connectivity-mgmt : ファームウェアポリシーの書き込みアクセスとして使用されます。 • tenant-ext-connectivity-util : traceroute、ping、oam、eprk などのデバッグ/監視/観察ポリシーに使用されます。 • tenant-ext-protocol-l1 : テナントの外部レイヤ1プロトコルの管理に使用されます。通常、ファームウェアポリシーの書き込みアクセスにのみ使用します。 • tenant-ext-protocol-l2 : テナントの外部レイヤ2プロトコルの管理に使用されます。通常、ファームウェアポリシーの書き込みアクセスにのみ使用します。 • tenant-ext-protocol-l3 : BGP、OSPF、PIM、IGMP などのテナントの外部レイヤ3プロトコルを管理するために使用されます。 • tenant-ext-protocol-mgmt : ファームウェアポリシーの書き込みアクセスとして使用されます。 • tenant-ext-protocol-util : traceroute、ping、oam、eprk などのデバッグ/監視/観察ポリシーに使用されます。 • tenant-network-profile : ネットワーク プロファイルの削除および作成、エンドポイントグループの削除および作成など、テナント設定の管理に使用されます。 • tenant-protocol-l1 : テナントの下でレイヤ1プロトコルの設定を管理するために使用されます。 • tenant-protocol-l2 : テナントの下でレイヤ2プロトコルの設定を管理するために使用されます。 • tenant-protocol-l3 : テナントの下でレイヤ3プロトコルの設定を管理するために使用されます。 • tenant-protocol-mgmt : ファームウェアポリシーの書き込みアクセスとして使用されます。

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • tenant-protocol-ops : テナント traceroute ポリシーに使用されます。 • tenant-protocol-util — traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • tenant-qos : ファームウェア ポリシーの書き込みアクセスとしてのみ使用されます。 • tenant-security : テナントの契約関連の設定に使用されます。 • vmm-connectivity : VM 接続に必要な APIC の VMM インベントリ内のすべてのオブジェクトを読み取るために使用されます。 • vmm-ep : APIC の VMM インベントリ内の VM およびハイパーバイザーエンドポイントを読み取るために使用されます。 • vmm-policy : VM ネットワーキングのポリシーの管理に使用されます。 • vmm-protocol-ops : VMM ポリシーでは使用されません。 • vmm-security : テナントの契約関連の設定に使用されます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した RBAC ルールの作成

このセクションでは、GUI を使用して RBAC ルールを作成する方法について説明します。

始める前に

セキュリティ ドメインの作成

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 [Intent] メニューの [Administrative] リストで、[RBAC ルールの作成 (Create RBAC Rule)] をクリックします。[RBAC ルールの作成 (Create RBAC Rule)] ダイアログボックスが表示されます。
- ステップ4 DN フィールドに、ルールの DN を入力します。
- ステップ5 セキュリティドメインを選択します。
- [セキュリティドメインの選択 (Select Security Domain)] をクリックします。[セキュリティドメインの選択 (Select Security Domain)] ダイアログボックスが表示されます。
 - [セキュリティドメインの選択 (Select Security Domain)] ダイアログで、左側の列のセキュリティドメインをクリックして選択し、[選択 (Select)] をクリックします。[RBAC ルールの作成] ダイアログボックスに戻ります。
- ステップ6 [書き込みを許可] フィールドで、[はい] をクリックして書き込みを許可するか、[いいえ] をクリックして書き込みを許可しません。
- ステップ7 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した認証局の作成

ここでは、GUI を使用して認証局を作成する方法について説明します。

始める前に

- 証明書チェーン (certificate chain) を設定します。
- 認証局がテナント用の場合は、テナントを作成します。

- ステップ1 インテントアイコンをクリックします。[インテント (Intent)] メニューが表示されます。
- ステップ2 [Intent] 検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative] を選択します。
[インテント (Intent)] メニューに管理オプションのリストが表示されます。
- ステップ3 [インテント (Intent)] メニューの [管理 (Administrative)] リストで、[証明書認証局の作成 (Create Certificate Authority)] をクリックします。[証明書認証局の作成 (Create Certificate Authority)] ダイアログボックスが表示されます。
- ステップ4 [証明書認証局の作成ダイアログボックスのフィールド (Create Certificate Authority Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力して、続行します。

表 25: 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。

[プロパティ (Properties)]	説明
用途	<p>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) : 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	<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。[証明書認証局の作成 (Create Certificate Authority)] ダイアログボックスが表示されます。
Certificate Chain	<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. サーバー

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したキー リングの作成

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

始める前に

- 認証局を作成します。
- 証明書を持っています。
- キー リングが特定のテナント用である場合は、テナントを作成します。

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

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 [インテント (Intent)]メニューの[管理 (Administrative)]リストで、[キー リングの作成 (Create Key Ring)]をクリックします。[キー リングの作成 (Create Key Ring)]ダイアログ ボックスが表示されます。

ステップ 4 次の [キー リングの作成ダイアログボックスのフィールド (Create Key Ring 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 26: キー リングの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
認証局	認証局を選択するには : <ol style="list-style-type: none"> <li data-bbox="911 348 1505 485">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。 <li data-bbox="911 512 1505 543">2. 左側の列で認証局をクリックして選択します。 <li data-bbox="911 571 1505 667">3. [選択 (Select)] をクリックします。[キー リングの作成 (Create Key Ring)] ダイアログボックスに戻ります。
秘密キー (Private Key)	次のいずれかを選択します。 <ul style="list-style-type: none"> <li data-bbox="943 768 1505 831">• [新しいキーの生成 (Generate New Key)] : 新しいキーを生成します。 <li data-bbox="943 858 1505 995">• [既存のキーのインポート (Import Existing Key)] : [秘密キー (Private Key)] テキストボックスが表示され、既存のキーを使用できます。
秘密キー (Private Key)	[秘密キー (Private Key)] テキストボックスに既存のキーを入力します ([既存のキーのインポート (Import Existing Key)] オプションの場合) 。
Modulus	[モジュール (Modulus)] ドロップダウン リストをクリックし、次の項目の中から選択します。 <ul style="list-style-type: none"> <li data-bbox="943 1268 1073 1299">• MOD 512 <li data-bbox="943 1320 1089 1352">• MOD 1024 <li data-bbox="943 1373 1089 1404">• MOD 1536 <li data-bbox="943 1425 1243 1457">• MOD 2048 : デフォルト
証明書	[証明書 (Certificate)] テキスト ボックスに証明書情報を入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したローカルユーザーの作成

このセクションでは、クラウド APIC GUI を使用したローカルユーザーの作成方法について説明します。

- ステップ 1** インテント アイコンをクリックします。[**インテント (Intent)**] メニューが表示されます。
- ステップ 2** [Intent] 検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative] を選択します。
[Intent] メニューに管理オプションのリストが表示されます。
- ステップ 3** [インテント (Intent)] メニューの [管理 (Administrative)] リストで、[ローカルユーザーの作成 (Create Local User)] をクリックします。[ローカルユーザーの作成 (Create New User)] ダイアログボックスが表示されます。
- ステップ 4** 次の [ローカルユーザーの作成ダイアログボックスのフィールド (Create Local User 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 27: ローカルユーザーの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	ローカルユーザーのユーザー名を入力します。
Password	ローカルユーザーのパスワードを入力します。
Confirm Password	ローカルユーザーのパスワードを再入力します。
説明	ローカルユーザーの説明を入力します。
Settings	
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。 • Inactive : ローカルユーザー アカウントを非アクティブにします。
[名 (First Name)]	ローカルユーザーの名を入力します。
姓 (Last Name)	ローカルユーザーの姓を入力します。
電子メール アドレス (Email Address)	ローカルユーザーの E メールアドレスを入力します。
Phone Number	ローカルユーザーの電話番号を入力します。

[プロパティ (Properties)]	説明
セキュリティドメイン	

[プロパティ (Properties)]	説明
	<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 28: ローカルユーザーの作成ダイアログボックスのフィールド：高度な設定

プロパティ	説明
Account Expires	[はい (Yes)]を選択すると、アカウントは選択した時点で期限切れになるように設定されます。
パスワードの更新が必要です	[はい (Yes)]を選択した場合、ユーザーは次回ログイン時にパスワードを変更する必要があります。
OTP	ユーザーのワンタイムパスワード機能を有効にするには、チェックボックスをオンにします。
ユーザー証明書	<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"> [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。 [Name] フィールドに名前を入力します。 [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。 [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. [Name] フィールドに名前を入力します。 3. [キー (Key)] テキストボックスに SSH キーを入力します。 4. [Add] をクリックします。[SSH キーの追加 (Add SSG Key)] ダイアログボックスが閉じます。[ローカル ユーザー] ダイアログボックスに戻ります。

ステップ 6 設定が終わったら **[Save]** をクリックします。

Cisco Cloud APIC GUI を使用したリージョンの管理（クラウドテンプレートの設定）

リージョンは、初回セットアップ時に構成されます。構成時に、Cisco Cloud APIC によって管理されるリージョンと、そのリージョンのサイト間およびリージョン間の接続を指定します。このセクションでは、初期インストール後に Cisco Cloud APIC GUI を使用してクラウドテンプレートでリージョンを管理する方法について説明します。

クラウドテンプレートの詳細については、[クラウドテンプレートの概要 \(46 ページ\)](#) を参照してください。

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

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

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

ステップ 3 **[インテント (Intent)]** メニューの **[構成 (Configuration)]** リストで、**[クラウド APIC セットアップ (Cloud APIC Setup)]** をクリックします。

[セットアップ - 概要] ダイアログボックスが表示されます。

ステップ 4 **[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。

[**セットアップ-リージョン管理**] ダイアログ ボックスが表示されます。**セットアップ-リージョン管理** の一連のステップの最初のステップ、**管理するリージョン**が表示され、管理対象リージョンのリストが表示されます。

ステップ 5 サイト間接続が必要な場合は、[**サイト間接続 (Inter-Site Connectivity)**] 領域の [**有効 (Enabled)**] ボックスをクリックしてオンにします。
このオプションを選択すると、ページ上部の [**セットアップ-リージョン管理 (Setup-Region Management)**] の手順に**サイト間接続**の手順が追加されます。

ステップ 6 Cisco Cloud APIC で管理するリージョンを選択するには、そのリージョンの**チェック** ボックスをクリックして**チェック** マークを付けます。

ステップ 7 クラウドルータをこのリージョンにローカルに展開するには、そのリージョンの [**Cloud Routers**] **チェック** ボックスをオンにします。

ステップ 8 クラウドサイトのファブリック インフラ接続を構成するには、[**次へ**] をクリックします。**セットアップ-リージョン管理**の一連のステップの次のステップである、**一般的な接続**が表示されます。

ステップ 9 CCR のサブネットプールを追加するには、[**クラウドルータのサブネットプールを追加する (Add Subnet Pool for Cloud Router)**] をクリックし、テキスト ボックスにサブネットを入力します。

(注) クラウド APIC の導入時に提供される /24 サブネットは、最大 2 つのクラウドサイトに十分です。3 つ以上のクラウドサイトを管理する必要がある場合は、さらにサブネットを追加する必要があります。

ステップ 10 [**CCR向け BGP 自律システム番号 (BGP Autonomous System Number for CCRs)**] フィールドに値を入力します。

BGP ASN の範囲は 1 ~ 65534 です。

ステップ 11 [**Assign Public IP to CCR Interface (パブリック IP を CCR インターフェイスに割り当てる)**] フィールドで、CCR インターフェイスにパブリック IP アドレスまたはプライベート IP アドレスを割り当てるかどうかを決定します。

- パブリック IP アドレスを CCR インターフェイスに割り当てるには、[**有効 (Enabled)**] **チェック** ボックスをオンのままにします。デフォルトでは、この [**有効**] **チェック** ボックスはオンになっています。
- パブリック IP アドレスを CCR インターフェイスに割り当てるには、[**有効 (Enabled)**] **チェック** ボックスをオンのままにします。この場合、接続にはプライベート IP アドレスが使用されます。

(注) パブリック IP アドレスの無効化または有効化は中断を伴う操作であり、トラフィック損失の原因となる可能性があります。

リリース 5.2(1) 以降では、CCR に割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、[**クラウドリソース (Cloud Resources)**] エリアにルータの他の詳細とともに表示されます。パブリック IP が CSR に割り当てられていない場合は、プライベート IP だけが表示されます。

ステップ 12 リージョンごとのルーター数を選択するには、[**リージョンごとのルーター数**] ドロップダウン リストをクリックし、[**2**]、[**3**]、または [**4**] をクリックします。

ステップ 13 [**ユーザー名 (Username)**] テキストボックスにユーザー名を入力します。

- ステップ 14** [パスワード (Password)] テキストボックスと [パスワードの確認 (Confirm Password)] テキストボックスに新しいパスワードを入力します。
- ステップ 15** スループット値を選択するには、[ルーターのスループット] ドロップダウンリストをクリックします。
- (注)
- クラウドルータは、ルータのスループットまたはログイン情報を変更する前に、すべてのリージョンから展開解除する必要があります。
 - リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。Cisco Catalyst 8000V のスループット値については、[Cisco Catalyst 8000V について \(29 ページ\)](#) を参照してください。
- ステップ 16** (オプション) ライセンス トークンを指定するには、[ライセンス トークン] テキストボックスに製品インスタンスの登録トークンを入力します。
- (注)
- リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。Cisco Catalyst 8000V のライセンス情報については、[Cisco Catalyst 8000V について \(29 ページ\)](#) を参照してください。
 - トークンが入力されていない場合、CCR は EVAL モードになります。
 - プライベート IP アドレスを使用して CCR のスマートライセンスを登録する場合、パブリック IP アドレスが [ステップ 11 \(141 ページ\)](#) の CCR に対して無効になっている場合、サポートされる唯一のオプションは、**AWS Direct Connect** または **Azure Express Route to Cisco Smart Software Manager (CSSM)** です ([管理用 (Administrative)] > [スマート ライセンス (Smart Licensing)] に移動して使用可能です)。この場合、AWS Direct Connect または Azure Express Route を介して CSSM への到達可能性を提供する必要があります。パブリック IP アドレスが無効になっている場合、プライベート IP アドレスが使用されているため、パブリック インターネットは使用できません。したがって、接続には AWS Direct Connect または Azure Express Route であるプライベート接続を使用する必要があります。
- ステップ 17** [次へ (Next)] をクリックします。
- これらの手順の前半で [サイト間接続] 領域の [有効] ボックスにチェック マークを付けた場合、**サイト間接続は、セットアップ-リージョン管理の一連のステップの次のステップとして表示されます。ステップ 18 (142 ページ) に進みます。**
 - これらの手順の前半で [サイト間接続] 領域の [有効] ボックスにチェック マークを付けなかった場合は、[ステップ 22 \(143 ページ\)](#) に進みます。
- ステップ 18** テキストボックスにオンプレミスの IPsec トンネルピアのピアパブリック IP アドレスを入力するには、[IPsec トンネルピアのパブリック IP を追加] をクリックします。
- ステップ 19** [エリア ID] フィールドに OSPF エリア ID を入力します。
- ステップ 20** 外部サブネットプールを追加するには、[外部サブネットの追加] をクリックし、テキストボックスにサブネットプールを入力します。
- ステップ 21** すべての接続オプションを設定したら、ページの下部にある [次へ (Next)] をクリックします。

ステップ 22 終了したら [Save and Continue (保存して続行)] ボタンをクリックします。

REST API を使用した Cisco Cloud APIC の構成

REST API を使用したテナントの作成

このセクションでは、REST API を使用してテナントを作成する方法を示します。

テナントを作成するには:

```
<polUni>
  <fvTenant name="infra">
    <cloudAwsProvider region="us-east-1" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"
      status=""/>
    </fvTenant>
  </polUni>
```

REST API を使用したコントラクトの作成

この例では、REST API を使用して Cisco Cloud APIC のコントラクトを作成する方法を示します。

始める前に

フィルタを作成します。

コントラクトを作成するには :

例 :

```
<polUni>
  <fvTenant name="t2" status="">
    <vzFilter descr="" name="http-family-destination" ownerKey="" ownerTag="">
      <vzEntry name="http" prot="tcp" etherT="ip" dFromPort="http" dToPort="http"/>
      <vzEntry name="https" prot="tcp" etherT="ip" dFromPort="https" dToPort="https"/>
    </vzFilter>
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjFiltAtt action="permit" directives="" tnVzFilterName="http-family-destination"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

REST API を使用したクラウド コンテキスト プロファイルの作成

このセクションでは、クラウド コンテキスト プロファイルを作成する方法を示します。

始める前に

VRF を作成します。

ステップ 1 リリース 25.0(2) より前のリリースの場合は、次のような投稿を入力して、クラウド コンテキスト プロファイルを作成します。

例 :

```
<polUni>
<fvTenant name="Corp1" status="">
  <cloudAwsProvider accessKeyId="" secretAccessKey="" providerId="aws" status="" accountId=""/>

  <fvCtx name="prod-1" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

  <fvCtx name="prod-2" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

  <cloudVpnGwPol name="VgwPol" status=""/>

  <cloudApp name="payment" status="">
    <cloudEPg name="web" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-1" />
    </cloudEPg>
  </cloudApp>
  <cloudApp name="billing">
    <cloudEPg name="app">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-2" />
    </cloudEPg>
  </cloudApp>

  <cloudCtxProfile name="prod-web-east-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-1"/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
      <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
      <cloudIntNetworkP name="IntNetworkP1"/>
    </cloudRouterP>

    <cloudCidr addr="60.10.10.1/16" primary="true">
      <cloudSubnet ip="60.10.10.1/24">
        <cloudRsZoneAttach tDn="uni/clouddomp/provp-aws/region-us-east-1/zone-us-east-1a"/>
      </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>

  <cloudCtxProfile name="prod-payment-east-1" status="">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
```

```

<cloudRsToCtx tnFvCtxName="prod-2" status=""/>
<cloudRouterP name="RouterP1" type="vpn-gw">
  <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
  <cloudIntNetworkP name="IntNetworkP1" status=""/>
</cloudRouterP>

<cloudCidr addr="70.10.10.1/16" primary="true" status="">
  <cloudSubnet ip="70.10.10.1/24" status="">
    <cloudRsZoneAttach tDn="uni/clouddomp/provp-aws/region-us-east-1/zone-us-east-1a"/>
  </cloudSubnet>
</cloudCidr>
</cloudCtxProfile>

</fvTenant>
</polUni>

```

ステップ 2 リリース 25.0(2) 以降サポートされている **クラウド アベイラビリティ ゾーン** を使用してクラウド コンテキスト プロファイルを作成するには、次の例のような投稿を入力します。

リリース 25.0(2) 以降、**ユーザー** テナントでクラウド コンテキスト プロファイルを作成している場合、**クラウド アベイラビリティ ゾーン** のみに制限されます。クラウド アベイラビリティ ゾーンは、以下で強調表示されているゾーン フィールドを介して作成されます。クラウド アベイラビリティ ゾーンの詳細については、[可用性ゾーン \(37 ページ\)](#) を参照してください。

例：

```

<polUni>
<fvTenant name="Corp1" status="">
  <cloudAwsProvider accessKeyId="" secretAccessKey="" providerId="aws" status="" accountId=""/>

  <fvCtx name="prod-1" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:400:400" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

  <fvCtx name="prod-2" status="">
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="export"/>
      <bgpRtTarget rt="route-target:as4-nn2:500:500" type="import"/>
    </bgpRtTargetP>
  </fvCtx>

  <cloudVpnGwPol name="VgwPol" status=""/>

  <cloudApp name="payment" status="">
    <cloudEPg name="web" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-1" />
    </cloudEPg>
  </cloudApp>
  <cloudApp name="billing">
    <cloudEPg name="app">
      <cloudRsCloudEPgCtx tnFvCtxName="prod-2" />
    </cloudEPg>
  </cloudApp>

  <cloudCtxProfile name="prod-web-east-1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
    <cloudRsToCtx tnFvCtxName="prod-1"/>
    <cloudRouterP name="RouterP1" type="vpn-gw">
      <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
      <cloudIntNetworkP name="IntNetworkP1"/>
    </cloudRouterP>
  </cloudCtxProfile>

```

```

</cloudRouterP>
<cloudCidr addr="10.10.0.0/16" primary="yes">
  <cloudSubnet ip="10.10.1.0/24" usage="gateway" scope="public" zone="us-west-1a"/>
  <cloudSubnet ip="10.10.2.0/24" scope="public" zone="us-west-1b"/>
</cloudCidr>
</cloudCtxProfile>

<cloudCtxProfile name="prod-payment-east-1" status="">
  <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-east-1"/>
  <cloudRsToCtx tnFvCtxName="prod-2" status=""/>
  <cloudRouterP name="RouterP1" type="vpn-gw">
    <cloudRsToVpnGwPol tnCloudVpnGwPolName="VgwPol"/>
    <cloudIntNetworkP name="IntNetworkP1" status=""/>
  </cloudRouterP>
  <cloudCidr addr="20.10.0.0/16" primary="yes">
    <cloudSubnet ip="20.10.1.0/24" scope="public" zone="us-west-1a"/>
  </cloudCidr>
</cloudCtxProfile>

</fvTenant>
</polUni>

```

REST API を使用したクラウド リージョンの管理

このセクションでは、REST API を使用してクラウド リージョンを管理する方法を示します。

クラウド リージョンを作成するには:

```

<polUni>
  <cloudDomP name="dom-us-east-2">
    <cloudBgpAsP asn="64513"/>
    <cloudProvP vendor="aws">
      <cloudRegion name="us-east-2" adminSt="managed">
        <cloudZone name="us-east-2a"/>
        <cloudZone name="us-east-2b"/>
      </cloudRegion>
    </cloudProvP>
  </cloudDomP>
</polUni>

```

REST API を使用したフィルタの作成

このセクションでは、REST API を使用してフィルタを作成する方法を示します。

フィルタを作成するには、次の手順を実行します。

```

https://<IP_Address>/api/node/mo/.xml
<polUni>
<fvTenant name="intervpc" >
<fvCtx name="VRF1"/>

```

```

<cloudApp name="CloudAP1" >
<cloudEPg name="CloudEPG1" >
  <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
  <fvRsProv tnVzBrCPName="Contract2" > </fvRsProv>
  <cloudEPSelector name="sel1" matchExpression="custom:epgtag=='cloudepg1'" />
</cloudEPg>
</cloudApp>

  <vzFilter name="http" annotation="orchestrator:misc" >
  <vzEntry name="Entry3" prot="tcp" etherT="ipv4" arpOpc="unspecified" stateful="no"
applyToFrag="no" sFromPort="unspecified" sToPort="unspecified" dFromPort="80" dToPort="80" > </vzEntry>

  </vzFilter>

<vzBrCP name="Contract2" scope="global">
  <vzSubj name="test-subj" >

    <vzRsSubjFiltAtt action="permit" tnVzFilterName="http" directives="none" />

  </vzSubj>
</vzBrCP>
</fvTenant>
</polUni>

```

REST API を使用したアプリケーション プロファイルの作成

このセクションでは、REST API を使用してアプリケーション プロファイルを作成する方法を示します。

始める前に

テナントを作成します。

アプリケーション プロファイルを作成する方法：

```

https://<IP_Address>/api/node/mo/.xml
<polUni>
<fvTenant name="intervpc" >
<fvCtx name="VRF1"/>
  <cloudApp name="CloudAP1" >

    <cloudEPg name="CloudEPG1" >
      <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
      <fvRsProv tnVzBrCPName="Contract2" > </fvRsProv>
      <cloudEPSelector name="sel1" matchExpression="custom:epgtag=='cloudepg1'" />
    </cloudEPg>

  </cloudApp>

  <vzFilter name="http" annotation="orchestrator:misc" >
  <vzEntry name="Entry3" prot="tcp" etherT="ipv4" arpOpc="unspecified" stateful="no"
applyToFrag="no" sFromPort="unspecified" sToPort="unspecified" dFromPort="80" dToPort="80" > </vzEntry>

  </vzFilter>

```

```

<vzBrCP name="Contract2" scope="global">
  <vzSubj name="test-subj" >
    <vzRsSubjFiltAtt action="permit" tnVzFilterName="http" directives="none" />
  </vzSubj>
</vzBrCP>
</fvTenant>
</polUni>

```

REST API を使用したクラウド EPG の作成

この例では、REST API を使用してクラウド EPG を作成する方法を示します。

始める前に

アプリケーション プロファイルと VRF を作成します。

クラウド EPG を作成するには、次の手順を実行します。

例：

```

<polUni>
  <fvTenant name="t2" status="">
    <!-- Tenant provide AWS credentials -->
    <cloudAwsProvider region="us-east-2" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"/>

    <fvCtx name="v1" status=""/>
    <cloudApp name="ap">
      <cloudEPg name="provEPG" status="">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='provfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='provbaz'"/>
        <fvRsProv tnVzBrCPName="httpFamily"/>
      </cloudEPg>
      <cloudEPg name="consEPG">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='consfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='consbaz'"/>
        <fvRsCons tnVzBrCPName="httpFamily"/>
      </cloudEPg>
    </cloudApp>
  </fvTenant>
</polUni>

```

REST API を使用した外部クラウド EPG の作成

この例では、REST API を使用して外部クラウド EPG を作成する方法を示します。

始める前に

アプリケーション プロファイルと VRF を作成します。

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：

```
<polUni>
  <fvTenant name="t2" status="">
    <!-- Tenant provide AWS credentials -->
    <cloudAwsProvider region="us-east-2" accessKeyId="123" secretAccessKey="ABCDE" providerId="admin"/>

    <fvCtx name="v1" status=""/>
    <cloudApp name="ap">
      <cloudEPg name="provEPGInternet" status="">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudEPSelector name="1" matchExpression="custom:tag=='provfoo'"/>
        <cloudEPSelector name="2" matchExpression="custom:tag=='provbaz'"/>
        <fvRsProv tnVzBrCPName="httpFamily"/>
      </cloudEPg>
      <cloudExtEPg name="consInternetEPG">
        <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
        <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
        <fvRsCons tnVzBrCPName="httpFamily"/>
      </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

REST API を使用したクラウドテンプレートの作成

このセクションでは、REST API を使用してクラウドテンプレートを作成する方法を示します。クラウドテンプレートの詳細については、[クラウドテンプレートの概要 \(46 ページ\)](#) を参照してください。

REST API は、選択したライセンスモデルのタイプによって異なります。Cisco Catalyst 8000V のライセンスタイプは、cloudtemplateProfile 管理対象オブジェクトの routerThroughput プロパティによって取得されます。

routerThroughput 値が **T0/T1/T2/T3** に属している場合、**BYOL** Cisco Catalyst 8000V が Cisco Cloud APIC に展開されます。routerThroughput 値が **PAYG** の場合、**PAYG** Cisco Catalyst 8000V が Cisco Cloud APIC に展開されます。

ステップ 1 **BYOL** Cisco Catalyst 8000V を展開するためのクラウドテンプレートポストを作成するには、次の手順を実行します。

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
      <cloudtemplateProfile name="default" routerUsername="admin" routerPassword="rtpssw"
routerThroughput="15"
      routerLicenseToken="hYjZhYjItYtg0mrtrL15ocStS%0AUzRSzZ0%3"
routerMgmtInterfacePublicIp="yes" routerDataInterfacePublicIp="yes"/>

      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
    </cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

```

<cloudtemplateIntNetwork name="default">
  <cloudRegionName provider="aws" region="us-west-1"/>
  <cloudRegionName provider="aws" region="us-west-2"/>
</cloudtemplateIntNetwork>

<cloudtemplateExtNetwork name="default">
  <cloudRegionName provider="aws" region="us-west-2"/>

  <cloudtemplateVpnNetwork name="default">

    <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
    <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
    <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

    <cloudtemplateOspf area="0.0.0.1"/>

  </cloudtemplateVpnNetwork>

  <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
/>

  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
</fvTenant>
</polUni>

```

(注) リリース 25.0(3) 以降、tier2 (T2) は、Cisco Cloud APIC がサポートするデフォルトのスループットであり、上記の cloudtemplateProfile 管理対象オブジェクトの routerThroughput プロパティで示されます。

ステップ 2 PAYG Cisco Catalyst 8000V を展開するためのクラウド テンプレート ポストを作成するには、次の手順を実行します。

```

<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
      <cloudtemplateProfile name="default" routerUsername="admin" routerPassword="rtppsw"
routerThroughput="PAYG"
      vmName="c5.4xlarge" routerMgmtInterfacePublicIp="yes"
routerDataInterfacePublicIp="yes"/>

      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-1"/>
        <cloudRegionName provider="aws" region="us-west-2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-2"/>

      <cloudtemplateVpnNetwork name="default">

        <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
        <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
        <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

        <cloudtemplateOspf area="0.0.0.1"/>

      </cloudtemplateVpnNetwork>

```



```

    <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
  />

  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>

```

PAYG スループットを選択する場合、ユーザは、Cloud APIC によって作成され、管理対象オブジェクト `vmName` によって表される `vmNames` のリストから **vmName** も選択する必要があります。

次の表に、`cloudtemplateProfile` のプロパティ `vmName` によって示される `vmNames` を示します。

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
c5.xlarge	最大 5 ギガビット スループット	4	8 GiB
c5.2xlarge	最大 10 ギガビット スループット	8	16 GiB
c5.4xlarge	最大 10 ギガビット スループット	16	32 GiB
c5.9xlarge	最大 10 ギガビット スループット	36	72 GiB
c5n.xlarge	最大 25 ギガビット スループット	4	10.5 GiB
c5n.2xlarge	最大 25 ギガビット スループット	8	21 GiB
c5n.4xlarge	最大 25 ギガビット スループット	16	42 GiB
c5n.9xlarge	最大 50 ギガビット スループット	36	96 GiB

REST API を使用して VRF リーク ルートの構成

始める前に

このセクションの手順を実行する前に、[内部 VRF 間のルート リーク \(10 ページ\)](#) と [グローバルな Inter-VRF ルート リーク ポリシー \(11 ページ\)](#) に記載されている情報を確認してください。

ステップ 1 次のような投稿を入力して、契約ベースのルーティングを有効または無効にします。

```
<fvTenant name="infra">
  <cloudVrfRouteLeakPol name="default" allowContractBasedRouting="true"/>
</fvTenant>
```

allowContractBasedRouting フィールドには、次のいずれかの設定があります。

- **true**: ルート マップがない場合、契約に基づいてルートが漏洩していることを示します。有効にすると、ルートマップが構成されていないときにコントラクトがルーティングを駆動します。ルートマップが存在する場合、ルート マップは常にルーティングを駆動します。
- **false**: デフォルト設定です。ルートが契約に基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。

ステップ 2 次のような投稿を入力して、leakInternalPrefix フィールドを使用して、VRF に関連付けられたすべてのクラウド CIDR のルート リークを設定します。

```
<fvTenant name="t1">
  <fvCtx name="v1">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t2" ctxName="v2" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>

<fvTenant name="t2">
  <fvCtx name="v2">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t1" ctxName="v1" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>
```

ステップ 3 次のような投稿を入力して、leakInternalSubnet フィールドを使用して、VRF のペア間の特定のルートをリークします。

```
<fvTenant name="anyTenant" status="">
  <fvCtx name="VRF1" >
    <leakRoutes status="">
      <leakInternalSubnet ip="110.110.1.0/24" >
        <leakTo ctxName="VRF2" scope="public" tenantName=" anyTenant " />
      </leakInternalSubnet>
    </leakRoutes>
  </fvCtx>
  <fvCtx name="VRF2" status="" >
    <leakRoutes status="">
      <leakInternalSubnet ip="110.110.2.0/24" >
        <leakTo ctxName="VRF1" scope="public" tenantName=" anyTenant " />
      </leakInternalSubnet>
    </leakRoutes>
  </fvCtx>
</fvTenant>
```

REST API を使用したトンネルのソース インターフェイス選択の構成

始める前に

このセクションの手順を実行する前に、[トンネルのソース インターフェイスの選択 \(13 ページ\)](#) に記載されている情報を確認してください。

次のような投稿を入力して、トンネルの送信元インターフェイスの選択を構成します。

```
<cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
  <cloudtemplateProfile name="defaultxyz" routerUsername="james" routerPassword="bond@7" />

  <cloudtemplateIpSecTunnelSubnetPool subnetpool="10.20.0.0/16" poolname="pool1" />

  <cloudtemplateIntNetwork name="default">
    <cloudRegionName provider="aws" region="us-west-1"/>
    <cloudRegionName provider="aws" region="us-west-2"/>
  </cloudtemplateIntNetwork>

  <cloudtemplateExtNetwork name="something" vrfName="xyz" >
    <cloudRegionName provider="aws" region="us-west-2"/>
    <cloudtemplateVpnNetwork name="default">
      <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" poolname="" presharedkey="abcd"
ikeVersion="v1|v2">
        <b><cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId="2" /></b>
      </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
```

REST API を使用したトンネルのソース インターフェイス 選択の構成



第 5 章

システムの詳細の表示

- VM ホスト メトリックのモニタリング (155 ページ)
- アプリケーション管理詳細の表示 (158 ページ)
- クラウドリソースの詳細の表示 (160 ページ)
- 操作の詳細の表示 (161 ページ)
- インフラストラクチャの詳細の表示 (164 ページ)
- 管理の詳細の表示 (164 ページ)
- Cisco Cloud APIC GUI を使用したヘルスの詳細の表示 (166 ページ)

VM ホスト メトリックのモニタリング

リリース 25.0(1) 以降では、Prometheus Node Exporter を使用して Cisco Cloud APIC が導入されている VM ホストのメトリックのモニタリングがサポートされます。Prometheus Node Exporter は、さまざまなハードウェアおよびカーネル関連のメトリックを可視化し、Linux ノードから CPU、ディスク、メモリの統計情報などの技術情報を収集します。Prometheus ノードエクスポー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 APIC がリリース 25.0(1) 以降で実行されている場合、Prometheus Node Exporter はデフォルトで自動的に使用可能になります。

注意事項と制約事項

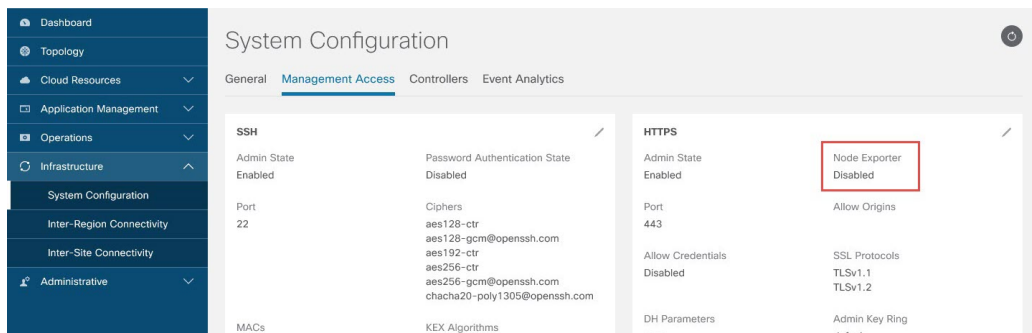
HTTP は、Prometheus Node Exporter を使用したモニタリングメトリックではサポートされていません。Prometheus Node Exporter を使用したメトリックのモニタリングでは、HTTPS のみがサポートされます。

GUI を使用した VM ホストメトリックのモニタリング

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

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

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

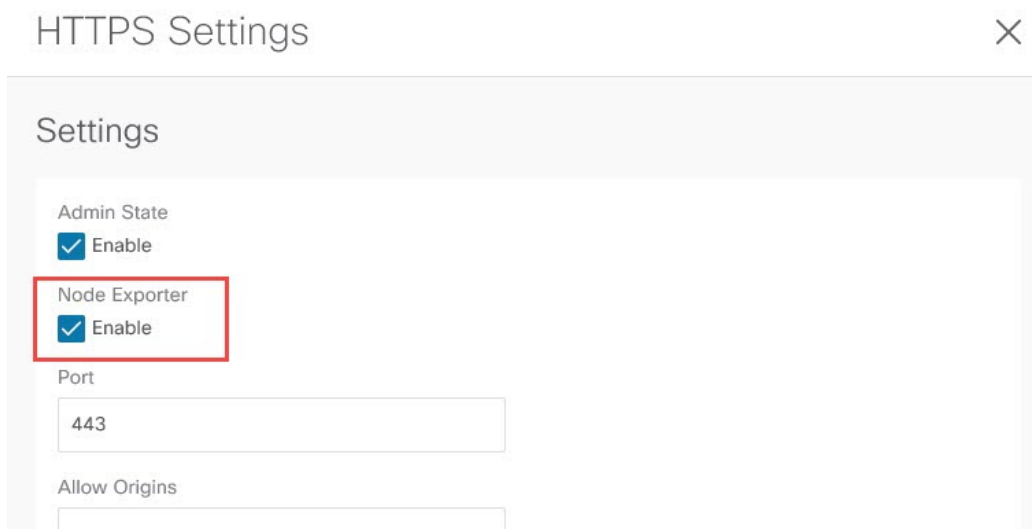


- **有効化 (Enabled)** : Prometheus Node Exporter はすでに有効になっています。この場合、これらの手順を続行する必要はありません。
- **無効化 (Disabled)** : Prometheus Node Exporter はまだ有効になっていません。Prometheus Node Exporter を有効にするには、次の手順に従います。

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。



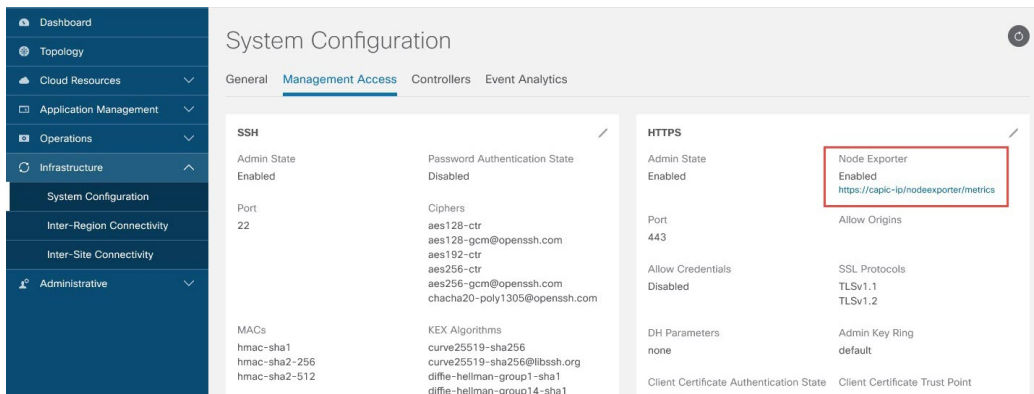
これらの設定を保存すると Web サービスが再起動され、要求への応答が再開されるまで少し時間がかかることを示す警告メッセージが表示されます。[OK] をクリックして、変更内容を確定します。

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 APIC が展開されている VM ホストのメトリックが示されます。

REST API を使用した VM ホストメトリックスの監視

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

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

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

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

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

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

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

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

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

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

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

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

アプリケーション管理詳細の表示

ここでは、Cisco Cloud APIC GUI を使用してアプリケーション管理の詳細を表示する方法について説明します。アプリケーション管理の詳細には、特定のテナント、アプリケーションプロファイル、EPG、コントラクト、フィルタ、VRF、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 29: 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
サービス (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。

サマリーテーブルは、テーブルの行として表示されます。たとえば、[テナント (Tenants)] サブタブを選択した場合、テナントのリストがサマリーテーブルの行として表示されます。

[属性でフィルタ (Filter by Attributes)] バーをクリックすると、行をフィルタリングできます。属性、演算子、およびフィルタ値を選択します。たとえば、テナントに基づくフィルタリングの場合は、Tenant=T1 (T1 はテナントの名前) を選択します。

ステップ 3 サマリー ペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。

ステップ 4 詳細については、表示する特定のコンポーネントを表すサマリーテーブルの行をダブルクリックします。

新しいダイアログ ボックスが、次のタブのいずれかと共に**作業**ペインの上に表示されます。

(注) 表示されるタブは、コンポーネントと構成が異なるように見えます。

- **概要 (Overview)** : クラウドリソース、設定関係、およびコンポーネントの設定の概要を示します。
- **クラウドリソース** : このコンポーネントに関連するクラウドリソース情報を表示するサブタブのリストを含みます。
- **構成** — コンポーネントに関連する構成情報を表示する 1 つ以上のサブタブが含まれています。
- **統計** : 選択したサンプリング間隔と統計タイプに基づいて統計を表示できるようにします。[統計] タブは表示しているコンポーネントに応じたサブタブを含みます。
- **イベント分析** : 障害、イベント、監査ログを表示するサブタブのリストを含みます。

(注) 作業ウィンドウの上部に表示されるダイアログボックスの右上隅には、**更新**ボタンと[アクション (Actions)] ボタンの間に**編集**ボタンがあります。[編集 (Edit)] ボタンをクリックすると、選択したコンポーネントを編集できます。

クラウドリソースの詳細の表示

ここでは、Cisco Cloud APIC GUI を使用してクラウドリソースの詳細を表示する方法について説明します。クラウドリソースの詳細には、特定のリージョン、アベイラビリティゾーン、VPC、ルータ、セキュリティグループ、エンドポイント、インスタンス、およびクラウドサービスに関する情報が含まれます。

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

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

表 30: クラウドリソース サブタブ

サブタブ名	説明
[Regions]	リージョンをサマリーテーブルの行として表示します。
可用性ゾーン	サマリーテーブルの行としてアベイラビリティゾーンを表示します。
VPC	サマリーテーブルの行としてVPCを表示します。
Routers	ルータをサマリーテーブルの行として表示します。
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。
Instances	インスタンスをサマリーテーブルの行として表示します。
クラウドサービス (Cloud Services)	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] タブ: クラウドサービスをサマリーテーブルの行として表示します。 • [ターゲットグループ] タブ: ターゲットグループをサマリーテーブルの行として表示します。

ステップ 2 表示する詳細のコンポーネントを表すタブをクリックします。

サマリーテーブルは、テーブルの行として表示されます。たとえば、[エンドポイント (Endpoints)] サブタブを選択した場合、エンドポイントのリストがサマリーテーブルの行として表示されます。

[属性によるフィルタ (Filter by attributes)] バーをクリックすると、ドロップダウンメニューから属性を選択して行をフィルタリングできます。ドロップダウンメニューに表示される属性は、選択したサブタブによって異なります。

ステップ 3 サマリー ペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。

ステップ 4 詳細については、表示する特定のコンポーネントを表すサマリーテーブルの行をダブルクリックします。

新しいダイアログ ボックスが、次のタブのいずれかと共に**作業**ペインの上に表示されます。

(注) 表示されるタブは、コンポーネントと構成が異なるように見えます。

- **概要 (Overview)** : クラウドリソース、設定関係、およびコンポーネントの設定の概要を示します。
- **クラウドリソース** : このコンポーネントに関連するクラウドリソース情報を表示するサブタブのリストを含みます。
- **アプリケーション管理** : コンポーネントに関連する ACI 関連情報を表示するサブタブのリストを含みます。
- **統計** : 選択したサンプリング間隔と統計タイプに基づいて統計を表示できるようにします。[統計] タブは表示しているコンポーネントに応じたサブタブを含みます。
- **イベント分析** : 障害、イベント、監査ログを表示するサブタブのリストを含みます。

操作の詳細の表示

ここでは、Cisco Cloud APIC GUI を使用して操作の詳細を表示する方法について説明します。操作の詳細には、特定の障害、イベント、監査ログ、アクティブセッション、バックアップおよび復元ポリシー、テクニカル サポート ポリシー、ファームウェア管理、スケジューラ ポリシー、およびリモート ロケーションの情報が含まれます。

ステップ 1 [ナビゲーション (Navigation)] メニューから [操作 (Operations)] タブを選択します。

[操作 (Operations)] タブが展開すると、サブタブ オプションのリストが表示されます。詳細については「操作オプション」の表を参照してください。

表 31: [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。 • [イベント (Events)] タブ: イベントをサマリー テーブルの行として表示します。 • [監査ログ (Audit Logs)] タブ: 監査ログをサマリー テーブルの行として表示します。
アクティブセッション	サマリー テーブルの行として、アクティブな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
[Tech Support]	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。 • [機能ごとのコンテナ] タブ - 機能ごとのコンテナをサマリー 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"> • [一般] タブ：一般的なファームウェア管理情報を表示します。 • [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。

[属性でフィルタ (Filter by Attributes)] バーをクリックすると、行をフィルタリングできます。属性、演算子、およびフィルタ値を選択します。たとえば、ユーザー名に基づいてフィルタリングするには、`username == user1` を選択します (user1は Cloud APIC にログインしているユーザーです)。

ステップ3 サマリー ペインを表示するために、表示する特定のコンポーネントを表す行をクリックします。

ステップ4 詳細については、表示する特定の項目を表すサマリーテーブルの行をダブルクリックします。

新しいダイアログボックスがサマリー テーブルから選択する項目の追加情報を表示する **作業** ペインの上に表示されます。

インフラストラクチャの詳細の表示

ここでは、Cisco Cloud APIC GUI を使用してインフラストラクチャの詳細を表示する方法について説明します。インフラストラクチャの詳細には、システム設定、リージョン間接続、および外部接続に関する情報が含まれます。

ステップ1 [ナビゲーション (Navigation)] メニューから [インフラストラクチャ (Infrastructure)] タブを選択します。

[インフラストラクチャ (Infrastructure)] タブが展開すると、サブタブオプションのリストが表示されます。詳細については、「インフラストラクチャ オプション」の表を参照してください。

表 32: インフラストラクチャ サブタブ

サブタブ名	説明
システム設定	一般的なシステム設定情報、管理アクセス情報、コントローラ、およびイベント分析を表示します。
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。

ステップ2 表示する詳細を含むコンポーネントを表すタブをクリックします。

管理の詳細の表示

ここでは、Cisco Cloud APIC GUI を使用して管理の詳細を表示する方法について説明します。管理の詳細には、認証、セキュリティ、ユーザ、およびスマートライセンスに関する情報が含まれます。

ステップ1 [ナビゲーション (Navigation)] メニューから [管理 (Administrative)] タブを選択します。

[管理 (Administrative)]タブが展開すると、サブタブ オプションのリストが表示されます。詳細については「Administrative Options」の表を参照してください。

表 33:管理サブタブ

サブタブ名	説明
Authentication	<p>以下の情報を含む [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)] 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。
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。

サブタブ名	説明
Users	次のサブタブを含みます。 <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	次のサブタブを含みます。 <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。 • [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。

(注) [属性でフィルタ (Filter by Attributes)] バーで属性を入力すると、行をフィルタリングできます。

Cisco Cloud APIC GUI を使用したヘルスの詳細の表示

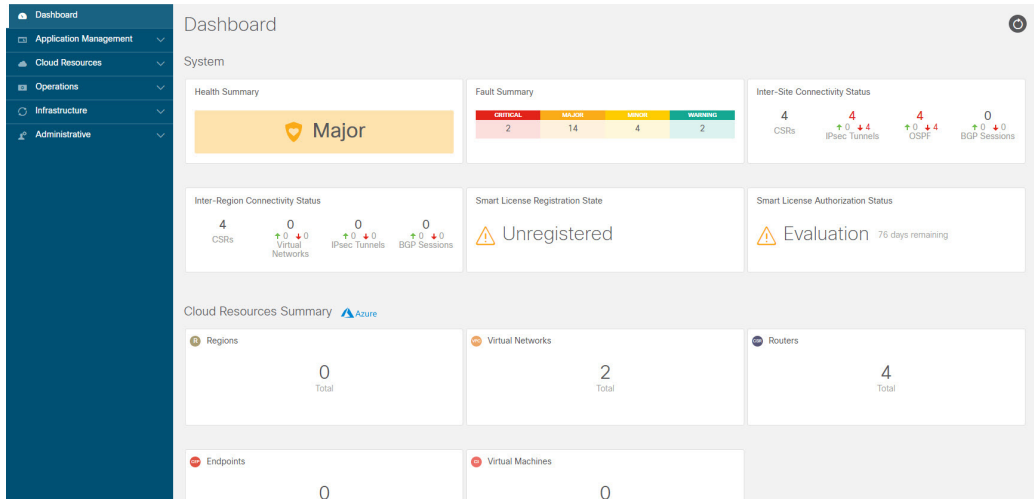
ここでは、Cisco Cloud APIC GUI を使用して正常性の詳細を表示する方法について説明します。Cisco Cloud APIC GUI の [クラウドリソース (Cloud Resources)] 領域で確認できるオブジェクトのヘルス詳細は、次のように表示できます。

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

- Instances
- クラウド サービス

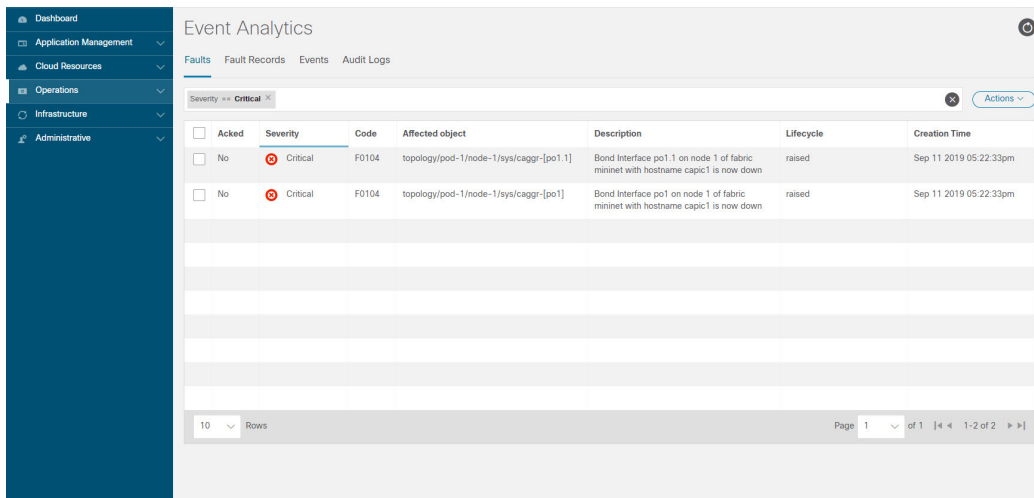
ステップ 1 [ナビゲーション (Navigation)] メニューから [ダッシュボード (Dashboard)] タブを選択します。

Cisco Cloud APIC システムの [ダッシュボード (Dashboard)] ウィンドウが表示されます。このウィンドウから、システムの全体的なヘルス ステータスを表示できます。



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

[イベント分析 (Event Analytics)] ウィンドウが表示され、クリックした特定の障害レベルの詳細情報が表示されます。次の画面は、重大度がクリティカルでリストされている障害の [イベント分析 (Event Analytics)] ウィンドウの例を示しています。



ステップ 3 重大度レベルの横にある [X] をクリックして、すべての障害のイベント分析情報を表示します。

Cisco Cloud APIC GUI を使用したヘルスの詳細の表示

[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/ryu/caggr-[po1.1]	Bond interface po1.1 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/ryu/caggr-[po1]	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-[overlay-1]-addr-[10.10.0.128/25]/osr-[cl-routerp_centralus_1_0]/instoper	Operational State of the hcloudInstanceOper is down with [computeVirtualMachinesClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceGroupNotFound" Message="Resource group 'APFC-infra-mininet-fchazel-centralus' could not be found.~]	raised	Sep 11 2019 07:36:27pm
No	Major	F3442	acct-[infra]/region-[centralus]/context-[overlay-1]-addr-[10.10.0.0/25]/osr-[cl-routerp_centralus_1_0]/instoper	Operational State of the hcloudInstanceOper is down with [computeVirtualMachinesClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceGroupNotFound" Message="Resource group 'APFC-infra-mininet-fchazel-centralus' could not be found.~]	raised	Sep 11 2019 07:36:27pm
No	Major	F3442	acct-[infra]/region-[eastus]/context-[overlay-1]-addr-[10.10.0.128/25]/osr-[cl-routerp_centralus_0_0]/instoper	Operational State of the hcloudInstanceOper is down with [computeVirtualMachinesClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceGroupNotFound" Message="Resource group 'APFC-infra-mininet-fchazel-centralus' could not be found.~]	raised	Sep 11 2019 07:36:27pm
No	Major	F3442	acct-[infra]/region-[centralus]/context-[overlay-1]-addr-[10.10.0.0/25]/osr-[cl-routerp_centralus_0_0]/instoper	Operational State of the hcloudInstanceOper is down with [computeVirtualMachinesClientCreateOrUpdate: Failure sending request: StatusCode=404 -- Original Error: Code="ResourceGroupNotFound" Message="Resource group 'APFC-infra-mininet-fchazel-centralus' could not be found.~]	raised	Sep 11 2019 07:45:10pm
No	Major	F3527	acct-[infra]/region-[eastus]/context-[overlay-1]-addr-[10.10.0.0/25]/osr-[cl-routerp_centralus_0_0]/instoper	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-[overlay-1]-addr-[10.10.0.0/25]/osr-[cl-routerp_centralus_1_0]/instoper	Operational State of the HcpPlatformLicense is down with administrative-down	raised	Sep 11 2019 05:21:36pm
No	Major	F0101	topology/pod-1/node-1/ryu/ctrl-p-[dev/vdb]-f-[dev/vdb]	Storage unit rdevvdb on node 1 with hostname capic1 has failed.	raised	Sep 11 2019 05:22:33pm
No	Minor	ERR001	hostname/ctrl-p-1/node-1/ryu/ctrl-p-[dev/vdb]-f-[dev/vdb]	Storage unit rdevvdb 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
canadeast	unmanaged	N/A	N/A	N/A	N/A
brazilsouth	unmanaged	N/A	N/A	N/A	N/A
australieeast	unmanaged	N/A	N/A	N/A	N/A
australacentral2	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



第 6 章

レイヤ 4 から レイヤ 7 サービスの展開

- 概要 (169 ページ)
- サービス グラフの展開 (173 ページ)

概要

Cisco Cloud APIC を使用すると、レイヤ 4 からレイヤ 7 のサービスデバイスをパブリッククラウドに展開できます。この初期リリースは、Amazon Web Services (AWS) でのアプリケーションロードバランサー (ALB) の展開をサポートしています。

アプリケーションロードバランサの概要

アプリケーションロードバランサ (ALB) は、パケットを検査し、HTTP および HTTPS ヘッダーへのアクセスポイントを作成するレイヤー 7 ロードバランサです。また、負荷を識別し、より高い効率でターゲットに分散します。サービスグラフを使用して ALB を展開します。これにより、トラフィックがネットワークにどのように流入するか、トラフィックが通過するデバイス、およびトラフィックがネットワークを離れる方法を定義できます。これらのアクションを指定するには、1 つ以上のリスナーを構成します。

リスナーを使用すると、ALB がトラフィックを受け入れるポートとプロトコル (HTTP または HTTPS) を指定できます。HTTPS を指定する場合は、セキュリティポリシーと SSL 証明書も選択します。



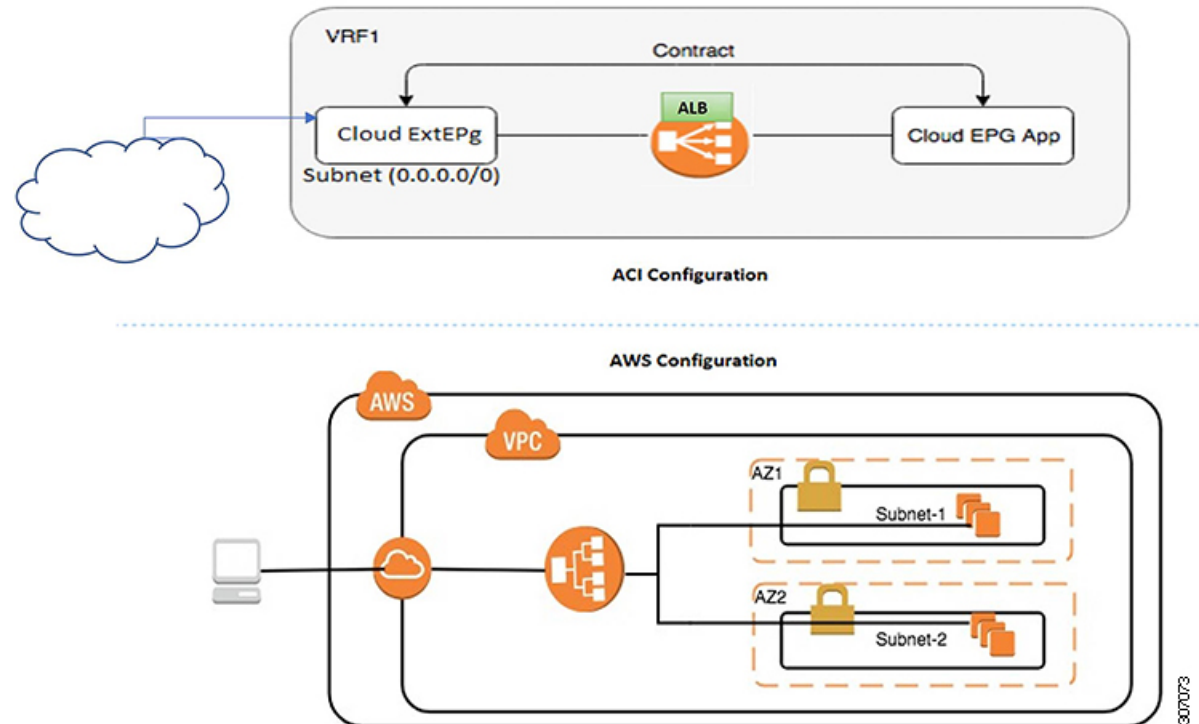
(注) リスナーは複数の証明書をもつことができます。

すべてのリスナーで、少なくとも 1 つのルール (条件のないデフォルトのルール) を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。たとえば、指定されたホスト名またはパスへの要求が行われたときに、トラフィックを指定された URL にリダイレクトするルールを作成できます。

展開には、インターネット向けと内部向けの 2 種類があります。インターネットに接続する展開では、コンシューマーの外部 EPG とプロバイダーのクラウド EPG の間にサービスとして

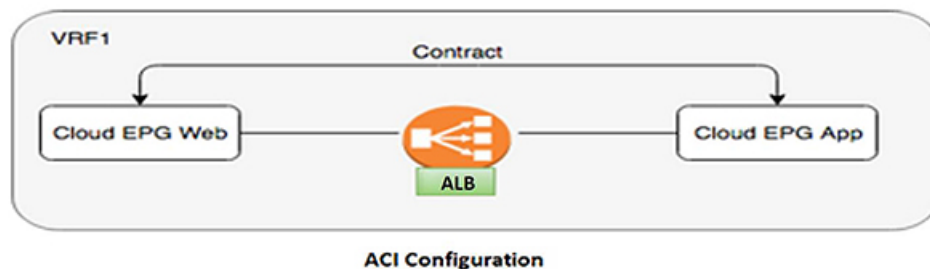
ALB が挿入されます。次の図は、VRF 内のコントラクト構成と、コンシューマーの外部 EPG とプロバイダーのクラウド EPG の間に挿入されるサービスとしての ALB を示しています。

図 21: インターネットに面した展開

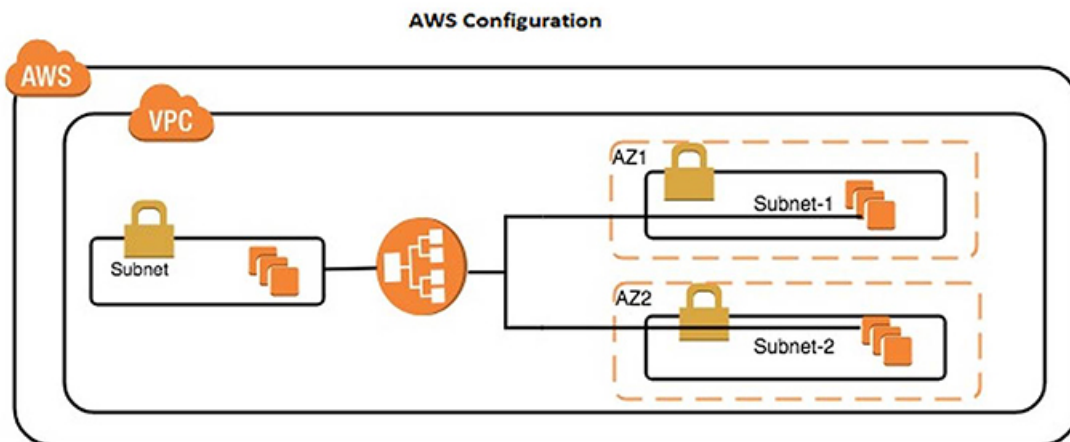


内部向け展開では、コンシューマークラウド EPG とプロバイダークラウド EPG の間にサービスとしての ALB が挿入されます。次の図は、コンシューマクラウド EPG とプロバイダークラウド EPG の間に挿入されるサービスとしての VRF および ALB 内の契約構成を示しています。

図 22: 内部に向けた展開



ACI Configuration



AWS Configuration



(注) ALBの詳細については、AWSのWebサイトのマニュアルを参照してください。

サーバー プールへのダイナミック サーバーのアタッチ

サーバープールまたはターゲットグループ内のサーバーはダイナミックに追加されます。ターゲットのIPアドレスまたはインスタンスIDを指定する必要はありません。リスナールールからプロバイダークラウド EPG への関係は、エンドポイントのダイナミックな選択に使用されます。この関係は、エンドポイントをターゲットグループに追加するためにも使用されます。デフォルトでは、エンドポイントはポート番号 80 で登録されています。

ALB で提供されるターゲットグループとセキュリティグループの関連付け、およびエンドポイントの EPG (セキュリティグループ) に基づいて、EC2 インスタンス (サーバー) は、ターゲットグループのデフォルトポートでダイナミックにターゲットグループに関連付けられます。または、ターゲットグループポートで EC2 インスタンスを登録する代わりに、次の表のポートを指定してカスタムポートをアタッチできます。

表 34: カスタム ポートベースのアタッチ

プロバイダー-EPG	ポート
EPGMap:<Epg1DN>	9090
EPGMap:<Epg2DN>	9091、9099

EPGMap:<EpgDN>をタグとして、さらに、コンマで区切られたリストとしてターゲットグループに登録されるポートのリストを指定できます。

サービス グラフについて

Cisco Application Centric Infrastructure (ACI) はアプリケーションの一部としてサービスを見なします。必要とされるすべてのサービスが、Cisco APIC から Cisco ACI ファブリックでインスタンス化されるサービス グラフとして扱われます。ユーザーは、アプリケーションに対してサービスを定義し、サービス グラフはアプリケーションが必要とする一連のネットワークまたはサービス機能を識別します。

サービス グラフは、次の要素を使ってネットワークを表します。

- 機能ノード：機能ノードは、ロードバランサなどのトラフィックに適用される機能を表します。サービス グラフ内の1つの機能は1つ以上のパラメータを必要とし、1つまたは複数のコネクタを持っている場合があります。
- 端末ノード：端末ノードはサービス グラフからの入出力を有効にします。
- コネクタ：コネクタはノードからの入出力を有効にします。

グラフが設定されると、Cisco APIC はサービス グラフに明記されたサービス機能の要件に従って、サービスを自動的に設定します。Cisco APIC もまた、サービス グラフで指定されるサービス機能のニーズに応じてネットワークを自動的に設定します。これにより、サービスデバイスを変更する必要がなくなります。

サービス グラフは、アプリケーションの複数の階層として表され、適切なサービス機能が階層間に挿入されます。

サービスアプライアンス (デバイス) は、グラフ内でサービス機能を実行します。1つ以上のサービスアプライアンスが、グラフに必要なサービスをレンダリングするために必要になることがあります。1つ以上のサービス機能が単一のサービス デバイスで実行できます。

サービス グラフおよびサービス機能には、次の特性があります。

- 特定のエンドポイントグループから送信されたトラフィックは、ポリシーに基づいてリダイレクトできます。
- サービス グラフのリダイレクトには方向があります。つまり、リダイレクトは両方のトラフィック方向またはいずれか一方のトラフィックに適用できます。
- 論理機能は、ポリシーに基づいて適切なデバイスでレンダリングできます。

- サービスグラフでは、エッジの分割と結合がサポートされ、管理者は線形サービスチェーンに制限されません。
- トラフィックは、サービスアプライアンスが発信した後にネットワーク内で再度分類できます。

サービスグラフを使用すると、サービス、ロードバランサを一度インストールして、異なる論理トポロジで何度も展開できます。グラフを展開するたびに、Cisco ACIは新しい論理トポロジでの転送を行えるように、サービスデバイスで設定の変更を行います。

機能ノードについて

機能ノードは、単一のサービス機能を表します。機能ノードには、サービス機能のネットワーク要件を表す機能ノードコネクタがあります。

サービスグラフ内の関数ノードには、次のパラメータが必要です。

- テナント
- 2つの可用性ゾーンにサブネットを持つクラウドコンテキストプロファイル

サービスグラフのレンダリング時に関数パラメータを指定できます。たとえば、関数ノードがロードバランサーである場合、リスナーとそのルールは、グラフのレンダリング時に関数ノードに対して指定できます。

端末ノードについて

端末ノードはサービスグラフとコントラクトを接続します。コントラクトに端末ノードを接続することにより、2つのアプリケーションクラウドEPG間のトラフィックにサービスグラフを挿入できます。接続されると、コントラクトのコンシューマクラウドEPGとプロバイダークラウドEPG間のトラフィックはサービスグラフにリダイレクトされます。

サービスグラフの展開

サービスグラフを使用すると、デバイス間のトラフィックフロー、ネットワークへのトラフィックの流入方法、トラフィックが通過するデバイス、およびトラフィックがネットワークから出る方法を定義できます。

サービスグラフを構成する前に、以下を構成する必要があります。

1. テナント
2. クラウドコンテキストプロファイル
3. サブネット
4. アプリケーションプロファイル

5. コンシューマ EPG
6. プロバイダー EPG
7. コントラクト

Cloud APIC GUI を使用したサービス グラフの展開

Cisco Cloud APIC GUI を使用したロード バランサの作成

このセクションでは、Cisco Cloud APIC GUI を使用したローカル ユーザーの作成方法について説明します。

ステップ 1 [アプリケーション管理 (Application Management)] > [サービス (Services)] をクリックします。

[サービス (Services)] ページが表示されます

ステップ 2 [デバイス (Device)] タブで、[アクション (Actions)] > [デバイスの作成 (Create Device)] をクリックします。

[デバイスの作成 (Create Device)] ページが表示されます。

ステップ 3 次の [デバイスの作成ダイアログボックスのフィールド (Create Device Dialog Box Fields)] の表にリストされた各フィールドに該当する値を入力し、続行します。

表 35: デバイス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	ロード バランサーの名前を入力します。
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)] ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択 (Select)] をクリックします。[デバイスの作成 (Create Device)] ダイアログボックスに戻ります。
[設定 (Settings)]	
サービス タイプ	[アプリケーション ロードバランサ (Application Load Balancer)] を選択します。

[プロパティ (Properties)]	説明
スキーム	[内部 (Internal)] または [インターネット向き (Internet Facing)] を選択します。
Subnets	<p>可用性ゾーンごとに1つのサブネットのみを指定できます。ロードバランサの可用性を高めるには、少なくとも2つの可用性ゾーンからサブネットを指定する必要があります。</p> <ol style="list-style-type: none"> [サブネットの追加 (Add Subnet)] をクリックします。 [サブネットの追加 (Add Subnet)] ダイアログボックスが表示されます。 [サブネットの追加 (Add Subnet)] ダイアログボックスで、[クラウドコンテキスト プロファイルの選択 (Select Cloud Context Profile)] をクリックします。 [クラウドコンテキスト プロファイルの選択 (Select Cloud Context Profile)] ダイアログボックスが表示されます。 [クラウドコンテキスト プロファイルの選択] ダイアログボックスで、クラウドコンテキスト プロファイルを選択し、[選択 (Select)] をクリックします。 再度[サブネットの追加 (Add Subnet)] ダイアログボックスが表示されます。 [サブネットの追加 (Add Subnet)] ダイアログボックスで、[サブネットの選択 (Select Subnet)] をクリックします。 [サブネットの選択] ダイアログボックスが表示されます。 [サブネットの選択 (Select Subnet)] ダイアログボックスでサブネットを選択し、[選択 (Select)] をクリックします。 再度[サブネットの追加 (Add Subnet)] ダイアログボックスが表示されます。 [サブネットの追加 (Add Subnet)] ダイアログボックスで、[追加 (Add)] をクリックします。 [デバイスの作成 (Create Device)] ページに戻ります。

ステップ4 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUIを使用したサービス グラフ テンプレートの作成

このセクションでは、Cisco Cloud APIC GUI を使用したサービス グラフ テンプレートの作成方法について説明します。

始める前に

デバイスはすでに作成されています。

ステップ 1 [アプリケーション管理 (Application Management)] > [サービス (Services)] をクリックします。

[サービス (Services)] ページが表示されます

ステップ 2 [サービス グラフ (Service Graphs)] タブをクリックし、[アクション (Actions)] > [サービス グラフの作成 (Create Service Graph)] をクリックします。

[サービス グラフの作成 (Create Service Graph)] ページが表示されます。

ステップ 3 次の [サービス グラフの作成ダイアログ ボックスのフィールド (Create Service Graph Dialog Box Fields)] の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 36: サービス グラフの作成ダイアログ ボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	サービス グラフ テンプレートの名前を入力します。
テナント	<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)] ダイアログが表示されます。 左側の列から、クリックしてテナントを選択します。 [選択 (Select)] をクリックします。[サービス グラフの作成 (Create Service Graph)] ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。
[設定 (Settings)]	

[プロパティ (Properties)]	説明
デバイスを選択	<p>デバイスを選択します。</p> <ol style="list-style-type: none"> 1. アプリケーションロードバランサアイコンをサービスグラフの[デバイスのドロップ (Drop Device)]エリアにドラッグアンドドロップします。 [サービスノード (Service Node)]ダイアログボックスが表示されます。 2. [アプリケーションロードバランサの選択 (Select Application Load Balancer)]をクリックします。 [アプリケーションロードバランサの選択 (Select Application Load Balancer)]ダイアログが表示されます。 3. 左側の列から、デバイスをクリックして選択します。 4. [選択 (Select)]をクリックします。 [サービスノード (Service Node)]ダイアログボックスに戻ります。 5. [追加] をクリックします。 [サービスグラフの作成 (Create Service Graph)]ウィンドウに戻ります。

ステップ4 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したレイヤ4からレイヤ7サービスの展開

このセクションでは、レイヤ4～レイヤ7サービスを展開する方法について説明します。

始める前に

- これでデバイスが構成されました。
- サービスグラフが構成されました。

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

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

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

- ステップ3** [**インテント (Intent)**] メニューの [**構成 (Configuration)**] リストで、[**EPG Communication**] をクリックします。[**EPG通信 (EPG Communication)**] ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。
- ステップ4** コントラクトを選択します。
- [**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。
 - [**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。
- [**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 EPG の選択 (Select Consumer EPGs)**] ダイアログが表示されます。
 - [**コンシューマ EPG の選択**] ダイアログの左側のペインで、チェックボックスをクリックしてチェックボックスをオンにして、クラウド EPG (内部向けロードバランサの場合) またはクラウド外部 EPG (インターネット向けロードバランサの場合) を選択します。[**選択**] をクリックします。[**コンシューマ EPG の選択 (Select Consumer EPGs)**] ダイアログボックスが閉じます。
- ステップ6** プロバイダー EPG を追加するには、次の手順を実行します。
- [**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。
 - [**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、[**選択**] をクリックします。[**プロバイダー EPG の選択 (Select Provider EPGs)**] ダイアログボックスが閉じます。
- ステップ7** サービス グラフを選択するには:
- [**EPF 通信の構成 (EPG Communication Configuration)**] ダイアログで、[**サービス グラフの選択 (Select Service Graph)**] をクリックします。[**サービス グラフの選択 (Select Service Graph)**] ダイアログボックスが表示されます。
 - [**サービス グラフの選択 (Select Service Graph)**] ダイアログの左側のペインで、サービス グラフをクリックして選択し、[**選択 (Select)**] をクリックします。[**サービス グラフの選択 (Select Service Graph)**] ダイアログボックスが閉じます。
- ステップ8** [**サービス グラフのプレビュー (Service Graph Preview)**] で、[**クラウド ロード バランサ リスナーの追加 (Add Cloud Load Balancer Listener)**] をクリックします。[**クラウド ロード バランサ リスナーの追加 (Add Cloud Load Balancer Listener)**] ダイアログが表示され、リスナーを追加できます。
- リスナーは、デバイスが動作するポートとプロトコルです。
- ステップ9** 次の [**クラウドロードバランサリスナーの追加ダイアログボックスのフィールド (Add Cloud Load Balancer Listener Dialog Box Fields)**] テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 37:クラウドロードバランサリスナーの追加ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	リスナーの名前を入力します。
[ポート (Port)]	デバイスがトラフィックを受け入れるポートを入力します。
プロトコル (Protocol)	HTTP または HTTPS を選択します。
Security Policy	ドロップダウンリストをクリックし、セキュリティポリシーを選択します (HTTPS が選択されている場合にのみ選択可能)。
SSL 証明書 (SSL Certificate)	<p>SSL 証明書を選択するには (HTTPS が選択されている場合にのみ選択可能):</p> <ol style="list-style-type: none"> 1. [SSL 証明書の追加] をクリックします。 2. クリックして、追加する証明書のチェックボックスをオンにします。 3. キーリングを選択してください: <ol style="list-style-type: none"> 1. [キーリングの選択] をクリックします。 [キーリングの選択 (Select Key Ring)] ダイアログが表示されます。 2. [キーリングの選択 (Select Key Ring)] ダイアログで、左側の列のキーリングをクリックして選択し、[選択 (Select)] をクリックします。[キーリングの選択 (Select Key Ring)] ダイアログボックスが閉じます。 4. [証明書ストア] ドロップダウンリストをクリックして、証明書を選択します。 <p>(注) リスナーは複数の証明書を持つことができます。</p>
ルールの追加	ルール設定をデバイスリスナーに追加するには、 [ルールの追加] をクリックします。 [ルール] リストに新しい行が表示され、 [ルール設定] フィールドが有効になります。

[プロパティ (Properties)]	説明
ルール設定	

[プロパティ (Properties)]	説明
	<p>[ルール設定 (Rule Settings)] ペインで、次のオプションを設定します。</p> <ul style="list-style-type: none"> • 名前 : 規則の名前を入力します。 • ホスト : ホスト名を入力して、ホストベースの条件を作成します。このホスト名に対して要求が行われると、指定したアクションが実行されます。 • パス : パスを入力して、パスベースの条件を作成します。このパスに対して要求が行われると、指定したアクションが実行されます。 • タイプ : アクションタイプは、実行するアクションをデバイスに通知します。アクションタイプのオプション: <ul style="list-style-type: none"> • 固定応答を返す : 次のオプションを使用して応答を返します。 <ul style="list-style-type: none"> • 固定応答本文 : 応答メッセージを入力します。 • 固定応答コード : 応答コードを入力します。 • 固定の応答コンテンツタイプ : コンテンツタイプを選択します。 • 転送 : 次のオプションを使用してトラフィックを転送します。 <ul style="list-style-type: none"> • ポート : デバイスがトラフィックを受け入れるポートを入力します。 • プロトコル : [HTTP] または [HTTPS] を選択します。 • プロバイダー EPG : トラフィックを処理する Web サーバーを持つ EPG。 • EPG : EPG を選択するには: <ol style="list-style-type: none"> 1. [EPGの選択] をクリックします。 [EPGの選択] ダイアログボックスが表示されます。 2. [EPGの選択] ダイアログで、左側の列の EPG をクリックして選択

[プロパティ (Properties)]	説明
	<p>し、[選択 (Select)]をクリックします。[EPGの選択]ダイアログボックスが閉じます。</p> <ul style="list-style-type: none"> • リダイレクト : 次のオプションを使用して、リクエストを別の場所にリダイレクトします。 <ul style="list-style-type: none"> • リダイレクト コード : [リダイレクト コード] ドロップダウン リストをクリックして、コードを選択します。 • リダイレクト ホスト名 : リダイレクトのホスト名を入力します。 • リダイレクト パス : リダイレクトパスを入力します。 • リダイレクト ポート : デバイスがトラフィックを受け入れるポートを入力します。 • リダイレクト プロトコル : [リダイレクト プロトコル (Redirect Protocol)] ドロップダウン リストをクリックして、[HTTP]、[HTTPS]、または[継承 (Inherit)]を選択します。 • リダイレクト クエリ : リダイレクトクエリを入力します。 <p>完了したら、[ルールの追加] をクリックします。</p>

ステップ 10 終了したら、[Add] をクリックします。
サービス グラフが展開されます。

REST API を使用したサービス グラフの展開

REST API を使用したインターネット向けロード バランサの作成

この例では、REST API を使用して内部向けのロード バランサを作成する方法を示します。

内部向けのロードバランサを作成するには:

例:

```
<polUni>
  <fvTenant name="t2" status="">
    <cloudLB name="ALB1" type="application" scheme="internal" status="">
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.7.0/24]"
status=""/>
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.8.0/24]"
status=""/>
    </cloudLB>
  </fvTenant>
</polUni>
```

REST API を使用したインターネット向けロードバランサの構成

この例では、REST API を使用してインターネット向けのロードバランサを作成する方法を示します。

インターネット向けのロードバランサを作成するには:

例:

```
<polUni>
  <fvTenant name="t2" status="">
    <cloudLB name="ALB1" type="application" scheme="internet" status="">
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.5.0/24]"
status=""/>
      <cloudRsLDevToCloudSubnet tDn="uni/tn-t2/ctxprofile-c1/cidr-[10.33.0.0/16]/subnet-[10.33.6.0/24]"
status=""/>
    </cloudLB>
  </fvTenant>
</polUni>
```

REST API を使用したサービスグラフの作成

この例では、REST API を使用してサービスグラフを作成する方法を示します。

サービスグラフを作成するには:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsTermNodeProv name="Input1">
        <vnsAbsTermConn name="C1"/>
      </vnsAbsTermNodeProv>
      <vnsAbsTermNodeCon name="Output1">
        <vnsAbsTermConn name="C2"/>
      </vnsAbsTermNodeCon>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```

```

</vnsAbsTermNodeCon>
<vnsAbsNode funcType="GoTo" name="N1" managed="yes">
  <vnsRsNodeToCloudLDev tDn="uni/tn-t2/clb-ALB1" status=""/>
  <vnsAbsFuncConn name="provider"/>
  <vnsAbsFuncConn name="consumer"/>
</vnsAbsNode>
<vnsAbsConnection connDir="consumer" connType="external" name="CON2">
  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsTermNodeCon-Output1/AbsTConn"/>

  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsNode-N1/AbsFConn-consumer"/>

</vnsAbsConnection>
<vnsAbsConnection connDir="provider" connType="internal" name="CON1">
  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsTermNodeProv-Input1/AbsTConn"/>

  <vnsRsAbsConnectionConns tDn="uni/tn-t2/AbsGraph-CloudGraph/AbsNode-N1/AbsFConn-provider"/>

</vnsAbsConnection>
</vnsAbsGraph>
</fvTenant>
</polUni>

```

REST API を使用してサービス グラフを添付する

この例では、REST API を使用してサービス グラフを作成する方法を示します。

サービス グラフを添付するには:

```

<polUni>
  <fvTenant name="t2">
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjGraphAtt tnVnsAbsGraphName="CloudGraph"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>

```

REST API を使用した HTTPS サービス ポリシーの構成

この例では、REST API を使用して HTTP サービス ポリシーを作成する方法を示します。

HTTP サービス ポリシーを作成するには:

```

<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="http_listener1" port="80" protocol="http" status="">
            <cloudListenerRule name="rule1" priority="10" default="yes" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"

```

```

epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
  </cloudListenerRule>
  <cloudListenerRule name="redirectRule" priority="20">
    <cloudRuleCondition type="path" value="/img/*"/>
    <cloudRuleAction type="redirect" RedirectPort="8080"/>
  </cloudListenerRule>
  <cloudListenerRule name="FixedRspRule" priority="30">
    <cloudRuleCondition type="host" value="example.com"/>
    <cloudRuleAction type="fixedResponse" FixedResponseCode="200"/>
  </cloudListenerRule>
  <cloudListenerRule name="redirectHPRule" priority="40" status="">
    <cloudRuleCondition type="host" value="example.com"/>
    <cloudRuleCondition type="path" value="/img/*"/>
    <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
  </cloudListenerRule>
</cloudListener>
</cloudSvcPolicy>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>

```

REST API を使用したキー リングの設定

この例では、REST API を使用したキー リングのリーク ルートを構成する方法を示します。キー リング構成の詳細については、*Cisco APIC 基本構成ガイド*を参照してください。

キー リングを設定するには:

```

<polUni>
  <fvTenant name="t2">
    <cloudCertStore>
      <pkiKeyRing status="" name="lbCert" tp="lbTP" key="-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEADGxaK+RHv/nToHLnmDBq2BfLimgX/zNJQC9bGuzr8Mj7dm0
XuHfQYGv0h1PtL4Pdx5f5qjB0NbhjAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCRE
Ginn/CgF75QPied568eScNDZPt/eMeHAuRX/PykKUatWWncGanJvHqc+SOLPF6TD
gQ5nwOHHFvYm2DY8bfdYWrWmGs07JqZzbPmptA2QWblILsSoIrdkIIgf6ZfYy/EN
bH+nYN2rJT81zYsxx0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8K0fdCZPEq
8takiWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQBAoIBAQQDQQA9IslYrdtqN
q6mZ3s2BNfF/4kgb7gn0Dws+9EJLcJNZVhFEo2ZxxyfPp6HRnjYS50W83/E1and
+GD1bSucTuxqFWIQVh7r1ebYZIwk+NYSjr5yNVxux8U2hCNNV8WWWqkJjKcUqICB
Bm47FKj53LV46zE0gyCaibFrYxZJ9+farGneyBdnoV+3thmez7534KCi0t3J3Eri
lgSY3ql6hPXB2ZXP4jdAoLgWDU4IIM6OqOiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5G1fv2A4xTBQMCTZUZJ9fYAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphED1AoGBAPVlvKfGW46qqRnYovfryxxx4OM1sVSGcJpQTQtBQi2koJ8OwEZJ
2s+CX0r+oDqWP23go/QEVYVkcic9RGkJBNgel+dm/bTjzgmQYtqSCNtecTsZD5JN
y1jkciiznDkjcjReS22kh3dGXIBRiYk7ezp2z7EKfDrHe5x5ouGMGcNaAoGBAOnh
buDEohv8KJaB+DiUfhftoa3aKNPBO+zWPCHP0HFGjPXshJcIYZc1GcycmuDKVnDd
MxhE/yOnQHowi4T9FMLpz5yh5zuCUVqOBgB1P6MzbC5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCW1OAFJRw3c/OiESwLMzchs18RnbwOi6kDAoGBANV1zmPb07zB3eGTCU0t
KGiqwFLncUkVadZRRFZYPPnwiRkoe73j9brkNbgCqxW+Nlp5UjoeFry0N6y106q/
ZA4I7FnXryLBw2HYuw41Vixl+XOZ/He03RmFN1z717dGmaGbv43aKIB9x+X5n8wF
6z1NtBhmBk7yNwom1IRag1sbAoGAX0p4cJ/tJNXSe7AswHDQCL68uimJdDfZ5nKG
k83nE+Qc0qQozDJAmCiSfmuSNRnSep3FiafjBFXK0X4h+mdbJcC7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztzTn+as6xKOUATEezy9DK9zMWzQhhtay
m9yZTp0CgYEA1UtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdGJt88ezM1Oej
Pdoab0G2PcFgJZoTSGk7N4XArVKeq7pgz0kwcYAsh06A2Hal+D1z/bGoZP+kmD/x

```


REST API を使用した HTTPS サービス ポリシーの作成

このセクションでは、REST API を使用して HTTPS サービス ポリシーを作成する方法を示します。



- (注) リスナーは複数の証明書をもつことができます。証明書のオプションは次のとおりです。
- ELBSecurityPolicy-2016-08 – セキュリティ ポリシーが選択されていない場合のデフォルト。
 - ELBSecurityPolicy-FS-2018-06
 - ELBSecurityPolicy-TLS-1-2-2017-01
 - ELBSecurityPolicy-TLS-1-2-Ext-2018-06
 - ELBSecurityPolicy-TLS-1-1-2017-01
 - ELBSecurityPolicy-2015-05
 - ELBSecurityPolicy-TLS-1-0-2015-04

複数の証明書を使用する場合は、デフォルトの証明書を指定する必要があります。デフォルトは、**cloudRsListenerToCert** の **defaultCert** プロパティを使用して指定されます。

始める前に

キー リング証明書は既に構成されています。

HTTPS サービス ポリシーを作成するには:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="https_listener" port="443" protocol="https"
secPolicy="eLBSecurityPolicy-2016-08" status="">
            <cloudRsListenerToCert defaultCert="yes" certStore="iam"
tDn="uni/tn-t2/certstore/keyring-lbCert" status=""/>
              <cloudListenerRule name="defaultRule" default="yes" priority="100" status="">
                <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t1/cloudapp-ap/cloudepg-ep1">
                  </cloudRuleAction>
                </cloudListenerRule>
              </cloudListener>
            </cloudSvcPolicy>
          </vnsAbsNode>
        </vnsAbsGraph>
      </fvTenant>
    </polUni>
```




第 7 章

Cisco Cloud APIC 統計

- [Cisco Cloud APIC 統計の概要 \(189 ページ\)](#)
- [AWS ネットワーク インターフェイス統計コレクション \(190 ページ\)](#)
- [Cisco Cloud APIC エンドポイントと cloudEPg 統計処理 \(190 ページ\)](#)
- [Cisco Cloud APIC 統計フィルタ \(191 ページ\)](#)
- [AWS Transit ゲートウェイ統計 \(191 ページ\)](#)
- [VPC フロー ログの有効化 \(192 ページ\)](#)
- [クラウドルータ統計 \(196 ページ\)](#)

Cisco Cloud APIC 統計の概要

Cisco Cloud Application Policy Infrastructure Controller (APIC) は、クラウドルータから収集される統計をサポートします。さらに、Amazon Web Services (AWS) フロー ログを処理することによって得られる統計をサポートします。AWS フロー ログは無料のサービスではないため、Cisco Cloud APIC によりこの機能を制御できるポリシーが提供されています。この機能は、デフォルトでイネーブルではありません。

CloudWatch とフロー ログの詳細については、AWS ウェブサイトの Amazon Virtual Private Cloud の「VPC フロー ログ」を参照してください。

Cisco Cloud APIC リリース 5.0(1) 以降、次のことを実行できます。

- フィルターを使用して、AWS フロー ログから特定の情報を表示できます。特定のフロー ログ ポリシー (または VPC) に対して同時に最大 8 つのフィルターを定義できます。送信元または宛先の IP アドレス、ポート、およびプロトコルの組み合わせでフィルタリングできます。詳細については、「[Cisco Cloud APIC 統計フィルタ \(191 ページ\)](#)」を参照してください。
- AWS Transit Gateway との間のトラフィックの統計を収集できます。このガイドの [AWS Transit ゲートウェイ統計 \(191 ページ\)](#) セクションを参照してください。

AWS ネットワーク インターフェイス統計コレクション

AWS は、フロー ログを通じてネットワーク インターフェイスごとの非リアルタイム IP トラフィック情報を提供します。Cisco Cloud APIC は、cloudCtxProfile ごとにフロー ログを有効にするためのポリシーを提供します。cloudCtxProfile は AWS の VPC にマッピングされるため、cloudCtxProfile または VPC ごとにフロー ログを有効にするということは、その VPC に属する各インターフェイスのフロー ログを有効にすることを意味します。フロー ログが有効になると、フロー レコードは定期的に AWS Cloudwatch にプッシュされます。次に、Cisco Cloud APIC はこれらのフロー レコードについて AWS CloudWatch を定期的にポーリングし、これらのレコードを解析して統計を抽出します。フロー レコードを CloudWatch に発行するのに最大 15 分かかるとあるため、Cisco Cloud APIC は CloudWatch へのフロー ログのクエリも 15 分遅らせます。これは、CloudWatch に存在するフロー ログと、Cisco Cloud APIC に表示される対応する統計との間にラグがあることを意味します。Cisco Cloud APIC は、CloudWatch への発行に 15 分以上かかるフロー レコードを処理しません。

Cisco Cloud APIC エンドポイントと cloudEPg 統計処理

Cisco Cloud APIC は、CloudWatch にフロー ログが存在する AWS ネットワーキング エンドポイントごとに、次の統計を抽出します。

- 送信されたバイト数またはパケット数 (送信側)
- 受信したバイト数またはパケット数 (受信側)
- 拒否されたバイト数またはパケット数 (送信側ドロップ)
- ドロップされたバイト数またはパケット数 (受信側ドロップ)

これらの統計は、cloudEpInfoHolder オブザーバブルに関連付けられています。

また、Cisco Cloud APIC は、フロー ログ レコードをリージョンごとに 1 つ以上の cloudEPg オブジェクトにマッピングします。これは、cloudEPg が複数のリージョンに存在する可能性があるためです。これらの統計は、cloudRgInfoHolder オブザーバブルに関連付けられています。このオブザーバブルは cloudEPg の子であり、cloudRgInfoHolder の子の統計を蓄積すると、cloudEPg の統計になります。cloudEPg は、次の統計をサポートしています。

- 送信されたバイト数またはパケット数 (送信側)
- 受信したバイト数またはパケット数 (受信側)
- 拒否されたバイト数またはパケット数 (送信側ドロップ)
- ドロップされたバイト数またはパケット数 (受信側ドロップ)

cloudEPg 統計は、fvApp まで集計され、次に fvTenant まで集計されます。

Cisco Cloud APIC 統計フィルタ

Cisco Cloud Application Policy Infrastructure Controller リリース 5.0(1) 以降、フィルタを使用して、Amazon Web Services (AWS) フロー ログから特定の情報を表示できます。

フィルタが展開されているエンドポイントごとに統計が収集されます。フィルタを使用すると、送信元または送信先の IP アドレス、ポート、およびプロトコルの組み合わせによってフィルタリングされたフローに関する情報を表示できます。特定の AWS ログ グループに対して同時に最大 8 つのフィルタを定義できます。

統計フィルタには、次の 3 つの属性があります。

- **PeerIP:** フィルタリングする IPv4 アドレス
- **PeerPort:** リッスンするポート番号
- **プロトコル:** リッスンするプロトコル番号



- (注) Cisco Cloud APIC GUI を使用して統計フィルタを構成することをお勧めします。代わりに REST API を使用することもできます。ただし、そうしてから GUI に切り替えると、機能が不完全に見えます。選択した方法に固執する必要があります。

統計フィルタの使用は、Virtual Private Cloud (VPC) フロー ログの有効化に依存します。統計フィルタを構成する前に、ログを有効にする必要があります。

AWS CloudWatch に保存されるフロー ログは、フロー ログ レコードで構成されます。Cisco Cloud Application Policy Infrastructure Controller (APIC) は、フロー ログ レコードを解析して統計を抽出します。

特定のフロー レコードが発生してから AWS CloudWatch に存在するまで、最大 15 分かかることがあります。Cisco Cloud APIC は過去 15 分以上に発生したフロー レコードをポーリングします。AWS CloudWatch に表示されるまでに 15 分以上かかるフロー レコードは処理しません。

AWS Transit ゲートウェイ統計

インフラテナントとユーザーテナントの両方で、Amazon Web Services (AWS) Transit Gateways を通過するトラフィックの統計を収集できます。ユーザーテナントについて報告される統計は、ユーザー VPC と AWS Transit Gateway 間のアタッチメントのトラフィックを表します。インフラテナントから報告される統計は、インフラ VPC と Transit Gateway 間の添付のトラフィックを表します。

AWS Transit Gateway について、次の統計が収集されます。

- 受信側パケット
- 受信側パケットバイト

- 受信側パケット ドロップ
- 受信側パケット ドロップ バイト
- 送信側パケット
- 送信側パケット バイト
- 送信側パケット ドロップ
- 送信側パケット ドロップ バイト

Cisco Cloud Application Policy Infrastructure Controller [セットアップ]-[リージョン管理] ページから、インフラテナント Transit Gateway の統計情報の収集を有効にすることができます。AWS [Transit Gateway](#) を使用して VPC 間の帯域幅を増やすことについては、「AWS Transit Gateway を使用するようにクラウドサイトをセットアップする」セクションを参照してください。

ユーザー VPC でフロー ログを有効にすることで、ユーザー テナントの Transit Gateway 統計収集を有効にすることができます。このガイドの [VPC フロー ログの有効化 \(192 ページ\)](#) と [Cisco Cloud APIC GUI を使用した VPC フロー ログの有効化 \(193 ページ\)](#) を参照してください。

AWS Transit Gateway の統計を表示するには、Cisco Cloud APIC GUI で [統計] タブをクリックし、左側のナビゲーションペインで [AWS Transit Gateway] をクリックします。中央のペインに情報が表示されます。

VPC フロー ログの有効化

VPC フロー ログを有効にする手順:

1. ログ グループ ポリシーを定義します。
2. フロー ログ ポリシーを定義し、最初の手順で定義したログ グループを関連付けます。
3. フロー ログ ポリシーを 1 つ以上の `cloudCtxProfile` に関連付けます。

ログ グループ プロパティ:

- **name** : フロー ログが送信される CloudWatch 内の場所。



(注) AWS でプログラムされている実際のログ グループ名は、`<tenant name><cloudCtxProfile name><log group name>` です。

- **retention** : CloudWatch にログを保存する期間の長さ。デフォルトは 5 日です。

フロー ログのプロパティ:

- **trafficType** : 収集するトラフィックのタイプ。サポートされているタイプは、**all**、**accept only**、**reject only** です。デフォルトは、**all** です。

Cisco Cloud APIC GUI を使用した VPC フロー ログの有効化

このセクションでは、Cisco Cloud APIC GUI を使用した VRF フロー ログを有効にする方法について説明します。



(注) フィルタを使用して AWS フロー ログから特定の情報を表示する場合は、この手順のオプションのステップを実行します。

ステップ 1 [ナビゲーション (Navigation)] メニュー > [アプリケーション管理 (Application Management)] > [テナント (Tenants)] の順にクリックします。

[テナント (Tenant)] ウィンドウが表示され、テナントがサマリー テーブルの行としてリストされます。

ステップ 2 テナントをダブルクリックします。

テナント ダイアログ ボックスが [Work] ペインの上に表示されます。テナント ダイアログ ボックスには、[概要 (Overview)]、[クラウドリソース (Cloud Resources)]、[アプリケーション管理 (Application Management)]、[統計 (Statistics)]、および [イベント分析 (Event Analytics)] タブが表示されます。

ステップ 3 [Statistics] タブをクリックします。

[EPG]、[CCR]、および [フロー ログ収集 (Flow Log Collection)] のサブタブが表示されます。

ステップ 4 [フローログの収集 (Flow Log Collection)] をクリックします。

[フローログの収集の設定 (Flow Log Collection Setting)] 情報がダイアログ ボックスの上部に表示され、右上隅に編集アイコンが表示されます。

ステップ 5 [Edit] アイコンをクリックします。

[フロー ログ収集設定] ダイアログ ボックスが表示されます。

ステップ 6 次の [フロー ログ収集設定 (Flow Log Collection Settings)] 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 38: フローログ収集設定ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
ログに記録するトラフィックのタイプ	<p>[ログに記録するトラフィックのタイプ] ドロップダウンリストをクリックし、次のオプションを選択します。</p> <ul style="list-style-type: none"> • デフォルトによるすべてのトラフィック • 許可されたトラフィックのみ • 拒否されたトラフィックのみ
宛先 (Destination)	<p>[接続先 (Destination)] ドロップダウンリストをクリックし、[CloudWatch (デフォルト)] を選択します。</p>
保持	<p>[冗長性 (Retention)] ドロップダウンリストをクリックし、次のオプションを選択します。</p> <ul style="list-style-type: none"> • 1日 • 3日 • 5日 (デフォルト) • 1 カ月 • 13 カ月 • 18 カ月 • 2 カ月 • 3 か月 • 4 カ月 • 5 カ月 • 6 カ月 • 1 週間 • 2 週間 • 1 年 • 10 年 • 2 年 • 5 年

ステップ 7 (オプション) 次のタスクを実行して、フロー フィルタを追加して、送信元と送信先の IP アドレス、ポート、またはプロトコルに関する情報を取得します。

統計フィルターの詳細については、セクション [Cisco Cloud APIC 統計フィルタ \(191 ページ\)](#) を参照してください。

- a) **[フロー フィルタの追加]** ダイアログ ボックスの下部にある **[フロー ログ収集設定 (Flow Log Collection Settings)]** をクリックします。

フィルタ属性のフィールドが表示されます。

[フロー フィルタの追加] ボタンをクリックすると、新しいフィルタが作成されていることがわかります。属性を入力します。

- b) **[ピア IP (Peer IP)]** フィールドで、ピアの IPv4 IP アドレスを入力します。

アドレスは x.x.x.x/x の形式である必要があります。どのネットワークを監視するかをフィルタに指示します。0.0.0.0/0 のアドレスはすべてに一致します。

- c) (オプション) **[プロトコル (Protocol)]** ドロップダウン リストから、プロトコルを選択します。

選択肢は 0 ~ 255 の整数です。255 を入力すると、どのプロトコルにも一致します。よく知られたプロトコルは、テキスト形式が指定されている場合に翻訳されます。

<ul style="list-style-type: none"> • "icmp": 1 • "igmp": 2 • "tcp": 6 • "egp(8) 	<ul style="list-style-type: none"> • "igp": 9 • "l2tp": 115 • "udp": 17 • "icmpv6": 58 	<ul style="list-style-type: none"> • "eigrp": 88 • "ospfigp": 89 • "pim": 103
---	--	--

- d) (オプション) **[ピア ポート]** フィールドに、リッスンするポート番号を入力します。

この番号は、0 ~ 65535 の整数、または既知のポート番号のテキスト入力である必要があります。0 を入力すると、すべてのポートに一致します。よく知られたプロトコルは、テキスト形式が指定されている場合に翻訳されます。

<ul style="list-style-type: none"> • "dns": 53 • "ftpData": 20 • "smtp": 25 	<ul style="list-style-type: none"> • "http": 80 • "https": 443 	<ul style="list-style-type: none"> • "rtsp": 554 • "pop3": 110
--	--	--

- e) (オプション) **[アクティブ]** チェックボックスをオンにして、チェック アイコンをクリックします。

ステップ 8 [保存 (Save)] をクリックします。

REST API を使用した VPC フロー ログの有効化

このセクションでは、REST API を使用して VPC フロー ログを有効にする方法を示します。

ステップ1 ロググループの作成:

```
<cloudAwsLogGroup name="lg1" retention="days-3" status="">
  </cloudAwsLogGroup>
```

ステップ2 フロー ログ ポリシーの作成:

```
<cloudAwsFlowLogPol name="flowLog1" trafficType="ALL" status="">
  <cloudRsToLogGrp tDn="uni/tn-t20/loggrp-lg1" status=""/>
</cloudAwsFlowLogPol>
```

ステップ3 CtxProfile からフロー ログ ポリシーへの関係を作成します。

```
<cloudCtxProfile name="vrfl" status="">
  <cloudRsCtxToFlowLog tnCloudAwsFlowLogPolName="flowLog1" status=""/>
</cloudCtxProfile>
```

クラウドルータ統計

これらの統計は、クラウドルータで利用できます。

- 受信側パケット
- 送信側パケット
- 受信側バイト
- 送信側バイト

Cisco Cloud Application Policy Infrastructure Controller(APIC) は、次の粒度でクラウドルータの統計情報を収集して保存します。

- 15分
- 1時間
- 1ヶ月
- 1年

収集メカニズム

各クラウドルータ インスタンスは、物理インターフェイスおよびトンネル インターフェイスごとに前述の 4-stat 値をキャプチャして保存します。

Cisco Cloud Application Policy Infrastructure Controller(APIC) は、これらの統計についてクラウドルータにクエリを実行し、応答を Cisco Cloud APIC のクラウドルータ統計にマッピングします。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。

RAW 統計情報

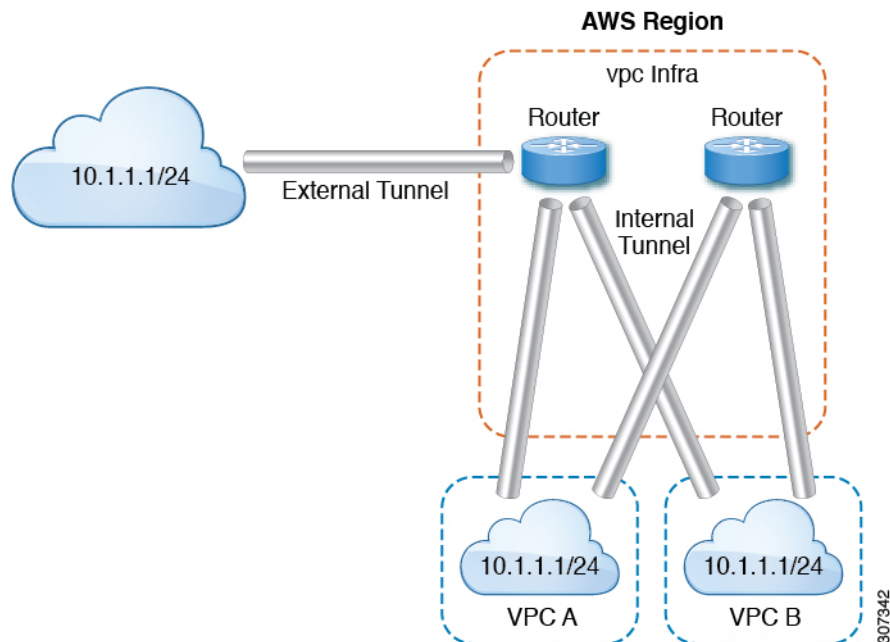
生の統計は 2 Dns の下に保存されます。

- uni/tn-<infraTenant>/ctx-<infraCtx>/region-<infraRegion>/router-<csrname>/to-<ip or user-region>/tunn-<tunnel-id>
- uni/tn-<userTenant>/ctx-<userCtx>/region-<userRegion>/region-<infraRegion>/router-<csrname>/tunn-<tunnel-id>

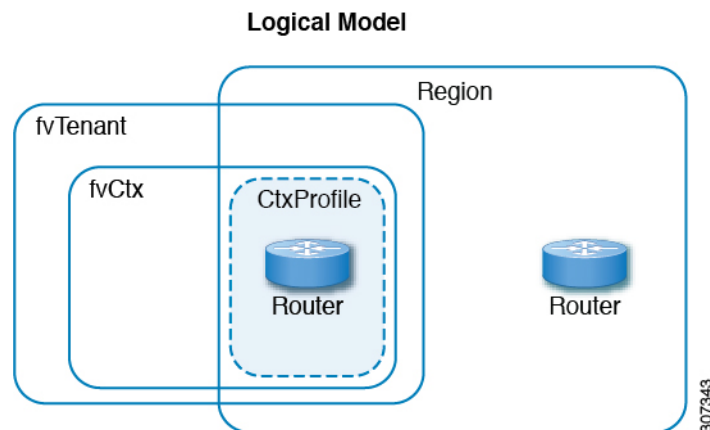


- (注)
- 2 番目の Dn ホルダーは、クラウドルータに接続されているユーザーエンドポイントから見た統計です。したがって、これらの統計は反転されます（CCR の受信側はユーザ領域の送信側になります）。
 - すべてのトンネルに対応するユーザー dn があるわけではありません。これは、内部トンネルにのみ適用されます。外部トンネルの統計は、1 番目の Dn でのみ使用できます。

次の図では、内部トンネルはユーザー VPC とインフラ VPC の間にあります。インフラ VPC には CCR ルータが含まれています。ユーザー VPC には、CCR または VGW ルータを含めることができます。Cisco Cloud APIC はこれらのトンネルを作成します。その結果、インフラ側とユーザー側の両方で統計を利用できます。外部トンネルは、インフラ VPC と外部 IP アドレスの間にあります。統計はインフラ側 (Dn-1) でのみ使用できます。



論理モデル図では、テナントはインフラまたはユーザー テナントです。VRF (または `fvCtx`) をテナント内 (テナントごと) に設定します。VRF は、1つのリージョン内にある場合もあれば、複数のリージョンにまたがる場合もあります。



集計された統計

統計は、DN の各親レベルで集計されます。前述のケースでは、トンネルの統計、統計は宛先 IP、クラウドルータ、リージョン、`vrf (ctx)`、およびテナントに集約されます。

たとえば、インフラクラウドルータからユーザーリージョンへのエグレスパケットを見つきたい場合は、

```
uni/tn-<infraTenant>/ctx-<infraCtx>/region-<infraRegion>/router-<csrname>/to-<ip or user-region>/
```

で利用できます。

ユーザー `region1` と `infra region2` の間のすべてのパケットを取得する場合は、

```
uni/tn-<userTenant>/ctx-<userCtx>/region-<userRegion>/region-<infraRegion>/
```

で使用できます。

また、`cloudCtxProfile` ごとの統計を検索する場合は、

```
uni/tn-<userTenant>/ctx-<userCtx>/region-<userRegion>/ または  
uni/tn-<infraTenant>/ctx-<infraCtx>/region-<infraRegion>/
```

で利用できます。

クラウドルータ GUI 統計

Cisco Cloud APIC GUI では、テナント、VRF、インフラリージョン、およびクラウドコンテキストプロファイルの下で使用可能な統計が表示されます。

Amazon Web Services (AWS) Transit Gateway の統計の場合は、[クラウドコンテキストプロファイル] 作業ペインで、[AWS Transit Gateway] をクリックします。他のすべての統計の場合は、[クラウドコンテキストプロファイル] 作業ペインで、[エンドポイント] をクリックします。



第 8 章

Cisco Cloud APIC セキュリティ

この章は、次の内容で構成されています。

- [アクセス、認証およびアカウントティング \(199 ページ\)](#)
- [TACACS+、RADIUS、LDAP、および SAML アクセスの構成 \(200 ページ\)](#)
- [HTTPS Access の構成 \(209 ページ\)](#)

アクセス、認証およびアカウントティング

Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) ポリシーは、認証、認可、アカウントティング (AAA) 機能を管理します。ユーザ権限、ロール、およびドメインとアクセス権限の継承を組み合わせることにより、管理者は細分化された方法で管理対象オブジェクトレベルで AAA 機能を設定することができます。これらの設定は、REST API または GUI を使用して実行できます。



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

アクセス、認証、およびアカウント構成情報の詳細については、<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> の *Cisco APIC Security Configuration Guide, Release 4.0(1)* をお読みください。

構成

初期構成スクリプトで、管理者アカウントが構成され、管理者はシステム起動時の唯一のユーザとなります。

ローカル ユーザの設定

[Cisco Cloud APIC GUI を使用したローカルユーザーの作成 \(136 ページ\)](#) を参照して、ローカル ユーザーを設定し、Cisco Cloud APIC GUI を使用して OTP、SSH 公開キー、および X.509 ユーザー証明書に関連付けます。

TACACS+、RADIUS、LDAP、および SAML アクセスの構成

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

概要

このトピックでは、RADIUS、TACACS+、LDAP、および SAML ユーザー (ADFS、Okta、PingID など) の Cisco Cloud APIC へのアクセスを有効にする方法について、順を追って説明します。

TACACS+、RADIUS、LDAP、および SAML の詳細については、<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> の『Cisco APIC セキュリティ構成ガイド、リリース 4.0(1)』を参照してください。

Cloud APIC for TACACS+ Access の構成

始める前に

- Cloud Application Policy Infrastructure Controller (Cloud APIC) はオンラインになっています。
- TACACS+ サーバのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cloud APIC 管理エンドポイント グループが使用できます。

ステップ 1 クラウド APIC で、TACACS+ プロバイダーを作成します。

- a) **グローバル作成 (Global Create)** アイコンをクリックします。

[**グローバル作成 (Global Create)**] メニューが表示されます。

- b) [管理] 領域が表示されるまで下にスクロールし、[管理] 領域の下にある [**プロバイダーの作成**] をクリックします。

[**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)**] フィールドで、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) グローバル作成 (Global Create) アイコンをクリックします。
[グローバル作成 (Global Create)] メニューが表示されます。
- b) [グローバル作成 (Global Create)] 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。
[グローバル作成 (Global Create)] メニューに管理オプションのリストが表示されます。
- c) [グローバル作成 (Global Create)] メニューの[管理] を選択し、[ログインドメインの作成 (Create Login Domain)] をクリックします。
[ログインドメインの作成 (Create Login Domains)] ダイアログボックスが表示されます。
- d) 次の [ログインドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから TACACS+ を選択します。
プロバイダ (Providers)	<p>プロバイダーを選択するには：</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. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

- e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

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

Cloud APIC for RADIUS Access の構成

始める前に

- Cloud Application Policy Infrastructure Controller (Cloud APIC) はオンラインになっています。
- RADIUS サーバーのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cloud APIC 管理エンドポイント グループが使用できます。

ステップ 1 Cloud APIC で、**RADIUS プロバイダー**を作成します。

- a) **グローバル作成 (Global Create)** アイコンをクリックします。
[グローバル作成 (Global Create)] メニューが表示されます。
- b) [管理] 領域が表示されるまで下にスクロールし、[管理] 領域の下にある [プロバイダーの作成] をクリックします。
[プロバイダーの作成 (Create Provider)] ダイアログボックスが表示されます。
- c) [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- d) [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- e) [タイプ (Type)] ドロップダウンリストをクリックし、[RADIUS] を選択します。
- f) [設定 (Settings)] セクションで、[キー (Key)]、[ポート (Port)]、[認証プロトコル (Authentication Protocol)]、[タイムアウト (Timeout)]、[再試行 (Retries)]、[管理 EPG (Management EPG)] を指定します。有効化 (Enabled) または 無効化 (Disabled) のいずれかを [サーバー監視 (Server Monitoring)] に対して選択します。

ステップ 2 RADIUS の [ログイン ドメイン]を作成します。

- a) **グローバル作成 (Global Create)** アイコンをクリックします。
[グローバル作成 (Global Create)] メニューが表示されます。
- b) [グローバル作成 (Global Create)] 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。
[グローバル作成 (Global Create)] メニューに管理オプションのリストが表示されます。
- c) [グローバル作成 (Global Create)] メニューの [管理] を選択し、[ログイン ドメインの作成 (Create Login Domain)] をクリックします。
[ログイン ドメインの作成 (Create Login Domains)] ダイアログボックスが表示されます。

- d) 次の [ログインドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから RADIUS を選択します。
プロバイダ (Providers)	<p>プロバイダを選択するには :</p> <ol style="list-style-type: none"> 1. [プロバイダの追加 (Add Providers)] をクリックします。[プロバイダの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

- e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

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

Cloud APIC への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の設定

『Cisco APIC Security Configuration Guide、Release 4.0 (1) 』の「Configuring a Cisco Secure Access Control Server for RADIUS and TACACS + Access to the APIC」の項を </docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で参照してください。

LDAP Access の構成

LDAP 設定には 2 つのオプションがあります。

- Cisco AVPair の設定
- クラウド APIC での LDAP グループ マップの設定

次のセクションには、両方の構成オプションの手順が含まれています。

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

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-security/Cisco-APIC-Security-Configuration-Guide-401.html>にある『*Cisco APIC Security Configuration Guide, Release 4.0(1)*』の「*Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair*」を参照してください。

Cloud APIC for LDAP Access の構成

始める前に

- Cloud Application Policy Infrastructure Controller (Cloud APIC) はオンラインになっています。
- LDAP サーバのホスト名または IP アドレス、ポート、バインド DN、ベース DN、およびパスワードを使用できること。
- Cloud APIC 管理エンドポイント グループが使用できます。

ステップ 1 Cloud APIC で、**LDAP プロバイダー**を作成します。

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

ステップ 2 LDAP の ログイン ドメイン を作成します。

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

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから [LDAP] 選択します。
プロバイダ (Providers)	<p>プロバイダを選択するには：</p> <ol style="list-style-type: none"> 1. [プロバイダの追加 (Add Providers)] をクリックします。[プロバイダの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
認証タイプ	<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。

Cloud APIC for SAML Access の構成

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

SAML について

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』の「About SAML」セクションを参照してください。

SAML の基本要素

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』の「Basic Elements of SAML」セクションを参照してください。

サポートされている IdPs および SAML コンポーネント

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』の「Supported IdPs and SAML Components」セクションを参照してください。

Cloud APIC for SAML Access の構成



(注) SAML ベースの認証は Rest に対するものではなく、Cloud APIC GUI のみに対するものです。

始める前に

- SAML サーバー ホスト名または IP アドレスと、IdP メタデータの URL を使用できます。
- Cloud APIC 管理エンドポイント グループが使用できます。
- 次の設定を行います。
 - 時刻同期と NTP
 - GUI を使用した DNS プロバイダーの構成
 - GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

ステップ 1 Cloud APIC で、SAML プロバイダーを作成します。

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

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

ステップ 2 SAML のログインドメインを作成します。

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

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

[プロパティ (Properties)]	説明
プロバイダ (Providers)	プロバイダーを選択するには : <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. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

d) [保存 (Save)] をクリックして、設定を保存します。

Okta で SAML アプリケーションの設定

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』のセクション「Setting Up a SAML Application」を参照してください。

AD FS で Relying Party Trust の設定

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0 (1)』の「Setting Up a Relying Party Trust in AD FS」セクションを参照してください。

HTTPS Access の構成

ここでは、HTTPS Access を構成する方法について説明します。

HTTPSアクセスについて

この記事は、Cisco ACI を使用する際の HTTPS アクセスのカスタム証明書を設定する方法の例を示します。

詳細については、<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> の『Cisco APIC Security Configuration Guide、Release 4.0(1)』の「HTTPS Access」の項を参照してください。

カスタム証明書の構成のガイドライン

- ワイルドカード証明書 (*.cisco.com など。複数のデバイス間で使用) およびそれに関連する他の場所で生成される秘密キーは、Cisco Cloud APIC ではサポートされません。これは、Cisco Cloud APIC に秘密キーまたはパスワードを入力するためのサポートがないためです。また、ワイルドカード証明書などのいかなる証明書の秘密キーもエクスポートできません。
- 証明書署名要求 (CSR) を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。Cisco Cloud APIC は、送信された証明書が設定された CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
 - 元の CSR にはキーリング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。
 - Cisco Cloud APIC で公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
 - 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキーリングを削除しないでください。キーリングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。
- ポッドあたり 1 つの証明書ベースのルートのみをアクティブにすることができます。
- このリリースでは、クライアント証明書認証はサポートされていません。

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

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

始める前に

注意：ダウンタイムの可能性があるので、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 Cloud APIC のすべての Web サーバの再起動が予期されます。

ステップ 1 メニューバーで、[管理 (Administrative)] > [セキュリティ (Security)] を選択します。

- ステップ 2 [作業 (Work)] ペインで、[証明書認証局 (Certificate Authorities)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [証明書認証局の作成 (Create Certificate Authorities)] を選択します。
- ステップ 3 [証明書認証局の作成 (Create Certificate Authority)] ダイアログボックスの [名前 (Name)] フィールドに、認証局の名前を入力します。
- ステップ 4 [用途 (Used for)] フィールドで [システム (System)] を選択します。
- ステップ 5 [証明書チェーン (Certificate Chain)] フィールドに、クラウドアプリケーション ポリシー インフラストラクチャ コントローラー (APIC) の証明書署名要求 (CSR) に署名する認証局の中間証明書とルート証明書をコピーします。証明書は、Base64 エンコード X.509 (CER) 形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。
- ```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 メニューバーで、[管理 (Administrative)] > [セキュリティ (Security)] を選択します。
- ステップ 8 [作業 (Work)] ペインで、[キー リング (Key Rings)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [キー リングの作成 (Create Key Ring)] を選択します。
- ステップ 9 [キー リングの作成 (Create Key Ring)] ダイアログボックスの [名前 (Name)] フィールドに、認証局の名前を入力し、[説明 (Description)] に説明を入力します。
- ステップ 10 [用途 (Used for)] フィールドで [システム (System)] を選択します。
- ステップ 11 [証明書認証局 (Certificate Authority)] フィールドで、[証明書認証局の選択 (Select Certificate Authority)] をクリックし、以前に作成した認証局を選択します。
- ステップ 12 [秘密キー (Private Key)] フィールドで、[新規キーの生成 (Generate New Key)] または [既存のキーのインポート (Import Existing Key)] を選択します。[既存のキーのインポート (Import Existing Key)] を選択した場合は、[秘密キー (Private Key)] テキスト ボックスに秘密キーを入力します。
- ステップ 13 [モジュラス (Modulus)] ドロップダウンからモジュラスを選択します。メニュー
- ステップ 14 [Certificate] フィールドには、コンテンツを追加しないでください。
- ステップ 15 [保存 (Save)] をクリックします。
- [Work] ペインの [Key Rings] 領域では、作成したキー リングに対する [Admin State] に [Started] と表示されます。
- ステップ 16 作成したキー リングをダブルクリックして、[作業 (Work)] ペインから [キー リング] [key\_ring\_name] ダイアログボックスを開きます。
- ステップ 17 [作業 (Work)] ペインで、[証明書要求の作成 (Create Certificate Request)] をクリックします。
- ステップ 18 [情報カテゴリ (Subject)] フィールドに、Cloud APIC の完全修飾ドメイン名 (FQDN) を入力します。
- ステップ 19 必要に応じて、残りのフィールドに入力します。
- ステップ 20 [保存 (Save)] をクリックします。
- [Key Ring] [key\_ring\_name] ダイアログボックスが表示されます。

- ステップ 21 フィールド [要求 (Request) ] からコンテンツを署名するために **証明書認証局** にコピーします。
- ステップ 22 [キー リング (Key Ring) ] [key\_ring\_name] ダイアログボックスで、[編集 (Edit) ] アイコンをクリックして [キー リング (Key Ring) ] [key\_ring\_name] ダイアログボックスを表示します。
- ステップ 23 [証明書 (Certificate) ] フィールドに、認証局から受信した署名付き証明書を貼り付けます。
- ステップ 24 [保存 (Save) ] をクリックして、[キー リング (Key Rings) ] 作業ウィンドウに戻ります。
- キーが確認されて [作業 (Work) ] ペインで [管理状態 (Admin State) ] が [完了済み (Completed) ] に変わり、HTTP ポリシーを使用できるようになります。
- ステップ 25 [インフラストラクチャ (Infrastructure) ] > [システム構成 (System Configuration) ] に移動し、[管理アクセス (Management Access) ] タブをクリックします。
- ステップ 26 [HTTPS] 作業ウィンドウの編集アイコンをクリックして、[HTTPS 設定 (HTTPS Settings) ] ダイアログボックスを表示します。
- ステップ 27 [管理キー リング (Admin Key Ring) ] をクリックし、以前に作成したキー リングを関連付けます。
- ステップ 28 [保存 (Save) ] をクリックします。
- すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキー リングが HTTPS アクセスに関連付けられています。

---

### 次のタスク

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキーリング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じ CSR を再送信する必要があります。キーリングを削除すると、Cloud APIC に内部的に保存されている秘密キーも削除されるため、新しいキーリングの削除または作成は行わないでください。



## 第 9 章

# 設定のばらつき

- 構成のばらつき通知と障害 (213 ページ)
- 構成ドリフトのメインページにアクセスする (215 ページ)
- 欠落しているコントラクト構成の確認 (217 ページ)
- 欠落している EPG 構成の確認 (219 ページ)
- 欠落している VRF 構成の確認 (221 ページ)
- 構成のばらつきのトラブルシューティング (223 ページ)

## 構成のばらつき通知と障害

パブリッククラウドに Cisco ACI を展開する場合、Cloud APIC からほとんどのファブリック構成を実行します。ただし、お客様または別のクラウド管理者が、AWS または Azure が提供するツールを使用して、クラウドプロバイダーの GUI で展開された構成を直接変更する場合があります。このような場合、Cloud APIC から展開した意図した構成とクラウドサイトの実際の構成が同期しなくなる可能性があります。これを構成のばらつきと呼びます。

リリース 5.0(2) 以降、Cloud APIC は、Cloud APIC から展開したものとクラウドサイトで実際に構成されたものとの間のセキュリティポリシー（コントラクト）構成の不一致を可視化します。



- (注)
- リリース 25.0(1) 以降、コントラクトに加えて、EPG および VRF の構成ドリフト情報を使用できます。
  - リリース 25.0(4) 以降では、レイヤ 4～レイヤ 7 のサービス グラフが添付されているかどうかに関わらず、コントラクト ドリフト情報が使用可能になりました。

詳細については、「[リリース 25.0\(4\) の更新 \(214 ページ\)](#)」を参照してください。

構成のばらつきの分析には 2 つの側面があります。

- Cloud APIC で構成され、クラウドファブリックにデプロイされる予定のすべてのファブリック要素が適切に展開されましたか?

このシナリオは、クラウドに展開できなかった Cloud APIC のユーザー構成エラー、クラウドプロバイダー側の接続または API の問題、またはクラウド管理者がクラウドプロバイダーの UI で直接セキュリティルールを手動で削除または変更した場合に発生する可能性があります。意図されていても欠落している構成は、Cloud APIC ファブリックに問題を引き起こす可能性があります。

- クラウドに存在するが、Cloud APIC から展開することを意図していない追加の構成はありますか？

前のシナリオと同様に、これは、接続または API の問題がある場合、またはクラウド管理者がクラウドプロバイダーの UI で直接追加のセキュリティルールを手動で作成した場合に発生する可能性があります。既存の、意図されていない構成では、問題が発生する可能性があります。

### リリース 25.0(4) の更新

リリース 25.0(1) 以降、コントラクトに加えて、EPG および VRF の構成ドリフト情報を使用できます。

リリース 25.0(4) 以降、構成ドリフトに対して次の変更が加えられました。

- 構成ドリフトがデフォルトで有効になりました。
- リリース 25.0(4) 以前では、構成ドラフト情報は、レイヤ 4～レイヤ 7 のサービス グラフが添付されたコントラクトは使用できませんでした。リリース 25.0(4) 以降では、レイヤ 4～レイヤ 7 のサービス グラフが添付されているかどうかに関わらず、コントラクトドリフト情報が使用可能になりました。詳細については、「[レイヤ 4 からレイヤ 7 サービスの展開 \(169 ページ\)](#)」を参照してください。
- 構成ドリフト情報は、[クラウド リソース (Cloud Resources)] > [ドリフト (Drifts)] にある 1 つのページに統合されました。

| Object                                                                                                                                                                                          | Status    | Drift Type   | Last Configuration Update     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------|-------------------------------|
| /subscriptions/630daf13-e0e6-40bf-b7e-17844309af73/resourceGroups/CAPIC_int_vr1_eastus/providers/Microsoft.Network/networkSecurityGroups/ALB2-subnet/securityRules/AzureInfraBackendHealthPorts | Unmanaged | Extra Object | Jul 08 2022 01:43:56am -07:00 |
| /subscriptions/630daf13-e0e6-40bf-b7e-17844309af73/resourceGroups/CAPIC_int_vr1_eastus/providers/Microsoft.Network/networkSecurityGroups/ALB2-subnet/securityRules/AzureLoadBalancer            | Unmanaged | Extra Object | Jul 08 2022 01:32:32am -07:00 |
| /subscriptions/630daf13-e0e6-40bf-b7e-17844309af73/resourceGroups/CAPIC_int_vr1_eastus/providers/Microsoft.Network/networkSecurityGroups/vr1-east-VM1-nsg/securityRules/SSH                     | Unmanaged | Extra Object | Jul 08 2022 01:32:32am -07:00 |

詳細については、「[構成ドリフトのメインページにアクセスする \(215 ページ\)](#)」を参照してください。



## 構成ドリフトのメインページにアクセスする

リリース 25.0(4)以降、構成ドリフト情報が単一の[ドリフト (Drifts)]ページに統合されるようになりました。

[ドリフト (Drifts)]ページは、次の情報を提供するために使用されます。

- 何か削除されたかどうかを確認するには
- 存在する必要があるものが正しく表示されていることを確認するには

**ステップ 1** Cloud APIC GUI にログインします。

**ステップ 2** 次の順に構成ドリフトのメインページに移動します。

[クラウドリソース (Cloud Resources)] > [ドリフト (Drifts)]

統合された[ドリフト (Drifts)]ページが表示されます。

| Detection Summary |                     |                               |  |
|-------------------|---------------------|-------------------------------|--|
| Unmanaged Objects | Objects with Drifts | Last Drift Check              |  |
| 32                | 0                   | Jul 08 2022 08:37:26am -07:00 |  |

| Object                                                                                                                                                                                           | Status    | Drift Type   | Last Configuration Update     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------|-------------------------------|
| /subscriptions/630daf13-e0e6-40bf-b87e-17844309af73/resourceGroups/CAPIC_int_vr1_eastus/providers/Microsoft.Network/networkSecurityGroups/ALB2-subnet/securityRules/AzureInfraBackendHealthPorts | Unmanaged | Extra Object | Jul 08 2022 01:43:56am -07:00 |
| /subscriptions/630daf13-e0e6-40bf-b87e-17844309af73/resourceGroups/CAPIC_int_vr1_eastus/providers/Microsoft.Network/networkSecurityGroups/ALB2-subnet/securityRules/AzureLoadBalancer            | Unmanaged | Extra Object | Jul 08 2022 01:43:56am -07:00 |
| /subscriptions/630daf13-e0e6-40bf-b87e-17844309af73/resourceGroups/CAPIC_int_vr1_eastus/providers/Microsoft.Network/networkSecurityGroups/vr1-east-VM1-rsg/securityRules/SSH                     | Unmanaged | Extra Object | Jul 08 2022 01:32:32am -07:00 |
| /subscriptions/630daf13-e0e6-40bf-b87e-17844309af73/resourceGroups/CAPIC_int_vr1_eastus/providers/Microsoft.Network/networkSecurityGroups/vr1-east-VM1-rsg/securityRules/SSH                     | Unmanaged | Extra Object | Jul 08 2022 01:32:32am -07:00 |

[ドリフト (Drifts)]ページでは、ファブリック内の構成の問題の概要を確認できます。

[検出の概要 (Detection Summary)]のエリアには、管理対象または管理対象外のオブジェクトとして検出された構成ドリフトの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある[更新]アイコンをクリックして情報を更新できます。

**ステップ 3** [検出の概要 (Detection Summary)]エリア下の表の情報を使用して、構成のドリフトを見つけます。

- **オブジェクト**：構成ドリフトに関連するオブジェクトに関する情報を提供します。
- **ステータス**：[ステータス (Status)]列に表示される可能性のあるさまざまな値を次に示します。
  - **Transient (低)**：最近の構成変更が原因である可能性が高いドリフト。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。

- **Presumed (中)** : 一時的である場合とそうでない場合があるドリフト。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。
  - **Raised (高)** : クリティカルなドリフト。Cloud APIC の構成を確認し、関連する障害を確認することをお勧めします。構成を再デプロイすると、Cloud APIC とクラウドサービス間の通信の問題を解決できる場合があります。問題が解決しない場合は、テクニカルサポートログを確認してください。
  - **Unmanaged** : Cisco Cloud APIC を介して作成されていない追加のインベントリ オブジェクトに関連する構成のドリフト。
- **ドリフト タイプ** : 以下は、[ドリフト タイプ (Drift Type) ]列に表示される可能性のあるさまざまな値です。
- **Configuration** : 意図した構成と実際の構成が同期しなくなる可能性がある、クラウドプロバイダー サイトの外部変更。EPG または VRF に関連する構成ドリフトに使用されます。
  - **Rule** : 意図したセキュリティ ルールと、コントラクトを通じて確立された予期されるルールとが同期しなくなる可能性がある、クラウドプロバイダー サイトの外部変更。コントラクトに関連する構成ドリフトに使用されます。
  - **Extra Object** : Cisco Cloud APIC を介して作成されなかった追加のインベントリ オブジェクトを表示するために使用されます。Cisco Cloud APIC は、これらのオブジェクトでドリフト検出を実行しません。
- **Last Configuration Update** : 最後に構成が更新された日時に関する情報を提供します。

**ステップ 4** 必要に応じて、フィルタ行に情報を入力して、表に示されている構成ドリフトをフィルタリングします。

- a) **[検出の概要 (Detection Summary) ]**エリアの下にあるフィルタ行をクリックします。次のフィルタタイプが表示されます。
- オブジェクト
  - ステータス
  - Drift Type
  - Last Configuration Update
  - 親パス

フィルタに適したタイプを選択します。

- b) 必要な演算子をクリックします。

次のオプションがあります。

- == : 等号演算子
- != : 不等号演算子

- c) 必要なドリフト タイプをクリックします。

オプションは、Extra Object、Rule、および Configuration です。詳細については、上記の **ドリフトタイプ** フィールドの説明を参照してください。

テーブルのエントリは、上記の選択に基づいてフィルタリングされます。

**ステップ 5** 必要に応じて、特定の構成ドリフトに関する追加情報を表示します。

このページにリストされているオブジェクトについては、**[構成ドリフト (Configuration Drifts)]** テーブルの該当する行をクリックして、追加の構成ドリフト情報を表示できます。サイドパネルにこの特定の構成ドリフトに関する情報がさらに表示されます。**[詳細 (Details)]** アイコン (🔍) をクリックすると、この特定のオブジェクト向けの適切な **[クラウド マッピング (Cloud Mapping)]** ページが自動で表示されます。

特定のオブジェクトに関する追加の構成ドリフト情報については、次のセクションを参照してください。

- [欠落しているコントラクト構成の確認 \(217 ページ\)](#)
- [欠落している EPG 構成の確認 \(219 ページ\)](#)
- [欠落している VRF 構成の確認 \(221 ページ\)](#)

---

## 欠落しているコントラクト構成の確認

このセクションでは、Cloud APIC から構成したが、クラウドファブリックに適切にデプロイされていないコントラクト設定を確認する方法について説明します。

**ステップ 1** Cloud APIC GUI にログインします。

**ステップ 2** **[アプリケーション管理 (Application Management)]** > **[コントラクト (Contracts)]** をクリックします。

**ステップ 3** 適切なコントラクトをダブルクリックして、そのコントラクトの **[概要 (Overview)]** ページを表示します。

**ステップ 4** 該当する場合は、**[サービス グラフ (Service Graph)]** エリアに表示されるサービス グラフ情報に注意してください。

リリース 25.0(4) 以前では、構成ドラフト情報は、レイヤ 4 ~ レイヤ 7 のサービス グラフが添付されたコントラクトは使用できませんでした。リリース 25.0(4) 以降では、レイヤ 4 ~ レイヤ 7 のサービス グラフが添付されているかどうかに関わらず、コントラクトドリフト情報が使用可能になりました。詳細については、「[レイヤ 4 から レイヤ 7 サービスの展開 \(169 ページ\)](#)」を参照してください。

**ステップ 5** **[クラウド マッピング (Cloud Mapping)]** タブをクリックします。

クラウド マッピング ビューには、コントラクトとそれが使用するクラウドリソースに関するすべての情報が表示されます。

The screenshot displays the 'Contract NFA\_contract' interface. At the top, there are navigation tabs: Overview, Topology, Cloud Resources, Application Management, Cloud Mapping (selected), and Event Analytics. A notification banner states 'Detection of configuration drifts is still in beta.' Below this, the 'Detection Summary' section provides a high-level overview: Configuration Drift Status (0 Drifts Found), Configured Cloud Resources (87), Expected Cloud Resources (87), and Last Drift Check (Jul 08 2022 08:37:26am -07:00). The 'Related Objects' section lists 1 Consumer EPG, 1 Provider EPG, and 1 Filter. The 'Configuration Drifts' section is a table with columns for Status, Type, Protocol, From Port, To Port, Source, Destination, Network Security Group, NSG Cloud Provider ID, Consumer EPGs, Provider EPGs, Drift Type, Description, and Recommendation. It currently shows 'No rows found'.

(注) [クラウドリソース (Cloud Resources)] > [ドリフト (Drifts)] の順にクリックしてこのページに移動することも可能で、その後 [構成ドリフト (Configuration Drifts)] の表で適切な行をクリックします。サイドパネルにこの特定の構成ドリフトに関する情報がさらに表示されます。[詳細 (Details)] アイコン (🔍) をクリックすると、この特定のオブジェクト向けの適切な [クラウドマッピング (Cloud Mapping)] ページが自動で表示されます。詳細については、「[構成ドリフトのメインページにアクセスする \(215 ページ\)](#)」を参照してください。

画面は、[検出の概要 (Detection Summary)]、[関連オブジェクト (Related Objects)]、[構成ドリフト (Configuration Drifts)] および [提示されたクラウドリソース (Presented Cloud Resources)] の4つのセクションに分かれています。各セクションには、選択したコントラクトに関するそれぞれの情報をリストした表が含まれています。

- [検出の概要 (Detection Summary)] の表には、検出された構成ドリフトの数、構成された意図された実際のクラウドリソースの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある [更新] アイコンをクリックして情報を更新できます。
- [関連オブジェクト (Related Objects)] エリアには、コントラクトに関連するその他のオブジェクト (コンシューマーやプロバイダーの EPG、フィルタなど) が表示されます。
- 構成のばらつきテーブルには、コントラクトルールに関するすべての問題が一覧表示されます。具体的には、展開することを意図していたが、実際のファブリック構成に欠落しているすべてのコントラクトルール。

この表には、使用されるプロトコル、ポート範囲、送信元と宛先の IP またはグループ、コンシューマーとプロバイダーの EPG、問題の説明、問題を解決するための推奨アクションなどの詳細情報が含まれています。構成ののばらつきごとに、[ステータス] フィールドに重大度と推奨されるアクションが示されます。

- **Transient (低)** : 最近の構成変更が原因である可能性が高いドリフト。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。

- Presumed（中）：一時的である場合とそうでない場合があるドリフト。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。
  - Raised（高）：クリティカルなドリフト。Cloud APIC の構成を確認し、関連する障害を確認することをお勧めします。構成を再デプロイすると、Cloud APIC とクラウドサービス間の通信の問題を解決できる場合があります。問題が解決しない場合は、テクニカルサポートログを確認してください。
- [提示されたクラウド リソース（Presented Cloud Resources）] の表には、クラウドで適切に構成されたすべてのリソースに関する情報が表示されます。この表は、特定のコントラクトのためにクラウドで構成されているルールをよりよく把握できるように設計されています。

## 欠落している EPG 構成の確認

このセクションでは、Cloud APIC から構成したが、クラウドファブリックに適切に展開されていない EPG 設定を確認する方法について説明します。

**ステップ 1** Cloud APIC GUI にログインします。

**ステップ 2** [アプリケーション管理（Application Management）] > [EPG] をクリックします。

**ステップ 3** 適切な EPG をダブルクリックして、その EPG の [概要（Overview）] ページを表示します。

**ステップ 4** [クラウドマッピング（Cloud Mapping）] タブをクリックします。

[クラウドマッピング（Cloud Mapping）] ビューには、EPG とそれが使用するクラウドリソースに関するすべての情報が表示されます。

The screenshot shows the Cisco Cloud APIC GUI for EPG vrf1-epg1. The 'Cloud Mapping' tab is active. A notification states 'Detection of configuration drifts is still in beta.' Below this, a 'Detection Summary' table shows 0 drifts found, 2 configured cloud resources, and 2 expected cloud resources. The last drift check was on Jul 08, 2022 at 08:46:00am -07:00. The 'Related Objects' section shows 2 application security groups, 2 network security groups, 2 provider contracts, and 0 consumer contracts. The 'Configuration Drifts' section has a filter for attributes and a table with columns: Status, Logical DN, Cloud Provider ID, Drift Type, Description, and Recommendation. The table currently shows 'No rows found'. At the bottom, there is a 'Presented Cloud Resources' section.

- (注) [クラウドリソース (Cloud Resources)] > [ドリフト (Drifts)] の順にクリックしてこのページに移動することも可能で、その後 [構成ドリフト (Configuration Drifts)] の表で適切な行をクリックします。サイドパネルにこの特定の構成ドリフトに関する情報がさらに表示されます。[詳細 (Details)] アイコン (🔍) をクリックすると、この特定のオブジェクト向けの適切な [クラウドマッピング (Cloud Mapping)] ページが自動で表示されます。詳細については、「[構成ドリフトのメインページにアクセスする \(215 ページ\)](#)」を参照してください。

画面は、[検出の概要 (Detection Summary)]、[関連オブジェクト (Related Objects)]、[構成ドリフト (Configuration Drifts)] および [提示されたクラウドリソース (Presented Cloud Resources)] の4つのセクションに分かれています。各セクションには、選択した EPG に関するそれぞれの情報をリストした表が含まれています。

- [検出の概要 (Detection Summary)] の表には、検出された構成ドリフトの数、構成された意図された実際のクラウドリソースの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある [更新] アイコンをクリックして情報を更新できます。
- [関連オブジェクト (Related Objects)] エリアには、セキュリティグループ、コントラクトなど、EPG に関連するその他のオブジェクトが表示されます。
- [構成ドリフト (Configuration Drifts)] テーブルには、EPG に関連付けられたセキュリティグループに関するすべての問題が一覧表示されます。具体的には、展開することを意図していたが、実際のファブリック構成に欠落しているすべてのセキュリティグループ。

この表には、論理 DN、クラウドプロバイダー ID、ドリフトタイプ、問題の説明、問題を解決するための推奨アクションなどの詳細情報が含まれています。構成ののばらつきごとに、[ステータス] フィールドに重大度と推奨されるアクションが示されます。

- **Transient (低)** : 最近の構成変更が原因である可能性が高いドリフト。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。
  - **Presumed (中)** : 一時的である場合とそうでない場合があるドリフト。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。
  - **Raised (高)** : クリティカルなドリフト。Cloud APIC の構成を確認し、関連する障害を確認することをお勧めします。構成を再デプロイすると、Cloud APIC とクラウドサービス間の通信の問題を解決できる場合があります。問題が解決しない場合は、テクニカルサポートログを確認してください。
- [提示されたクラウドリソース (Presented Cloud Resources)] の表には、クラウドで適切に構成されたすべてのリソースに関する情報が表示されます。このテーブルは、クラウド内の特定の EPG に関連付けられているセキュリティグループをより適切に可視化できるように設計されています。

## 欠落している VRF 構成の確認

このセクションでは、Cloud APIC から構成したが、クラウドファブリックに適切にデプロイされていない VRF 設定を確認する方法について説明します。

ステップ 1 Cloud APIC GUI にログインします。

ステップ 2 [アプリケーション管理 (Application Management)] > [VRF] をクリックします。

ステップ 3 適切な VRF をダブルクリックして、その VRF の [概要 (Overview)] ページを表示します。

ステップ 4 [クラウドマッピング (Cloud Mapping)] タブをクリックします。

[クラウドマッピング (Cloud Mapping)] ビューには、VRF とそれが使用するクラウドリソースに関するすべての情報が表示されます。

The screenshot shows the Cloud APIC GUI for VRF vrf1. The 'Cloud Mapping' tab is active. A notification at the top states 'Detection of configuration drifts is still in beta.' Below this is a 'Detection Summary' section with a table:

| Configuration Drift Status | Configured Cloud Resources | Expected Cloud Resources | Last Drift Check              |
|----------------------------|----------------------------|--------------------------|-------------------------------|
| 0 Drifts Found             | 13                         | 13                       | Jul 08 2022 08:46:00am -07:00 |

Below the summary is a 'Related Objects' section with a table:

| Application Security Group | Network Security Groups | CIDRs | Subnets |
|----------------------------|-------------------------|-------|---------|
| 8                          | 7                       | 4     | 7       |

At the bottom is a 'Configuration Drifts' section with a table that currently shows 'No rows found'.

(注) [クラウドリソース (Cloud Resources)] > [ドリフト (Drifts)] の順にクリックしてこのページに移動することも可能で、その後 [構成ドリフト (Configuration Drifts)] の表で適切な行をクリックします。サイドパネルにこの特定の構成ドリフトに関する情報がさらに表示されます。[詳細 (Details)] アイコン (🔍) をクリックすると、この特定のオブジェクト向けの適切な [クラウドマッピング (Cloud Mapping)] ページが自動で表示されます。詳細については、「[構成ドリフトのメインページにアクセスする \(215 ページ\)](#)」を参照してください。

画面は、[検出の概要 (Detection Summary)]、[関連オブジェクト (Related Objects)]、[構成ドリフト (Configuration Drifts)] および [提示されたクラウドリソース (Presented Cloud Resources)] の 4 つのセクションに分かれています。各セクションには、選択した VRF に関するそれぞれの情報をリストした表が含まれています。

- [検出の概要 (Detection Summary)] の表には、検出された構成ドリフトの数、構成された意図された実際のクラウドリソースの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある [更新] アイコンをクリックして情報を更新できます。

- **[関連オブジェクト (Related Objects)]** 領域には、セキュリティグループ、CIDR、サブネットなど、VRF に関連するその他のオブジェクトが表示されます。
- **[構成ドリフト (Configuration Drifts)]** の表には、仮想ネットワーク、仮想ネットワークに関連付けられている CIDR、およびそれらの CIDR 内のサブネットに関するすべての問題が一覧表示されます。具体的には、展開することを意図していたが、実際のファブリック構成に欠落しているすべての仮想ネットワーク、CIDR およびサブネット。

いずれかのレベルで構成ドリフトがある場合、表にはそのレベルでの構成ドリフトが表示され、それより下のレベルでの構成ドリフトは表示されないことに注意してください。たとえば、構成ドリフトが CIDR レベルで発生し、その CIDR 内の対応するサブネットの場合、テーブルには CIDR エリアの構成ドリフトが表示されますが、その CIDR 内の対応するサブネットの構成ドリフトは表示されません。

この表には、次のエリアの詳細情報が含まれています。

- **仮想ネットワーク**：論理 DN、リージョン、プライマリ CIDR、ドリフトタイプ、問題の説明、およびそれを解決するための推奨されるアクションに関する情報を提供します。
- **CIDR**：論理 DN、リージョン、CIDR ブロック範囲、プライマリ CIDR かどうか、CIDR 内のサブネット、ドリフトタイプ、問題の説明、およびそれを解決するための推奨されるアクションに関する情報を提供します。
- **サブネット**：論理 DN、リージョン、IP アドレス、ドリフトタイプ、問題の説明、およびそれを解決するための推奨されるアクションに関する情報を提供します。

構成ののばらつきごとに、[ステータス] フィールドに重大度と推奨されるアクションが示されます。

- **Transient (低)**：最近の構成変更が原因である可能性が高いドリフト。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。
  - **Presumed (中)**：一時的である場合とそうでない場合があるドリフト。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。
  - **Raised (高)**：クリティカルなドリフト。Cloud APIC の構成を確認し、関連する障害を確認することをお勧めします。構成を再デプロイすると、Cloud APIC とクラウドサービス間の通信の問題を解決できる場合があります。問題が解決しない場合は、テクニカルサポートログを確認してください。
- **[提示されたクラウド リソース (Presented Cloud Resources)]** の表には、クラウドで適切に構成されたすべてのリソースに関する情報が表示され、**[構成ドリフト (Configuration Drifts)]** の表（仮想ネットワーク、CIDR、およびサブネット）に表示されるのと同じ階層に分割されます。このテーブルは、クラウド内の特定の VRF に関連付けられている仮想ネットワーク、CIDR、およびサブネットをより適切に可視化できるように設計されています。



## 構成のばらつきのトラブルシューティング

このセクションでは、構成のばらつきプロセスが Cloud APIC で稼働していることを確認し、アプリケーション ログを確認し、必要に応じてテクニカル サポート情報を生成するためのいくつかの便利なコマンドを提供します。

**ステップ 1** root ユーザーとしてコンソール経由で Cisco Cloud APIC にログインします。

**ステップ 2** 構成のばらつきアプリケーションのステータスを確認します。

```
ACI-Cloud-Fabric-1# moquery -d pluginContr/plugin-Cisco_CApicDrift | egrep "dn |pluginSt |operSt |version"
dn: pluginContr/plugin-Cisco_CApicDrift
operSt: active
pluginSt: active
Verison: 5.1.0
```

**ステップ 3** アプリケーション コンテナのステータスを確認します。

```
ACI-Cloud-Fabric-1# docker ps | grep drift
CONTAINER ID IMAGE COMMAND CREATED STATUS
NAMES
649af6feb72c a5ea08bbf541 "/opt/bin/conit.bi..." 13 hours ago Up 13
hours drift-api-b703e569-0aa6-859f-c538-a5fecbc5708f
```

**ステップ 4** すべての Docker コンテナによって消費されるメモリを確認します。

消費されるメモリの合計量は 12GB 未満である必要があります。

```
ACI-Cloud-Fabric-1# systemctl status ifc-scheduler_allocations.slice | grep Memory
```

**ステップ 5** 必要に応じて、テクニカル サポート ログを収集します。

ログは、コントローラの /data/techsupport ディレクトリに保存されます。

```
ACI-Cloud-Fabric-1# trigger techsupport controllers application CApicDrift
ACI-Cloud-Fabric-1# trigger techsupport controllers application CApicDrift vendorName Cisco
```

**ステップ 6** アプリケーション ログを確認します。

構成のばらつきプロセスのログは、/data2/logs/Cisco\_CApicDrift ディレクトリに保存されます。

runhist.log ファイルには、アプリケーションが開始されるたびに情報が記録されます。次に例を示します。

```
cat runhist.log
1 - Thu Jun 11 23:55:59 UTC 2020
2 - Fri Jun 12 01:19:41 UTC 2020
```

drift.log ファイルはアプリケーション ログ ファイルであり、構成ドリフトが更新された回数と各更新にかかった時間を表示するために使用できます。

```
cat drift.log | grep ITER
{"file": "online_snapshot.go:178", "func": "Wait", "level": "info", "msg": "ITER# 109
```

```
ENDED === RDFGEN TIME: 1m40.383751649s, MODEL UPLOAD TIME 5m54.245550374s;
TOTAL TIME:: 7m34.629447083s, "time":"2020-06-12T19:53:13Z"}
```

---



## 第 10 章

# Cisco Cloud APIC の AWS Transit Gateway

- [Cisco Cloud APIC の AWS Transit Gateway \(225 ページ\)](#)

## Cisco Cloud APIC の AWS Transit Gateway

Cisco Cloud Application Policy Infrastructure Controller (APIC) リリース 5.0(1) 以降、Cisco Cloud APIC で Amazon Web Services (AWS) Transit Gateway を使用できます。AWS Transit Gateway は、仮想プライベートクラウド (VPC) 間の接続を自動化する内部ルーターとして機能するサービスです。VPC は、クラウドサイトのさまざまな AWS リージョンに配置できます。

仮想プライベートクラウド (VPC) は、追加の構成を行わないと相互に通信できません。AWS Transit Gateway を使用せずに、VPC ピアリングを設定することで VPC 間通信を設定できます。または、VPN トンネルと CCR を使用できます。

ただし、Cisco Cloud APIC で AWS Transit Gateway を使用すると、VPC または VRF を同じ AWS Transit Gateway に関連付けるだけで、クラウドサイトの VPC または VRF を接続できます。

Cisco Cloud APIC で AWS Transit Gateway を使用すると、パフォーマンスの向上、シンプルさ、スケーラビリティ、潜在的なコスト削減など、いくつかの利点が得られます。



- (注) Cisco Cloud APIC ユーザー テナントの VPC (CtxProfile) を AWS Transit Gateway (ハブ ネットワーク) にアタッチできるのは、管理者権限があり、ユーザーがセキュリティドメイン「all」の一部である場合のみです。このようなアクセスがないと、ユーザー テナントの VPC を AWS Transit Gateway にアタッチできません。

Cisco Cloud APIC で AWS Transit Gateway の使用の詳細については、「[AWS トランジットゲートウェイまたは AWS トランジットゲートウェイ コネクトを使用した VPC 間の帯域幅の増加](#)」を参照してください。





## 付録 **A**

# Cisco Cloud APIC エラーコード

- [Cisco Cloud APIC エラーコード \(227 ページ\)](#)

## Cisco Cloud APIC エラーコード

ここでは、Cisco Cloud APIC のエラー コードについて説明します。

表 39: Cisco Cloud APIC エラーコード

| コンポーネント        | エラー コード (Error Code)                        | 制約                                                                   |
|----------------|---------------------------------------------|----------------------------------------------------------------------|
| cloud-template | CT_INFRANETWORK_COUNT                       | cloudtemplateInfraNetwork MO の数はほぼ 1 です                              |
| cloud-template | CT_INFRANETWORK_COUNT                       | cloudtemplateInfraNetwork MO の数はほぼ 1 です                              |
| cloud-template | CT_INFRANETWORK_VRF                         | cloudtemplateInfraNetwork MOでは、vrfName を overlay-1 にする必要があります。       |
| cloud-template | CT_INFRANETWORK_PARENT                      | cloudtemplateInfraNetworkMO の場合、親 MO は uni/tn-infra である必要があります。      |
| cloud-template | CT_INFRANETWORK_NUMROUTERSPERREGION_MINIMUM | cloudtemplateInfraNetwork MO では、属性 numRoutersPerRegion の最小許容値は 2 です。 |
| cloud-template | CT_INFRANETWORK_NUMROUTERSPERREGION_MAXIMUM | cloudtemplateInfraNetwork MO では、属性 numRoutersPerRegion の最大許容値は 4 です。 |

| コンポーネント        | エラーコード (Error Code)                             | 制約                                                                                                 |
|----------------|-------------------------------------------------|----------------------------------------------------------------------------------------------------|
| cloud-template | CT_INFRANETWORK_NUMREMOTESITESUBNETPOOL_MINIMUM | cloudtemplateInfraNetwork MO では、属性 numRemoteSiteSubnetPool の最小許容値は 2 です。                           |
| cloud-template | CT_INFRANETWORK_NUMREMOTESITESUBNETPOOL_MAXIMUM | cloudtemplateInfraNetwork MO では、属性 numRemoteSiteSubnetPool の最大許容値は 2 です。                           |
| cloud-template | CT_INTNETWORK_COUNT                             | cloudtemplateIntNetwork MO の数は最大 1 です                                                              |
| cloud-template | CT_EXTNETWORK_COUNT                             | cloudtemplateIntNetwork MO の数は最大 1 です                                                              |
| cloud-template | CT_VPNNETWORK_COUNT                             | cloudtemplateVpnNetwork MO の数は最大 1 です                                                              |
| cloud-template | CT_OSPF_COUNT                                   | cloudtemplateIntNetwork MO の数は最大 1 です                                                              |
| cloud-template | CT_INTNETWORK_REGION_MATCH                      | cloudtemplateIntNetwork で cloudRegionName に よって指定されたリージョンには、cloudProvP で対応する cloudRegion が必要です。    |
| cloud-template | CT_INTNETWORK_REGION_MANAGED                    | cloudtemplateIntNetwork の cloudRegionName の子によって指定されたリージョンには、adminSt が管理対象の対応する cloudRegion が必要です。 |
| cloud-template | CT_INTNETWORK_REGION_MAXIMUM                    | cloudtemplateIntNetwork で指定されるリージョンの最大数 (cloudRegionName) は 4 です                                   |

| コンポーネント        | エラーコード (Error Code)                      | 制約                                                                                                                          |
|----------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| cloud-template | CT_EXTNETWORK_REGION_SUBSET              | cloudtemplateExtNetwork の cloudRegionName の子によって指定されたリージョンは、cloudtemplateIntNetwork の下の cloudRegionName の子によっても指定する必要があります。 |
| cloud-template | CT_EXTSUBNETPOOL_COUNT                   | cloudtemplateIntNetwork MO の数は最大 1 です                                                                                       |
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_ADDRESS      | cloudtemplateExtSubnetPool では、サブネットプールにネットワークアドレスが含まれている必要があります                                                             |
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_IP_VERSION   | cloudtemplateExtSubnetPool では、サブネットプールに IPv4 アドレスが含まれている必要があります                                                             |
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_ADDRESS_TYPE | cloudtemplateExtSubnetPool では、サブネットプールの IP アドレスはマルチキャストまたはループバックアドレス空間からのものであってはなりません                                       |
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_MINIMUM_SIZE | cloudtemplateExtSubnetPool では、サブネット プールは /22 以上である必要があります (ネットマスクは 22 以下である必要があります)。                                        |

| コンポーネント        | エラーコード (Error Code)                  | 制約                                                                                                                                                                                                                                  |
|----------------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cloud-template | CT_INTNETWORK_MISSING_HOME           | cloudtemplateIntNetworkの下にcloudRegionNameがある場合は、cloudRegionNameの1つをcAPICのホームリージョン (capicDeployed) に関連付ける必要があります。                                                                                                                    |
| cloud-template | CT_CLOUD_APICSUBNETPOOL_INSUFFICIENT | cloudApicSubnetPool MOは、cloudApicSubnet MOを生成するために十分な数である必要があります。これにより、cloudtemplateIntNetworkで指定されたすべてのcloudRegionName MOを一意的にcloudApicSubnet MOに関連付けることができます。cloudApicSubnet MOからのサブネットは、対応するリージョンのcloudCtxProfileでCIDRとして使用されます。 |
| cloud-template | CT_IPSECTUNNEL_PEERADDR_IP_VERSION   | cloudtemplateIpSecTunnelでは、peeraddrにIPv4アドレスを含める必要があります。                                                                                                                                                                            |
| cloud-template | CT_IPSECTUNNEL_PEERADDR_IS_HOST      | cloudtemplateIpSecTunnelでは、peeraddrはホストアドレス (/32 など) である必要があります。                                                                                                                                                                    |
| cloud-template | CT_PROFILE_COUNT                     | cloudtemplateProfile MOのカウントは最大1です                                                                                                                                                                                                  |



| コンポーネント        | エラーコード (Error Code)                | 制約                                                                                                                              |
|----------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| cloud-template | CT_PROFILE_DELETE                  | cloudtemplateProfile MO は、親の cloudtemplateInfraNetwork も削除されない限り、削除できません。                                                       |
| cloud-template | CT_PROFILE_ROUTERUSERNAME_NONEMPTY | cloudtemplateProfile では、routerUsername は空でない必要があります。                                                                            |
| cloud-template | CT_PROFILE_ROUTERPASSWORD_NONEMPTY | cloudtemplateProfile では、routerPassword は空でない必要があります。                                                                            |
| cloud-template | CT_PROFILE_ROUTERUSERNAME_MODIFY   | cloudtemplateProfile では、routerUsername は、いずれかのリージョン (つまり、cloudtemplateIntNetwork の下にある cloudRegionName) にルータが展開されている場合は変更できません。 |
| cloud-template | CT_PROFILE_ROUTERPASSWORD_MODIFY   | cloudtemplateProfile では、routerPassword は、いずれかのリージョン (つまり、cloudtemplateIntNetwork の下にある cloudRegionName) にルータが展開されている場合は変更できません。 |

| コンポーネント        | エラーコード (Error Code)                    | 制約                                                                                                                                                                    |
|----------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cloud-template | CT_PROFILE_ROUTERTHROUGHPUT_MODIFY     | cloudtemplateProfile<br>では、<br>routerThroughput は、<br>いずれかのリージョン<br>(つまり、<br>cloudtemplateIntNetwork<br>の下にある<br>cloudRegionName) に<br>ルータが展開されてい<br>る場合は変更できませ<br>ん。 |
| クラウド           | CT_APICSUBNET_INVALID_HOME_REGION      | cloudApicSubnet MO で<br>は、capicDeployed と<br>してマークされたリー<br>ジョンは有効なリー<br>ジョンである必要があ<br>ります。                                                                            |
| クラウド           | CT_APICSUBNET_REPEATED_REGION          | cloudApicSubnet MO で<br>は、リージョンを最大<br>1つのサブネットに関<br>連付けることができま<br>す。                                                                                                  |
| クラウド           | CT_APICSUBNET_MULTIPLE_HOME_REGION     | cloudApicSubnet MO で<br>は、最大で1つのリー<br>ジョンが<br>capicDeployedを true に<br>設定できます。                                                                                        |
| クラウド           | CLOUD_APICSUBNETPOOL_CREATEDBY_USER    | cloudApicSubnetPool で<br>は、createdBy 属性は<br>USER である必要があ<br>ります                                                                                                       |
| クラウド           | CLOUD_APICSUBNETPOOL_SUBNET_IP_VERSION | cloudApicSubnetPool で<br>は、サブネットに IPv4<br>アドレスが含まれてい<br>る必要があります。                                                                                                     |
| クラウド           | CLOUD_APICSUBNETPOOL_SUBNET_SIZE       | cloudApicSubnetPool で<br>は、サブネットは /24<br>である必要がありま<br>す。                                                                                                              |

| コンポーネント | エラーコード (Error Code)                   | 制約                                                                          |
|---------|---------------------------------------|-----------------------------------------------------------------------------|
| クラウド    | CLOUD_APICSUBNETPOOL_DELETE_USAGE     | cloudApicSubnetPool は、その cloudApicSubnet 子の少なくとも1つがリージョンで使用されている場合は削除できません。 |
| クラウド    | CLOUD_APICSUBNETPOOL_DELETE_CREATEDBY | createdBy 属性が USER ではない cloudApicSubnetPool は削除できません。                       |

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。