AWS ユーザー ガイド向け Cisco クラウド ネットワーク コントローラ、リリース 26.0（5）

初版：2021 年 9 月 20 日

最終更新：2023 年 2 月 28 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Trademarks

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

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

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

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

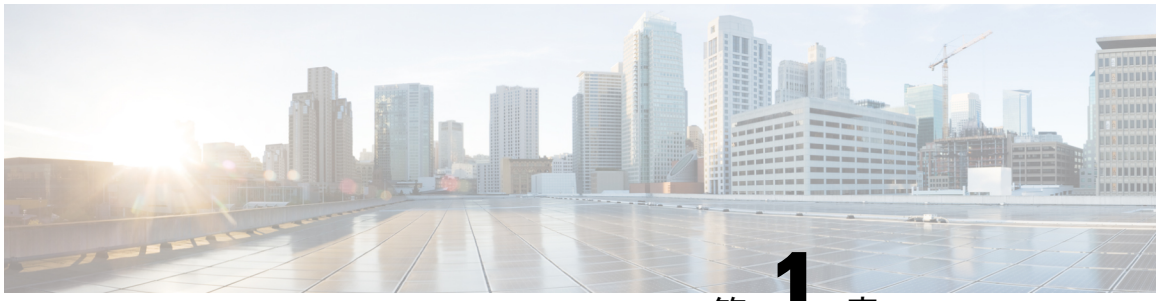
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

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

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

Trademarks

目 次



第 1 章

新機能および変更された機能に関する情報

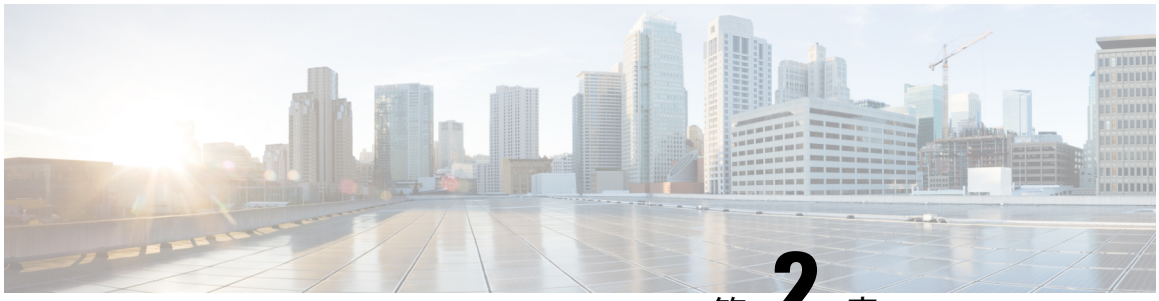
新機能および変更された機能に関する情報

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

表 *1 : Cisco Cloud* ネットワーク コントローラ リリース *26.0*（*1*）の新機能と変更された動作

機能または変更	説明	参照先
UI 新しい外観と操作性	このドキュメントのスクリーンショットと図は、最近の UI の変更を反映するように更新されています。新しい UI の外観と操作性は異なりますが、画面の配置と構成オプションは同じままです。	

新機能および変更された機能に関する情報



第 2 章

Cisco Cloud Network Controller について

概要

Cisco クラウド ネットワーク コントローラは、クラウドベース仮想マシン（VM）で展開可能なソフトウェアです。Amazon Web Services（AWS）、Azure、および Google Cloud は、Cisco Cloud Network Controller でサポートされるクラウド プロバイダーです。

展開されると、Cisco Cloud Network Controller は以下を実行します。

- 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 Nexus Dashboard Orchestrator 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 Network Controller はポリシーをクラウド向けに変換して、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 Network Controller Installation Guide* を参照してください。

Cisco Cloud Network Controller が稼働している場合は、Cisco Cloud Network Controller 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 Network Controller 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 Network Controller 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

AWS と Cisco Cloud Network Controller 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。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ます。この IPSec/BGP 外部接続により、Cisco Cloud Network Controller をブランチ オフィスに接続できます。

次の項では、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 Network Controller で使用されるどのクラウド コンテキスト プロファイルでも参照されません。

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

非 ACI 外部デバイスへの接続

AWS CCR から ACI 以外の外部デバイスへの接続もサポートされています。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

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 Network Controller 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。

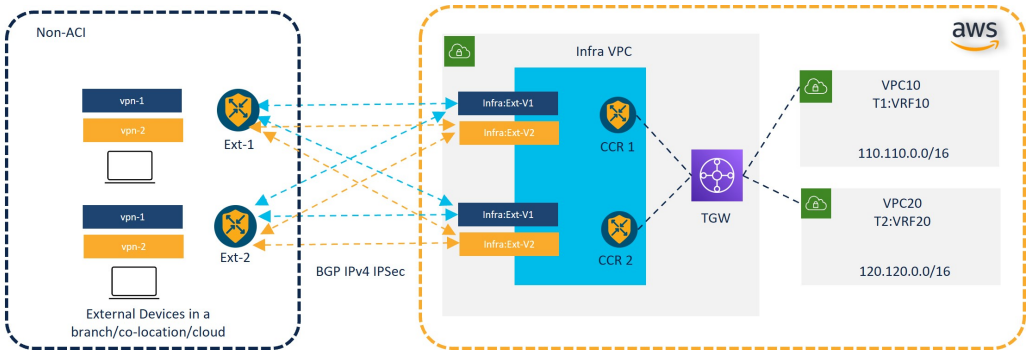
（注） このセクションで説明するルーティングおよびセキュリティ ポリシーは、25.0(1) リリース専用であり、内部と外部 VRF の間でのみ適用されます。 25.0(2) リリースでのルーティング ポリシーとセキュリティ ポリシーの変更については、ルーティング ポリシー: リリース 25.0(2) （8 ページ） を参照してください。

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 Network Controller GUI を使用した VRF 間ルート リークの構成 （67 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 Network Controller GUI を使用した EPG の作成 （78 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 Network Controller GUI を使用したコントラクトの作成 （84 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 Network Controller 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 ポリシーを構成できます。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) （5 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) （5 ページ） で説明されているように引き続き分割されますが、特にルーティング ポリシーに次の変更が追加されています。

内部 VRF 間のルート リーク

以前の 25.0(1) リリースでは、内部 VRF と外部 VRF のペア間でリークするルートを指定する独立したルーティング ポリシーを設定できる、VRF 間ルート マップベースのルーティング機能が導入されました。このルート マップ ベースのルーティング機能は、特に内部 VRF と外部 VRF の間に適用されます。内部 VRF のペア間のルーティングを設定する場合、ルーティングおよびセキュリティ ポリシー: リリース 25.0(1) （5 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 Network Controller で作成されたポリシーです。
- 契約ベースのルーティングは、グリーンフィールド ケースに対してデフォルトで無効になっています（オフになっています）（Cisco Cloud Network Controller 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 Network Controller 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、ルート マップ不在で契約がルートでドライブできるかをはいまたは、いいえを使用して表示する初期設定画面の **[詳細設定（Advanced Settings）]** の後の **[構成編集（Edit Configuration）]** で構成されたグローバル ポリシーです：

- **[いいえ（No）]**: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。
- **[はい（Yes）]**: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。有効に設定されている場合、ルートマップが構成されていないときに、ドライブ回送を契約します。ルート マップが存在するときに、ルート マップは常にドライブ回送です。

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 ポリシーを設定間でスイッチす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 Network Controller GUI を使用した内部 VRF のリーク ルートの構成 （71 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 Network Controller 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スイッチす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、**[いいえ（No）]** に設定をスイッチする前にルート 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スイッチするために、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スイッチす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スイッチす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

異なる外部ネットワークから同じ接続先への複数のトンネルを使用するためのサポートが利用可能です。これは、GUI でさまざまなソース インターフェイス (2、3、または 4) を使用するか、`cloudtemplateIpseTunnlSourceInterface` を使用して REST API を介して実行されます。

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

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

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

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

```
    <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId="3" />
</cloudtemplateIpSecTunnel>
```

注意事項と制約事項

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

Cisco Cloud Network Controller の一般的な注意事項と制限事項

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

- 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 にアドバタイズするために、外部でアドバタイズされたオンプレミス サイトのブリッジ ドメイン サブネットを設定します。
- 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。アカウントを管理していた以前の Cisco Cloud Network Controller インスタンスから古い設定を適切に消去していなかった場合、残っている可能性があります。

（注） テナント アカウント ID を追加した後、Cisco Cloud Network Controller が古いクラウド リソースを検出するには時間がかかります。

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 Network Controller 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（Automatically Clean Up Stale Cloud Objects）]** 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 Network Controller は、作成した Azure リソースの管理を試みます。既存のリソースをインベントリとしてリストするのではなく、他のアプリケーションによって作成されたリソースの管理を試みません。同時に、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 アカウントには、Cisco Cloud Network Controller が作成するリソースを妨害しないことが求められます。このため、Cisco Cloud Network Controller が AWS 上で作成するすべてのリソースには、次の 2 つのタグの少なくとも 1 つがあります。
  - AciDnTag
  - AciOwnerTag

  Cisco Cloud Network Controller 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 Network Controller によって作成さ

れ、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 ポリシーがあれば、Cisco Cloud Network Controller 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 Network Controller 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 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 Network Controller 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 *2:* 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
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

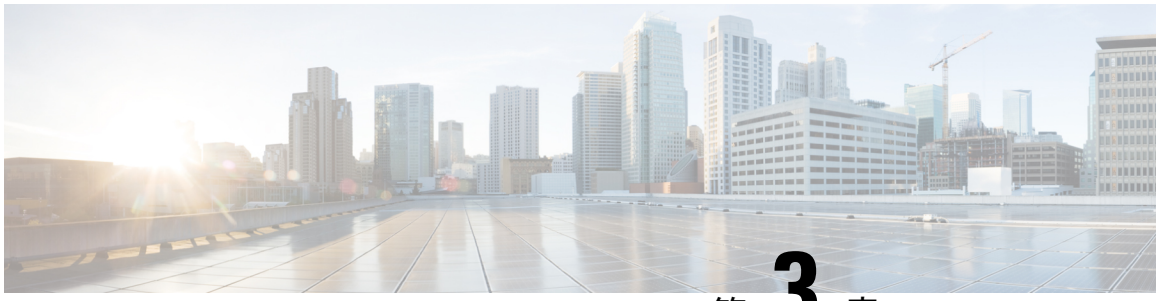
Cisco Cloud Network Controller GUI について

Cisco Cloud Network Controller GUI は、関連するウィンドウのグループに分類されます。各ウィンドウでは、特定のコンポーネントにアクセスして管理できます。GUIの左側にある**[ナビゲーション（Navigation）]**メニューを使用して、ウィンドウ間を移動します。メニューのいずれかの部分にマウスを移動すると、**[ダッシュボード（Dashboard）]**、**[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。

Cisco Cloud Network Controller コンポーネントの構成の詳細については、Cisco Cloud Network Controller コンポーネントの構成 （47 ページ） を参照してください。



第 3 章

Cisco Cloud Network Controller ポリシー モデル

CNC ポリシーモデルについて

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

ポリシー モデルの主な特性

ポリシー モデルの主な特性には次のものがあります。

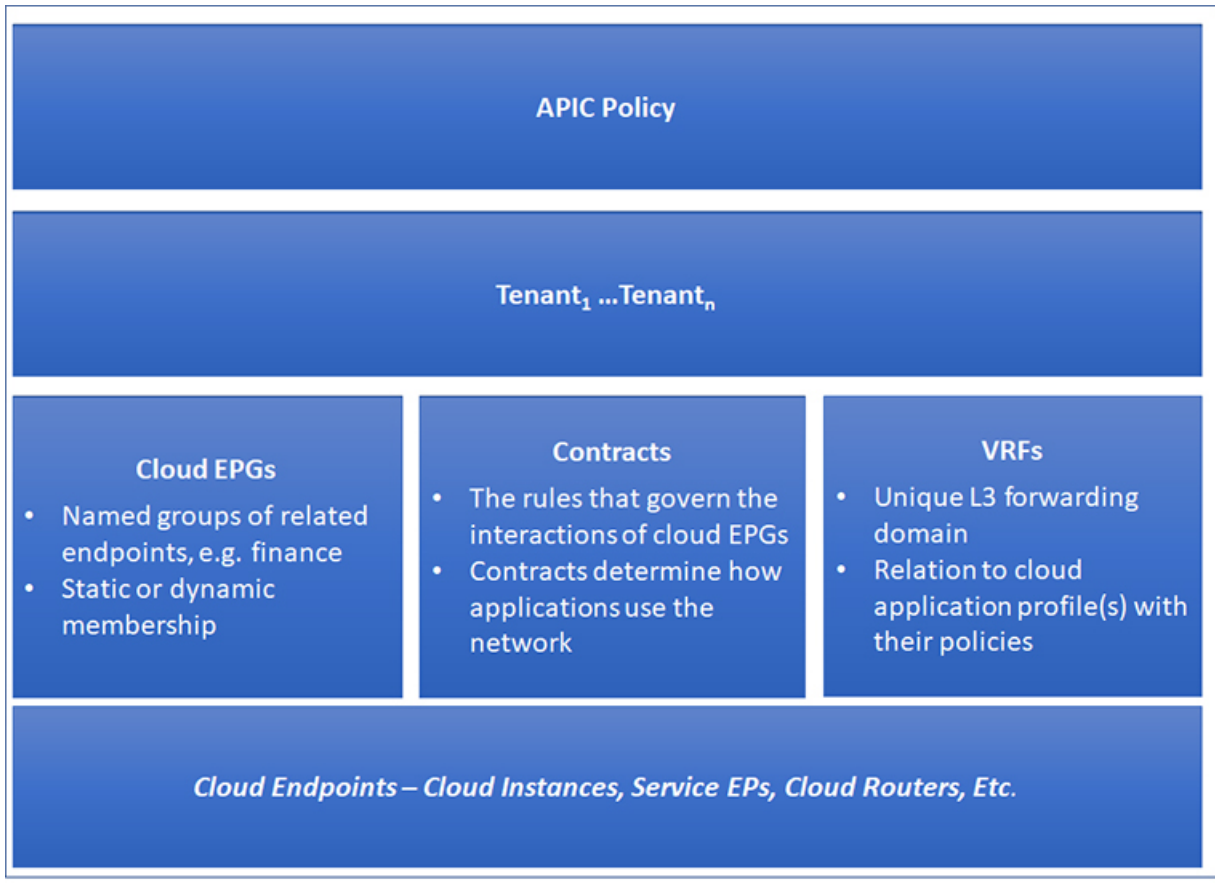
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

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

論理構造

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、CNC ポリシー モデルの論理構造の概要を示します。

図 *1 : CNC* ポリシー モデルの論理構造の概要



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

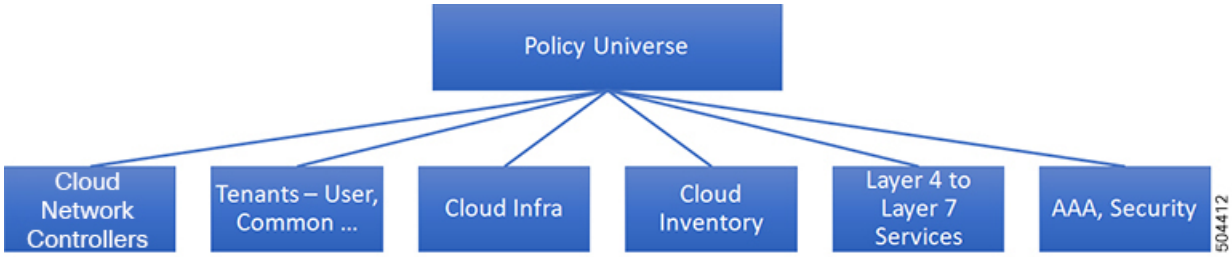
Cisco CNC ポリシー管理情報モデル

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

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

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

図 *2 : Cisco CNC* ポリシー管理情報モデルの概要



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

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

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

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

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

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

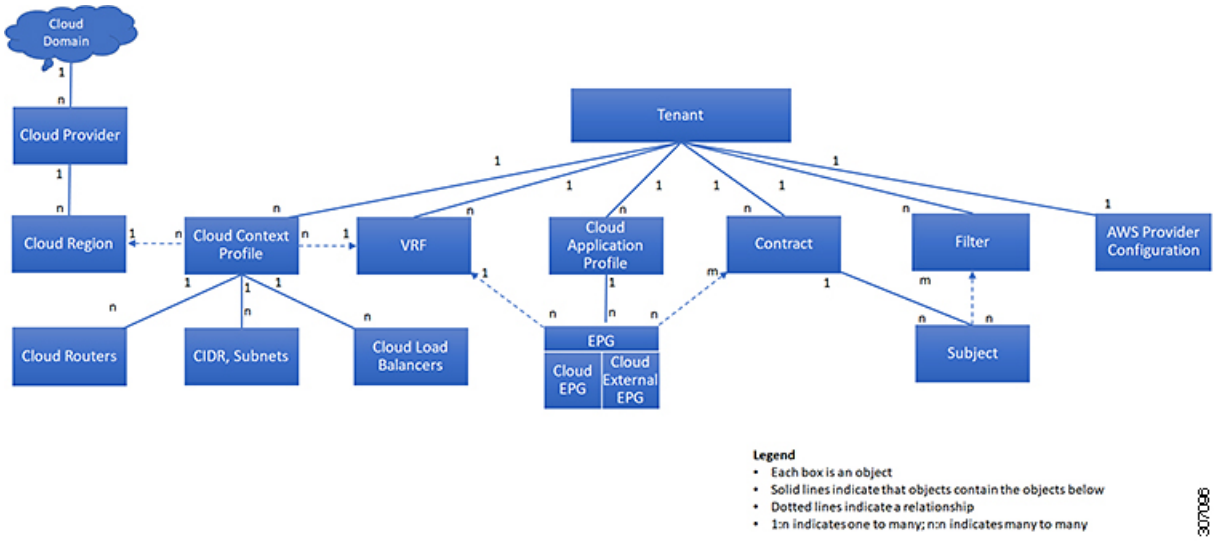
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ 4 ～ レイヤ 7 のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、レイヤ 4 から レイヤ 7 サービスの展開 （163 ページ）を参照してください。
- アクセス、認証、およびアカウンティング（AAA）ポリシーは、Cisco Cloud Network Controller クラウド インフラストラクチャのユーザー権限、ロール、およびセキュリティ ドメインを管理します。詳細については、Cisco Cloud Network Controller のセキュリティ （193 ページ）を参照してください。

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

テナント

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

図 *3:* テナント



テナントは相互に分離することも、リソースを共有することもできます。テナントに、フィルタ、コントラクト、Virtual Routing and Forwarding（VRF）インスタンス、クラウド コンテキスト プロファイル、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 プロファイルが含まれるプライマリ要素です。テナントのエンティティはそのポリシーを継承します。VRF はコンテキストとも呼ばれ、それぞれを複数のクラウド コンテキスト プロファイルに関連付けることができます。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 プロファイルは、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。CNC 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 構成のみをサポートします。

クラウド コンテキスト プロファイル

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

- 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

The CCR is a virtual router that delivers comprehensive WAN gateway and network services into virtual and cloud environments. The CCR enables enterprises to extend their WANs into provider-hosted clouds. Two CCRs are required for Cisco Cloud Network Controller solution.

The **Cisco Catalyst 8000V** is used with the Cisco Cloud Network Controller. For more information on this type of CCR, see the Cisco Catalyst 8000V Edge software documentation.

About the Cisco Catalyst 8000V

Following are the updates for the Cisco Catalyst 8000V.

- Licensing, on page 23
- Throughput, on page 24

Licensing

The Cisco Catalyst 8000V on Cisco Cloud Network Controller supports the following licensing models:

1. **Bring Your Own License (BYOL)** Licensing Model
2. **Pay As You Go (PAYG)** Licensing Model

BYOL Licensing Model

The BYOL licensing model on Cisco Catalyst 8000V which requires you to purchase your Catalyst 8000V Cisco DNA license from Cisco and deploy it in the cloud.

- For instructions on subscribing to one of the tier-based Cisco Catalyst 8000V licenses, see Cisco Catalyst 8000V Edge Software.
- For more information on different throughputs based on the tiers, see Throughput, on page 24.

Cisco Cloud Network Controller makes use of the “Cisco DNA Advantage” subscription. For features supported by the “Cisco DNA Advantage” subscription, see Cisco DNA Software SD-WAN and Routing Matrices.

PAYG Licensing Model

Beginning with the 25.0(4) release, Cisco Cloud Network Controller supports Pay-As-You-Go (PAYG) Licensing Model on Cisco Catalyst 8000V which allows users to deploy a Catalyst 8000V instance in the cloud based on the VM size and purchase the usage on an hourly basis.

As you completely depend on the VM size to get the throughput, the PAYG licensing model can be enabled only by first un-deploying the current Cisco Catalyst 8000V and then re-deploying it using the First Time Set Up with the new VM size. For more information, see the chapter "Configuring Cisco Cloud Network Controller Using the Setup Wizard" in the *Cisco Cloud Network Controller for AWS Installation Guide*

Note The procedure for switching between licenses can also be used if you would like to switch between the two licensing types available.

Note There are two PAYG options for consuming licenses in the AWS marketplace: **Catalyst 8000V Cisco DNA Essentials** and **Catalyst 8000V Cisco DNA Advantage**. Cisco Cloud Network Controller will make use of **Catalyst 8000V Cisco DNA Advantage**. For features supported by the "Cisco DNA Advantage" subscription, see Cisco DNA Software SD-WAN and Routing Matrices

Throughput

The Cisco Catalyst 8000V on Cisco Cloud Network Controller supports the following licensing models:

1. **Bring Your Own License (BYOL)** Licensing Model
2. **Pay As You Go (PAYG)** Licensing Model

1. Bring Your Own License (BYOL)

For this model, the Cisco Catalyst 8000V supports tier-based (T0/T1/T2/T3) throughput options. The following table lists what AWS EC2 instance is used for different router throughput settings for the Cisco Catalyst 8000V:

CCR Throughput	AWS EC2 Instance
T0 (up to 15M throughput)	c5.xlarge
T1 (up to 100M throughput)	c5.xlarge
T2 (up to 1G throughput)	c5.xlarge
T3 (up to 10G throughput)	c5.9xlarge

Tier2 (T2) is the default throughput supported by Cisco Cloud Network Controller.

2. Pay-As-You-Go Licensing Model

For this model, Cisco Cloud Network Controller supports a range of AWS EC2 instances for cloud networking needs powered by Cisco's Catalyst 8000V virtual router.

The table below shows the cloud instance type supported by Cisco Cloud Network Controller on AWS.-

AWS EC2 Instance	CCR Throughput	vCPUs	Memory
c5.xlarge	up to 5 Gigabit throughput	4	8 GiB
c5.2xlarge	up to 10 Gigabit throughput	8	16 GiB
c5.4xlarge	up to 10 Gigabit throughput	16	32 GiB

AWS EC2 Instance	CCR Throughput	vCPUs	Memory
c5.9xlarge	up to 10 Gigabit throughput	36	72 GiB
c5n.xlarge	up to 25 Gigabit throughput	4	10.5 GiB
c5n.2xlarge	up to 25Gigabit throughput	8	21 GiB
c5n.4xlarge	up to 25 Gigabit throughput	16	42 GiB
c5n.9xlarge	up to 50 Gigabit throughput	36	96 GiB

AWS の Cisco クラウド ネットワーク コントローラおよび CCR 向けプライベート IP アドレス サポート

デフォルトで 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 Network Controller GUI を使用したリージョンの管理（クラウド テンプレートの構成）（134 ページ） の手順を参照してください。

デフォルトでプライベート IP アドレスは Cisco Cloud Network Controller 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。接続にプライベート IP アドレスが使用されるように Cisco Cloud Network Controller へのパブリック IP を無効にするには、*[AWS インストール ガイド向け Cisco クラウド ネットワーク コントローラ（Cisco Cloud Network Controller for AWS Installation Guide）]*の*[AWS 内の Cisco クラウド ネットワーク コントローラを展開（Deploying the Cisco Cloud Network Controller in AWS）]*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 クラウドネットワーク コントローラ サイトに接続するためのクラウドバックボーン

Communicating to External Sites From Regions Without a CCR

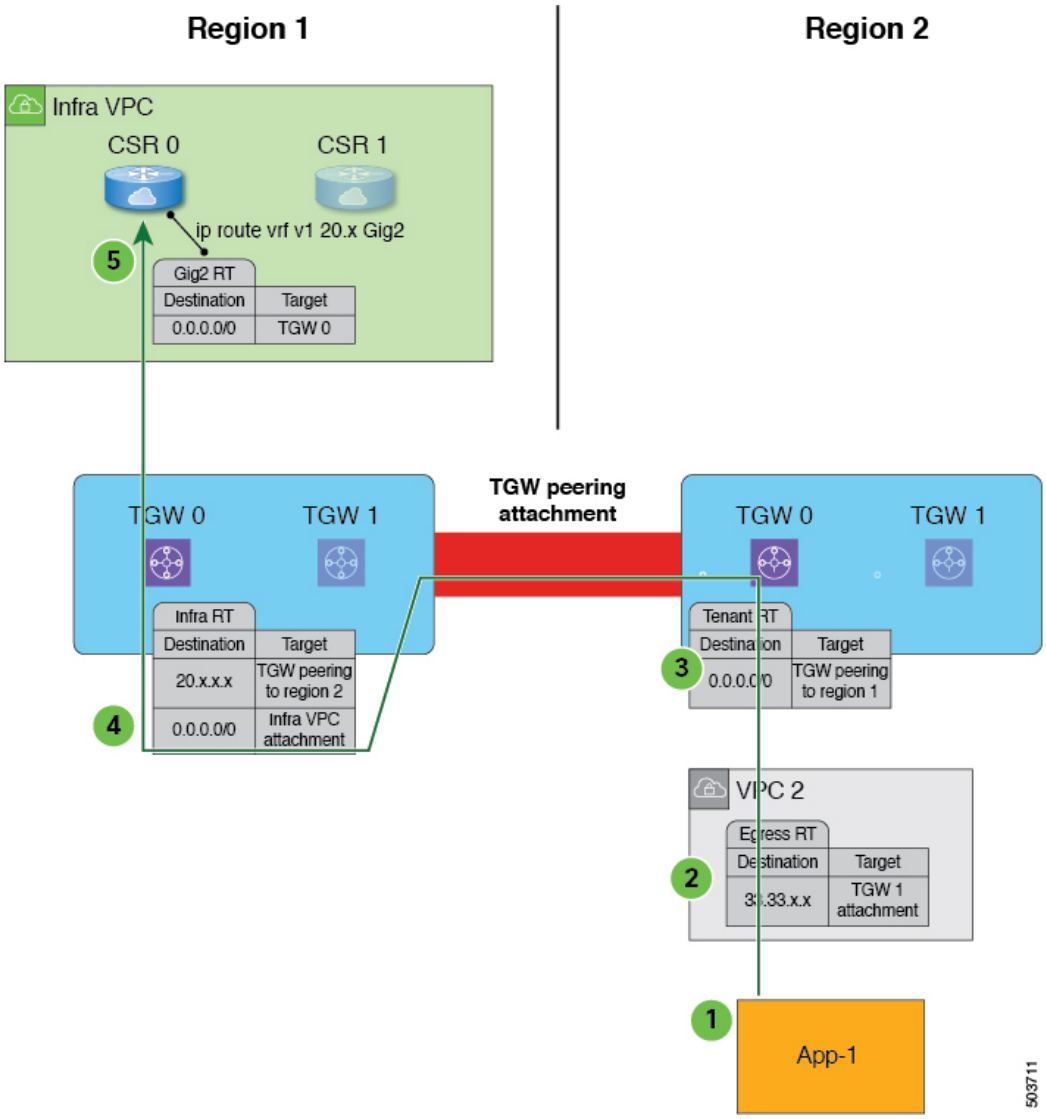
Support is available for communication with an external site from regions without a CCR. This is accomplished by making use of the AWS Transit Gateway feature. When you enable the AWS Transit Gateway feature on Cisco Cloud Network Controller, you also enable peering between all managed regions on AWS. In this way, the AWS Transit Gateway peering feature allows the Cisco Cloud Network Controller to address the issue of communicating with external sites from regions without a CCR. It addresses this issue by having traffic rerouted to a region with a CCR.

Using the AWS Transit Gateway feature, when traffic from a region without a CCR tries to egress out of a site, this traffic will be routed to the infra VPC for the closest region with a CCR. After the traffic is rerouted to that region's infra VPC, that CCR is used to egress out the packet. For ingress traffic, packets coming from an external site can reach any region's CCR and then be routed to the destination region using the AWS Transit Gateway peering in the ingress data path.

In these situations, traffic is rerouted automatically when the system recognizes that external traffic is egressing or ingressing through a region without a CCR. However, you must have the following components configured in order for the system to automatically perform this rerouting task:

- AWS Transit Gateway must be configured. If AWS Transit Gateway is not already configured, see Increasing Bandwidth Between VPCs by Using AWS Transit Gateway for those instructions.
- CCRs must be deployed in at least one region. Even though this enhancement allows you to communicate with an external site from a region that *does not* contain a CCR, in order to do this, you must have another separate region that *does* contain a CCR so that traffic can be rerouted from the region without a CCR to the region with a CCR.

The following figure shows an example scenario where traffic is rerouted automatically when the system recognizes that external traffic is egressing from a region without a CCR.



The following occurs when the Cisco Cloud Network Controller recognizes that Region 2 does not have a CCR, but traffic is egressing out to an external site (shown with the green arrow and circles):

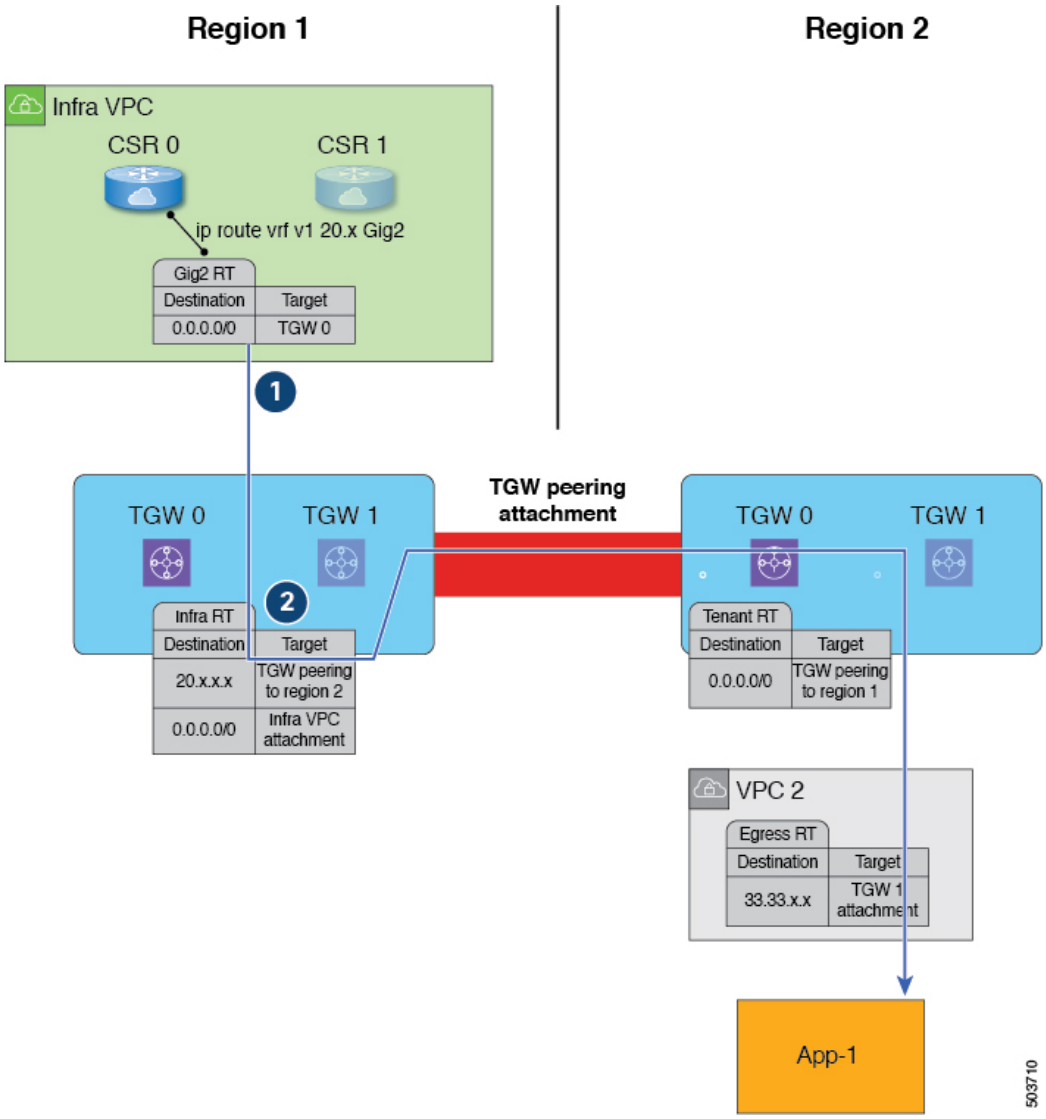
1. Traffic flow begins egressing out from the CIDR in App-1 in Region 2 to a remote site. Note that the endpoint is configured with the appropriate outbound rule to allow the remote site CIDR.
2. The VPC 2 egress route table has the remote site CIDR, which then has the AWS Transit Gateway as the next hop. The AWS Transit Gateway information is programmed automatically based on the configured contracts.
3. A 0.0.0.0/0 route is inserted in the AWS Transit Gateway route table, which essentially tells the system to take the AWS Transit Gateway peering attachment if traffic is egressing out to an external site but there is no CCR in this region. In this situation, the AWS Transit Gateway peering attachment goes to another region that does have a CCR (Region 1 in the example scenario). The region with a CCR that will be used is chosen based on geographical proximity to the region that does not have a CCR.

4. The packet is first forwarded to the infra VPC in the region with the CCR (Region 1), and is then forwarded to the gigabit ethernet network interface on the CCR that is associated with the appropriate VRF group.
5. The gigabit 2 inbound security group on the CCR in Region 1 is configured to allow traffic from the remote region VPC.

It's useful to note that in the egress example shown above:

- For steps 1 and 2, there is no change from pre-release 5.2(1) behavior.
- Step 3 is behavior that is new and unique to this feature in release 5.2(1), where the redirect occurs to the TGW peering attachment from the region without a CCR to the region with a CCR. In addition, step 3 occurs on the AWS cloud.
- Steps 4 and 5 would normally occur in Region 2 before release 5.2(1), but only if Region 2 had a CCR. However, because Region 2 does not have a CCR, with this feature in release 5.2(1), these steps are taking place in Region 1 where a CCR is present.

The following figure shows an example scenario where traffic is rerouted automatically when the system recognizes that external traffic is ingressing to a region without a CCR.



The following occurs when the Cisco Cloud Network Controller recognizes that Region 2 does not have a CCR, but traffic is ingressing in from an external site to a CIDR in App-1 in Region 2 (shown with the blue arrow and circles):

1. Normally, the CCR in Region 1 would only advertise the CIDRs that are local to that region. However, with this enhancement that is part of release 5.2(1), all CCRs in all regions now advertise CIDRs from all remote regions. Therefore, in this example, the CCR in Region 1 will also advertise the CIDRs that are in Region 2 (assuming AWS Transit Gateway peering is configured between both regions and the contracts are configured correctly). In this situation, the traffic ingresses in from an external site to the CCR in Region 1, where the CCR in Region 1 advertises the static route for the remote region VPC CIDRs.
2. The infra route table (the AWS Transit Gateway route table in Region 1) has the next hop to the AWS Transit Gateway peering attachment to Region 2.

It's useful to note that in the ingress example shown above:

- Both steps (steps 1 and 2) in the ingress example shown above are new and unique to this feature in release 5.2(1).
- Step 1 in the ingress example shows configurations programmed on the CCR.
- Step 2 in the ingress example occurs on the AWS cloud.

CCR のリモートサイトからの ECMP 転送のサポート

CCR を使用した ECMP がサポートが利用可能です。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。このサポートは自動的に有効になり、有効にするために手動で構成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

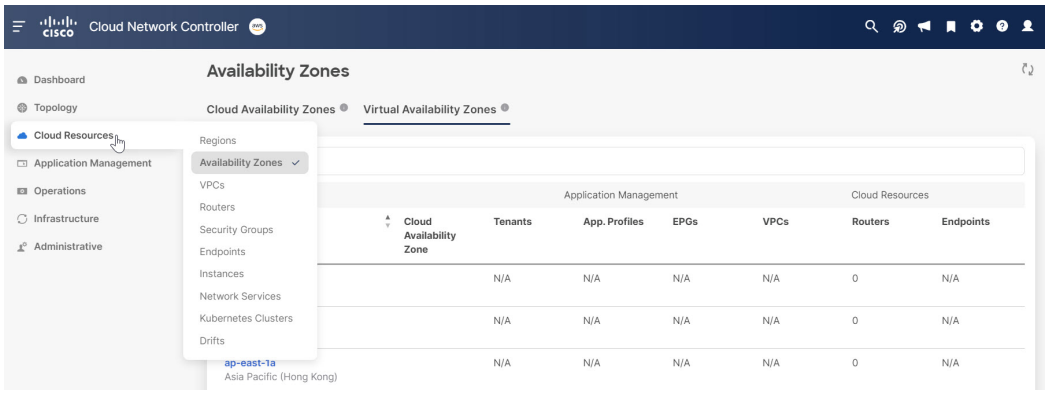
構成されているすべての CIDR は、特定のリージョンに対してローカルです。クラウド内に複数のリージョンがある場合、すべてのリージョンの CCR は冗長性のために CIDR をアドバタイズします。ただし、すべてのリージョンの CCR が同じプリファレンスの CIDR をアドバタイズするのではなく、CIDR がローカルであるリージョンからより高いプリファレンスで CCR をアドバタイズするためのサポートを使用できます。これにより、オンプレミスサイトまたはリモートクラウドサイトは、CIDR がローカルであるリージョンにトラフィックを直接送信します。ローカル リージョンの CCR に障害が発生した場合、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

Cisco クラウド ネットワーク コントローラでは、次の 2 種類の可用性ゾーンがサポートされています。

- **仮想アベイラビリティ ゾーン**：Cisco Cloud Network Controller は、AWS のリージョンごとに 2 つの仮想アベイラビリティ ゾーンのみをサポートします。その際、Cisco Cloud Network Controller は、<リージョン名>a と <リージョン名>b という命名法により、リージョンごとに 2 つの仮想アベイラビリティ 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 Network Controller 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。

  Cisco Cloud Network Controller 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（Cloud Resources）]** > **[アベイラビリティ ゾーン（Availability Zones）]** に移動し、**[仮想アベイラビリティ ゾーン（Virtual Availability Zones）]** タブをクリックします。



- **クラウド アベイラビリティ ゾーン**: このタイプのアベイラビリティ ゾーンでは、Cisco Cloud Network Controller を使用して AWS リージョンごとに複数のアベイラビリティ ゾーンを使用できます。

  Cisco Cloud Network Controller 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（Cloud Resources）]** > **[アベイラビリティ ゾーン（Availability Zones）]** に移動し、**[クラウドアベイラビリティ ゾーン（Cloudl Availability Zones）]** タブをクリックします。

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

仮想可用性ゾーンが構成されている展開がある場合は、仮想可用性ゾーンからクラウド可用性ゾーンに移行することをお勧めします。

- アベイラビリティー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、インテント 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ーゾーンからクラウドアベイラビリティー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

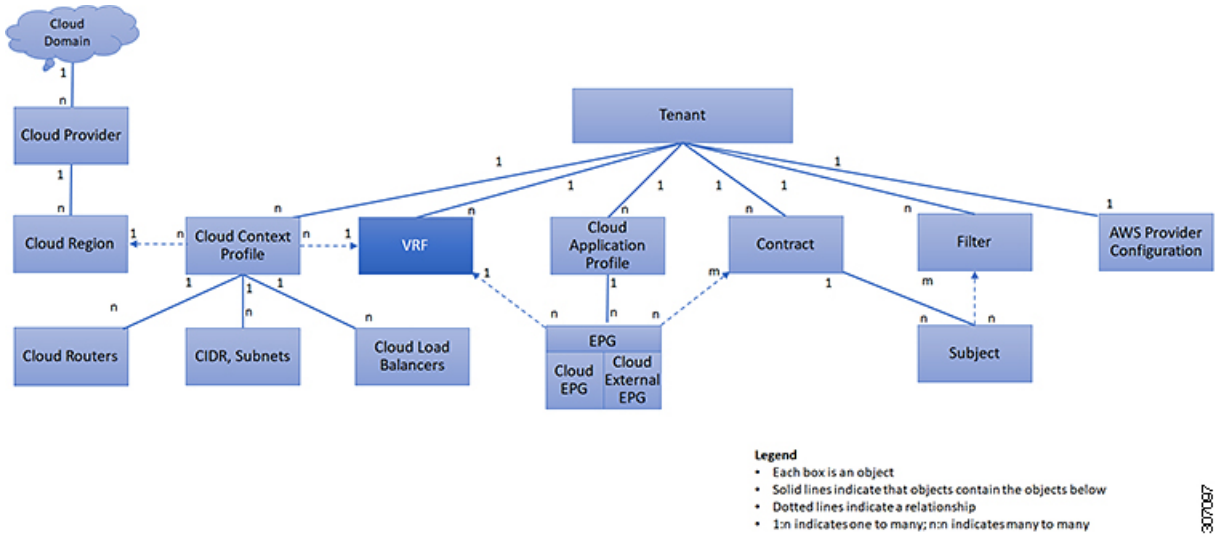
次に、複数のアベイラビリティ ゾーンのサポートに関するガイドラインと制限事項を示します。

- 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 ゾーンのサポートは、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 クラウド ネットワーク コントローラ 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 *4 : VRF*

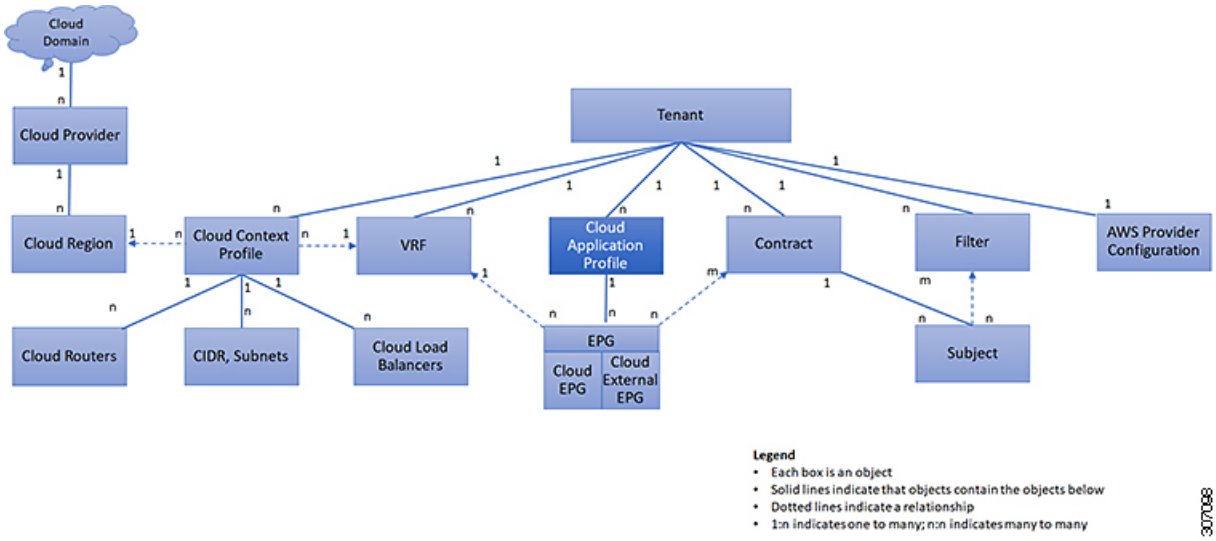


VRF は、レイヤ 3 のアドレス ドメインを定義します。1 つ以上のクラウド コンテキスト プロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウド コンテキスト プロファイルは 1 つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイス クラスタの選択基準ポリシーを提供する論理デバイスの VRF 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 *5:* クラウド アプリケーション プロファイル



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

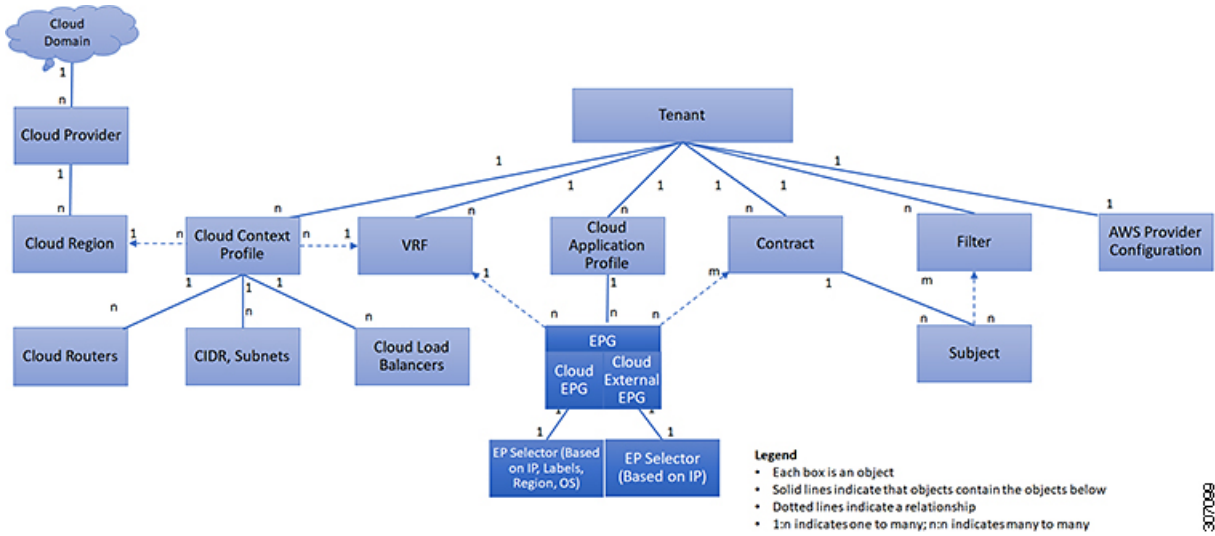
クラウド EPG は次のいずれかに従って組織化できます。

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

クラウド エンドポイント グループ

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

図 *6:* クラウド エンドポイント グループ



クラウド EPG は、エンドポイントの集合を含む名前付き論理エンティティである管理対象オブジェクトです。エンドポイントは、ネットワークに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で、他のすべての ID の詳細にアクセスすることもできます。クラウド EPG は、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ストレージ サービス、またはクライアントが含まれます。クラウド EPG 内のエンドポイント メンバシップは、ダイナミックまたはスタティックにできます。

CNC 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

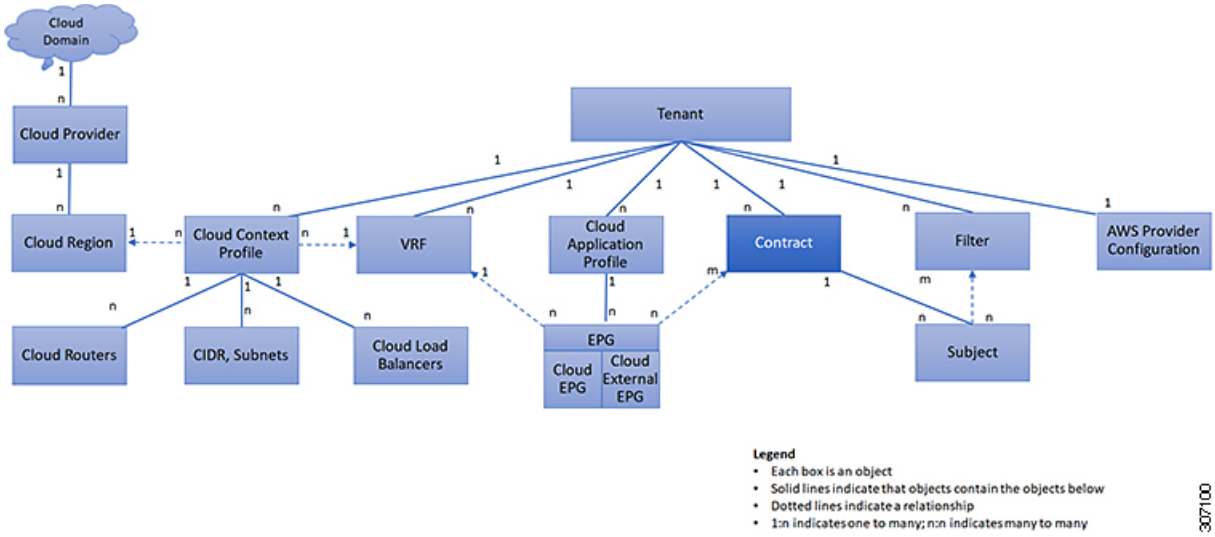
学習します。エンドポイントを学習すると、クラウドインフラストラクチャは、それに基づいて cloudExtEPg クラウド EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション（cloudEPg）クラウド EPG 内でサーバとの TCP セッションを開始すると、cloudExtEPg クラウドEPG は、cloudExtEPg クラウド EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアント サーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、その WAN エンドポイントはもうクラウド インフラストラクチャ内に存在しません。

Cisco Cloud Network Controller 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 CNC 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 7: コントラクト



管理者は、コントラクトを使用して許可されるプロトコルやポートを含む EPG 間を通過できるトラフィックの 1 つまたは複数のタイプを選択します。コントラクトがなければ、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）

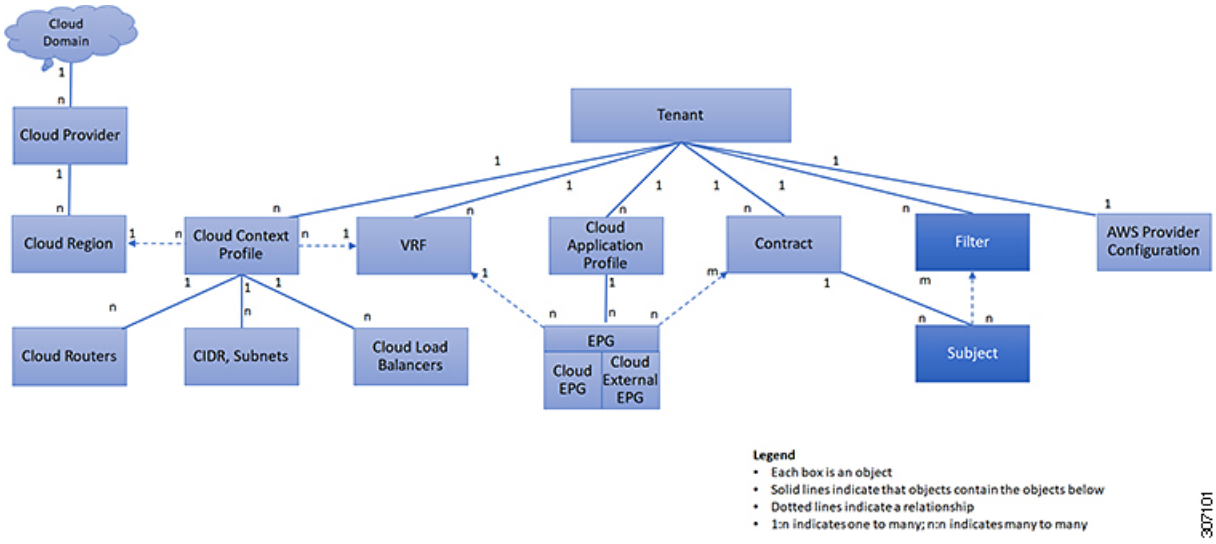
コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付されたクラウド EPG 間の通信を制御します。クラウド EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。クラウド EPG がコントラクトを提供すると、通信が提供されたコントラクトに準拠している限り、そのクラウド EPG との通信は他のクラウド EPG から開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウド エンドポイントは、コントラクトを指定したクラウドEPGのクラウドエンドポイントと通信を開始できます。

（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 *8*: サブジェクトおよびフィルタ



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

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

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 Network Controller 管理対象オブジェクト（MO）は、`cloudCtxProfile` です。クラウド テンプレートで指定されたすべてのリージョンに対して、`cloudCtxProfile` 設定が生成されます。`cloudCtxProfile`は、リージョンに対応するすべての設定の最上位 MO です。その下には、特定の設定をキャプチャするためのツリーとして編成された他の多くの MO があります。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 Network Controller 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 Network Controller AMI を展開する 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 Network Controller に直接提供します。Cisco Cloud Network Controller 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 *3:* クラウド テンプレート *MO*

MO	目的
`cloudtemplateInfraNetwork`	クラウド テンプレート設定のルート。次の属性が含まれます。 `numRoutersPerRegion`：`cloudtemplateIntNetwork` で指定された各 `cloudRegionName` のクラウド ルータの数。
`cloudtemplateProfile`	すべてのクラウドルータの設定プロファイル。次の属性が含まれます。 • `routerUsername` • `routerPassword` • `routerThroughput` • `routerLicenseToken` • `routeDataInterfacePublicIP` • `routerMgmtInterfacePublicIP`
`cloudtemplateIntNetwork`	クラウドルータを展開する場所を指定するリージョンのリストが含まれます。各リージョンは、`cloudRegionName`子 MO を介してキャプチャされます。

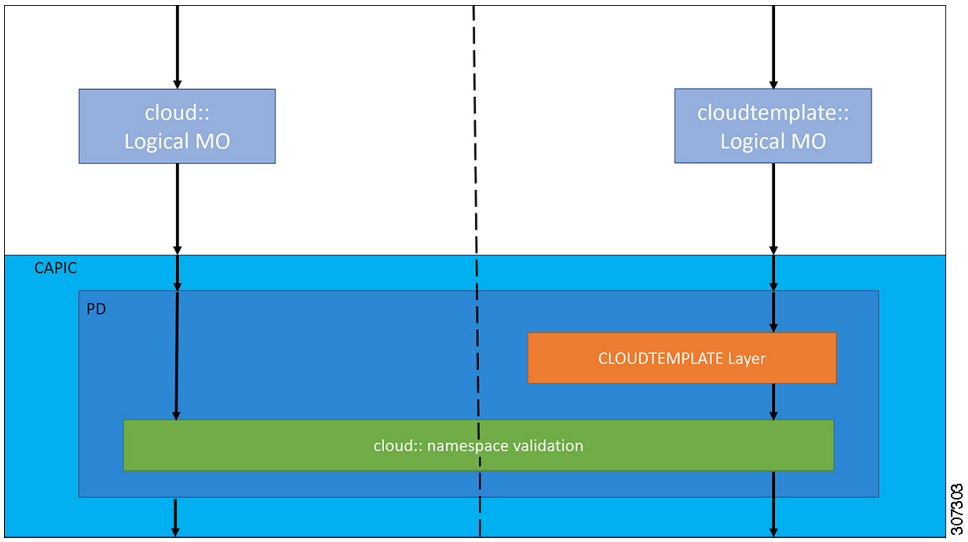
MO	目的
cloudtemplateExtNetwork	クラウド外部のインフラ ネットワーク設定入力が含まれます。 クラウド ルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。 各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateVpnNetwork	ACI オンプレミス サイトまたは別の Cisco Cloud Network Controller サイトで VPN を設定するための情報が含まれています。
cloudtemplateIpSecTunnel	ACI オンプレミス サイトの IPSec ピアの 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 Network Controller では、クラウド テンプレートにより、MO の階層化は通常の Cisco APIC とは若干異なります。通常の Cisco APIC では、2 つの変換レイヤを通過する論理 MO をポストします。

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

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

図 *9:* クラウドおよびクラウド テンプレート*MO*変換



（注） クラウド テンプレートの設定については、Cisco Cloud Network Controller コンポーネントの構成 （47 ページ） を参照してください。

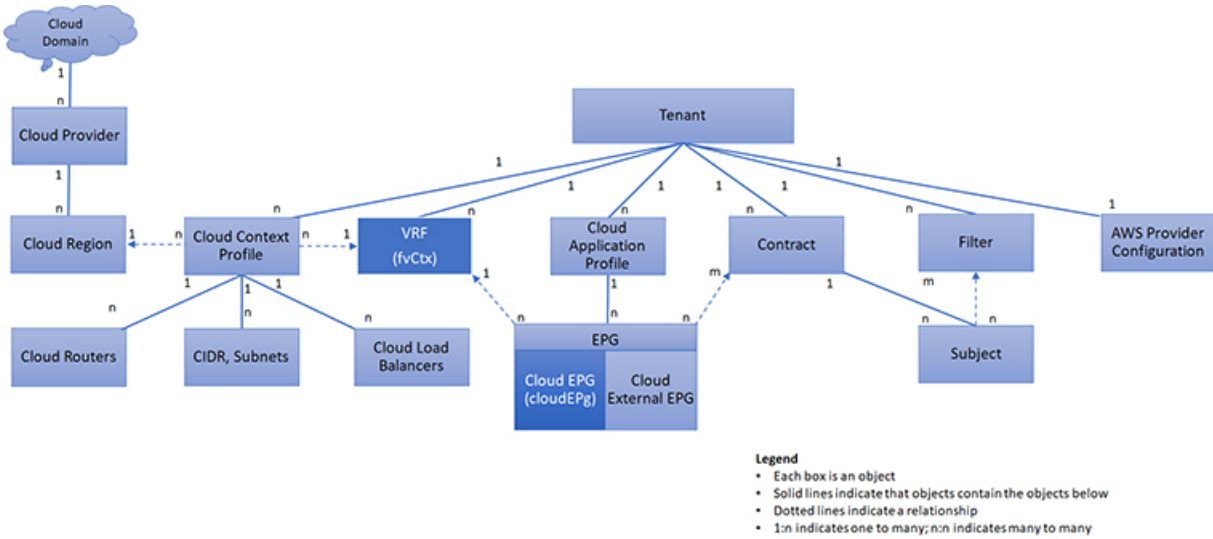
管理対象オブジェクトの関係とポリシー解決

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 *10 : MO* の関係



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

名前付き関係に基づくポリシー解決の場合は、一致する名前を持つターゲット MO が現在のテナントに見つからない場合、CNC 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、CNC 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、CNC クラウド インフラストラクチャは共通のテナントでデフォルト ポリシーを検索します。クラウド コンテキスト プロファイル、VRF およびコントラクト（セキュリティ ポリシー）の名前付き関係はデフォルトに解決されません。

デフォルト ポリシー

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

CNC 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 Network Controller はデフォルトのポリシーを適用します。管理者はデフォルトのポリシーを作成でき、管理者が明示ポリシーを提供しない限り、Cisco Cloud Network Controller はそのポリシーを使用します。

次のシナリオでは、一般的なポリシー解決の動作について説明します。

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

（注） 上記のシナリオは、テナントの VRF には適用されません。

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

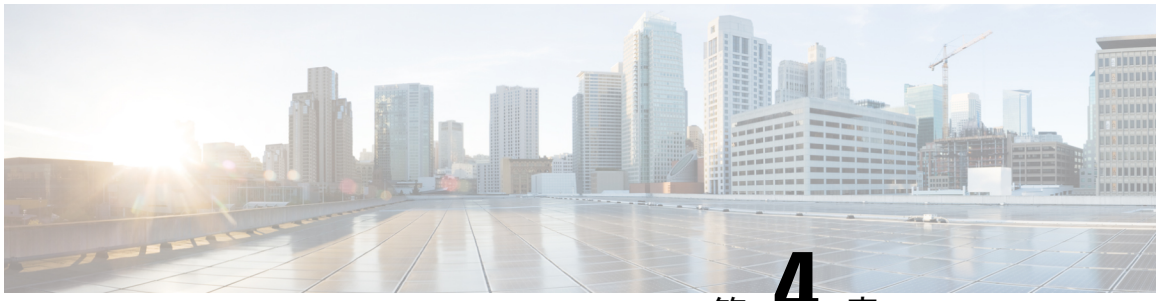
共有サービス

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 Network Controller コンポーネントの構成

Cisco Cloud Network Controller の設定について

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

（注）

- 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 （163 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 Network Controller GUI について （15 ページ） を参照してください。

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

Cisco Cloud Network Controller GUI を使用したテナントの作成

このセクションでは、Cisco Cloud Network Controller GUI を使用したテナント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 *4:* テナント ダイアログボックス フィールドの作成

[プロパティ（Properties）]	説明
名前（Name）	テナント名を入力します。
説明	テナントの説明を入力します。
[設定（Settings）]	
セキュリティ ドメインの追加（Add Security Domain）	セキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。
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	クリックしてテナント タイプを有効にします。 • **信頼できない** • **信頼できる** • **[組織（Organization）]**

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 Network Controller 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 Network Controller 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） Cisco Cloud Network Controller は、他のアプリケーションまたはユーザ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"
        }
    ]
}
```

- Cisco Cloud Network Controller 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 アカウントに Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller がサブスクリプションにインストールされ、次に削除され、Cisco Cloud Network Controller が別のサブスクリプションにインストールされます。既存のすべてのテナント リージョンの展開が失敗します。
  - 別の Cisco Cloud Network Controller 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。避策として、他の Cisco Cloud Network Controller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、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller で AWS プロバイダー（LDAP Provider）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 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。

テナント AWS プロバイダーの構成

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 Network Controller 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 Network Controller 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 Network Controller 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） Cisco Cloud Network Controller は、他のアプリケーションまたはユーザ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"
       }
    ]
}
```

- Cisco Cloud Network Controller 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、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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"
      }
   ]
}
```

- Cisco Cloud Network Controller 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 アカウントに Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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、CNC2 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 Cisco Cloud Network Controller 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。

```
CNC1:
IA1-R1: TA1-R1- ok
        TA1-R2- ok

CNC2:
IA1-R2: TA1-R1- not allowed
        TA1-R3- ok

CNC3:
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 Cisco Cloud Network Controller によって管理される場合、リソース グループ CNC_TA1_R2 （例：CNC_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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller がサブスクリプションにインストールされ、次に削除され、Cisco Cloud Network Controller が別のサブスクリプションにインストールされます。既存のすべてのテナント リージョンの展開が失敗します。
- 別の Cisco Cloud Network Controller 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。避策として、他の Cisco Cloud Network Controller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、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller で AWS プロバイダー（LDAP Provider）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) **[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。

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

このセクションでは、Cisco Cloud Network Controller GUI を使用してアプリケーション プロファイルを作成する方法を説明します。

始める前に

テナントを作成します。

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

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

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

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

ステップ 4 [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 Network Controller GUI を使用した VRF の作成

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

始める前に

テナントを作成します。

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

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

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

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

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

表 *5 : [VRF* の作成（*Create VRF*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	**[Name]** フィールドに、VRF の表示名を入力します。 すべての VRF に *vrfEncoded* 値が割り当てられます。テナントと VRF 名の組み合わせが 32 文字を超える場合、VRF 名（テナント名も含む）は *vrfEncoded* 値を使用してクラウド ルータで識別されます。*vrfEncoded* 値を表示するには、**[Application Management]** > **[VRFs]** サブタブに移動します。右側のペインで VRF をクリックし、クラウド ルータで *[Encoded VRF Name]* を探します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログボックスに戻ります。
説明	VRF の説明を入力します。

[プロパティ（Properties）]	説明
設定 > IPv4 ユニキャスト アドレス ファミリ BGP ターゲット	
フィルタの追加	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。 • **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 Network Controller 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 *6 : [*外部ネットワークの作成（***Create External Network***）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	外部ネットワーク名を入力します。
VRF	この 外部 VRF は、外部の非 ACI デバイスとの外部接続に使用されます。この目的で複数の外部 VRF を作成できます。 この VRF は、VRF が次の 3 つの特性をすべて備えている場合に 外部 VRF として識別されます。 • インフラ テナントの下で構成された • 外部ネットワークに関連付けられている • クラウド コンテキスト プロファイルに関連付けられていない 外部ネットワークに関連付けられているVRFはすべて 外部 VRF になります。外部 VRF をクラウド コンテキスト プロファイルまたはサブネットに関連付けることはできません。 外部 VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成（+ Create VRF）] オプションを使用してVRFを作成することもできます。 3. **[選択（Select）]**をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。
ルータ タイプ	ルータ タイプを選択します。 • **CCR**： • 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	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。 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。

[プロパティ（Properties）]	説明
ハブ ネットワーク	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。 ハブ ネットワークを選択するには: 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（Settings）]	
地域	リージョンを選択するには: 1. **[地域の追加（Add Region）]** をクリックします。 **[地域の選択（Select Regions）]** ダイアログボックスが表示されます。 初回セットアップの一部として選択した地域がここに表示されます。 2. **[地域の選択（Select Regions）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
VPN ネットワーク	

[プロパティ（Properties）]	説明
	VPN ネットワーク エントリは、外部接続に使用されます。設定されたすべてのVPNネットワークが、選択したすべてのリージョンに適用されます。 VPN ネットワークを追加するには、次の手順を実行します。 1. **[VPNネットワークの追加（Add VPN Network）]** をタップします。 **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスが表示されます。 2. **[名前（Name）]** フィールドに VPN ネットワークの名前を入力します。 3. **[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。 **[IPSec 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。 • **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。 （注） 必要に応じて、追加の IPsec トンネル サブネット プールを **[外部ネットワーク]** ページに追加するか、クラウド ネットワーク コントローラーの初回セットアップを介して追加できます。詳細については、*[AWS*インストール ガイドの *Cisco* クラウド ネットワーク コントローラリリース 25.1（x）の「設定ウィザードを使用した Cisco クラウド ネットワーク コントローラの構成」の章を参照してください。サブネット プールのサイズは、作成される IPsec トンネルの数に対応できる十分な大きさにする必要があります。 • **[IPsec トンネル ソース インターフェイス（IPsec Tunnel Source Interfaces）]**：このフィールドのエントリを使用して、Cisco Cloud Network Controller 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。

[プロパティ（Properties）]	説明
	gig3 は、デフォルトで選択されます。次の中から 1 つまたは複数のインターフェイスを選択します • **gig2**: GigabitEthernet2 インターフェイス • **gig3**: GigabitEthernet3 インターフェイス • **gig4**: GigabitEthernet4 インターフェイス （注） この外部ネットワークで IPsec トンネル ソース インターフェイスを構成した後、ルーティング ポリシー: リリース 25.0(2) （8 ページ）で説明されているように、同じ接続先へのトンネルを形成できる追加のネットワークで IPsec トンネル ソース インターフェイスを構成できます。 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。 6. **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスで **[追加（Add）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

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

グローバル VRF 間ルート リーク ポリシーの構成

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

始める前に

[Cisco Cloud Network Controller セットアップ（Cisco Cloud Network Controller 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 （9 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 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。**[ワークフロー（Workflows）]** で、**[Cisco クラウド ネットワーク コントローラの設定（Cisco Cloud Network Controller Setup）]**をクリックします。**[セットアップ - 概要（Setup - Overview）]** ダイアログ ボックスが表示されます。

ステップ 3 詳細設定内で**[構成を編集（Edit Configurations）]**をクリックします。**[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、**[はい（Yes）]**または、**[いいえ（No）]**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。

- **[いいえ（No）]**:デフォルト設定。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。
- **[はい（Yes）]**: 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。有効に設定されている場合、ルート マップが構成されていないときに、ドライブ回送を契約します。ルート マップが存在するときに、ルート マップは常にドライブ回送です。

ステップ 4 **[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スイッチする場合は、次の手順に従います。

- **はい設定からいいえへのスイッチ (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スイッチす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スイッチする前にルート マップ ベースのルーティングが構成されていない場合、これは混乱を招く可能性があります。

  この状況で**[はい（Yes）]**設定から**[いいえ（No）]**設定にスイッチする前に、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 Network Controller GUI を使用したリーク ルートの構成 （67 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] フィールドを **[はい（Yes）]** 設定から **[いいえ（No）]** 設定にスイッチして、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スイッチします。

  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。

- **いいえ設定からはいへのスイッチ (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スイッチす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、**[いいえ（No）]**設定から**[はい（Yes）]**設定にスイッチす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**[はい（Yes）]**設定にスイッチする前に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 5 **[コントラクト ベースのルーティング]** エリア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スイッチします。

ステップ 6 **[Cisco クラウド ネットワーク コントローラ セットアップ（Cisco Cloud Network Controller Setup）]** の構成が完了したら、**[保存して継続（Save and Continue）]** をクリックします。

Cisco Cloud Network Controller GUI を使用したリーク ルートの構成

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

- 25.0(2) より前のリリースでは、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先の間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。これらの手順については、Cisco Cloud Network Controller GUI を使用した VRF 間ルート リークの構成 （67 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 Network Controller GUI を使用した内部 VRF のリーク ルートの構成 （71 ページ） を参照してください。

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

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（5 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 （73 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 Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *7:* リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）

[プロパティ（Properties）]	説明
Source VRF	送信元 VRF を選択するには： 1. **[送信元 VRF の選択（Select Source VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。 送信元 VRF は、内部または 外部 VRF であることに注意してください。 3. **[選択（Select）]** をクリックして、この送信元 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。

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

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

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

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

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （68 ページ）ーステップ 5 （69 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 （68 ページ）ーステップ 5 （69 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 （68 ページ） の情報を使用して、必要な情報を入力します。**送信元VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

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

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （68 ページ） の情報を使用して、必要な情報を入力します。**宛先VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

次のタスク

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

- Cisco Cloud Network Controller GUI を使用した EPG の作成 （78 ページ）：次の手順を使用して、外部 EPG を作成します。
- Cisco Cloud Network Controller GUI を使用したコントラクトの作成 （84 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 Network Controller 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 （8 ページ） で説明されているように、内部 VRF のペア間のルート マップベースのルート リークがサポートされます。この機能は、リリース 25.0(1) で提供されたルーティングとセキュリティの分割更新を拡張したもので、ルーティングとセキュリティ ポリシーが別々に設定されています。

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

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

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

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

表 *8 :* リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）

[プロパティ（Properties）]	説明
Source VRF	送信元 VRF を選択するには： 1. **[送信元 VRF の選択（Select Source VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続元 VRF には内部 VRF を選択します。 3. **[選択（Select）]** をクリックして、この送信元 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。

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

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

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

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

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （71 ページ）ーステップ 5 （72 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 （71 ページ）ーステップ 5 （72 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 （71 ページ）の情報を使用して、必要な情報を入力します。**送信元VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

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

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （71 ページ）の情報を使用して、必要な情報を入力します。**宛先VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

AWS サイトと外部デバイスの間の接続の有効化

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 Network Controller GUI で、**[ダッシュボード（Dashboard）]** をクリックします。
Cisco Cloud Network Controller の **[ダッシュボード（Dashboard）]** ビューが表示されます。

ステップ 2 **[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 外部ネットワーキング デバイスを接続するための構成情報を入力します。

外部デバイス構成ファイルのダウンロード （73 ページ） の手順を使用して外部デバイス構成ファイルをダウンロードした場合、最初のトンネルの構成情報を見つけて、その構成情報を入力します。

最初のトンネルの外部デバイス設定ファイルの例を示します。

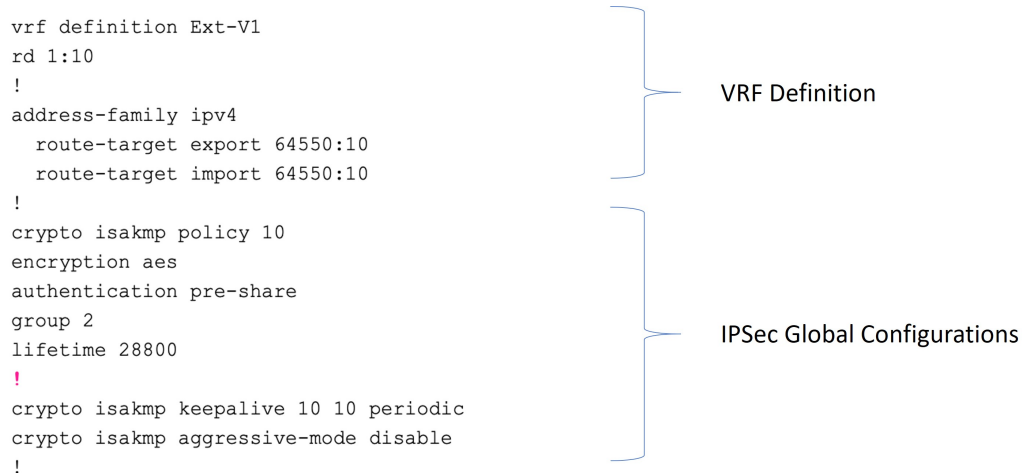
```
! The following file contains configuration recommendation to connect an external networking device
 with the cloud ACI Fabric
! The configurations here are provided for an IOS-XE based device. The user is expected to understand
 the configs and make any necessary amends before using them
! on the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

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

vrf definition infra:externalvrf1
    rd 1:1
```

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

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

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

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

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

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

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

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

ip route 13.88.168.176 255.255.255.255 GigabitEthernet2 GIG-GATEWAY

router bgp 65015

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

    neighbor 5.16.1.9 remote-as 65008
```

```
    neighbor 5.16.1.9 ebgp-multihop 255
    neighbor 5.16.1.9 activate
    neighbor 5.16.1.9 send-community both

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

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

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



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

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

IPSec and Ikev1
Per Tunnel Configurations

BGP Configurations for VRF Neighbor

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

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

Ikev2 Global Configurations

IPSec and Ikev2
Per Tunnel Configurations

ステップ 4 前の手順を繰り返して、追加のトンネルを構成します。

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

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

始める前に

アプリケーション プロファイルと VRF を作成します。

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

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

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

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

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

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

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

[プロパティ（Properties）]	説明
アプリケーション プロファイル	アプリケーション プロファイルを選択します。 1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。 2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーションプロファイルをクリックして、**[選択]** 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	EPG タイプを選択します。 • **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。
ルート到達可能性	(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。 • **オンプレミス** • **インターネット** • **[Unspecified]**
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]**をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
エンドポイントセレクタ	

[プロパティ（Properties）]	説明
	（注） エンドポイント セレクタ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 （95 ページ） を参照してください。 エンドポイント セレクタを追加するには： 1. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックして、**[エンドポイント セレクタの追加]** ダイアログを開きます。 2. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ダイアログの **[Name（名前）]** フィールドに名前を入力します。 3. **[セレクタ式（Selector Expression）]** をクリックします。**[キー（Key）]**、**[演算子（Operator）]**、および **[値（Value）]** フィールドが有効になります。 4. **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。次のオプションがあります。 • エンドポイント セレクタに IP アドレスまたはサブネットを使用する場合は、**[IP]** を選択します。 • エンドポイント セレクタにアベイラビリティ 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。 （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**）。

[プロパティ（Properties）]	説明
	5. **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。次のオプションがあります。 • **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。 • **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。 • **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。 • **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。 • **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。 • **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。 **6.** **[値（Value）]** フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。入力する値は、**[キー（Key）]** フィールドと **[演算子（Operator）]** フィールドで選択した内容によって異なります。たとえば、**[キー（Key）]** フィールドが **[IP]** に設定され、**[演算子（Operator）]** フィールドが **[等しい（equals）]** に設定されている場合、**[値（Value）]** フィールドはIPアドレスまたはサブネットでなければなりません。ただし、**[演算子（Operator）]** フィールドが **[キー（keys）]** に設定されている場合、**[値（Value）]** フィールドは無効になります。 **7.** 完了したら、チェックマークをクリックしてセレクタ式を検証します。

[プロパティ（Properties）]	説明
	8. エンドポイント セレクタに追加のエンドポイント セレクタ式を作成するかどうかを決定します。単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理ANDがあるものとみなされます。 たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。 • エンドポイント セレクタ 1、式 1: • **[キー (Key):]** 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: • **[キー (Key):]** IP • **演算子 (Operator）**： equals • **[値 (Value):]** 192.0.2.1/24 この場合、これらの式の両方が真になる場合(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。

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

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したコントラクトの作成

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

始める前に

フィルタを作成します。

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

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

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

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

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

表 *10 : [*コントラクトの作成（*Create Contract*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	契約の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。
説明	コントラクトの説明を入力してください。
[設定（Settings）]	

[プロパティ（Properties）]	説明
スコープ	このスコープは、同じアプリケーションプロファイル内、同じVRFインスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイント グループにコントラクトを制限します。 （注） 共有サービスにより、異なるテナントのEPG間および異なるVRFのEPG間の通信が可能になります。 1つのテナントのEPGが別のテナントのEPGと通信できるようにするには、**[グローバル（Global）]** スコープを選択します。 1つのVRFのEPGが別のVRFの別のEPGと通信できるようにするには、**[グローバル（Global）]** または **[テナント（Tenant）]** スコープを選択します。 共有サービスの詳細については、共有サービス （44 ページ） を参照してください。 ドロップダウン矢印をクリックして、次のスコープオプションから選択します。 • **アプリケーション プロファイル** • **VRF** • **Global** • **テナント**
フィルタを両方向に適用	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を適用する場合は、ボックスにチェックを入れないでください。 デフォルトでチェックボックスはオンになっています。

[プロパティ（Properties）]	説明
フィルタの追加	フィルタを選択します。 1. [フィルタの追加（Add Filter）] をクリックします。フィルタ行が表示され、**[フィルタの選択（Select Filter）]** オプションが表示されます。 2. **[フィルタの選択（Select Filter）]** をクリックします。**[フィルタの選択（Select Filter）]** ダイアログボックスが表示されます。 3. **[フィルタの選択（Select Filter）]** ダイアログで、左側の列のフィルタをクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller 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 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。**[ワークフロー（Workflows）]** で、**[EPG 通信（EPG Communication）]** をクリックします。**[EPG通信（EPG Communication）]** ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

ステップ 3 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 4 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 5 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 Network Controller GUI を使用したフィルタの作成

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

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

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

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

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

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

表 *11* : フィルタの作成ダイアログボックスのフィールド

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

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

[プロパティ（Properties）]	説明
Add Filter	

[プロパティ（Properties）]	説明
	フィルタを追加するには、次の手順を実行します。 1. **[フィルタ エントリの追加（Add Filter Entry）]** をクリックします。**[フィルタ 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。 • **IP** • **[Unspecified]** （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。 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。 • **icmp** • **tcp** • **udp** • **[Unspecified]** （注） 残りのフィールドは、**tcp** または **udp** が選択されている場合にのみ有効になります。 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
	フィールドに適切なポート情報を入力します。 8. フィルタ エントリ情報の入力が完了したら、**[追加（Add）]** をクリックします。**[フィルタの作成（Create Filter）]** ダイアログボックスに戻り、別のフィルタ エントリを追加する手順を繰り返すことができます。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。

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

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

始める前に

VRF を作成します。

ステップ 1 **[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 Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *12*：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	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
説明	（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	リージョンを選択するには: 1. **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。 2. **[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
VRFの選択(Select VRF)	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
CIDR の追加（Add CIDR）	（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。 • 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） CIDR を追加するには、次の手順を実行します。 **1.** **[CIDR の追加（Add CIDR）]** をクリックします。**[CIDR の追加（Add CIDR）]** ダイアログボックスが表示されます。 **2.** **[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: **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。 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 （30 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 Network Controller のためのエンドポイント セレクタを構成するとき Cisco Cloud Network Controller のために構成するエンドポイント セレクタに対応する AWS で必要なインスタンスについても構成することが必要になります。

このトピックでは、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 Network Controller のためのエンドポイント セレクタを設定する前に、または後で、これらの手順を使用して AWS のインスタンスを構成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 Network Controller のカスタム タグまたはラベルを使用して、エンドポイント セレクタを作成することができます。または、 Cisco Cloud Network Controller でカスタムタグまたはラベルを使用してエンドポイント セレクタを作成してから、AWS のアカウントに移動し、以降の 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 Network Controller 用に作成したクラウド コンテキスト プロファイルのリストが表示されます。

c) この 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 Network Controller ユーザー 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 Network Controller 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 セレ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 Network Controller 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 セレ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、エンドポイントセレ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 Network Controller GUI を使用したバックアップ構成の作成

ここでは、バックアップ構成を作成する方法を説明します。

始める前に

必要に応じて、リモート ロケーションとスケジューラを作成します。

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

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

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

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

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

表 *13*：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	

[プロパティ（**Properties**）]	説明
Backup Destination	バックアップ接続先を選択します。 • **Local** • **[リモート（Remote）]**

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

[プロパティ（Properties）]	説明
	バックアップで考慮するルート階層コンテンツを選択します • ポリシー ユニバース • セレクタオブジェクト（Selector Object）：これを選択すると、[オブジェクトタイプ（Object Type）] ドロップダウンリストと [オブジェクト DN（Object DN）] フィールドが追加されます。 1. オブジェクトタイプ（Object Type）ドロップダウン リストで、次のオプションから選択します。 • テナント（Tenant）：選択すると、[テナントの選択（Select Tenant）] オプションが表示されます。 • アプリケーション プロファイル（Application Profile）：選択すると、[アプリケーション プロファイルの選択（Select Application Profile）] オプションが表示されます。 • EPG：これを選択すると [EPG の選択（Select EPG）] オプションが表示されます。 • コントラクト（Contract）：これを選択すると、[コントラクトの選択（Select Contract）] オプションが表示されます。 • フィルタ（Filter）：これを選択すると、[フィルタの選択（Select Filter）] オプションが表示されます。 • VRF：これを選択すると、[VRFの選択（Select VRF）] オプションが表示されます。 • デバイス：[SelectfvcloudLBCtx] プションが表示されます。 • サービス グラフ：選択すると、[Select Service Graph] オプションが表示されます。 • [クラウド コンテキスト プロファイル（Cloud Context Profile）]：これを選

[プロパティ（Properties）]	説明
	択すると、**[クラウド コンテキスト プロファイルの選択**（Select Cloud Context Profile）]オプションが表示されます。 2. **Select <object_name>** をクリックjします。**Select <object_name>** ダイアログが表示されます。 3. **Select <object_name>** ダイアログから左側の列のオプションからクリックして選んで、**[選択（Select）]** をクリックします。**[バックアップ構成の作成（Create Backup Configuration）]** ダイアログ ボックスに戻ります。 （注） **[オブジェクトDN（Object DN）]** フィールドには、バックアップするオブジェクト ツリーのルートとして使用するオブジェクトの DN が自動的に入力されます。 • **DN の入力（Enter DN）**：このオプションを選択すると、**[オブジェクト DN（Object DN）]** フィールドが表示されます。 1. **[オブジェクトDN（Object DN）]** フィールドに、バックアップするオブジェクト ツリーのルートとして使用する特定のオブジェクトの DN を入力します。
スケジューラ	1. **[スケジューラの選択（Select Scheduler）]** をクリックして **[スケジューラの選択（Select Scheduler）]** ダイアログを開き、左側の列からスケジューラを選択します。 2. 終了したら、右下隅にある **[選択（Select）]** ボタンをクリックします。

[プロパティ（Properties）]	説明
作成後のバックアップのトリガー	次のいずれかを選択します。 • はい（Yes）：（デフォルト）バックアップ設定の作成後にバックアップをトリガーします。 • いいえ（No）：バックアップ設定の作成後にバックアップをトリガーしません。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したテクニカル サポート ポリシーの作成

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

始める前に

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

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

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

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

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

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

表 *14 :* テクニカル サポートの作成ダイアログボックスのフィールド

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

[プロパティ（Properties）]	説明
エクスポート先	エクスポート先を選択します。 • コントローラ • [リモート ロケーション（Remote Location）]：選択すると、[リモート ロケーションの選択（Select Remote Location）] オプションが表示されます。 1. [リモート ロケーションの選択（Select Remote Location）] をクリックします。[リモート ロケーションの選択（Select Remote Location）] ダイアログボックスが表示されます。 2. [[リモート ロケーションの選択（Select Remote Location）] ダイアログで、左側の列のリモート ロケーションをクリックして選択し、[選択（Select）] をクリックします。[テクニカル サポートの作成（Create Tech Support）] ダイアログボックスに戻ります。
アップグレード前のログを含める	テクニカル サポート ポリシーにアップグレード前のログを含める場合は、[有効（Enabled）] チェックボックスをオンにします。
作成後のトリガー	ポリシーの作成後にテクニカル サポート ポリシーを作成する場合は、[有効] (デフォルト) チェックボックスをクリックしてオンにします。無効にするには、チェックボックスをオフにします。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller 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 Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *15 :* 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	**[繰り返しウィンドウの追加（Add Recurring Window）]** をクリックします。**[繰り返しウィンドウの追加（Add Recurring Window）]** ダイアログ ウィンドウが表示されます。 1. **[スケジュール（Schedule）]** ドロップダウンリストから、次のいずれかを選択します。 • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日 2. **[開始時間（Start Time）]** フィールドに、時間を入力します。 3. **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドから数値を入力するか、フィールドを空白のままにして無制限を指定します。 4. **[最大実行時間（Maximum Running Time）]** で、**[無制限（Unlimited）]** または **[カスタム（Custom）]** をクリックして選択します。 5. 終了したら、[Add] をクリックします。

[プロパティ（Properties）]	説明
ワンタイム ウィンドウの追加	[ワンタイムウィンドウの追加（Add One Time Window）] をクリックします。[ワンタイムウィンドウの追加（Add One Time Window）] ダイアログが表示されます。 1. [開始時間（Start Time）] フィールドに、時間を入力します。 2. [最大同時タスク数（Maximum Concurrent Tasks）] フィールドに数値を入力するか、フィールドを空白のままにして無制限を指定します。 3. [最大実行時間（Maximum Running Time）] で、[無制限（Unlimited）] または [カスタム（Custom）] をクリックして選択します。 4. 終了したら、[Add] をクリックします。

ステップ 5 設定が終わったら [Save] をクリックします。

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

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

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

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

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

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

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

表 *16 :* リモート ロケーションの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	

[プロパティ（Properties）]	説明
名前	リモート ロケーション ポリシーの名前を入力します。
説明	リモート ロケーション ポリシーの説明を入力します。
Settings	
Hostname/IP Address	リモート ロケーションのホスト名または IP アドレスを入力します
Protocol	プロトコルを選択します。 • **FTP** • **SFTP** • **SCP**
Path	リモート ロケーションのパスを入力します。
Port	リモート ロケーションのポートを入力します。
Username	リモートロケーションのユーザー名を入力します。
認証タイプ	SFTP または SCP を使用する場合は、認証タイプを選択します。 • **[Password]** • **SSH キー（SSH Key）**
SSH キー コンテンツ	SSH キーのコンテンツを入力します。
SSH キー パスフレーズ	SSH キー パスフレーズ
Password	リモート ロケーションにアクセスするためのパスワードを入力します。
Confirm Password	リモート ロケーションにアクセスするためのパスワードを再入力します。
管理EPG	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 Network Controller GUI を使用したログイン ドメインの作成

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

始める前に

非ローカルドメインを作成する前に、プロバイダーを作成します。

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

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

[Intent]メニューに管理オプションのリストが表示されます。

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

ステップ 4 次の *[ログイン ドメインダイアログボックスのフィールド（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 *17:* ログイン ドメインダイアログボックスの作成のフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	ログイン ドメインの名前を入力します。
説明	ログイン ドメインの説明を入力します。
レルム	レルムを選択します。 • **Local** • **LDAP**：プロバイダーを追加し、認証タイプを選択する必要があります。 • **RADIUS**：プロバイダーを追加する必要があります。 • **TACACS+**：プロバイダーの追加が必要です。 • **SAML**：プロバイダーの追加が必要です。

[プロパティ（Properties）]	説明
プロバイダ	プロバイダーを追加するには、次の手順を実行します。 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. クリックしてプロバイダーを選択します。 3. **[選択 (Select)]** をクリックして、プロバイダを追加します。
詳細設定	**[認証タイプ（Authentication Type）]** および **[LDAP グループ マップ ルール（LDAP Group Map Rules）]** フィールドを表示します。
認証タイプ	レルム オプションにLDAP を選択した場合は、次のいずれかの認証タイプを選択します。 • **Cisco AV ペア**：（デフォルト） • **LDAP グループ マップ ルール**：LDAP グループ マップ ルールを追加する必要があります。

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

[プロパティ（Properties）]	説明
	LDAP グループ マップ ルールを追加するには、次の手順を実行します。 1. **[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. **[名前（Name）]** フィールドに、ルールの名前を入力します。 3. **[説明（Description）]** フィールドに、ルールの説明を入力します。 4. **[グループ DN（Group DN）]** フィールドにルールのグループ DN を入力します。 5. セキュリティ ドメインの追加： 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。 2. **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。 3. セキュリティ ドメインをクリックして選択します。 4. **[選択（Select）]** をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）] ダイアログボックスに戻ります。** 5. ユーザー ロールを追加する: 1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログボックスが表示され、左側のペインにロールのリストが表

[プロパティ（Properties）]	説明
	示されます。 2. クリックしてロールを選択します。 3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。 4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスから、**[権限タイプ（Privilege Type）]** ドロップダウンリストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。 5. **[権限タイプ（Privilege Type）]** ドロップダウン リストの右側のチェックマークをクリックして、確認します。 6. 終了したら、[Add] をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログボックスに戻り、別のセキュリティドメインを追加できます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したプロバイダーの作成

このセクションでは、Cisco Cloud Network Controller 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 Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *18 :* 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（Hostname/IP Address）]	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	**[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。 • **LDAP** • **RADIUS** • **TACACS+** • **SAML** （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。
[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。デフォルトでは有効になっています。

[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。 • 許可（Permissive） • Strict
[属性（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。 • 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: 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。
サーバーモニターリング	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。デフォルトでは無効になっています。
[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。 • **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 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: 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。
サーバーモニターリング	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。デフォルトでは無効になっています。
[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。 • **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 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: 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。
サーバーモニターリング	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。デフォルトでは無効になっています。
[SAML] 設定	
ID プロバイダ	次のアイデンティティ プロバイダーから選択します。 • **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	認証局を選択するには： 1. **[認証局の選択（Select Certificate Authority）]** をクリックします。**[認証局の選択（Select Certificate Authority）]** ダイアログが表示され、左側のペインに証明書の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 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）]	**[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。 • **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。デフォルトでは有効になっています。

[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。デフォルトでは有効になっています。
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。デフォルトでは有効になっています。
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。デフォルトでは有効になっています。

ステップ 5 設定が終わったら [Save] をクリックします。

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

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

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

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

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 [Intent]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 Network Controller GUI を使用したロールの作成

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

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

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

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[Intent]** メニューの **[Administrative]** リストで、**[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。**[ロールの作成（Create Role）]** ダイアログ ボックスが表示されます。

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

表 *19 :* ロールの作成ダイアログボックスのフィールド

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

[プロパティ（Properties）]	説明
特権	

[プロパティ（Properties）]	説明
	クリックして、ユーザに割り当てる権限のチェックボックスをオンにします。権限は次のとおりです。 • **aaa**：認証、許可、アカウンティング、インポート/エクスポート ポリシーの設定に使用されます。 • **access-connectivity-l1** インフラの下のレイヤ 1 設定に使用されます。例：セレクタとポート レイヤ 1 のポリシー設定。 • **access-connectivity-l2** ：インフラの下のレイヤ 2 設定に使用されます。例：セレクタおよび接続可能なエンティティ設定をカプセル化します。 • **access-connectivity**：インフラでのレイヤ 3 の設定、テナントの L3Out でのスタティック ルート設定に使用されます。 • **access-connectivity-mgmt** ：管理インフラ ポリシーに使用されます。 • **access-connectivity-util** ：テナント ERSPAN ポリシーに使用されます。 • **access-equipment**：アクセスポートの設定に使用されます。 • **access-protocol-l1** ：インフラのレイヤ 1 プロトコル設定に使用されます。 • **access-protocol-l2** ：インフラのレイヤ 2 プロトコル設定に使用されます。 • **access-protocol-l3** ：インフラでのレイヤ 3 プロトコル設定に使用されます。 • **access-protocol-mgmt** ：NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • **access-protocol-ops** ：クラスタ ポリシーやファームウェア ポリシーなどの操作関連のアクセス ポリシーに使用されます。 • **access-protocol-util** ：テナント ERSPAN ポリシーに使用されます。 • **access-qos**：CoPP および QoS に関連するポリシーの変更に使用されます。

[プロパティ（Properties）]	説明
	• **admin**：すべてへのアクセス（すべてのロールの組み合わせ） • **fabric-connectivity-l1** ：ファブリックの下のレイヤ 1 設定に使用されます。例：セレクタおよびポート 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
	• **nw-svc-device** ：レイヤ 4 からレイヤ 7 のサービス デバイスを管理するために使用されます。 • **nw-svc-devshare** ：共有レイヤ 4 ～ レイヤ 7 サービス デバイスの管理に使用されます。 • **nw-svc-params**：レイヤ 4 ～ レイヤ 7 のサービス ポリシーの管理に使用されます。 • **nw-svc-policy**：レイヤ 4 ～ レイヤ 7 のネットワーク サービス オーケストレーションの管理に使用されます。 • **ops**：アトミック カウンタ、SPAN、TSW、技術サポート、トレースルート、分析、コア ポリシーなど、ポリシーのモニタリングとトラブルシューティングを含む動作ポリシーに使用されます。 • **tenant-connectivity-l1** ：ブリッジ ドメインやサブネットなど、レイヤ 1 接続の変更に使用されます。 • **tenant-connectivity-l2** ：ブリッジ ドメインやサブネットなど、レイヤ 2 接続の変更に使用されます。 • **tenant-connectivity-l3** ：VRF を含むレイヤ 3 接続の変更に使用されます。 • **tenant-connectivity-mgmt** ：テナントのインバンドおよびアウトオブバンドの管理接続構成、およびアトミック カウンターやヘルス スコアなどのポリシーのデバッグ/監視に使用されます。 • **tenant-connectivity-util**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • **tenant-epg**：エンドポイント グループ、VRF、ブリッジ ドメインの削除/作成など、テナント設定の管理に使用されます。 • **tenant-ext-connectivity-l2**：テナントの L2Out 構成を管理するために使用されます。 • **tenant-ext-connectivity-l3**：テナント L3Out 構成の管理に使用されます。

[プロパティ（Properties）]	説明
	• **tenant-ext-connectivity-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。 • **tenant-ext-connectivity-util** ： traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-ext-protocol-l1**：テナントの外部レイヤ 1 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。 • **tenant-ext-protocol-l2** ：テナントの外部レイヤ 2 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。 • **tenant-ext-protocol-l3** ：BGP、OSPF、PIM、IGMP などのテナントの外部レイヤ 3 プロトコルを管理するために使用されます。 • **tenant-ext-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。 • **tenant-ext-protocol-util**：traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-network-profile**：ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。 • **tenant-protocol-l1** ：テナントの下でレイヤ 1 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-l2** ：テナントの下でレイヤ 2 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-l3** ：テナントの下でレイヤ 3 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。

[プロパティ（Properties）]	説明
	• **tenant-protocol-ops** ：テナント traceroute ポリシーに使用されます。 • **tenant-protocol-util** — traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-qos**：ファームウェア ポリシーの書き込みアクセスとしてのみ使用されます。 • **tenant-security**：テナントの契約関連の設定に使用されます。 • **vmm-connectivity**：VM 接続に必要な APIC の VMM インベントリ内のすべてのオブジェクトを読み取るために使用されます。 • **vmm-ep**：APIC の VMM インベントリ内の VM およびハイパーバイザーエンドポイントを読み取るために使用されます。 • **vmm-policy**：VM ネットワーキングのポリシーの管理に使用されます。 • **vmm-protocol-ops**：VMM ポリシーでは使用されません。 • **vmm-security**：テナントの契約関連の設定に使用されます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller 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。

a) **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログ ボックスが表示されます。

b) **[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログで、左側の列のセキュリティ ドメインをクリックして選択し、**[選択（Select）]** をクリックします。**[RBAC ルールの作成]** ダイアログ ボックスに戻ります。

ステップ 6 **[書き込みを許可]** フィールドで、**[はい]** をクリックして書き込みを許可するか、**[いいえ]** をクリックして書き込みを許可しません。

ステップ 7 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用した認証局の作成

ここでは、GUI を使用して認証局を作成する方法について説明します。

始める前に

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

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

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

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

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[証明書認証局の作成（Create Certificate Authority）]** をクリックします。**[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスが表示されます。

ステップ 4 *[*証明書認証局の作成ダイアログボックスのフィールド（*Create Certificate Authority Dialog Box Fields*）*]* のテーブルにリストされた各フィールドに適切な値を入力して、続行します。

表 *20 :* 証明書認証局の作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	証明書認証局の名前を入力してください。
説明	証明書認証局の説明を入力してください。

[プロパティ（Properties）]	説明
用途	次のオプションから選択します。 • テナント（Tenant）：認証局が特定のテナント用かどうかを選択します。選択すると、[テナントの選択（Select Tenant）] オプションがGUIに表示されます。 • システム（System）：認証局がシステム用である場合に選択します。
テナントの選択	テナントを選択します。 1. [テナントの選択（Select Tenant）] をクリックします。[テナントの選択（Select Tenant）] ダイアログボックスが表示されます。 2. [テナントの選択（Select Tenant）] ダイアログで、左側の列のテナントをクリックして選択し、[選択（Select）] をクリックします。[証明書認証局の作成（Create Certificate Authority）] ダイアログボックスが表示されます。
Certificate Chain	[証明書チェーン (Certificate Chain)] フィールドに、証明書チェーンを入力します。 （注） チェーンの証明書を次の順序で追加します。 1. CA 2. Sub-CA 3. サブサブCA 4. サーバー

ステップ 5 設定が終わったら [Save] をクリックします。

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

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

始める前に

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

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

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

[Intent]メニューに管理オプションのリストが表示されます。

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

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

表 ***21 :*** キー リングの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（**Name**）	キー リングの名前を入力します。
説明	キー リングの説明を入力します。
用途	• **System**：キー リングはシステム用です。 • **Tenant**：キー リングは特定のテナント用です。テナントを指定する **[テナント（Tenant）]** フィールドを表示します。
テナントの選択	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。
Settings	

[プロパティ（Properties）]	説明
認証局	認証局を選択するには： 1. **[認証局の選択（Select Certificate Authority）]** をクリックします。**[認証局の選択（Select Certificate Authority）]** ダイアログが表示されます。 2. 左側の列で認証局をクリックして選択します。 3. **[選択（Select）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。
秘密キー（Private Key）	次のいずれかを選択します。 • **[新しいキーの生成（Generate New Key）]**：新しいキーを生成します。 • **[既存のキーのインポート（Import Existing Key）]**：**[秘密キー（Private Key）]** テキスト ボックスが表示され、既存のキーを使用できます。
秘密キー（Private Key）	**[秘密キー（Private Key）]** テキスト ボックスに既存のキーを入力します（**[既存のキーのインポート（Import Existing Key）]** オプションの場合）。
Modulus	**[モジュール（Modulus）]** ドロップダウン リストをクリックし、次の項目の中から選択します。 • **MOD 512** • **MOD 1024** • **MOD 1536** • **MOD 2048**：デフォルト
証明書	**[証明書（Certificate）]** テキスト ボックスに証明書情報を入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したローカル ユーザーの作成

このセクションでは、Cisco Cloud Network Controller GUI を使用してローカル ユーザーを作成する例を示します。

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

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

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ローカル ユーザーの作成（Create Local User）]** をクリックします。**[ローカル ユーザーの作成（Create New User）]** ダイアログボックスが表示されます。

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

表 *22 :* 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。 • **Active**：ローカル ユーザー アカウントをアクティブにします。 • **Inactive**：ローカル ユーザー アカウントを非アクティブにします。
[名（First Name）]	ローカル ユーザーの名を入力します。
姓（Last Name）	ローカル ユーザーの姓を入力します。
電子メール アドレス（Email Address）	ローカル ユーザーの E メール アドレスを入力します。
Phone Number	ローカル ユーザーの 電話番号を入力します。

[プロパティ（**Properties**）]	説明
セキュリティ ドメイン	

[プロパティ（Properties）]	説明
	セキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]**をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。 2. **[セキュリティ ドメインの選択（Select Security Domain）]**をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。 3. セキュリティ ドメインをクリックして選択します。 4. **[選択（Select）]**をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]ダイアログボックスに戻ります。** 5. ユーザー ロールを追加する: 1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログ ボックスが表示され、左側のペインにロールのリストが表示されます。 2. クリックしてロールを選択します。 3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。 4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスから、**[権限タイプ（Privilege Type）]** ドロップダウン リストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。 5. **[権限タイプ（Privilege Type）]** ドロップダウンリストの右側のチェックマークをクリッ

[プロパティ（Properties）]	説明
	クして、確認します。 6. 終了したら、[Add]をクリックします。**[ローカル ユーザーの作成（Create Local User）]** ダイアログボックスに戻り、別のセキュリティ ドメインを追加できます。

ステップ 5 **[高度な設定（Advanced Settings）]**をクリックして、*[*ローカルユーザーの作成ダイアログボックスのフィールド：高度な設定（*Create Local User Dailog Box Fields: Advanced Settings*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *23 :* ローカル ユーザーの作成ダイアログボックスのフィールド：高度な設定

プロパティ	説明
Account Expires	**[はい（Yes）]**を選択すると、アカウントは選択した時点で期限切れになるように設定されます。
パスワードの更新が必要です	**[はい（Yes）]**を選択した場合、ユーザーは次回ログイン時にパスワードを変更する必要があります。
OTP	ユーザーのワンタイムパスワード機能を有効にするには、チェックボックスをオンにします。
ユーザー証明書	ユーザー証明書を追加するには、次の手順を実行します。 1. **[X509 証明書の追加（Add X509 Certificate）]**をクリックします。**[X509 証明書の追加（Add X509 Certificate）]** ダイアログボックスが表示されます。 2. [Name] フィールドに名前を入力します。 3. **[ユーザー X509 証明書（User X509 Certificate）]** テキストボックスにX509証明書を入力します。 4. [Add] をクリックします。**[ユーザー X509 証明書の X509 証明書]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。

プロパティ	説明
SSH キー	SSH キーを追加するには、次の手順を実行します。 1. **[SSH キーを追加（Add SSG Key）]** をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが表示されます。 2. [Name] フィールドに名前を入力します。 3. **[キー（Key）]** テキストボックスに SSH キーを入力します。 4. [Add] をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。

ステップ 6 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したリージョンの管理（クラウド テンプレートの構成）

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 Network Controller 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 Network Controller 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 （39 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 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。**[ワークフロー（Workflows）]** で、**[Cisco クラウド ネットワーク コントローラの設定（Cisco Cloud Network Controller Setup）]**をクリックします。**[設定-概要（Set up-Overview）]** ダイアログボックスが表示され、**[DNS と NTPサーバー（DNS and NTP Servers）]**、**[リージョン管理（Region Management）]**、**[詳細設定（Advanced Settings）]** と **[スマート ライセンシング（Smart Licensing）]** のオプションが示されます。

ステップ 3 **[リージョン管理（Region Management）]** 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 4 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（Inter-Site Connectivity）]**の手順が追加されます。

ステップ 5 Cisco Cloud Network Controller 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 6 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 7 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（Setup- Region Management）]の一連のステップの次のステップである、**[一般的な接続（General Connectivity）]**が表示されます。

ステップ 8 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） Cisco クラウド Network Controller 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 9 **[CCR 用 BGP自律システム番号（BGP Autonomous System Number for CCRs）]** フィールドに値を入力します。

BGP ASN の範囲は 1 ー 65534 です。

ステップ 10 **[パブリック IP の CCR インターフェイスへの割り当て（Assign Public IP to CCR Interface）]** フィールドで、パブリック IP アドレスを Catalyst 8000V インターフェイスに割り当てるかどうかを決定します。

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

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

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

Catalyst 8000V 接続をプライベートからパブリック、またはその逆に変更すると、ネットワークが中断する可能性があることに注意してください。

（注） 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 11 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 12 **[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 13 **[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 14 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。
- Cisco Catalyst 8000V のスループット値については、About the Cisco Catalyst 8000V （23 ページ） を参照してください。

ステップ 15 (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）
- Cisco Catalyst 8000V のライセンス情報については、About the Cisco Catalyst 8000V （23 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 10 （135 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 16 [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 17 （136 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 21 （137 ページ） に進みます。

ステップ 17 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 18 **[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 19 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 20 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 21　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 Network Controller 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 Network Controller のコントラクトを作成する方法を示します。

始める前に

フィルタを作成します。

コントラクトを作成するには：

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。

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、次の例のようなポストを入力します。

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する場合、**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 （30 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>
    <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:msc" >
      <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:msc" >
      <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 （39 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、Cisco Catalyst 8000V は **BYOL** で Cisco Cloud Network Controller に展開されます。`[routerThroughput]` 値が **[PAYG]** の場合、Cisco Catalyst 8000V は **PAYG** で Cisco Cloud Network Controller に展開されます。

ステップ 1 **BYOL** の Cisco Catalyst 8000V を展開するためのクラウドテンプレートを作成するには、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"/>

      <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） Tier2（T2）は、Cisco Cloud Network Controller 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** の Cisco Catalyst 8000V を展開するためのクラウドテンプレートを作成するには、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="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、 vmNames のリストから **vmName** も選択する必要があります。これは、Cisco Cloud Network Controller によってすでに作成され、管理対象オブジェクト `cloudProvVmType` によって表されているものです。

次の表に、`cloudtemplateProfile` のプロパティ `vmName` によって示される vmNamesTypes 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 （8 ページ） と グローバルな Inter-VRF ルート リーク ポリシー （9 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。有効に設定されている場合、ルートマップが構成されていないときに、ドライブ回送を契約します。ルートマップが存在するときに、ルート マップは常にドライブ回送です。
- **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>
```

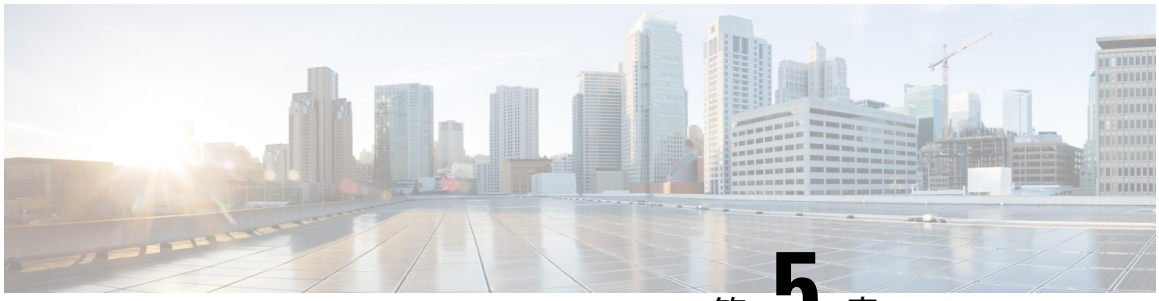
REST API を使用したトンネルのソース インターフェイス選択の構成

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 （10 ページ） に記載されている情報を確認してください。

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

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

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

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

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



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

Prometheus ノードエクスポータを使用して Cisco クラウド ネットワーク コントローラが導入されている VM ホストのメトリックのモニタリングがサポートされます。Prometheus Node Exporter は、さまざまなハードウェアおよびカーネル関連のメトリックを可視化し、Linux ノードから CPU、ディスク、メモリの統計情報などの技術情報を収集します。Prometheus ノードエクスポータの概要については、以下を参照してください。

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

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

注意事項と制約事項

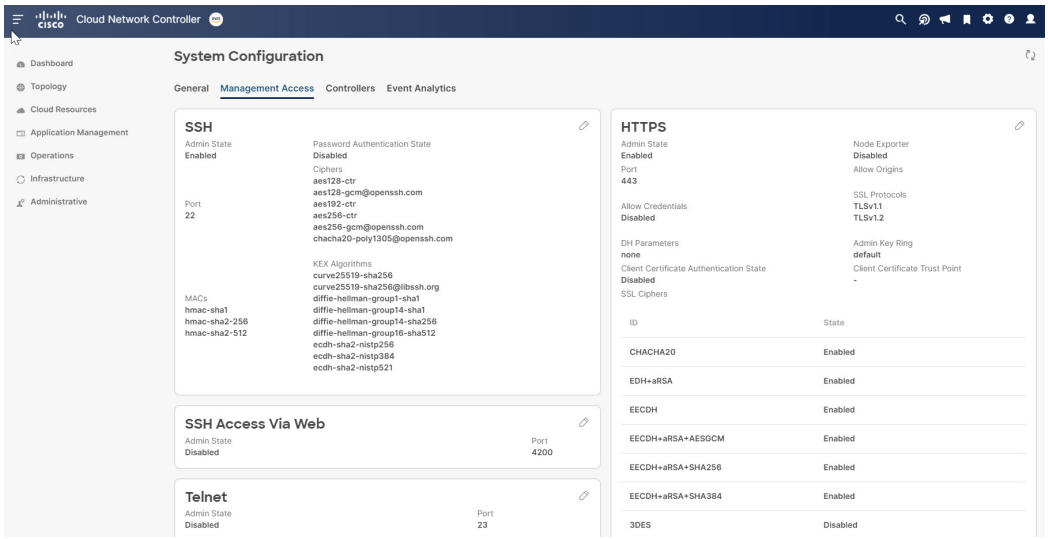
HTTP は、Prometheus Node Exporter を使用したモニタリング メトリックではサポートされていません。Prometheus Node Exporter を使用したメトリックのモニタリングでは、HTTPS のみがサポートされます。

GUI を使用した VM ホストメトリックのモニタリング

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

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

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

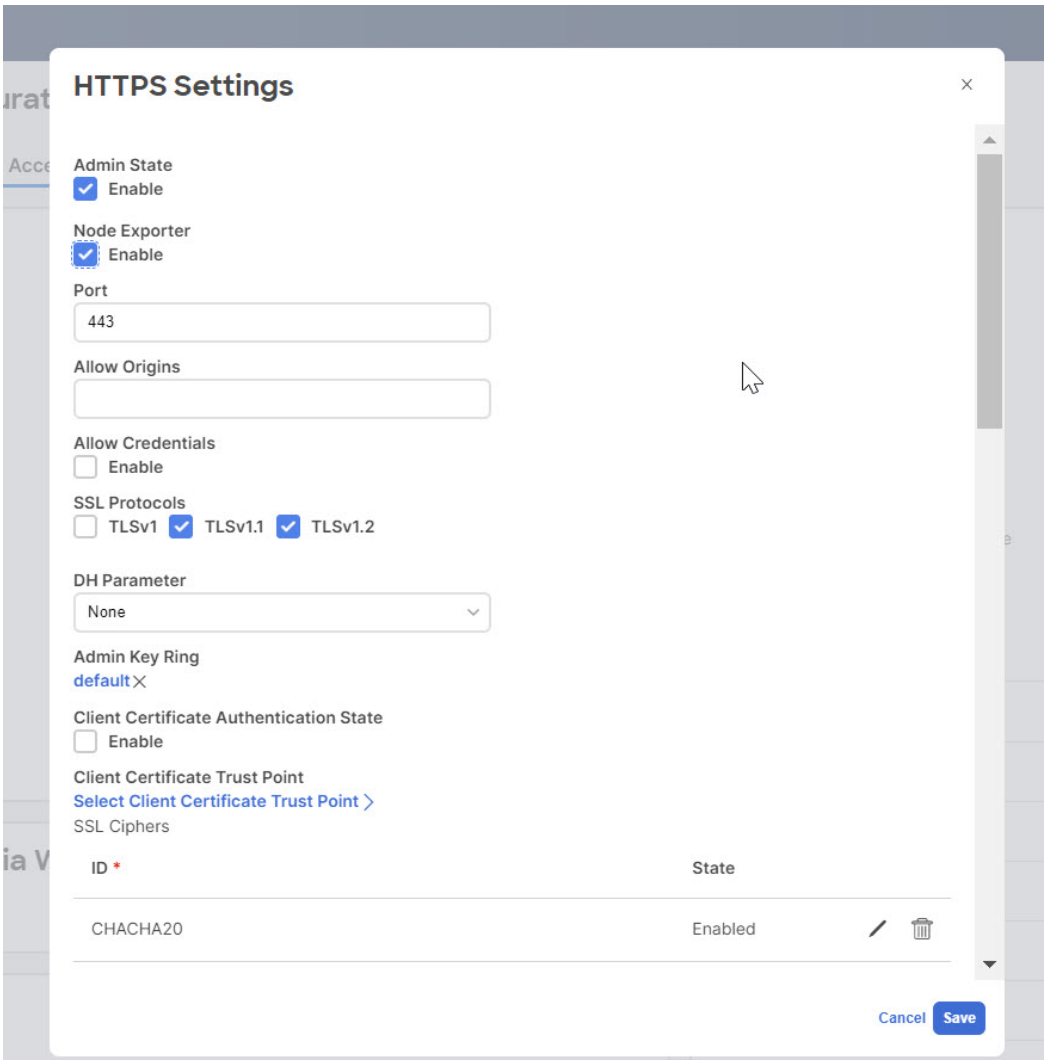


- **有効化（Enabled）**：Prometheus Node Exporter はすでに有効になっています。この場合、これらの手順を続行する必要はありません。
- **無効化（Disabled）**：Prometheus Node Exporter はまだ有効になっていません。Prometheus Node Exporter を有効にするには、次の手順に従います。

ステップ 3 **[HTTPS]** 領域の鉛筆アイコンをクリックして、HTTPS 設定を編集します。

[HTTPS 設定（HTTPS Settings）] ウィンドウが表示されます。

ステップ 4 **[ノード エクスポータ（Node Exporter）]** フィールドを見つけ、**[有効化（Enable）]** をクリックします。



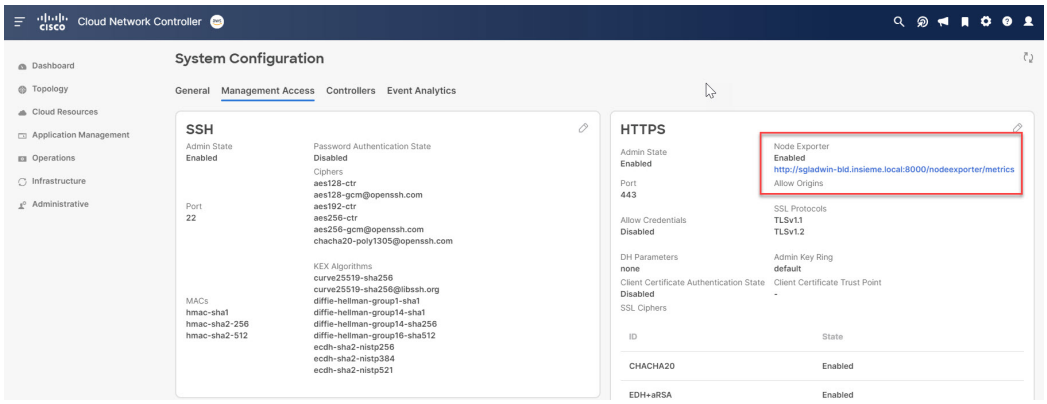
これらの設定を保存すると Web サービスが再起動され、要求への応答が再開されるまで少し時間がかかることを示す警告メッセージが表示されます。**[OK]** をクリックして、変更内容を確定します。

ステップ 5 ウィンドウの左下の **[保存（Save）]** をクリックします。

[システム構成/管理アクセス（System Configuration/Management Access）] ウィンドウに戻ります。Web サービスが再起動し、数秒後にオンラインに戻ります。

ステップ 6 ウィンドウの右側の **[HTTPS]** 領域で、**[ノード エクスポータ（Node Exporter）]** フィールドのエントリが **[有効化（Enabled）]** に設定されていることを確認します。

これにより、Prometheus Node Exporter が有効になっていることが確認されます。



ステップ 7 **[ノード エクスポータ（Node Exporter）]** 領域の **[有効化（Enabled）]** テキストの下にあるリンクをクリックします。

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

REST API を使用した VM ホスト メトリックスの監視

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

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

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

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

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

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

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

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

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

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

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

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

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

アプリケーション管理詳細の表示

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

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

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

表 *24 :* アプリケーション管理サブタブ

サブタブ名	説明
テナント	テナントをサマリー テーブルの行として表示します。
アプリケーション プロファイル	サマリー テーブルの行としてアプリケーション プロファイルを表示します。
EPG	EPG をサマリー テーブルの行として表示します。
契約	コントラクトをサマリーテーブルの行として表示します。
フィルタ（**Filters**）	サマリー テーブルの行としてフィルタを表示します。
VRF	サマリー テーブルの行として VRF を表示します。
サービス（**Services**）	次の 2 つのサブタブと情報が含まれています。 • **デバイス**：サマリーテーブルの行としてデバイスを表示します。 • **サービス グラフ**：サービス グラフをサマリーテーブルの行として表示します。

サブタブ名	説明
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 Network Controller GUI を使用してクラウド リソースの詳細を表示する方法について説明します。クラウド リソースの詳細には、特定のリージョン、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 *25*：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。 • **[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係する ACI 関連情報を表示するサブタブのリストを含みます。
- **統計**：選択したサンプリング間隔と統計タイプに基づいて統計を表示できるようにします。**[統計]** タブは表示しているコンポーネントに応じたサブタブを含みます。
- **イベント分析**：障害、イベント、監査ログを表示するサブタブのリストを含みます。

操作の詳細の表示

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

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

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

表 26 : [操作（Operations）] サブタブ

サブタブ名	説明
イベント分析	次のサブタブを含みます。 • **[障害（Faults）]** タブ：サマリー テーブルの行として障害を表示します。 • **[イベント（Events）]** タブ：イベントをサマリー テーブルの行として表示します。 • **[監査ログ（Audit Logs）]** タブ：監査ログをサマリー テーブルの行として表示します。
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。

サブタブ名	説明

バックアップと復元	次のサブタブを含みます。
	• **[バックアップ（Backups）]** タブ：バックアップをサマリーテーブルの行として表示します。
	• **[バックアップ ポリシー（Backup Policies）]** タブ：バックアップ ポリシーをサマリー テーブルの行として表示します。
	• **[ジョブ ステータス（Job Status）]** タブ：ジョブのステータスをサマリーテーブルの行として表示します。
	• **[イベント分析（Event Analytics）]** タブ：次のサブタブが含まれます。
	  • **[障害（Faults）]** タブ：サマリー 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。

[Tech Support]	次のサブタブを含みます。 • **[Tech Support]** タブ：テクニカル サポート ポリシーをサマリー テーブルの行として表示します。 • **[コア ログ（Core Logs）]**タブ：コア ログをサマリー テーブルの行として表示します。 • **[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。

サブタブ名	説明

Firmware Management	次のサブタブを含みます。
	• **[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。
	  • **[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 Cisco クラウド ネットワーク コントローラにログインしているユーザーです）。

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

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

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

インフラストラクチャの詳細の表示

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

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

[インフラストラクチャ（Infrastructure）] タブが展開すると、サブタブ オプションのリストが表示されます。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 *27*: インフラストラクチャ サブタブ

サブタブ名	説明
システム設定	**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 Network Controller GUI を使用して管理の詳細を表示する方法について説明します。管理の詳細には、認証、セキュリティ、ユーザ、およびスマートライセンスに関する情報が含まれます。

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

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

表 *28* : 管理サブタブ

サブタブ名	説明
Authentication	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。 • **[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	次のサブタブのリストが含まれます。 • **[セキュリティ デフォルト設定（Security Default Settings）]** タブ：デフォルトのセキュリティ設定情報を表示できます。 • **[セキュリティ ドメイン（Security Domains）]** タブ：サマリー テーブルにセキュリティ ドメイン情報を表示できます。 • [ロール（Roles）] タブ：ロール情報をサマリー テーブルに表示できます。 • **[RBAC ルール（RBAC Rules）]** タブ：サマリー テーブルにRBACルール情報を表示できます。 • [証明書権限（Certificate Authorities）] タブ：サマリーテーブルの認証局情報を表示できます。 • **[キー リング（Key Rings）]** タブ：キー リング情報をサマリー テーブルに表示できます。

サブタブ名	説明
Users	次のサブタブを含みます。 • **[ローカル（Local）]** タブ：ローカル ユーザーをサマリー テーブルの行として表示します。 • **[リモート（Remote）]** タブ：リモート ユーザーをサマリー テーブルの行として表示します。
スマート ライセンス	次のサブタブを含みます。 • **[一般（General）]** タブ：ライセンスをサマリー テーブルの行として表示します。 • **[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 Network Controller GUI を使用したヘルス詳細の表示

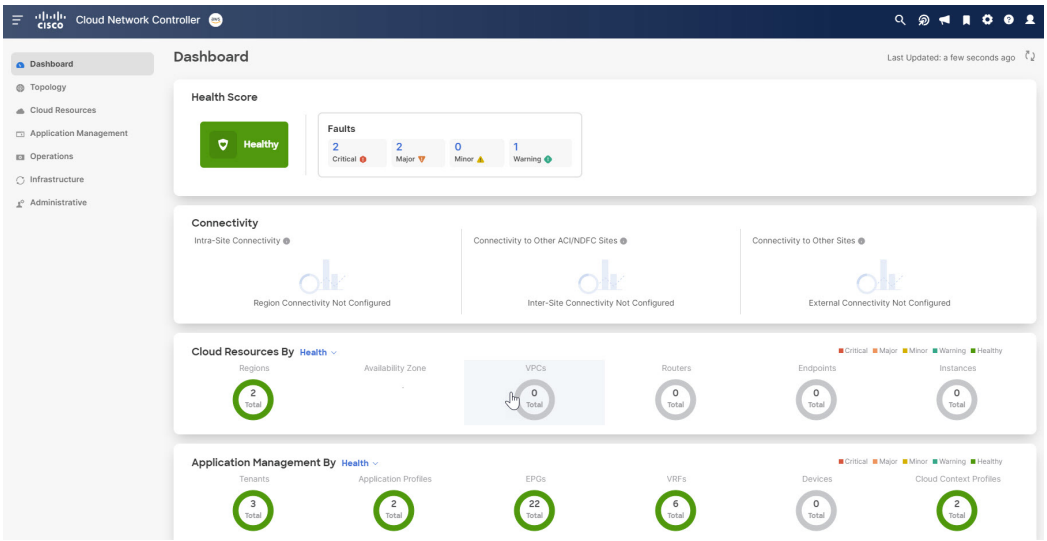
ここでは、Cisco Cloud Network Controller GUI を使用して正常性の詳細を表示する方法について説明します。Cisco Cloud Network Controller GUI のクラウド リソース エリアで確認できるオブジェクトの正常性の詳細は、次のように表示できます。

- [Regions]
- アベイラビリティー ゾーン (AWS クラウド サイトの場合)
- VPC (AWS クラウド サイト用)
- VNET (Azure クラウド サイト用)
- ルータ

- セキュリティ グループ
- エンドポイント
- Instances
- クラウド サービス

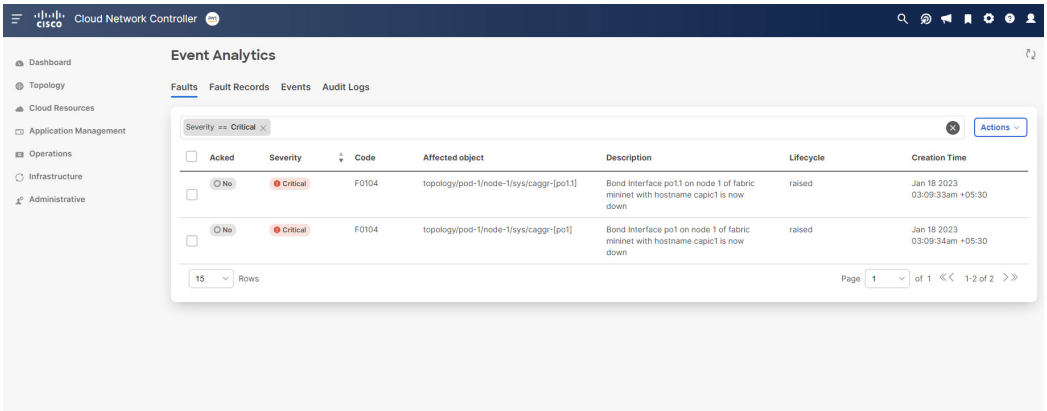
ステップ 1 **[ナビゲーション（Navigation）]** メニューから **[ダッシュボード（Dashboard）]** タブを選択します。

Cisco Cloud Network Controller の **[ダッシュボード（Dashboard）]** ビューを表示します。このウィンドウから、システムの全体的なヘルス ステータスを表示できます。



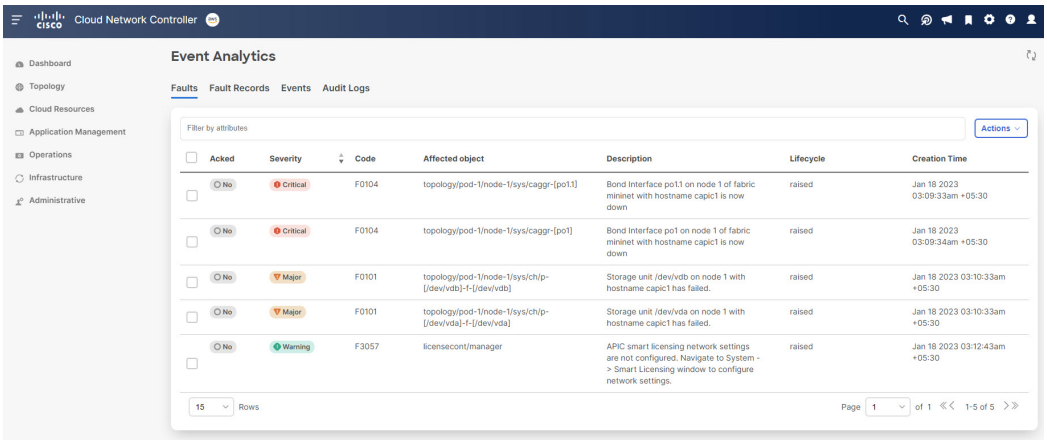
ステップ 2 **[ダッシュボード（Dashboard）]** ウィンドウの [障害サマリー] 領域内をクリックします。

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



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

[イベント分析（Event Analytics）] ウィンドウに表示される情報が変更され、重大度がクリティカル、メジャー、および警告レベルのイベントが表示されます。

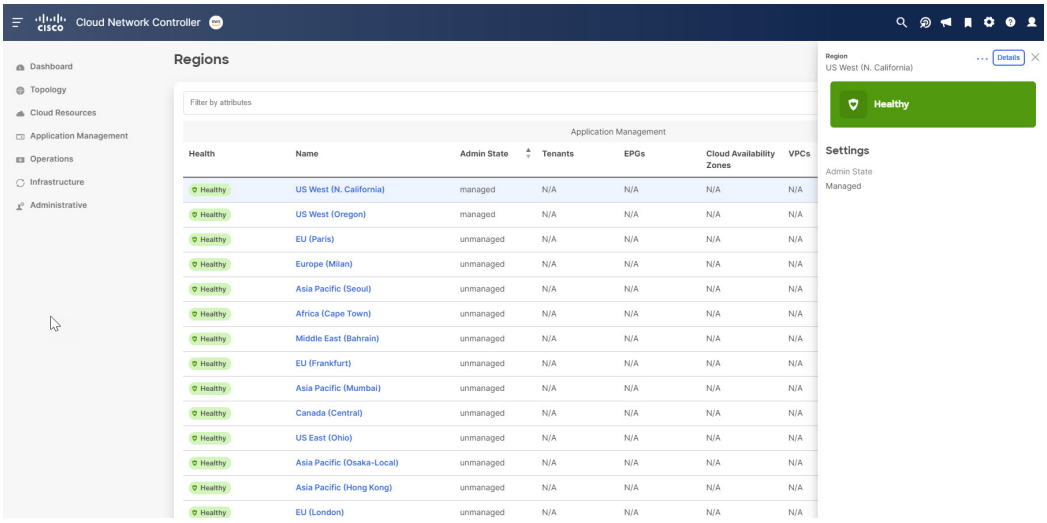


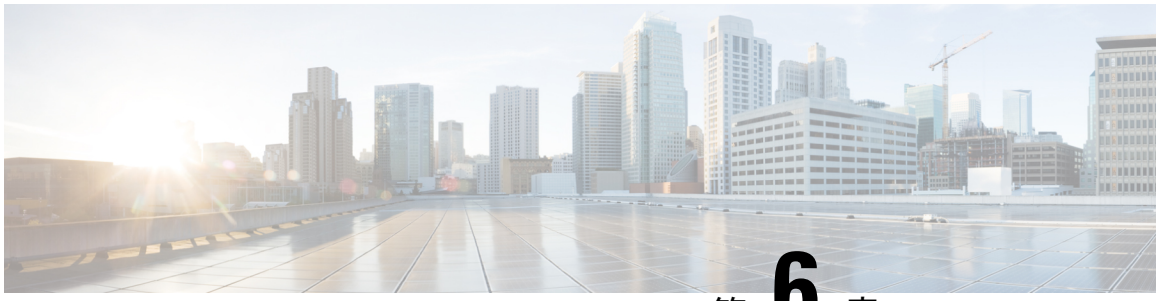
ステップ 4 **[ナビゲーション（Navigation）]** メニューから、**[クラウド リソース（Cloud Resources）]** タブを選択します。

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

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

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





第 6 章

レイヤ 4 から レイヤ 7 サービスの展開

概要

Cisco Cloud Network Controller 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。

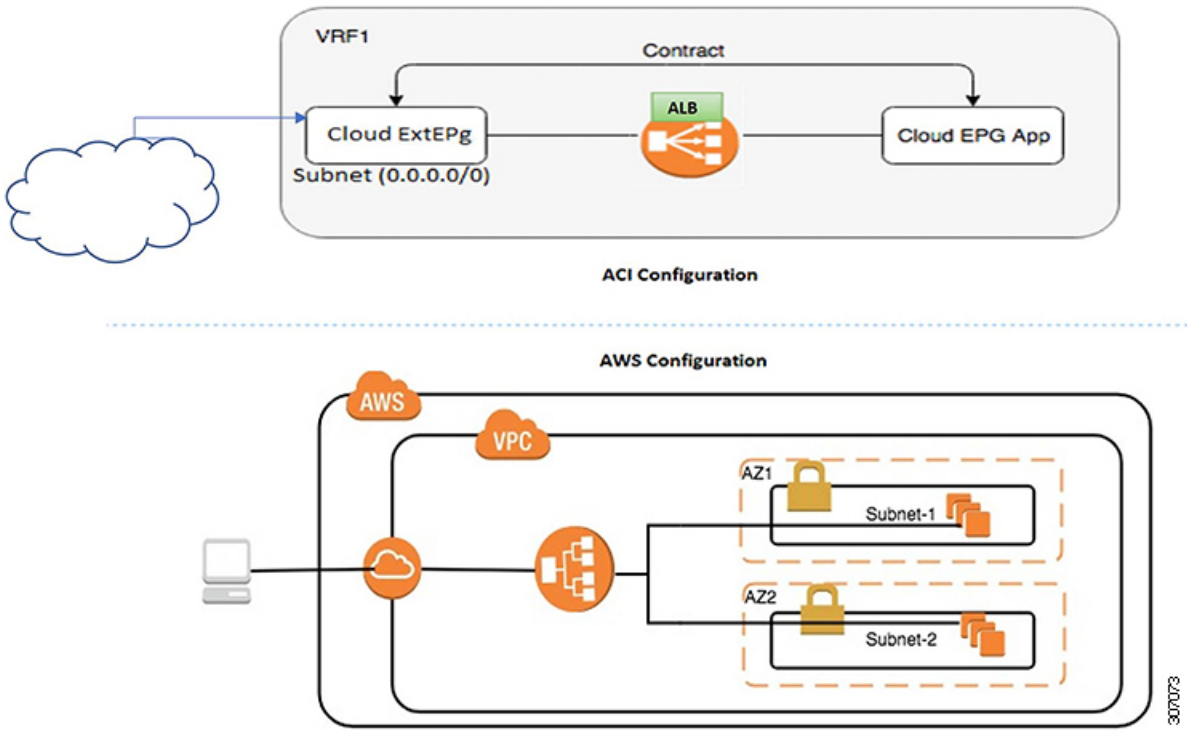
（注） リスナーは複数の証明書をもつことができます。

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

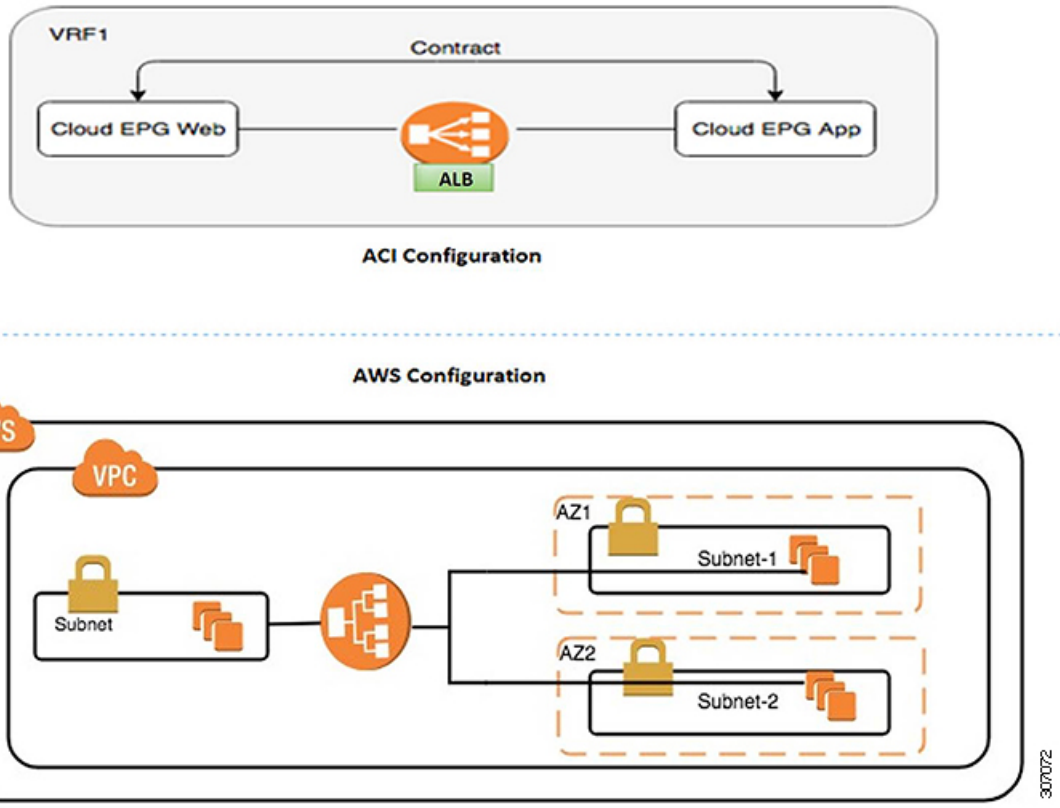
ALB が挿入されます。次の図は、VRF 内のコントラクト構成と、コンシューマーの外部 EPG とプロバイダーのクラウド EPG の間に挿入されるサービスとしての ALB を示しています。

図 *11* : 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 *12 :* 内部に向けた展開



（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 *29:* カスタム ポートベースのアタッチ

プロバイダEPG	ポート（Ports）
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 個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

Cisco Cloud Network Controller GUI を使用したサービス グラフの展開

Cisco Cloud Network Controller 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 Network Controller GUI を使用してロードバランサを作成する例を示します。

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 Dailog Box Fields）]* の表にリストされた各フィールドに該当する値を入力し、続行します。

表 *30* : 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	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[デバイスの作成（Create Device）]** ダイアログボックスに戻ります。
[設定（Settings）]	
サービス 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	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。 1. **[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。 2. **[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。 3. **[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。 4. **[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。 5. **[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。 6. **[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 Network Controller 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 Network Controller 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 *31* : 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	テナントを選択します。 **1.** **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 **2.** 左側の列から、クリックしてテナントを選択します。 **3.** [選択（Select）] をクリックします。**[サービス グラフの作成（Create Service Graph）]** ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。
[設定（Settings）]	

[プロパティ（Properties）]	説明
デバイスを選択	デバイスを選択します。 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（Add）] 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 Network Controller 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。

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

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

ステップ 5 コンシューマ EPG を追加するには、次の手順を実行します。

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

b) **[コンシューマ EPG の選択]** 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。

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、**[選択]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログボックスが閉じます。

ステップ 7 サービス グラフを選択するには:

a) **[EPF 通信の構成（EPG Communication Configuration）]** ダイアログで、**[サービス グラフの選択（Select Service Graph）]** をクリックします。**[サービス グラフの選択（Select Service Graph）]** ダイアログボックスが表示されます。

b) **[サービス グラフの選択（Select Service Graph）]** ダイアログの左側のペインで、サービス グラフをクリックして選択し、**[選択（Select）]** をクリックします。**[サービス グラフの選択（Select Service Graph）]** ダイアログボックスが閉じます。

ステップ 8 **[サービス グラフのプレビュー（Service Graph Preview）]** で、**[クラウド ロード バランサ リスナーの追加（Add Cloud Load Balancer Listner）]** をクリックします。**[クラウド ロード バランサ リスナーの追加（Add Cloud Load Balancer Listner）]** ダイアログが表示され、リスナーを追加できます。

リスナーは、デバイスが動作するポートとプロトコルです。

ステップ 9 次の *[クラウドロードバランサ リスナーの追加ダイアログボックスのフィールド（Add Cloud Load Balancer Listener Dialog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *32 :* 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	**HTTP** または **HTTPS** を選択します。
Security Policy	ドロップダウンリストをクリックし、セキュリティポリシーを選択します (**HTTPS** が選択されている場合にのみ選択可能)。
SSL 証明書（SSL Certificate）	SSL 証明書を選択するには (**HTTPS** が選択されている場合にのみ選択可能): **1.** **[SSL 証明書の追加]** をクリックします。 **2.** クリックして、追加する証明書のチェックボックスをオンにします。 **3.** キー リングを選択してください: 　**1.** **[キー リングの選択]** をクリックします。**[キー リンクの選択（Select Key Ring）]** ダイアログが表示されます。 　**2.** **[キー リンクの選択（Select Key Ring）]** ダイアログで、左側の列のキー リングをクリックして選択し、**[選択（Select）]** をクリックします。**[キー リンクの選択（Select Key Ring）]** ダイアログボックスが閉じます。 **4.** **[証明書ストア]** ドロップダウン リストをクリックして、証明書を選択します。 （注） リスナーは複数の証明書を持つことができます。
ルールの追加	ルール設定をデバイス リスナーに追加するには、**[ルールの追加]** をクリックします。**[ルール]** リストに新しい行が表示され、**[ルール設定]** フィールドが有効になります。

[プロパティ（Properties）]	説明
ルール設定	

[プロパティ（Properties）]	説明
	[ルール設定（Rule Settings）] ペインで、次のオプションを設定します。 • **名前** ：規則の名前を入力します。 • **ホスト**：ホスト名を入力して、ホストベースの条件を作成します。このホスト名に対して要求が行われると、指定したアクションが実行されます。 • **パス**：パスを入力して、パスベースの条件を作成します。このパスに対して要求が行われると、指定したアクションが実行されます。 • **タイプ**：アクション タイプは、実行するアクションをデバイスに通知します。アクション タイプのオプション: • **固定応答を返す**：次のオプションを使用して応答を返します。 • **固定応答本文**：応答メッセージを入力します。 • **固定応答コード**：応答コードを入力します。 • **固定の応答コンテンツ タイプ**：コンテンツ タイプを選択します。 • **転送**：次のオプションを使用してトラフィックを転送します。 • **ポート**：デバイスがトラフィックを受け入れるポートを入力します。 • **プロトコル**：**[HTTP]** または **[HTTPS]** を選択します。 • **プロバイダー EPG**：トラフィックを処理する Web サーバーを持つ EPG。 • **EPG**：EPG を選択するには: 1. **[EPG の選択]** をクリックします。**[EPG の選択]** ダイアログボックスが表示されます。 2. **[EPG の選択]** ダイアログで、左側の列の EPG をクリックして選択

[プロパティ（Properties）]	説明
	し、**[選択（Select）]** をクリックします。**[EPG の選択]** ダイアログボックスが閉じます。 • **リダイレクト**：次のオプションを使用して、リクエストを別の場所にリダイレクトします。 • **リダイレクト コード**：**[リダイレクト コード]** ドロップダウン リストをクリックして、コードを選択します。 • **リダイレクト ホスト名** ：リダイレクトのホスト名を入力します。 • **リダイレクト パス**：リダイレクト パスを入力します。 • **リダイレクト ポート**：デバイスがトラフィックを受け入れるポートを入力します。 • **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。 完了したら、**[ルールの追加]** をクリックします。

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

REST API を使用したサービス グラフの展開

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>
      <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-----
MIIEpQIBAAKCAQEA4DGxaK+RHv/nToHLnmDBq2BfLimgX/zNJQC9bGuzr8Mj7dm0
XuHfQYGv0h1PtL4Pdxf5qjB0NbHjAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCRe
Ginn/CgF75QPIed568eScNDZPt/eMeHAuRX/PykKUatWWncGanjvHqc+SOLPF6TD
gQ5nwOHHFvyM2DY8bfdYWrWmGsO7JqZzbPMptA2QWblILsSoIrdkIIgf6ZfYy/EN
bH+nYN2rJT8lzYsxz0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8KOfdCZPEq
8takiWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQABAoIBAQDQqA9IslYrdtqN
q6mZ3s2BNfF/4kgb7gn0DWs+9EJJLCJNZVhFEo2ZxxyfPp6HRnjYS50W83/E1anD
+GD1bSucTuxqFWIQVh7r1ebYZIWk+NYSjr5yNVxux8U2hCNNV8WWVqkJjKcUqICB
Bm47FKj53LV46zE0gyCaibFrYxZJ9+farGneyBdnoV+3thmez7534KCi0t3J3Eri
lgSY3ql6hPXB2ZXAP4jdAoLgWDU4I1M6OqOiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5GlfV2A4xTBQMCTZUZJ9fYAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphEDlAoGBAPVlvKfGW46qqRnYovfryxxz4OMlsVSgcJpQTQtBQi2koJ8OwEZJ
2s+CX0r+oDqwP23go/QEVYVkcic9RGkJBNge1+dm/bTjzgMQYtqSCNtecTsZD5JN
y1jkciizznDkjcjReSZ2kh3dGXIbRiYk7ezp2z7EKfDrHe5x5ouGMgCnAoGBAOnh
buDEohv8KJaB+DiUfhtoa3aKNPBO+zWPCHp0HFGjPXshJcIYZc1GcycmuDKVNnDd
MxhE/yOnQHowi4T9FMLpz5yh5zuCUVqOBgB1P6MzbC5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCW1OAFJRw3c/OiESwLMzchsl8RnbwOi6kDAoGBANVlzmPb07zB3eGTCU0t
KGiqwFLncUkVaDZZRFZYPpNwiRkoe73j9brkNbgCqxW+NLp5UjoeFry0N6y106q/
ZA4I7FnXryLBw2HYuw41Vixl+XOZ/HeO3RmFN1z717dGmaGbv43aKIB9x+X5n8wF
6z1NtBHmBk7yNwom1IRag1sbAoGAX0p4cJ/tJNXSe7AswHDQCL68uimJdDfZ5nKG
k83nE+Qc0qQozDJAmCiSFmuSNRnSep3FiafjBFXK0X4h+mdbJCc7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztzTn+as6xKOUATEezy9DK9zMWzQhhtaY
m9yZTp0CgYEA1UtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdGJt88ezM1Oej
Pdoab0G2PcfgJZoTSGk7N4XArVKeq7pgZ0kwcYAshO6A2Hal+D1z/bGoZP+kmD/x
```

```
Ny82phxYOXCnEc5Vv92lU59+j7e067UFLAYJe6fu+oFImvofRnP4DIQ= -----END RSA PRIVATE KEY-----"
cert="-----BEGIN CERTIFICATE----- MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
 VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRIwEAYDVQQK
EwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVoXDTE5MTAwMjIwNTMwNVowgY0xCzAJBgNVBAYTAlVTMQswCQYDVQQI
EwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBgNVBAoTCU15Q29tcGFueTEOMAwG
A1UECxMFTXlPcmcxGDAWBgNVBAMUDyouYW1hem9uYXdzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDgMbFor5Ee/+dOgcueYMGrYF8uKaBf/M0lAL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXvlA8h53nrx5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqeO8epz5I4s8XpMOBDmfA
4ccW/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZHShFAdOI3Y2INj9lXrfLEJd8uD2qk1kK4Pwo590Jk8Sry1qSJ
YHGJHn8dE+xxYB1ZCyiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMEgbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BAcTCFNhbiBKb3NlMRIwEAYDVQQKEwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvbmF3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAe/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5ml5baCYZZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoelewv+wRl0oVRChlTfKtXO68TUk6vrqpw76hKfOHIa7b2h1IIMdq6VA/
+A5FQ0xqYfqKdVd2RaINpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfGPlVesFEyJEL
gHBUiPt8TIbaMYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjmDL3tpFwg qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
 -----END CERTIFICATE-----">
      </pkiKeyRing>
      <pkiTP status="" name="lbTP" certChain="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRIwEAYDVQQK
EwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVoXDTE5MTAwMjIwNTMwNVowgY0xCzAJBgNVBAYTAlVTMQswCQYDVQQI
EwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBgNVBAoTCU15Q29tcGFueTEOMAwG
A1UECxMFTXlPcmcxGDAWBgNVBAMUDyouYW1hem9uYXdzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDgMbFor5Ee/+dOgcueYMGrYF8uKaBf/M0lAL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXvlA8h53nrx5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqeO8epz5I4s8XpMOBDmfA
4ccW/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZHShFAdOI3Y2INj9lXrfLEJd8uD2qk1kK4Pwo590Jk8Sry1qSJ
YHGJHn8dE+xxYB1ZCyiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMEgbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BAcTCFNhbiBKb3NlMRIwEAYDVQQKEwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvbmF3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAe/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5ml5baCYZZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoelewv+wRl0oVRChlTfKtXO68TUk6vrqpw76hKfOHIa7b2h1IIMdq6VA/
+A5FQ0xqYfqKdVd2RaINpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfGPlVesFEyJEL
gHBUiPt8TIbaMYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjmDL3tpFwg qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
 -----END CERTIFICATE-----">
       </pkiTP>
   </cloudCertStore>
  </fvTenant>
</polUni>
```

REST API を使用した HTTPS サービス ポリシーの作成

このセクションでは、REST API を使用して HTTPS サービス ポリシーを作成する方法を示します。

（注） リスナーは複数の証明書をもつことができます。証明書のオプションは次のとおりです。

- ELBSecurityPolicy-2016-08 – セキュリティ ポリシーが選択されていない場合のデフォルト。
- ELBSecurityPolicy-FS-2018-06
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2015-05
- ELBSecurityPolicy-TLS-1-0-2015-04

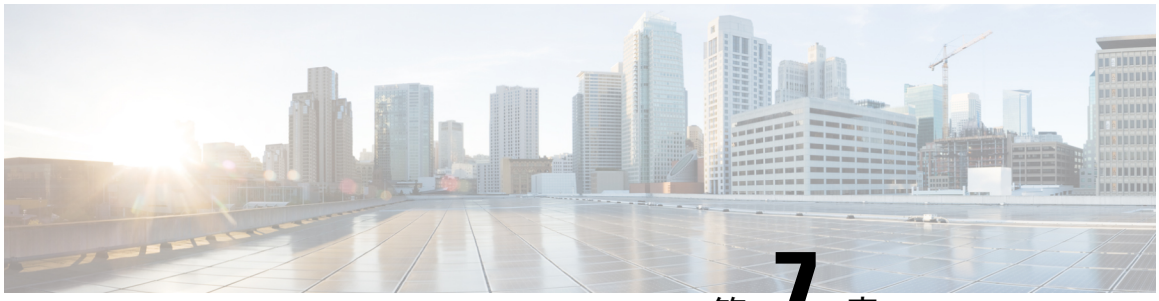
複数の証明書を使用する場合は、デフォルトの証明書を指定する必要があります。デフォルトは、**cloudRsListenerToCert** の **defaultCert** プロパティを使用して指定されます。

始める前に

キー リング証明書は既に構成されています。

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 Network Controller 統計情報

Cisco Cloud Network Controller 統計情報について

Cisco クラウド ネットワーク コントローラは、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 クラウド ネットワーク コントローラ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 クラウドネットワーク コントローラ 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 Network Controller 統計フィルタ （185 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 Gateway Statistics （185 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 クラウド ネットワーク コントローラ 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 クラウド ネットワーク コントローラはこれらのフロー 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 分かかることがあるため、Cisco クラウド ネットワーク コントローラ 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 クラウド ネットワーク コントローラ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 クラウド ネットワーク コントローラは、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 Network Controller のエンドポイントと cloudEPg 統計情報処理

Cisco クラウド ネットワーク コントローラは、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 クラウド ネットワーク コントローラは、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 Network Controller 統計フィルタ

Cisco クラウド ネットワーク コントローラ 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。

フィルター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 クラウド ネットワーク コントローラ 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 クラウド ネットワーク コントローラは、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 クラウド ネットワーク コントローラは、15 分以上前に発生したフロー 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 Gateway Statistics

You can collect statistics for traffic going through Amazon Web Services (AWS) Transit Gateways on both the infra tenant and the user tenant. Statistics reported for user tenant represent the traffic of an attachment between an user VPC and an AWS Transit Gateway. Statistics reported from infra tenant represents the traffic of an attachment between an infra VPC and a Transit Gateway.

The following statistics are collected for AWS Transit Gateway:

- Ingress packets
- Ingress packet bytes

- Ingress packet drops
- Ingress packet drop bytes
- Egress packets
- Egress packet bytes
- Egress packet drops
- Egress packet drop bytes

You can enable infra tenant Transit Gateway statistics collection from the Cisco Cloud Network Controller **Setup- Region Management** page. See the section "Set Up the Cloud Site to Use AWS Transit Gateway" in *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway*.

You can enable user tenant Transit Gateway statistics collection by enabling flow logs on the user VPC. See the sections VPC フロー ログの有効化, on page 186 and Cisco Cloud Network Controller GUI を使用した VPC フロー ログの有効化, on page 187 in this guide.

To view AWS Transit Gateway statistics, in the Cisco Cloud Network Controller GUI, click the **Statistics** tab and then click **AWS Transit Gateway** in the left navigation pane. The central pane displays the information.

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 Network Controller 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 ネットワーク コントローラ 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 *33 :* 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	**[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。 • 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**

[プロパティ（Properties）]	説明
宛先（Destination）	**[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。
保持	**[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。 • **1日** • **3日** • **5 日** (デフォルト) • **1 ヵ月** • **13 ヵ月** • **18 ヵ月** • **2ヵ月** • **3 か月** • **4 ヵ月** • **5 ヵ月** • **6 ヵ月** • **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 Network Controller 統計フィルタ （185 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。

• "icmp": 1 • "igmp": 2 • "tcp": 6 • egp(8)	• "igp": 9 • "l2tp": 115 • "udp": 17 • "icmpv6": 58	• "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。

• "dns": 53 • "ftpData": 20 • "smtp": 25	• "http": 80 • "https": 443	• "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=" vrf1" 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 クラウド ネットワーク コントローラは、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 クラウド ネットワーク コントローラは、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 クラウド ネットワーク コントローラのクラウド 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

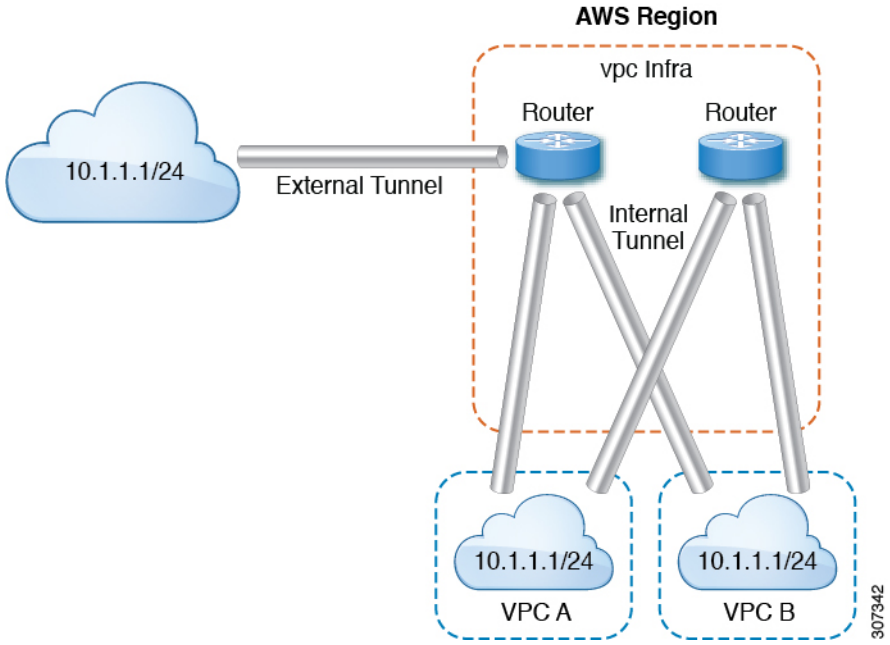
生の統計は 2 Dns の下に保存されます。

- `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>`

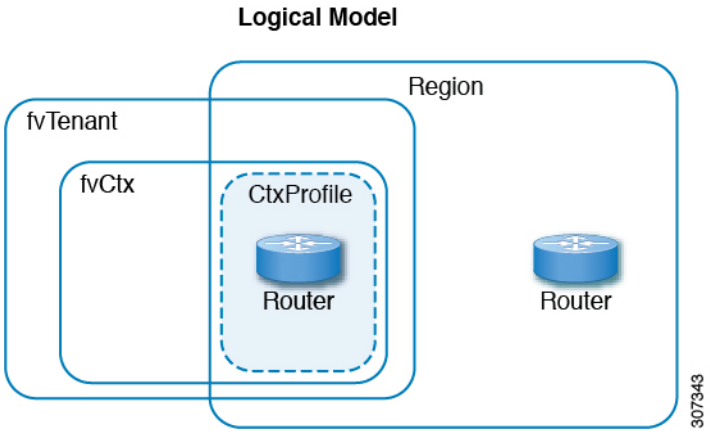
（注）

- 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 クラウド ネットワーク コントローラは、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 パケットを見つけたい場合は、
`uni/tn-<infraTenant>/ctx-<infraCtx>/region-<infraRegion>/router-<csrname>/to-<ip or user-region>/` で利用できます。

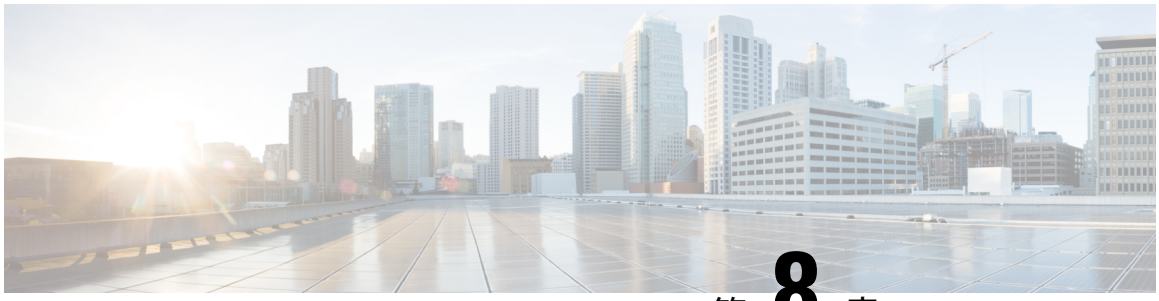
ユーザー region1 と infra region2 の間のすべてのパケットを取得する場合は、
`uni/tn-<userTenant>/ctx-<userCtx>/region-<userRegion>/region-<infraRegion>/` で使用できます。

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 クラウド ネットワーク コントローラ 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 Network Controller のセキュリティ

この章は、次の内容で構成されています。

Access, Authentication, and Accounting

Cisco Cloud Network Controller policies manage the authentication, authorization, and accounting (AAA) functions. The combination of user privileges, roles, and domains with access rights inheritance enables administrators to configure AAA functions at the managed object level in a granular fashion. These configurations can be implemented using the REST API or the GUI.

Note There is a known limitation where you cannot have more than 32 characters for the login domain name. In addition, the combined number of characters for the login domain name and the user name cannot exceed 64 characters.

For more access, authentication, and accounting configuration information, see Cisco Cloud Network Controller Security Configuration Guide.

構成

初期構成スクリプトで、管理者アカウントが構成され、管理者はシステム起動時の唯一のユーザーとなります。

ローカル ユーザの設定

Cisco Cloud Network Controller GUI を使用したローカル ユーザーの作成 （130 ページ） を参照して、ローカル ユーザーを設定し、 Cisco Cloud Network Controller GUI を使用して OTP、SSH 公開キー、および X.509 ユーザー証明書に関連付けます。

TACACS+、RADIUS、LDAP、および SAML アクセスの構成

次のトピックは、Cisco クラウド ネットワーク コントローラの TACACS+、RADIUS、LDAP および SAML アクセスを構成する方法を説明します。

Overview

This topic provides step-by-step instructions on how to enable access to the Cisco Cloud Network Controller for RADIUS, TACACS+, LDAP, and SAML users, including ADFS, Okta, and PingID.

For additional TACACS+, RADIUS, LDAP, and SAML information, see Cisco Cloud Network Controller Security Configuration Guide.

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

始める前に

- Cisco Cloud Network Controller はオンラインです。
- TACACS+ サーバのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。

ステップ 1 Cisco クラウド ネットワーク コントローラで、**[TACACS+ プロバイダ（TACACS+ Provider）]** 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）	プロバイダーを選択するには： **1.** **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 **2.** クリックして、左側の列のプロバイダーを選択します。 **3.** **[選択（Select）]** をクリックします。**[ログイン ドメインの作成]** ダイアログボックスに戻ります。

e) [保存（Save）] をクリックして、設定を保存します。

次のタスク

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

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

始める前に

- Cisco Cloud Network Controller はオンラインです。
- RADIUS サーバーのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。

ステップ 1 Cisco クラウド ネットワーク コントローラで、**[RADIUS プロバイダ（LDAP Provider）]** 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	

[プロパティ（Properties）]	説明
名前	ログイン ドメインの名前を 入力します
説明	ログイン ドメインの説明を入力します。
Settings	
Realm	ドロップダウン メニューから **RADIUS** を選択します。
プロバイダ（Providers）	プロバイダーを選択するには： 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. **[選択（Select）]** をクリックします。**[ログイン ドメインの作成]** ダイアログボックスに戻ります。

e) [保存（Save）] をクリックして、設定を保存します。

次のタスク

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

Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the Cisco Cloud Network Controller

Refer to the section *Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the APIC*in the Cisco Cloud Network Controller Security Configuration Guide.

LDAP Access の構成

LDAP 設定には 2 つのオプションがあります。

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

次のセクションには、両方の構成オプションの手順が含まれています。

Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair

Refer to the section *Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair* in the Cisco Cloud Network Controller Security Configuration Guide.

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

始める前に

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

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

a) メニュー バーで、**[管理（Administrative）]** > **[認証（Authentication）]** を選択します。
b) 作業ペインで、**[プロバイダー（Providers）]** タブをクリックして、**[アクション（Actions）]** ドロップダウンをクリックして、**[プロバイダーの作成（Create Provider）]** を選択します。
c) **[ホスト名/IP アドレス（Host name/IP Address）]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
d) **[説明（Description）]** フィールドに、プロバイダーの説明を入力します。
e) **[タイプ（Type）]** ドロップダウン リストをクリックし、**[LDAP]** を選択します。
f) **バインド DN**、**ベース DN**、**パスワード**、**ポート**、**属性**、**フィルタ タイプ**、および**管理 EPG** を指定します。

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

ステップ 2 LDAP の **ログイン ドメイン** を作成します。

a) メニュー バーで、**[管理（Administrative）]** > **[認証（Authentication）]** を選択します。

b) [Work]ペインで、[Login Domains]タブをクリックし、[Actions]ドロップダウンをクリックして[Create Login Domain]を選択します。

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

[プロパティ（Properties）]	**説明**
全般	
名前	ログイン ドメインの名前を 入力します
説明	ログイン ドメインの説明を入力します。
Settings	
Realm	ドロップダウン メニューから **[LDAP]** 選択します。
プロバイダ（Providers）	プロバイダーを選択するには： **1.** **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 **2.** クリックして、左側の列のプロバイダーを選択します。 **3.** **[選択（Select）]** をクリックします。**[ログイン ドメインの作成]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
認証タイプ	1. プロバイダーが**属性**として **CiscoAVPair** を使用して設定されている場合は、**[Cisco AV ペア（Cisco AV Pairs）]** を選択します。 2. プロバイダーが**属性**として **memberOf** で設定されている場合は、**[LDAP Group Map Rules]** を選択します。 1. **[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** をクリックします。ダイアログボックスが表示されます。 2. マップの**名前**と**説明**（オプション）および**グループ DN** を指定します。 3. **[セキュリティ ドメインの追加（Add Security Domain）]** の横にある [+] をクリックします。ダイアログボックスが表示されます。 4. [+] をクリックして、**[ロール（Role）]**の名前およびロールの **[権限（Privilege）]** タイプ（**Read** または **Write**）フィールドにアクセスします。チェックマークをクリックします。 5. さらにロールを追加するには、手順 4 を繰り返します。次に、[追加（Add）] をクリックします。 6. 手順3を繰り返して、さらにセキュリティドメインを追加します。次に、[追加（Add）] をクリックします。

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

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

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

About SAML

Refer to the section *About SAML* in the Cisco Cloud Network Controller Security Configuration Guide.

Basic Elements of SAML

Refer to the section *Basic Elements of SAML* in the Cisco Cloud Network Controller Security Configuration Guide.

Supported IdPs and SAML Components

Refer to the section *Supported IdPs and SAML Components* in the Cisco Cloud Network Controller Security Configuration Guide.

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

（注） SAML ベースの認証は Rest に対するものではなく、 Cisco Cloud Network Controller GUI のみに対するものです。

始める前に

- SAML サーバー ホスト名または IP アドレスと、IdP メタデータの URL を使用できます。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。
- 次の設定を行います。
  - 時刻同期と NTP
  - GUI を使用した DNS プロバイダーの構成
  - GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

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

a) メニュー バーで、**[管理（Administrative）]** > > **[認証（Authentication）]**を選択します。
b) **[作業（Work）]**ペインで、**[プロバイダー（Providers）]** タブをクリックし、**[アクション（Actions）]** ドロップダウンをクリックして **[プロバイダーの作成（Create Provider）]** を選択します。
c) **[ホスト名/IP アドレス（Host name/IP Address）]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
d) **[説明（Description）]** フィールドに、プロバイダーの説明を入力します。
e) **[タイプ（Type）]** ドロップダウン リストをクリックし、**[SAML]** を選択します。
f) **[設定（Settings）]** ペインで、次の手順を実行します。
   - IdP メタデータ URL を指定します。
     - AD FS の場合、IdP メタデータ URL は *https://<FQDN ofADFS>/FederationMetadata/2007-06/FederationMetadata.xml* という形式になります。

- Okta の場合、IdP メタデータの URL を取得するには、Okta サーバから該当 SAML アプリケーションの [Sign On] セクションに、**アイデンティティ プロバイダー メタデータ**のリンクをコピーします。

- SAML ベースのサービスの**エンティティ ID** を指定します。
- IdP メタデータの URL にアクセスする必要がある場合は、**メタデータ URL の HTTPS プロキシ（HTTPS Proxy for Metadata URL）** を構成します。
- IdP はプライベート CA によって署名された場合は、**[認証局（Certificate Authority）]** を選択します。
- ドロップダウン リストから、**[署名アルゴリズム認証ユーザー要求（Signature Algorithm Authentication User Requests）]**を選択します。
- **SAML 認証要求の署名、SAML 応答メッセージの署名、SAML 応答の署名アサーション、SAML アサーションの暗号化**を有効にするには、チェックボックスをオンにします。

g) [保存（Save）] をクリックして、設定を保存します。

ステップ 2 SAML のログイン ドメインを作成します。

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

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

[プロパティ（Properties）]	説明
プロバイダ（Providers）	プロバイダーを選択するには： 1. **[プロバイダーの追加（Add Providers）]** をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. **[選択（Select）]** をクリックします。**[ログインドメインの作成]** ダイアログボックスに戻ります。

d) [**保存（Save**）] をクリックして、設定を保存します。

Setting Up a SAML Application in Okta

Refer to the section *Setting Up a SAML Application in Okta* of Cisco Cloud Network Controller Security Configuration Guide.

Setting Up a Relying Party Trust in AD FS

Refer to the section *Setting Up a Relying Party Trust in AD FS* in the Cisco Cloud Network Controller Security Configuration Guide.

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。

About HTTPS Access

This article provides an example of how to configure a custom certificate for HTTPS access when using Cisco ACI.

For more information, see the section *HTTPS Access* in the Cisco Cloud Network Controller Security Configuration Guide.

カスタム証明書の構成のガイドライン

- ワイルドカード証明書（*.cisco.com など。複数のデバイス間で使用）およびそれに関連する他の場所で生成される秘密キーは、Cisco Cloud Network Controller ではサポートされません。これは、Cisco Cloud Network Controller に秘密キーまたはパスワードを入力するためのサポートがないためです。また、ワイルドカード証明書などのいかなる証明書の秘密キーもエクスポートできません。
- 証明書署名要求（CSR）を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。Cisco Cloud Network Controller は、送信された証明書が設定された CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
  - 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。
  - Cisco クラウド ネットワーク コントローラで公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
  - 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキー リングを削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。
- ポッドあたり 1 つの証明書ベースのルートのみをアクティブにすることができます。
- このリリースでは、クライアント証明書認証はサポートされていません。

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

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

始める前に

注意：ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。この操作中に Cisco Cloud Network Controller のすべての Web サーバの再起動が予期されます。

ステップ 1 メニュー バーで、**[管理（Administrative）]** > **セキュリティ（Security）]** を選択します。

ステップ 2 [作業（Work）] ペインで、**[証明書認証局（Certificate Authorities）]** タブをクリックし、**[アクション（Actions）]** ドロップダウンをクリックして **[証明書認証局の作成（Create Certificate Authorities）]** を選択します。

ステップ 3 **[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスの **[名前（Name）]** フィールドに、認証局の名前を入力します。

ステップ 4 **[用途（Used for）]** フィールドで **[システム（System）]** を選択します。

ステップ 5 **[証明書チェーン（Certificate Chain）]** フィールドで、 Cisco Cloud Network Controller の証明書署名要求（CSR）に署名する認証局の中間証明書とルート証明書をコピーします。証明書は、Base64 エンコード X.509（CER）形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 メニュー バーで、**[管理（Administrative）]** > **セキュリティ（Security）]** を選択します。

ステップ 8 [作業（Work）]ペインで、**[キー リング（Key Rings）]** タブをクリックし、[アクション（Actions）] ドロップダウンをクリックして **[キー リングの作成（Create Key Ring）]** を選択します。

ステップ 9 **[キー リングの作成（Create Key Ring）]** ダイアログボックスの **[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、 Cisco クラウド ネットワーク コントローラの完全修飾ドメイン名（FQDN）を入力します。

ステップ 19 必要に応じて、残りのフィールドに入力します。

ステップ 20 [保存（Save）] をクリックします。

[Key Ring] *[key_ring_name]* ダイアログボックスが表示されます。

ステップ 21 フィールド [要求（Request）] からコンテンツを署名するために**証明書認証局** にコピーします。

ステップ 22 **[キー リング（Key Ring）]** *[key_ring_name]* ダイアログボックスで、[編集（Edit）] アイコンをクリックして **[キー リング（Key Ring）]** *[key_ring_name]* ダイアログボックスを表示します。

ステップ 23 **[証明書（Certificate）]** フィールドに、認証局から受信した署名付き証明書を貼り付けます。

ステップ 24 **[保存（Save）]** をクリックして、**[キー リング（Key Rings）]** 作業ウィンドウに戻ります。

キーが確認されて **[作業（Work）]** ペインで **[管理状態（Admin State）]** が **[完了済み（Completed）]** に変わり、HTTP ポリシーを使用できるようになります。

ステップ 25 **[インフラストラクチャ（Infrastructure）]** > **[システム構成（System Configuration）]** に移動し、**[管理アクセス（Management Access）]** タブをクリックします。

ステップ 26 **[HTTPS]** 作業ウィンドウの編集アイコンをクリックして、**[HTTPS 設定（HTTPS Settings）]**ダイアログボックスを表示します。

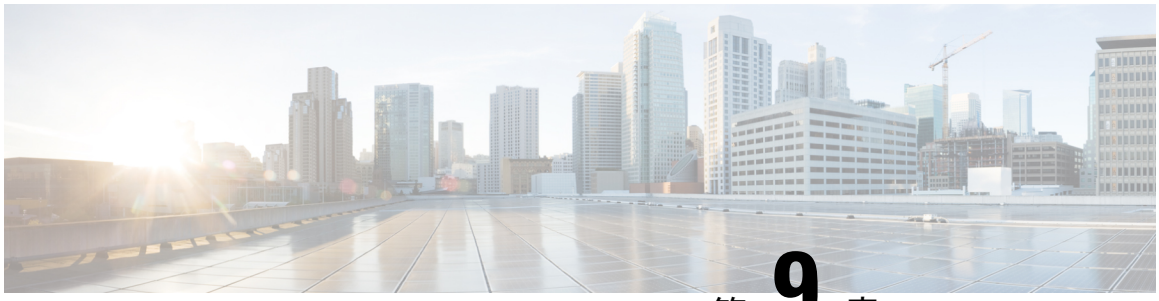
ステップ 27 **[管理キー リング（Admin Key Ring）]** をクリックし、以前に作成したキー リングを関連付けます。

ステップ 28 [保存（Save）] をクリックします。

すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキー リングが HTTPS アクセスに関連付けられています。

次のタスク

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じ CSR を再送信する必要があります。キー リングを削除すると、 Cisco クラウド ネットワーク コントローラ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

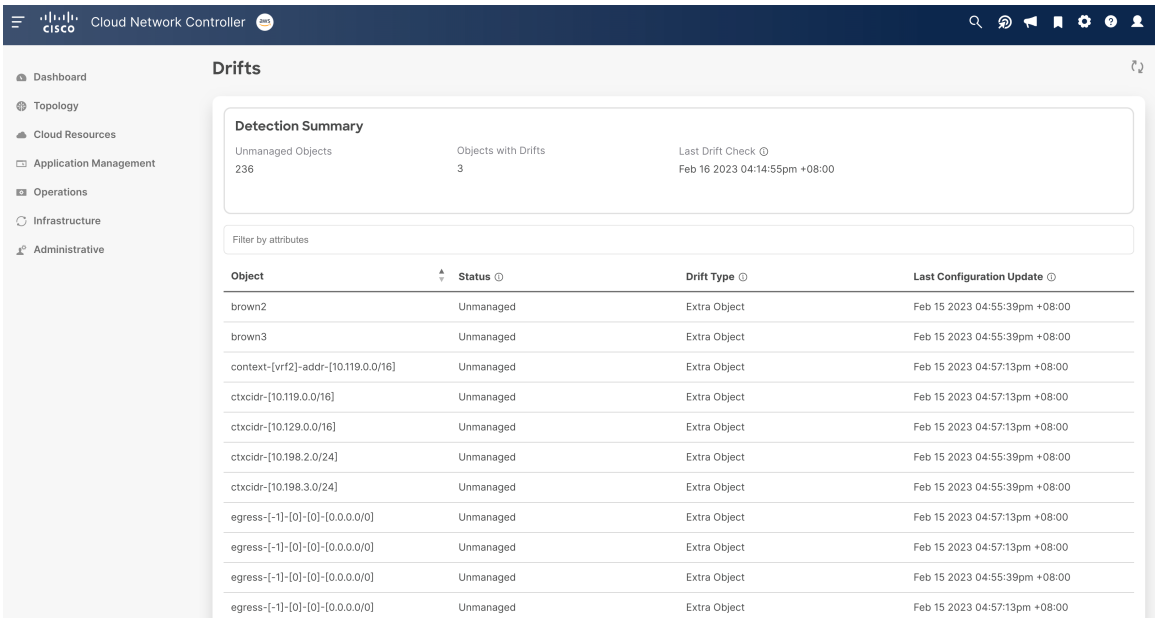
設定のばらつき

構成のばらつき通知と障害

クラウドネットワーク コントローラが展開されたら、そのGUIまたはREST APIインターフェイスを使用してほとんどの設定を実行します。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 Network Controller 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。

Cloud Network Cotroller は、Cloud Network Controller 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。構成のばらつきの表示はデフォルトで有効になっており、構成のばらつき情報は、EPG、VRF、およびレイヤ 4 からレイヤ 7 のサービス グラフがアタッチされているかどうかに関係なく使用できます。

構成のばらつき情報は、**[クラウド リソース（Cloud Resources）]**>>**[ドリフト（Drifts）]**で表示される 1 つのページに統合されました。



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 （208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 Network Controller で構成され、クラウドファブリックに展開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 Network Controller 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 Network Controller 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 Network Controller から展開することを意図していない追加の構成はありますか?

  前のシナリオと同様に、これは、接続または API の問題がある場合、またはクラウド管理者がクラウドプロバイダーの UI で直接追加のセキュリティルールを手動で作成した場合に発生する可能性があります。既存の、意図されていない構成では、問題が発生する可能性があります。

構成ドリフトのメイン ページにアクセスする

構成ドリフト情報が単一の **[ドリフト（Drifts）]** ページに統合されています。

[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。

- 何かが削除されたかどうかを確認するには

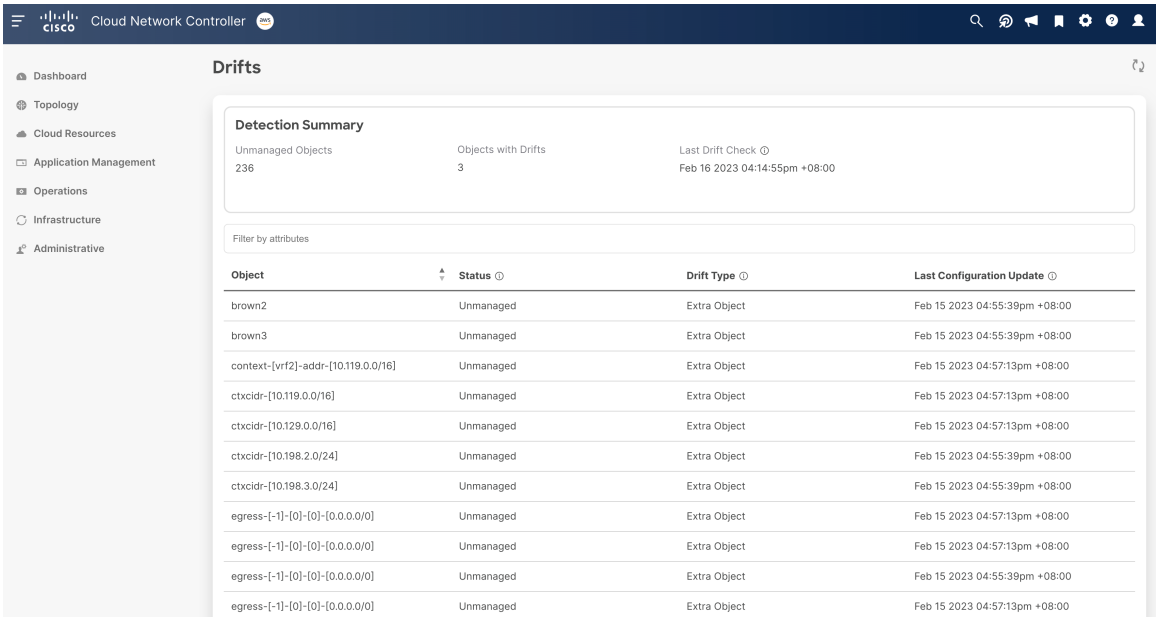
• 存在する必要のあるものが正しく表示されていることを確認するには

ステップ 1 Cisco Cloud Network Controller 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。



[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 Network controller 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。構成を再展開すると、Cloud Network Controller 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 Network Controller 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のある、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 Network Controller 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 Network Controller 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（Status）
- `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 （211 ページ）
- 欠落している EPG 構成の確認 （213 ページ）
- 欠落している VRF 構成の確認 （214 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、Cisco Cloud Network Controller 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契約設定を確認する方法について説明します。

ステップ 1 Cloud Network Controller 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。

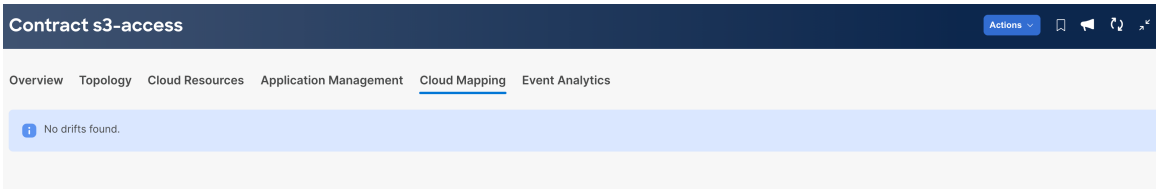
ステップ 3 適切なコントラクトをダブルクリックして、そのコントラクトの **[概要（Overview）]** ページを表示します。

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。

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 （163 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。



（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 （208 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 Ojects）]**、**[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 Network controller 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。構成を再展開すると、Cloud Network Controller 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 Network Controller 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。

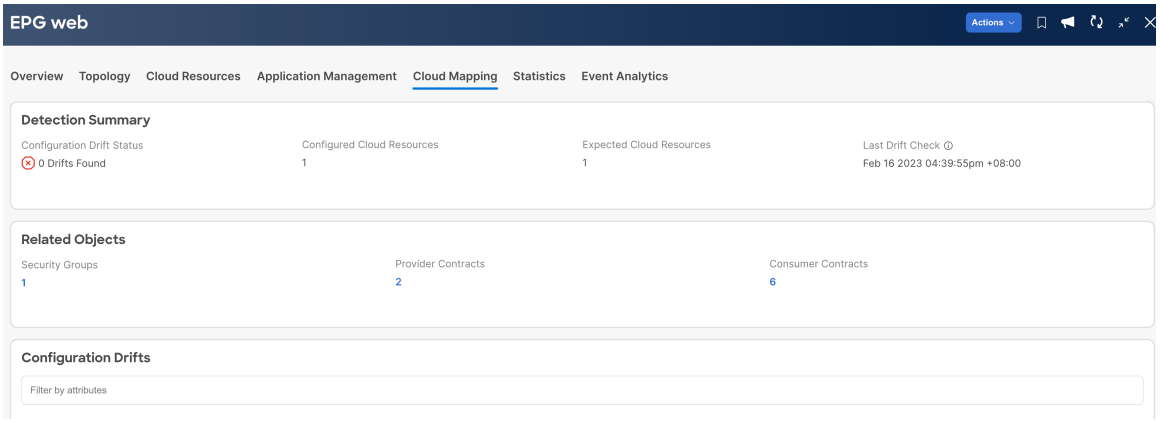
ステップ 1 Cloud Network Controller GUI にログインします。

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。



（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 （208 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 Ojects）]**、**[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 Ovjects）]**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 Network controller 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。構成を再展開すると、Cloud Network Controller 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 Network Controller 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 VRF 設定を確認する方法について説明します。

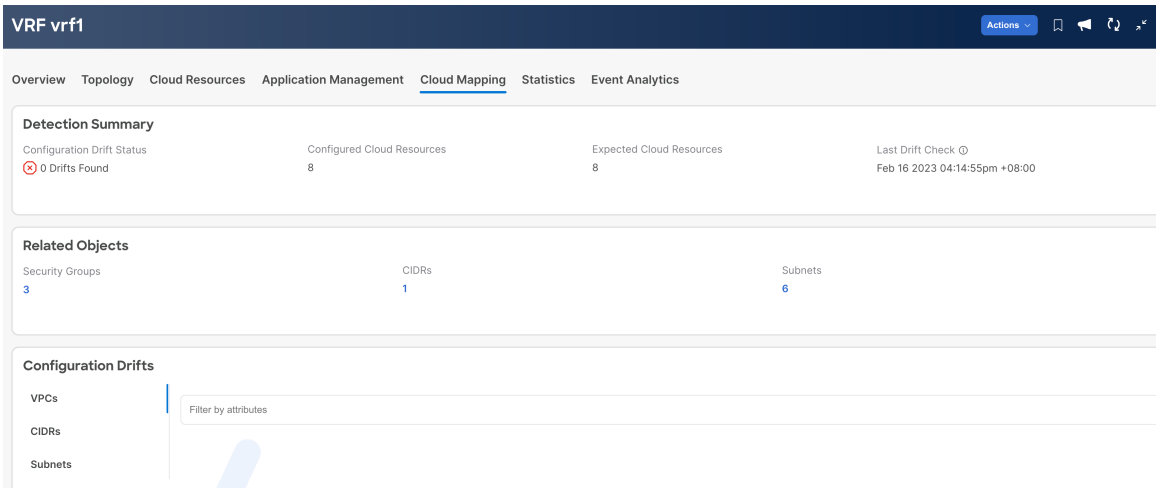
ステップ 1 Cloud Network Controller GUI にログインします。

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。



（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 （208 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 Ojects）]**、**[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 Ovjects）]** エリアには、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 Network controller 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。構成を再展開すると、Cloud Network Controller 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、構成のばらつきのあるプロセスが Cloud Network Controller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 Network Controller 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。

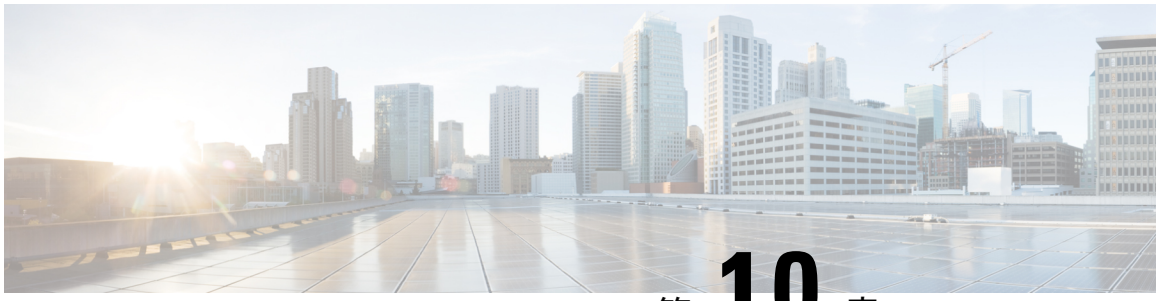
構成のばらつきプロセスのログは、`/data2/logs/Cisco_CApicDrift` ディレクトリに保存されます。

`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 Network Controller 上の AWS トランジット ゲートウェイ

AWS Transit Gateway on Cisco Cloud Network Controller

You can use Amazon Web Services (AWS) Transit Gateway with Cisco Cloud Network Controller. AWS Transit Gateway is a service that functions as an internal router to automate connectivity between virtual private clouds (VPCs). The VPCs can be in different AWS regions in a cloud site.

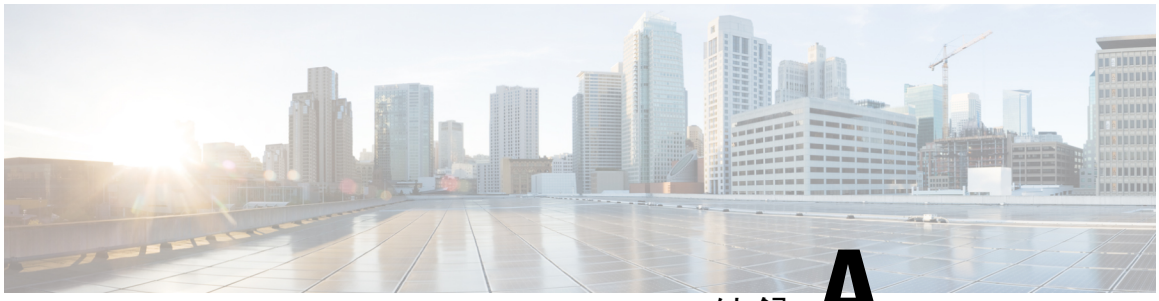
Virtual private clouds (VPC) can't communicate with each other without additional configuration. Without using AWS Transit Gateway, you can configure inter-VPC communication by configuring VPC peering. Alternatively, you can use VPN tunnels and CCRs.

However, when you use AWS Transit Gateway with Cisco Cloud Network Controller, you connect VPCs or VRFs in the cloud site simply by associating the VPCs or VRFs to the same AWS Transit Gateways.

Using AWS Transit Gateway with Cisco Cloud Network Controller provides several benefits: higher performance, simplicity, scalability and potential lower cost.

Note You can attach a Cisco Cloud Network Controller user tenant’s VPC (CtxProfile) to an AWS Transit Gateway (hub network) only if you have administrator privileges and the user is part of security domain “all". Without such access, you cannot attach the user tenant’s VPC to an AWS Transit Gateway.

For detailed information about using AWS Transit Gateway with Cisco Cloud Network Controller, see *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway*.



付録 A

Cisco Cloud Network Controller エラー コード

Cisco Cloud Network Controller エラー コード

ここでは、Cisco Cloud Network Controller のエラー コードについて説明します。

表 *34 : Cisco Cloud Network Controller* 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。

コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_INFRANETWORK_NUMROUTERSPERREGION_MAXIMUM	cloudtemplateInfraNetwork MO では、属性 numRoutersPerRegion の最大許容値は 4 です。
cloud-template	CT_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。

コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_INTNETWORK_REGION_MAXIMUM	cloudtemplateIntNetwork で指定されるリージョンの最大数（cloudRegionName）は 4 です
cloud-template	CT_EXTNETWORK_REGION_SUBSET	cloudtemplateExtNetwork の cloudRegionName の子によって指定されたリージョンは、cloudtemplateIntNetwork の下の cloudRegionName の子によっても指定する必要があります。
cloud-template	CT_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)。

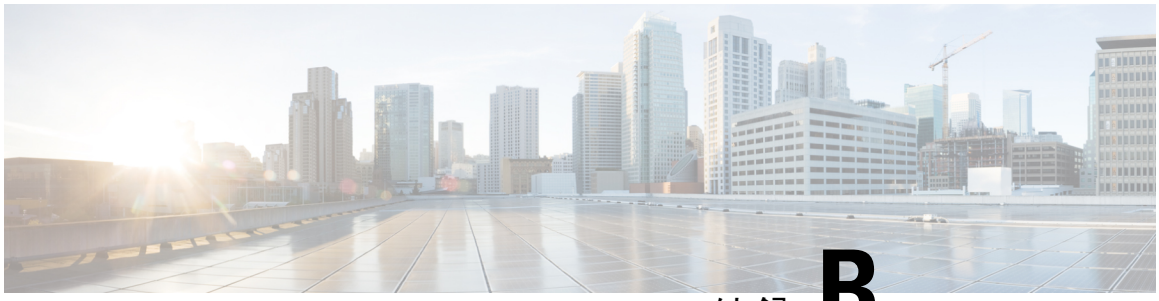
コンポーネント	エラー コード（**Error Code**）	制約
cloud-template	CT_INTNETWORK_MISSING_HOME	cloudtemplateIntNetwork の下に cloudRegionName がある場合は、cloudRegonName の 1 つを Cisco クラウド ネットワーク コントローラのホーム リージョン（capicDeployed）に関連付ける必要があります。
cloud-template	CT_CLOUD_APICSUBNETPOOL_INSUFFICIENT	cloudApicSubnetPool MO は、cloudApicSubnet MO を生成するために十分な数である必要があります。これにより、cloudtemplateIntNetwork で指定されたすべての cloudRegionName MO を一意の cloudApicSubnet MO に関連付けることができます。cloudApicSubnet MO からのサブネットは、対応するリージョンの cloudCtxProfile で CIDR として使用されます。
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` では、`routerThroughput` は、いずれかのリージョン（つまり、`cloudtemplateIntNetwork` の下にある cloudRegionName）にルータが展開されている場合は変更できません。
クラウド	CT_APICSUBNET_INVALID_HOME_REGION	`cloudApicSubnet` MO では、`capicDeployed` としてマークされたリージョンは有効なリージョンである必要があります。
クラウド	CT_APICSUBNET_REPEATED_REGION	`cloudApicSubnet` MO では、リージョンを最大 1 つのサブネットに関連付けることができます。
クラウド	CT_APICSUBNET_MULTIPLE_HOME_REGION	`cloudApicSubnet` MO では、最大で 1 つのリージョンが `capicDeployed`を true に設定できます。
クラウド	CLOUD_APICSUBNETPOOL_CREATEDBY_USER	`cloudApicSubnetPool` では、`createdBy` 属性は USER である必要があります
クラウド	CLOUD_APICSUBNETPOOL_SUBNET_IP_VERSION	`cloudApicSubnetPool` では、サブネットに IPv4 アドレスが含まれている必要があります。
クラウド	CLOUD_APICSUBNETPOOL_SUBNET_SIZE	`cloudApicSubnetPool`では、サブネットは /24 である必要があります。

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。

Cisco Cloud Network Controller エラー コード



付録 B

セキュリティ グループとルールの作成

セキュリティグループルール

このセクションでは、クラウドネットワーク コントローラのホーム リージョンおよび非ホーム リージョンで Cisco Catalyst 8000V を有効にして AWS でプログラムするセキュリティ グループ ルールについて説明します。

（注） 外部ネットワークは、「クラウドコントローラ起動時のクラウド形成テンプレート」から取得され、クラウド ネットワーク コントローラまたは Cisco Catalyst 8000V にアクセスするネットワークです。

クラウドネットワーク コントローラの起動後に AWS で作成されたセキュリティ グループ ルール

1. **セキュリティグループ**：uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   目的：Cisco クラウド ネットワーク コントローラ管理インターフェイスに接続します。

   インバウンドルール

   1. ルール *1*：（クラウド ネットワーク コントローラへの HTTPS アクセス）

      送信元：外部ネットワーク

      接続先: クラウド ネットワーク コントローラ

      プロトコル- TCP

      ポート – 443

   2. ルール *2*：（デフォルトのルールは、セキュリティグループ内のすべてのトラフィックを許可することです）（このルールは、将来、クラスタとして複数のクラウドネットワークコントローラに使用されます。現在、このルールは、セキュリティ グループに接続されているコントローラ NIC が 1 つしかないため、使用されません。）

セキュリティ グループとルールの作成

送信元：uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

接続先：クラウド ネットワーク コントローラ

プロトコル - 全て

ポート - 全て

3. ルール *3*：（クラウド ネットワーク コントローラへの HTTP アクセス）

送信元：外部ネットワーク

接続先: クラウド ネットワーク コントローラ

プロトコル – TCP

ポート – 80

（注） このルールは、クラウドネットワーク コントローラへのHTTPアクセスに対して有効になっています。HTTPアクセスは、クラウドネットワーク コントローラの通信ポリシーを使用して無効にできます。

4. ルール *4*：

送信元：外部ネットワーク

接続先：クラウド ネットワーク コントローラ

プロトコル – ICMP

ポート：全て

5. ルール *5*：（Kafka ルール）

送信元：外部ネットワーク

接続先：クラウド ネットワーク コントローラ

プロトコル – TCP

ポート：9095

6. ルール *6*：（クラウド ネットワーク コントローラへの ssh アクセス）

送信元：外部ネットワーク

接続先：クラウド ネットワーク コントローラ

プロトコル – TCP

ポート – 22

アウトバウンドルール

1. ルール *1*：（クラウド ネットワーク コントローラからのアウトバウンド通信に必要）

送信元：クラウド ネットワーク コントローラ

接続先：0/0

プロトコル - 全て

ポート - 全て

（注） このルールは、クラウドネットワークコントローラがCiscoライセンスサーバー、DNS、NTPなどの外部サービスにアクセスするために必要です。

2. *ルール 2*：（セキュリティ グループ内の全てのトラフィックを許可するデフォルトルール）

   送信元：クラウド ネットワーク コントローラ

   接続先：uni/tn-infra/cloudapp-cloud-infra / cloudepg-controllers

   プロトコル- 全て

   ポート：全て

（注） このルールは、上記で説明したセキュリティ グループ内の全ての着信を許可するルールに似ています。現在は使用されていません。

2. セキュリティグループ：capic-rCAPICInfra SecurityGroup

   これは、Cisco Catalyst 8000V が展開されるとすぐにインターフェイスから切り離され、インターフェイスは同じルール セットとこのセキュリティ グループを使用して uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers-infra-nic に接続されますはクラウドにそのまま残されます。

   目的：このセキュリティ グループは、クラウド ネットワーク コントローラのインフラ インターフェイスに接続されます。これは、複数のクラウド ネットワーク コントローラ インスタンスをサポートする場合にクラスタリングに使用されます。

（注） このインフラ インターフェイスは外部に公開されず、柔軟性 IP は接続されません。全てのトラフィックは、セキュリティ グループと VPC 内でのみ許可されます。このルールは現在使用されていません。

インバウンドルール

1. *ルール 1*：

   送信元：0/0

   接続先：クラウド ネットワーク コントローラ

   プロトコル – 全て

セキュリティ グループとルールの作成

ポート – 全て

アウトバウンドルール

1. ルール *1*：

   送信元：クラウド ネットワーク コントローラ

   接続先：0/0

   プロトコル – 全て

   ポート：全て

Cisco Catalyst 8000V をホームリージョンと非ホームリージョンに展開した後、ホームリージョンセキュリティグループ cloudepg-controllers でクラウドネットワークコントローラ用に作成されたルール

（注） **uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers** セキュリティ グループの場合、クラウド ネットワーク コントローラの起動時に展開されたルールに加えて、次のルールが追加されます。これらのルールは、Cisco Catalyst 8000V を自宅および自宅以外の地域に展開した後に追加されます。これらのルールは、クラウド ネットワーク コントローラ が Cisco Catalyst 8000V を管理するために必要です。

1. **セキュリティグループ**：uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   Cisco Catalyst 8000V を有効にした後、追加のインバウンドルールは作成されません。

   アウトバウンドルール

   1. ルール *1*：（このルールは、自宅以外の地域の Cisco Catalyst 8000V ごとに追加されます）。

      送信元：クラウド ネットワーク コントローラ

      接続先：Cisco Catalyst 8000V プライベート IP

      プロトコル- TCP

      ポート 22

   2. ルール *2*：（このルールは、各地域の Cisco Catalyst 8000V ごとに追加されます）。

      送信元：クラウド ネットワーク コントローラ

      宛先: /uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra-csr: < **CAT8KV-NAME** > : interface: 3.

      プロトコル- 全て

      ポート：全て

セキュリティ グループとルールの作成

3. *ルール 1*：（このルールは、自宅以外の地域の Cisco Catalyst 8000V ごとに追加されます）。

   送信元：クラウド ネットワーク コントローラ

   接続先：Cisco Catalyst 8000V プライベート IP

   プロトコル- TCP

   ポート- 830

4. *ルール 4*：（このルールは、非ホーム リージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

   送信元：クラウド ネットワーク コントローラ

   接続先：非ホーム リージョン Cisco Catalyst 8000V プライベート IP

   プロトコル- 全て

   ポート - 全て

5. *ルール 5*：

   送信元：クラウド ネットワーク コントローラ

   接続先：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra -routers

   プロトコル- TCP

   ポート- 830

6. *ルール 6*：

   送信元：クラウド ネットワーク コントローラ

   接続先：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra -routers

   プロトコル- TCP

   ポート- 22

2. **セキュリティ グループ**：capic-uni/tn-infra/cloudapp-cloud -infra/cloudepg-controllers-infra-nic

   目的：このセキュリティ グループは、クラウド ネットワーク コントローラのインフラ インターフェイスに接続されます。

（注） このインターフェイスは外部に公開されず、柔軟性 IP は接続されません。全てのトラフィックは、セキュリティ グループと VPC 内でのみ許可されます。

インバウンドルール

1. *ルール 1*：（クラウド ネットワーク コントローラ：デフォルト ルール）

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers- infra -nic

セキュリティ グループとルールの作成

接続先：クラウド ネットワーク コントローラ

プロトコル – 全て

ポート：全て

アウトバウンドルール

1. *ルール 1*：

   送信元：クラウド ネットワーク コントローラ

   接続先：/uni/tn-infra/cloudapp-cloud -infra/cloudepg-controllers-infra-nic

   プロトコル – 全て

   ポート – 全て

Cisco Catalyst 8000V のホームリージョンで作成されたセキュリティグループとルール

1. セキュリティ グループ- uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

   インバウンドルール

   1. *ルール 1*：

      送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

      接続先：Cisco Catalyst 8000V

      プロトコル – TCP

      ポート 22

   2. *ルール* 2：（*Netconf*）

      送信元：クラウドネットワークコントローラのパブリック IP

      接続先：Cisco Catalyst 8000V

      プロトコル- TCP

      ポート- 830

   3. *ルール 3*：（これは、非ホーム リージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

      送信元：リモート Cisco Catalyst 8000V プライベート IP

      接続先：Cisco Catalyst 8000V

      プロトコル – 全て

      ポート - 全て

   4. *ルール 4*：

      送信元：外部ネットワーク

      接続先：Cisco Catalyst 8000V

セキュリティ グループとルールの作成

プロトコル- TCP

ポート- 22

5. *ルール 5*：

送信元：外部ネットワーク

接続先：Cisco Catalyst 8000V

プロトコル- TCP

ポート- 80

6. *ルール 6*：

送信元：外部ネットワーク

接続先：Cisco Catalyst 8000V

プロトコル- TCP

ポート- 443

7. *ルール 7*：

送信元：クラウドネットワークコントローラのパブリック IP

接続先：Cisco Catalyst 8000V

プロトコル- TCP

ポート- 22

8. *ルール 8*：

送信元：外部ネットワーク

接続先：Cisco Catalyst 8000V

プロトコル- ICMP

9. *ルール 9*：（このルールは、Cisco Catalyst 8000V 間の通信を有効にするために必要です）。

送信元：/uni/tn -infra/cloudapp-cloud-infra/cloudepg-infra-routers

接続先：Cisco Catalyst 8000V

プロトコル- 全て

ポート - 全て

10. *ルール 10*：

送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

接続先：Cisco Catalyst 8000V

プロトコル- TCP

セキュリティ グループとルールの作成

ポート- 830

アウトバウンドルール

1. *ルール 1*：（このルールは、非ホーム リージョンの Cisco Catalyst 8000V ごとにプライベート IP を持つ 2 つのインターフェイス用に作成されます）。

   送信元: Cisco Catalyst 8000V

   接続先：リモート（非ホームリージョン）Cisco Catalyst 8000V プライベート IP

   プロトコル- 全て

   ポート - 全て

2. *ルール 2*：（このルールは、Cisco Catalyst 8000V（ホーム リージョンと非ホームリージョンの両方）インターフェイス 3-Gig4 ごとに 1 つ作成されます。）

   送信元: Cisco Catalyst 8000V

   接続先：/uni/tn-infra/cloudapp-cloud/-infra/cloudepg-infra-csr：<CAT8KV_NAME> ：interface：3

   プロトコル – 全て

   ポート - 全て

3. *ルール 3*：

   送信元: Cisco Catalyst 8000V

   接続先：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

   プロトコル- 全て

   ポート - 全て

4. *ルール 4*：

   送信元: Cisco Catalyst 8000V

   接続先：0.0.0.0/0

   プロトコル- 全て

   ポート - 全て

5. *ルール 5*：（リモートリージョン Cisco Catalyst 8000V の gig4 インターフェイスのプライベート IP アドレスごとに 1 つのルールが作成されます）

   送信元: Cisco Catalyst 8000V

   接続先：リモートリージョン Cisco Catalyst 8000V Gig4（Interface-3）プライベート IP

2. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra-csr: <**CAT8KV_NAME**_NONHOME>: interface: 2

（注） 非ホーム リージョン Cisco Catalyst 8000V インターフェイス 2 ごとに 1 つのセキュリティ グループが作成されます。このセキュリティグループは現在使用されておらず、将来の目的のために作成されています。

インバウンドルール

1. *ルール 1*：（自宅以外の地域の Cisco Catalyst 8000V ごとに 1 つ）

   送信元：非ホームリージョン Cisco Catalyst 8000V インターフェイス 2 プライベート IP

   プロトコル- 全て

   ポート：全て

2. *ルール 2*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）

   送信元：uni/tn-infra /cloudapp -cloud- infra/cloudepg-infra-csr：**<CAT8KV_NAME>** ：interface：2

   プロトコル- 全て

   ポート - 全て

3. **セキュリティ グループ**-
   uni/tn-dmmy/cloudapp-dmmy/cloudepg-CAPIC_INTERNAL_EP_SG_DEFAULT

   目的- インフラで作成された未使用のセキュリティ グループ。EPG にセグメント化されるまでエンドポイントを配置するデフォルトのセキュリティグループ。

4. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >: interface: 3

（注） ホーム リージョンの Catalyst 8000V インターフェイス3（Gig4）ごとに 1 つのセキュリティ グループが作成されます。これは、それぞれのローカルリージョン Cisco Catalyst 8000V インターフェイス 3（Gig4）に接続されます。

インバウンドルール

1. *ルール 1*：（このようなルールは 8 個あります）

   送信元：リモート Cisco Catalyst 8000V のプライベート IP（各リモート Cisco Catalyst 8000V のインターフェイスごとに 1 つ）

   プロトコル- 全て

   ポート - 全て

2. *ルール 2*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）（インターフェイスごとに 2 つの Cisco Catalyst 8000V があるため、このようなルールは 4 つになります）。

セキュリティ グループとルールの作成

送信元：uni/tn-infra /cloudapp -cloud- infra/cloudepg-infra-csr：**<HOME and NON HOME REGION CAT8KV_NAME>** ：interface: 1

プロトコル- 全て

ポート - 全て

3. ルール *3*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）（インターフェイスごとに 2 つの Cisco Catalyst 8000V があるため、このようなルールは 4 つになります）。

   送信元：/uni/tn-infra/ cloudapp-cloud-infra/cloudepg-infra-csr<<**HOME and NON HOME REGION CAT8KV_NAME>**>: interface: 2

   プロトコル- 全て

   ポート - 全て

4. ルール *4*：（Cisco Catalyst 8000V ごとに 1 つ作成されます）（インターフェイスごとに 2 つの Cisco Catalyst 8000V があるため、このようなルールは 4 つになります）。

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr<<**HOME and NON HOME REGION CAT8KV_NAME>**: interface: 3

   プロトコル- 全て

   ポート - 全て

5. ルール *5*：

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

   プロトコル- 全て

   ポート - 全て

6. ルール *6*：

   送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   プロトコル- 全て

   ポート - 全て

アウトバウンドルール

1. ルール *1*：

   接続先：外部ネットワーク

   プロトコル – 全て

   ポート - 全て

2. ルール *2*：

   接続先：インターフェイス 3（Gig4）のリモート Cisco Catalyst 8000V プライベート IP（非ホームリージョンの Cisco Catalyst 8000V ごとに 1 つ）

   プロトコル- 全て

セキュリティ グループとルールの作成

ポート - 全て

3. *ルール 3*：（自宅と自宅以外の両方の地域で Cisco Catalyst 8000V ごとに 1 つ作成）

   送信元：/uni/tn -infra/ cloudapp -cloud -infra/ cloudepg -infra -csr：**<CAT8KV_NAME >** ：interface：3

   プロトコル- 全て

   ポート - 全て

5. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >: interface: 2 (Cisco Catalyst 8000V ごとに 1 つ)

   インバウンドルール

   1. *ルール 1*：（Cisco Catalyst 8000V ごとに 1 つ作成）

      送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >:Interface: 2

      プロトコル- 全て

      ポート - 全て

   2. *ルール 2*：（リモートリージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

      送信元：Cisco Catalyst 8000V のリモート プライベート IP

      プロトコル- 全て

      ポート - 全て

   アウトバウンドルール

   1. *ルール 1*：

      接続先：インターフェイス 2（Gig3）およびインターフェイス 3（Gig4）のプライベート IP のリモート Cisco Catalyst 8000V

      プロトコル – 全て

      ポート - 全て

   2. *ルール 2*：（このルールは、ホームリージョンと非ホームリージョンの両方の Cisco Catalyst 8000V に追加されます）。

      接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface：2

      プロトコル- 全て

      ポート - 全て

   3. ルール 3：（このルールは、ホームリージョンと非ホームリージョンの両方の Cisco Catalyst 8000V に追加されます）。

セキュリティ グループとルールの作成

接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface：3

プロトコル- 全て

ポート - 全て

4. *ルール 4*：

接続先：0/0

プロトコル- 全て

ポート - 全て

6. **セキュリティ グループ** - uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >: interface: 1 (Cisco Catalyst 8000V ごとに 1 つ)

インバウンドルール

1. ルール 1：（自宅および自宅以外の地域の Cisco Catalyst 8000V を含む Cisco Catalyst 8000V インターフェイス 1 ごとに 1 つのルールが作成されます）。

送信元：/uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:< **CAT8KV_NAME** >:Interface: 1

プロトコル- 全て

ポート - 全て

2. *ルール 2*：（リモート リージョン Cisco Catalyst 8000V ごとに 1 つ作成されます）

送信元：リモート リージョン Cisco Catalyst 8000V インターフェイス 1（Gig2）のリモート プライベート IP

プロトコル- 全て

ポート - 全て

アウトバウンドルール

1. *ルール 1*：

接続先：インターフェイス 3（Gig4）およびインターフェイス 1（Gig2）のリモート リージョン Cisco Catalyst 8000V プライベート IP

プロトコル – 全て

ポート - 全て

2. *ルール 2*：

接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface: 1

プロトコル- 全て

ポート - 全て

セキュリティ グループとルールの作成

3. *ルール 3*：

   接続先：uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra- csr：**<CAT8KV_NAME>** ：interface：3

   プロトコル- 全て

   ポート - 全て

4. *ルール 4*：

   接続先：0/0

   プロトコル- 全て

   ポート - 全て

Cisco Catalyst 8000V の非ホーム リージョンでは、セキュリティ グループとルールは、ホーム リージョンの上記のセクションで説明したものと同様ですが、次の例外があります。セキュリティ グループを接続先として使用する代わりに、一部のルールにはクラウド ネットワーク コントローラの特定の IP アドレス。

セキュリティ グループとルールの作成

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。