



Azure 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](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



目次

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

第 1 章	新機能および変更された機能に関する情報 1
	新機能および変更された機能に関する情報 1

第 2 章	Cisco Cloud Network Controller について 3
	概要 3
	overlay-2 (セカンダリ) VRF について 4
	外部ネットワーク接続 5
	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 6
	ルーティングおよびセキュリティポリシー: リリース 25.0(1) 以前のリリース 6
	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) 6
	ルーティング ポリシー: リリース 25.0(2) 9
	トンネルのソース インターフェイスの選択 11
	注意事項と制約事項 12
	Cisco Cloud Network Controller GUI について 15

第 3 章	Cisco Cloud Network Controller ポリシー モデル 17
	CNC ポリシーモデルについて 17
	ポリシー モデルの主な特性 18
	論理構造 18
	Cisco CNC ポリシー管理情報モデル 19
	テナント 21
	テナント、ID、およびサブスクリプションについて 22

クラウドコンテキストプロファイル	25
CCR	26
Cisco Catalyst 8000V について	26
CCR の数を変更する	28
Cisco Cloud Network Controller および CCR 向けプライベート IP アドレス サポート	30
VRF	31
クラウドアプリケーションプロファイル	32
クラウドエンドポイント グループ	33
クラウドサービスエンドポイント グループ	35
サービス タイプについて	38
展開タイプについて	41
セキュリティ グループ	43
ASG および NSG の注意事項と制限事項	45
セキュリティ ルール	46
ソフトウェア アップグレードまたはダウングレードによる NGS 動作	47
コントラクト	49
コントラクト ルール統合のためのコンマ区切りフィルタのサポート	50
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	51
クラウドテンプレートの概要	52
管理対象オブジェクトの関係とポリシー解決	56
デフォルト ポリシー	57
共有サービス	58

第 4 章

Cisco Cloud Network Controller コンポーネントの構成	59
Cisco Cloud Network Controller の設定について	59
GUI を使用した Cisco Cloud Network Controller の構成	59
Cisco Cloud Network Controller GUI を使用したテナントの作成	59
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	65
Cisco Cloud Network Controller GUI を使用した VRF の作成	66
Cisco Cloud Network Controller GUI を使用した外部ネットワークの作成	67
グローバル VRF 間ルート リーク ポリシーの構成	71

Cisco Cloud Network Controller GUI を使用したリーク ルートの構成	73
Cisco Cloud Network Controller GUI を使用した VRF 間ルート リークの構成	73
Cisco Cloud Network Controller GUI を使用した内部 VRF のリーク ルートの構成	76
Azure サイトから外部デバイスへの接続を有効にする	79
外部デバイス構成ファイルのダウンロード	79
Azure サイトから外部デバイスへの接続を有効にする	80
Cisco Cloud Network Controller GUI を使用した EPG の作成	83
Cisco Cloud Network Controller GUI を使用したアプリケーション EPG の作成	83
Cisco Cloud Network Controller GUI を使用した外部 EPG の作成	89
サービス EPG の作成	94
Cisco Cloud Network Controller GUI を使用したフィルタの作成	108
Cisco Cloud Network Controller GUI を使用したコントラクトの作成	111
Cisco Cloud Network Controller GUI を使用したテナント間契約の作成	113
Cisco Cloud Network Controller GUI を使用したネットワーク セキュリティ グループの構成	116
セキュリティ グループの詳細の表示	120
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	122
Creating a Cloud Context Profile Using the Cisco Cloud Network Controller GUI	123
Azure での仮想マシンの構成	127
Cisco Cloud Network Controller GUI を使用したバックアップ構成の作成	128
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	133
Cisco Cloud Network Controller GUI を使用したスケジューラの作成	134
Cisco Cloud Network Controller GUI を使用してリモートの場所を作成する	137
Cisco Cloud Network Controller GUI を使用したログイン ドメインの作成	139
Cisco Cloud Network Controller GUI を使用したセキュリティ ドメインの作成	143
Cisco Cloud Network Controller GUI を使用したロールの作成	144
Cisco Cloud Network Controller GUI を使用した認証局の作成	150
Cisco Cloud Network Controller GUI を使用したキー リングの作成	152
Cisco Cloud Network Controller GUI を使用したローカル ユーザーの作成	154
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)	159

スマート ライセンスの設定	162
クラウドリソースの命名	163
命名ルールに使用できる変数	163
命名ルールのガイドラインと制限事項	166
クラウドリソースの命名規則の表示	167
REST API を使用した Cisco Cloud Network Controller の構成	168
REST API を使用したテナントの作成	168
REST API を使用したコントラクトの作成	170
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	170
REST API を使用したクラウドリージョンの管理	171
REST API を使用したフィルタの作成	172
REST API を使用したアプリケーションプロファイルの作成	172
REST API を使用したネットワーク セキュリティ グループの構成	173
REST API を使用した EPG の作成	173
REST API を使用したクラウド EPG の作成	174
REST API を使用した外部クラウド EPG の作成	174
REST API を使用したサービス EPG の作成	175
REST API を使用したクラウドテンプレートの作成	176
REST API を使用して VRF リーク ルートの構成	178
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	179
グローバルクラウドリソースの命名規則の定義または特定のオブジェクトの名前のオーバーライド	180
<hr/>	
第 5 章	システムの詳細の表示 183
VM ホスト メトリックのモニタリング	183
GUI を使用した VM ホストメトリックのモニタリング	183
REST API を使用した VM ホストメトリックスの監視	186
アプリケーション管理詳細の表示	187
クラウドリソースの詳細の表示	188
操作の詳細の表示	190
インフラストラクチャの詳細の表示	193

管理の詳細の表示 193

Cisco Cloud Network Controller GUI を使用したヘルス詳細の表示 196

第 6 章

レイヤ 4 から レイヤ 7 サービスの展開 199

概要 199

サービス グラフについて 199

クラウド ネイティブおよびサードパーティ サービスでのサービス グラフの使用 200

アプリケーション ロード バランサの概要 201

ネットワーク ロードバランサについて 202

Azure ネットワーク ロードバランサの複数のフロントエンド IP アドレスの構成について 203

サードパーティのロードバランサについて 205

すべてのトラフィックを許可のオプションについて 205

サーバー プールへのダイナミック サーバーのアタッチ 208

VNet 間サービスについて 208

マルチノードについて 209

レイヤ 4 ~ レイヤ 7 サービス リダイレクト 209

パススルー ルール 210

リダイレクト プログラミング 210

リダイレクト ポリシー 211

リダイレクトを構成するためのワークフロー 212

ユースケースの例 212

クラウド ネイティブおよびサードパーティ サービスによるサービス グラフの使用例 230

リダイレクトのないユースケースの例 230

リダイレクトの使用例 239

リダイレクトの注意事項と制約事項 255

Cisco Cloud Network Controller GUI を使用したセカンダリ VRF への新しい CIDR の追加 257

サービス グラフの展開 260

GUI を使用したサービス グラフの展開 260

Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 261

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 272

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	275
REST API を使用したサービス グラフの展開	282
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	282
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	283
REST API を使用したサードパーティ ファイアウォールの作成	284
REST API を使用したサードパーティ ロードバランサの作成	285
アプリケーション ゲートウェイの REST API を使用したサービス グラフの作成	285
Azure ロードバランサの REST API を使用してサービス グラフを作成する	286
サードパーティ ロードバランサの REST API を使用したサービス グラフの作成	287
REST API を使用してマルチノード サービス グラフを作成する	288
REST API を使用してリダイレクトでマルチノード サービス グラフを作成する	291
REST API を使用してサービス グラフを添付する	295
REST API を使用した HTTPS サービス ポリシーの構成	296
REST API を使用したキー リングの設定	297
REST API を使用した HTTPS サービス ポリシーの作成	299

第 7 章

Cisco Cloud Network Controller のセキュリティ	301
アクセス、認証およびアカウントिंग	301
構成	301
TACACS+、RADIUS、LDAP、および SAML アクセスの構成	302
Overview	302
TACACS+ アクセス用の Cisco Cloud Network Controller の構成	302
RADIUS アクセス用の Cisco Cloud Network Controller の構成	304
Cisco Cloud Network Controller への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の構成	305
LDAP Access の構成	305
Cisco AVPair を使用した APIC アクセス用の Windows Server 2008 LDAP の設定	306
LDAP アクセスのための Cisco Cloud Network Controller の構成	306
SAML アクセス用の Cisco Cloud Network Controller の構成	308
About SAML	309
SAML アクセス用の Cisco Cloud Network Controller の構成	309

	Okta で SAML アプリケーションの設定	311
	AD FS で Relying Party Trust の設定	311
	HTTPS Access の構成	311
	HTTPSアクセスについて	311
	カスタム証明書の構成のガイドライン	312
	GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定	312
<hr/>		
第 8 章	アクセスの制限	315
	ドメイン別にアクセスを制限する	315
	RBAC ルール	316
	RBACルール	321
	制限付きドメインのガイドラインと制限事項	321
	Cisco Cloud Network Controller GUI を使用した RBAC ルールの作成	322
<hr/>		
第 9 章	設定のばらつき	325
	構成のばらつき通知と障害	325
	構成ドリフトのメイン ページにアクセスする	326
	欠落しているコントラクト構成の確認	329
	欠落している EPG 構成の確認	331
	欠落している VRF 構成の確認	332
	構成のばらつきのトラブルシューティング	334
<hr/>		
第 10 章	Cisco クラウド ネットワーク コントローラで管理されたクラウド サイトと非 ACI リモート サイト間の接続の設定	337
	エクスプレス ルート ゲートウェイを使用して接続を構成する	337
	リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて	337
	リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて	339
	リダイレクトなしの Express Route ゲートウェイの展開について	341
	リダイレクトなしのエクスプレス ルート ゲートウェイの展開	342
	VPN ゲートウェイ (仮想ネットワーク ゲートウェイ) を使用した接続の構成	344
	Configuring Connectivity Using VPN Gateway	345

付録 A :	Cisco Cloud Network Controller エラー コード 353
	Cisco Cloud Network Controller エラー コード 353

付録 B :	サービス EPG 構成例 361
	Azure Kubernetes Services (AKS) サービス EPG 構成例 361
	クラウドコンテキストプロファイルでサブネットの作成 362
	AKS のクラウド サービス EPG の作成 363
	アウトバウンドセキュリティ ルールの確認 365
	Kubernetes サービスの作成 366
	新しい Kubernetes サービスの確認 370
	Azure および AKS CLI のインストール 373



第 1 章

新機能および変更された機能に関する情報

この章は、次の項で構成されています。

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

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。	



第 2 章

Cisco Cloud Network Controller について

- [概要 \(3 ページ\)](#)
- [overlay-2 \(セカンダリ\) VRF について \(4 ページ\)](#)
- [外部ネットワーク接続 \(5 ページ\)](#)
- [サポートされているルーティングとセキュリティ ポリシーの概要 \(6 ページ\)](#)
- [トンネルのソース インターフェイスの選択 \(11 ページ\)](#)
- [注意事項と制約事項 \(12 ページ\)](#)
- [Cisco Cloud Network Controller GUI について \(15 ページ\)](#)

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。

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



- (注)
- Cisco 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ネイティブコンストラクトに変換して、ポリシーをオンプレミスサイトと一致させます。

パブリッククラウドに Cisco ACI を拡張することの詳細については、*Cisco Cloud 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。

overlay-2 (セカンダリ) VRF について

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

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

- インフラテナントで、overlay-2 VRF を含む任意のセカンダリ VRF でクラウド EPG を作成できます。インフラ VNet で新しい CIDR を作成すると、それらの CIDR は overlay-2 VRF に暗黙的にマッピングされないため、新しい CIDR をセカンダリ VRF にマッピングするのはユーザの責任です。
- インフラ VNet のクラウドコンテキストプロファイルは、複数の VRF (インフラ VNet の overlay-1 および overlay-2 VRF) にマッピングできます。
- クラウドでは、サブネットのルートテーブルは、ネットワークの分離を実現するための最も詳細なエンティティです。したがって、overlay-1 VRF のすべてのシステム作成クラウド

サブネットと、overlay-2 VRF のユーザ作成サブネットは、ネットワークセグメンテーションを実現するためにクラウド内の個別のルートテーブルにマッピングされます。



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

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

外部ネットワーク接続

AWS と Cisco Cloud Network Controller の外部ネットワーク接続は、インフラ VNet の CCR からの EVPN 接続を使用することによってのみ利用可能でした。インフラ VNet CCR から IPSec/BGP を使用する任意の外部デバイスへの IPv4 接続もサポートされます。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、リリース 25.0(1) で提供される新しい外部ネットワーク接続を可能にするコンポーネントの詳細について説明します。

外部 VRF

外部 VRF は、クラウドに存在しない一意の VRF ですが、1 つ以上の外部ネットワークに関連付けられています。VNet 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 ネットワークコントローラ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

Azure 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 VNet CCR からこれらの非 ACI 外部デバイスへの IPv4 セッションが外部 VRF で作成され、外部 VRF とサイト ローカル VRF の間で VRF 間ルーティングが設定されます。

このタイプの接続に関する注意事項と制限事項を次に示します。

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

注意事項と制約事項

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：リリース 25.0(1) 以前のリリース

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

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

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

ルーティングおよびセキュリティポリシー: リリース 25.0(1)

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



- (注) このセクションで説明するルーティング ポリシーは、25.0(1) リリース専用であり、内部と外部 VRF の間でのみ適用されます。25.0(2) リリースでのルーティング ポリシーとセキュリティ ポリシーの変更については、[ルーティング ポリシー: リリース 25.0\(2\) \(9 ページ\)](#) 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 \(73 ページ\)](#) 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 を使用した外部 EPG の作成 \(89 ページ\)](#) 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 \(111 ページ\)](#) を参照してください。

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

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

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

ルート リークは、ルート マップを使用して内部 VRF と外部 VRF の間で発生します。Cisco Cloud 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

注意事項および制約事項

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

- ルートは常に、内部 VRF と外部 VRF の間で双方向にリークされます。
たとえば、内部 VRF (V1) と外部 VRF (Ext-V1) を持つユーザー テナント (t1) があるとしします。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\(1\) \(6 ページ\)](#) 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\(1\) \(6 ページ\)](#) 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 \(9 ページ\)](#)
- [グローバルな Inter-VRF ルート リーク ポリシー \(9 ページ\)](#)
- [注意事項と制約事項 \(11 ページ\)](#)

内部 VRF 間のルート リーク

以前の 25.0(1) リリースでは、内部 VRF と外部 VRF のペア間でリークするルートを指定する独立したルーティング ポリシーを設定できる、VRF 間ルート マップベースのルーティング機能が導入されました。このルート マップベースのルーティング機能は、特に内部 VRF と外部 VRF の間に適用されます。内部 VRF のペア間のルーティングを設定する場合、[ルーティングおよびセキュリティ ポリシー: リリース 25.0\(1\) \(6 ページ\)](#) 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 (Cisco Cloud ネットワーク コントローラ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) より前に構成された Cisco Cloud ネットワーク コントローラがある場合、コントラクトベースのルーティングが有効になります。

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 \(76 ページ\)](#) 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 スイッチを無効にして、コントラクトベースのルーティングからルートマップベースのルーティングに切り替える場合、**[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せん。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。
- レイヤ 4 からレイヤ 7 へのサービス挿入は引き続きコントラクトを介して行われるため、このような状況では、グローバル レベルでコントラクト ベースのルーティングを有効にする必要があります。
- Azure エキスプレッスルートとの外部接続では、引き続きコントラクトベースのルーティングが使用されます。
- `leakExternalPrefix` は、SSH を実行する外部 EPG 用に構成された外部エンドポイントセレクタと重複しないようにしてください。そうしないと、SSH が壊れます。この場合、プレフィックスは、Azure のインターネットへのデフォルトルートではなく、ネットワークロードバランサを指します。
- インターネット トラフィックをリモートサイトにリダイレクトする必要がない限り、`leakInternalPrefix` (**Leak All**、または `0.0.0.0/0`) は使用しないでください。そうしないと、SSH が破損します。この場合、インターネットへのデフォルトルートは、ネットワークロードバランサを指す新しい UDR によって上書きされます。

トンネルのソース インターフェイスの選択

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、`cloudtemplateIpseTunnelSourceInterface` 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。

```
<cloudtemplateIpseTunnel peeraddr="173.36.19.2" preSharedKey="def" poolname="pool11">
```

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

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

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

注意事項と制約事項

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

注意事項と制約事項

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

- クラウド CCR (クラウドルータ) で VRF 間ルートリークを使用しているときに、オンプレミスとクラウドの間で複数の VRF をストレッチすることはできません。たとえば、EPG1 を持つ VRF1 が拡張され、EPG2 を持つ VRF2 も拡張される状況では、EPG1 は EPG2 とコントラクトできません。ただし、クラウド内に複数の VRF を設定して、1つのオンプレミス VRF と 1つ以上のコントラクトを共有することができます。
- クラウド上の CSR にアドバタイズするために、外部でアドバタイズされたオンプレミスサイトのブリッジドメインサブネットを設定します。
- テナントのオブジェクトを設定する前に、古いクラウドリソース オブジェクトを確認します。アカウントを管理していた以前の Cisco Cloud Network Controller 仮想マシンから適切に消去されなかった場合、古い設定が存在する可能性があります。Cisco Cloud Network Controller は古いクラウドオブジェクトを表示できますが、削除することはできません。クラウドアカウントにログインし、手動で削除する必要があります。



- (注) テナント サブスクリプション 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。

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

古いクラウドリソースを確認するには、次の手順を実行します。

1. Cisco Cloud Network Controller GUI から、[ナビゲーション (Navigation)]メニュー> [アプリケーション管理 (Application Management)]> [テナント (Tenants)]の順にクリックします。[テナント (Tenants)]サマリー テーブルは、テナントのリストとともに、サマリー テーブルの行として作業ペインに表示されます。
 2. オブジェクトを作成するテナントをダブルクリックします。[概要 (Overview)]、[クラウドリソース (Cloud Resources)]、[アプリケーション管理 (Application Management)]、[統計 (Statistics)]、および[イベント分析 (Event Analytics)]タブが表示されます。
 3. [クラウドリソース (Cloud Resources)]>[アクション (Actions)]>[古いクラウドリソース (View Stale Cloud Objects)]の順にクリックします。[古いクラウドオブジェクト (Stale Cloud Objects)]ダイアログボックスが表示されます。
- Cisco Cloud 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、Azure インフラテナントサブスクリプションの Azure IAM ユーザ、および他のテナントアカウントが、Cisco Cloud Network Controller が作成するリソースを妨害しないことも期待されます。このため、Cisco Cloud Network Controller が Azure 上で作成するすべてのリソースには、次の 2 つのタグの少なくとも 1 つがあります。
 - AciDnTag
 - AciOwnerTag

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

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

- 共有 L3Out を構成する場合:
 - オンプレミスの L3Out とクラウド EPG をテナント共通にすることはできません。
 - オンプレミスの L3Out とクラウド EPG が異なるテナントにある場合は、テナント共通でコントラクトを定義します。オンプレミス サイトまたはクラウドテナントでコントラクトすることはできません。
 - オンプレミスの L3Out 外部 EPG (l3extInstP) でクラウド EPG の CIDR を指定します。

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



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

表 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 プロファイル	500
EPG	500
クラウド エンドポイント	1000
VRF	20
クラウド コンテキスト プロファイル	40
コントラクト	1000
サービスグラフ	200
サービス デバイス	100

Cisco Cloud Network Controller GUI について

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

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

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

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 \(59 ページ\)](#) 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 \(17 ページ\)](#)
- [ポリシー モデルの主な特性 \(18 ページ\)](#)
- [論理構造 \(18 ページ\)](#)
- [Cisco CNC ポリシー管理情報モデル \(19 ページ\)](#)
- [テナント \(21 ページ\)](#)
- [クラウド コンテキスト プロファイル \(25 ページ\)](#)
- [VRF \(31 ページ\)](#)
- [クラウド アプリケーション プロファイル \(32 ページ\)](#)
- [クラウド エンドポイント グループ \(33 ページ\)](#)
- [セキュリティ グループ \(43 ページ\)](#)
- [コントラクト \(49 ページ\)](#)
- [クラウド テンプレートの概要 \(52 ページ\)](#)
- [管理対象オブジェクトの関係とポリシー解決 \(56 ページ\)](#)
- [デフォルト ポリシー \(57 ページ\)](#)
- [共有サービス \(58 ページ\)](#)

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。

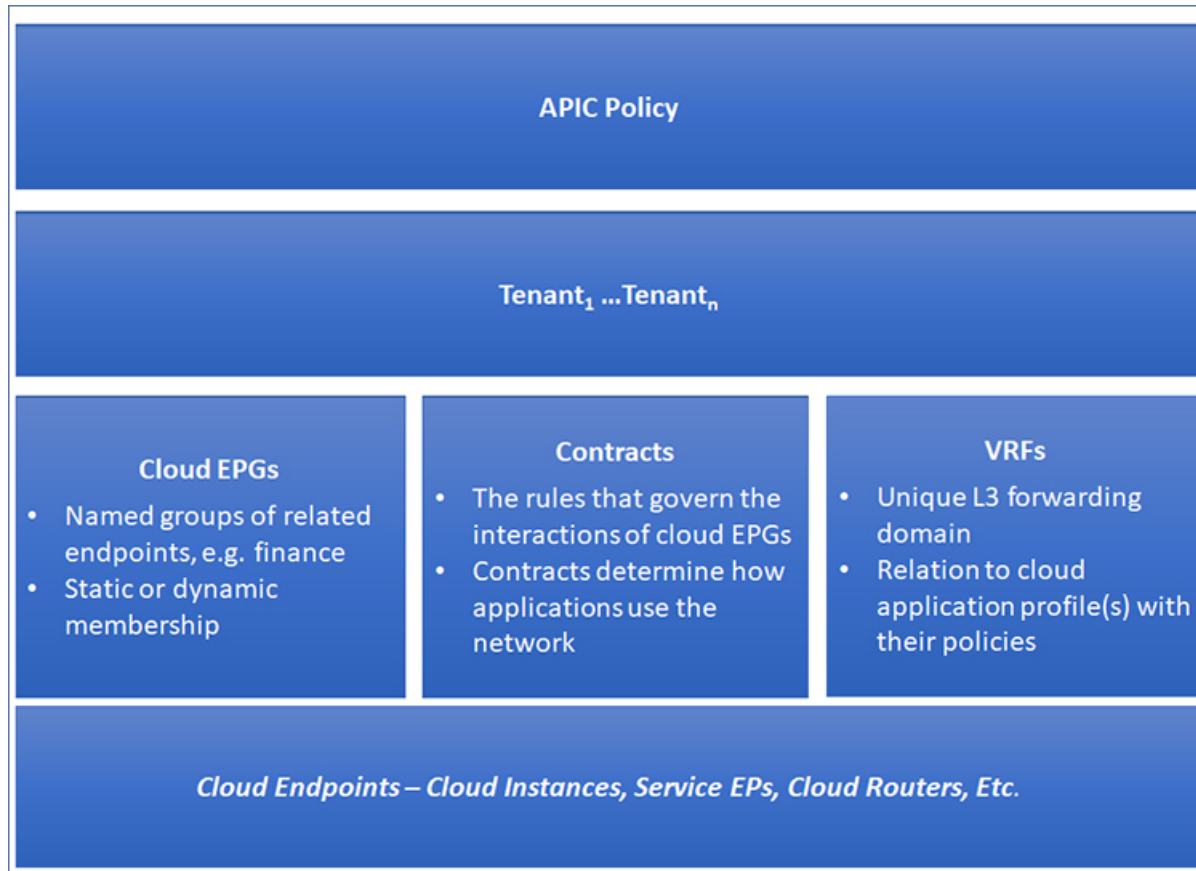
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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、ネットワークの動作を誘導する必要があり、その逆ではありません。

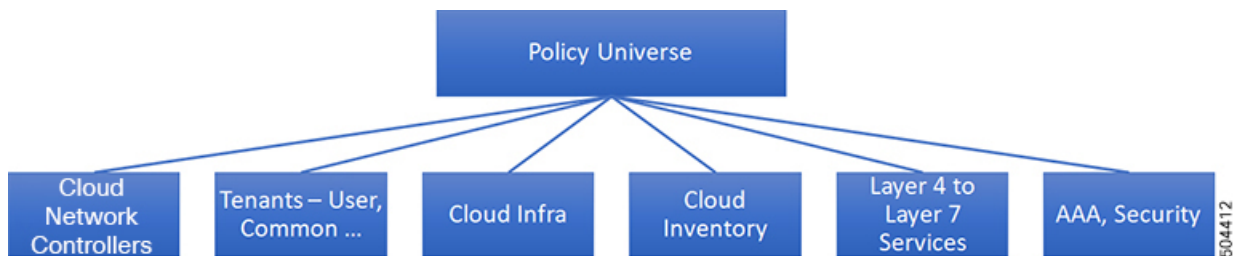
Cisco CNC ポリシー管理情報モデル

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 バリエーションと同様に、Cisco Cloud Network Controller によって、MIT の階層構造内のオブジェクトの場所に応じて継承できるオブジェクトのプロパティとして管理可能な特性を示すことにより、管理対象リソースの制御が可能になります。

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

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

図 2: Cisco 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。

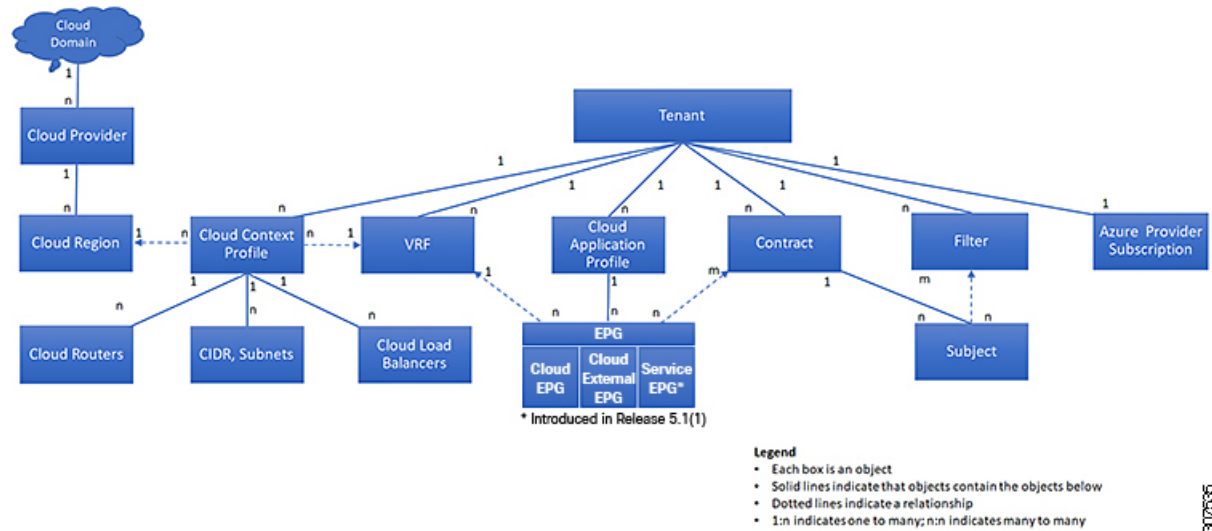
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ4～レイヤ7のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、[レイヤ4からレイヤ7サービスの展開 \(199 ページ\)](#) を参照してください。
- アクセス、認証、およびアカウントिंग (AAA) ポリシーは、Cisco Cloud 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 \(301 ページ\)](#) 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、仮想ルート転送（VRF）インスタンス、クラウドコンテキストプロファイル、Azure プロバイダー構成、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。クラウドコンテキストプロファイルは、VRF、テナント、およびリージョンとともに、Azure のリソースグループを表します。VNET は、VRF 名に基づいてリソースグループ内に作成されます。

テナントはアプリケーションポリシーの論理コンテナです。クラウドインフラストラクチャには、複数のテナントを含めることができます。レイヤ4～7のサービスを展開する前に、テナントを設定する必要があります。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。

テナント、ID、およびサブスクリプションについて

AzureにはActive Directory構造があります。最上位レベルの構造は組織であり、その下にディレクトリ（Azureテナントとも呼ばれます）があります。ディレクトリ内には、1つ以上のAzureサブスクリプションを設定できます。

特定のAzureコンポーネント間の関係は次のとおりです。

テナントサブスクリプションリソースグループリソース >>>

それぞれの説明は次のとおりです。

- 1つのテナントは複数のサブスクリプションを持つことができますが、各サブスクリプションは1つのテナントにのみ属することができます。

- 1つのサブスクリプションに複数のリソースグループを含めることができますが、各リソースグループは1つのサブスクリプションにのみ属することができます。
- 1つのリソースグループは複数のリソースを持つことができますが、各リソースは1つのサブスクリプションにのみ属することができます。

次のセクションでは、これらのコンポーネントについて詳しく説明します。

- [Azure と Cisco Cloud Network Controller コンポーネントのマッピング \(23 ページ\)](#)
- [Azureサブスクリプションについて \(23 ページ\)](#)
- [テナントとアイデンティティについて \(23 ページ\)](#)

Azure と Cisco Cloud Network Controller コンポーネントのマッピング

Cisco Cloud Network Controller では、各 Azure リソース グループは1つの Cisco Cloud Network Controller テナントにマッピングされます。1つの Cisco Cloud Network Controller テナントには複数の Azure リソース グループがあります。

特定の Cisco Cloud Network Controller コンポーネント間の関係は次の通りです。

テナントVRFリージョン >>

Cisco Cloud Network Controller で VRF を作成すると、新しいリソース グループも Azure に作成されます。

Azureサブスクリプションについて

Azureサブスクリプションは、Azureクラウドサービスの支払いに使用されます。Azureサブスクリプションには、Azure Active Directory (Azure AD) との信頼関係があり、Azure ADを使用してユーザ、サービス、およびデバイスを認証します。複数のサブスクリプションは同じAzure ADを信頼できますが、各サブスクリプションは1つのAzure ADのみを信頼できます。

Azureでは、同じ Azure サブスクリプション識別子を複数の CNC テナントに使用できます。これは、1つのAzureサブスクリプションを使用してインフラテナントを設定し、同じサブスクリプションで複数のユーザテナントを設定できることを意味します。CNC テナントはAzureサブスクリプションに関連付けられています。

テナントとアイデンティティについて

Azure および Cisco Cloud Network Controller で使用できるさまざまなタイプのテナントとアイデンティティを次に示します。



- (注) マネージドアイデンティティとサービスプリンシパルの両方が、インフラ テナントとユーザテナントのアクセス タイプとしてサポートされます。

マネージドアイデンティティ

マネージドアイデンティティは、Azure AD認証をサポートするリソースに接続するときに使用するアプリケーションのアイデンティティを提供します。アプリケーションは管理対象IDを使用してAzure ADトークンを取得できます。たとえば、開発者が安全な方法でクレデンシャルを保存したり、ストレージアカウントにアクセスしたりするために、アプリケーションでマネージドアイデンティティを使用してAzure KeyVaultなどのリソースにアクセスできます。

<https://docs.microsoft.com/en-us/azure/key-vault/general/overview>

管理対象IDを使用する利点は次のとおりです。

- クレデンシャルにはアクセスできないため、クレデンシャルを管理する必要はありません。
- マネージドIDを使用して、独自のアプリケーションを含むAzure AD認証をサポートする任意のリソースを認証できます。
- マネージドIDは追加コストなしで使用できます。

Azureの管理対象アイデンティティの詳細については、以下を参照してください。

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

[**マネージドアイデンティティ (managed identity)**]を使用して Cisco Cloud Network Controller のテナントを構成する場合、Azure ポータルおよび Cisco Cloud Network Controller の次の構成を作成します。

1. Azureポータルで、仮想マシンのロール割り当てを追加します。このオプションは、Azureサブスクリプションが（同じ組織の）同じAzureディレクトリにある場合に使用します。



(注) Azureサブスクリプションが異なるディレクトリにあり、マネージドIDを使用してテナントを設定する場合は、Azureコンソールに移動し、各サブスクリプションをクリックして同じAzureディレクトリの下にサブスクリプションを移動できます。これは、（異なるサブスクリプションを含む）ディレクトリが同じ親組織の子である場合にのみ実行できます。

2. Cisco クラウドネットワーク コントローラでは、Cisco クラウドネットワーク コントローラでテナントを構成するとき [管理対象アイデンティティ (Managed Identity)] オプションを選択します。

これらの構成の詳細については、[Cisco Cloud Network Controller GUI を使用したテナントの作成 \(59 ページ\)](#) を参照してください。

サービス プリンシパル (Service Principal)

Azureサービスプリンシパルは、Azureリソースにアクセスするためのアプリケーション、ホステッドサービス、および自動化ツールで使用するために作成されたIDです。異なるサブスクリプションでテナントを設定する場合は、サービスプリンシパルIDを使用します。サブスクリプションが同じ組織内の異なる Azure ディレクトリ (Azure テナント) にあるか、サブスクリプションが異なる組織にある可能性があります。

[サービスプリンシパル (**service principal**)] を使用して Cisco Cloud Network Controller でテナントを構成する場合は、Azure ポータルと Cisco Cloud Network Controller で次の構成を行います。

1. Azureポータルで、**アプリケーション**のロール割り当てを追加します。この場合、クラウドリソースは特定のアプリケーションを介して管理されます。
2. Cisco Cloud Network Controller では、Cisco Cloud Network Controller でテナントを構成するとき **[サービスプリンシパル (**service principal**)]** オプションを選択します。このページに入力するサブスクリプションは、同じ組織内の異なるAzureディレクトリ (Azureテナント) に配置することも、異なる組織に配置することもできます。

これらの構成の詳細については、[Cisco Cloud Network Controller GUI を使用したテナントの作成 \(59 ページ\)](#) を参照してください。

共有テナント

Azureサブスクリプションを上記の2つの方法のいずれかにすでに関連付けており、そのサブスクリプションにさらにテナントを作成する場合は、このオプションを選択します。

[共有テナント (**shared tenant**)] を使用して Cisco Cloud Network Controller でテナントを構成する場合は、Azure ポータルと Cisco Cloud Network Controller で次の構成を行います。

1. 上記の2つの方法のいずれかでAzureサブスクリプションをすでに関連付けているため、Azureで共有テナント専用の設定を行う必要はありません。共有テナントでは、既存のサブスクリプションにさらにテナントを作成します。
2. Cisco Cloud Network Controller では、Cisco Cloud Network Controller でテナントを構成するとき **[共有 (**Shared**)]** オプションを選択します。

これらの構成の詳細については、[Cisco Cloud Network Controller GUI を使用したテナントの作成 \(59 ページ\)](#) を参照してください。

クラウドコンテキストプロファイル

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

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

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](#).

Cisco Catalyst 8000V について

以下は、Cisco Catalyst 8000V の更新です。

- [ライセンス](#) (26 ページ)
- [Throughput](#) (27 ページ)

ライセンス

Cisco Cloud Network Controller 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

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

BYOL ライセンス モデル

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

- ティアベースの Cisco Catalyst 8000V ライセンスの1つにサブスクライブする手順については、[Cisco Catalyst 8000V Edge ソフトウェア](#)を参照してください。
- 層に基づくさまざまなスループットの詳細については、[Throughput \(27 ページ\)](#) を参照してください。

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

PAYG ライセンス モデル

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

スループットを得るために VM サイズに完全に依存しているため、PAYG ライセンス モデルを有効にするには、まず現在の Cisco Catalyst 8000V の展開を解除してから、新しい VM サイズでの初回セットアップを使用して再度展開します。詳細については、[\[Cisco Cloud Network Controller for Azuru 設置ガイド \(Cisco Cloud Network Controller for Azure Installation Guide\)\]](#)の

セットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。



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



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

Throughput

Cisco Cloud Network Controller 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

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

1. 所有ライセンス持ち込み (BYOL)

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

CCR スループット	Azure VMサイズ
T0 (最大 15M のスループット)	DS3_v2
T1 (最大 100M のスループット)	DS3_v2
T2 (最大 1G のスループット)	DS3_v2
T3 (最大 10G のスループット)	F16s_v2

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

2. ペイアズユーゴー (PAYG) ライセンス モデル

このモデル向けに、Cisco Cloud Network Controller は Cisco Catalyst 8000V 仮想ルータを使用し、クラウドネットワークキングのニーズに合わせて Azuru コンピュートインスタンスの範囲をサポートします。

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

Azure 上の VmName	メモリー	vCPU の数	NetworkBw
DS3V2	14GiB	4	最大 3 ギガビット
DS4V2	28GiB	8	最大 6 ギガビット
F16SV2	32GiB	16	最大 12.5 ギガビット
F32SV2	64GiB	32	最大 16 ギガビット

CCR の数を変更する

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

次の点に注意してください。

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

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

- [クラウド コンテキスト プロファイルの作成 (Create Cloud Context Profile)] ページに移動します。
[アプリケーション管理 (Application Management)] >> [クラウド コンテキスト プロファイル (Cloud Context Profiles)]
- インフラクラウド コンテキスト プロファイルの [名前 (Name)] 列の下にあるリンクをクリックします。
このクラウド コンテキスト プロファイルの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。
- [詳細 (Details)] アイコンをクリックします (🔍)。
このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。
- ウィンドウの右上隅の鉛筆アイコンをクリックします。
[クラウド コンテキスト プロファイルの編集 (Edit Cloud Context Profile)] ウィンドウが表示されます。
- [ハブ ネットワーク ピアリング (Hub Network Peering)] フィールドのチェックを外します (無効にします)。
- 設定が終わったら [Save] をクリックします。

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

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

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

- a) Cisco Cloud Network Controller GUI で、インテントアイコン (🔗) をクリックし、**[Cloud Network Controller セットアップ (Cloud Network Controller Setup)]** を選択します。
- b) **[リージョン管理 (Region Management)]** エリアで、**[設定の編集 (Edit Configuration)]** をクリックします。
- c) **[管理するリージョン (Regions to Manage)]** ウィンドウで、**[次へ (Next)]** をクリックします。
[一般接続 (General Connectivity)] ウィンドウが表示されます。
- d) **[全般 (General)]** 領域の **[クラウドルータのサブネットプール (Subnet Pools for Cloud Routers)]** フィールドで、CCR のサブネットを追加する場合は、**[クラウドルータのサブネットプールの追加 (Add Subnet Pool for Cloud Routers)]** をクリックします。

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


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

- a) 使用する Cisco Cloud Network Controller GUI で、インテントアイコン (🔗) をクリックし、**[Cloud Network Controller セットアップ (Cloud Network Controller Setup)]** を選択します。
- b) **[リージョン管理 (Region Management)]** エリアで、**[設定の編集 (Edit Configuration)]** をクリックします。
[管理するリージョン (Regions to Manage)] ウィンドウが表示されます。
- c) **[次へ (Next)]** をクリックして、以前に選択したリージョンと CCR をそのままにします。
[一般接続 (General Connectivity)] ウィンドウが表示されます。
- d) **[一般接続 (General Connectivity)]** ウィンドウで **[CCR]** エリアを見つけ、**[リージョンごとのルータ数 (Number of Routers Per Region)]** フィールドで、必要な変更を加えて CCR の数を増減します。
- e) **[次へ (Next)]** をクリックし、次のページに必要な情報を入力して、**[保存して続行 (Save and Continue)]** をクリックします。

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

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

- a) **[クラウドコンテキストプロファイルの作成 (Create Cloud Context Profile)]** ページに移動します。
[アプリケーション管理 (Application Management)]]>>**[クラウドコンテキストプロファイル (Cloud Context Profiles)]**]

- b) インフラクラウドコンテキストプロファイルの **[名前 (Name)]** 列の下にあるリンクをクリックします。
このクラウドコンテキストプロファイルの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。
- c) **[詳細 (Details)]** アイコンをクリックします ()。
このクラウドコンテキストプロファイルの詳細情報を提供する別のウィンドウが表示されます。
- d) ウィンドウの右上隅の鉛筆アイコンをクリックします。
[クラウドコンテキストプロファイルの編集 (Edit Cloud Context Profile)] ウィンドウが表示されます。
- e) **[ハブネットワークピアリング (Hub Network Peering)]** フィールドをチェック (有効) します。
- f) 設定が終わったら **[Save]** をクリックします。
これらの手順を繰り返して、すべてのインフラクラウドコンテキストプロファイルで Azure VNet ピアリングを有効にします。

Cisco Cloud Network Controller 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 は、BGP および OSPF ルータ ID として使用されます。CCR にプライベート IP アドレスが割り当てられている場合、エクスプレス ルートを介したオンプレミスの ACI サイトを持つハイブリッドクラウドがサポートされます。

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 \(クラウドテンプレートの構成\) \(159 ページ\)](#) 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、*[Azure 向け Cisco Cloud Network Controller Installation Guide (Cisco Cloud Network Controller for Azure Installation Guide)]* の *[Deploying the Cisco Cloud Network Controller in Azure]* 手順を参照してください。

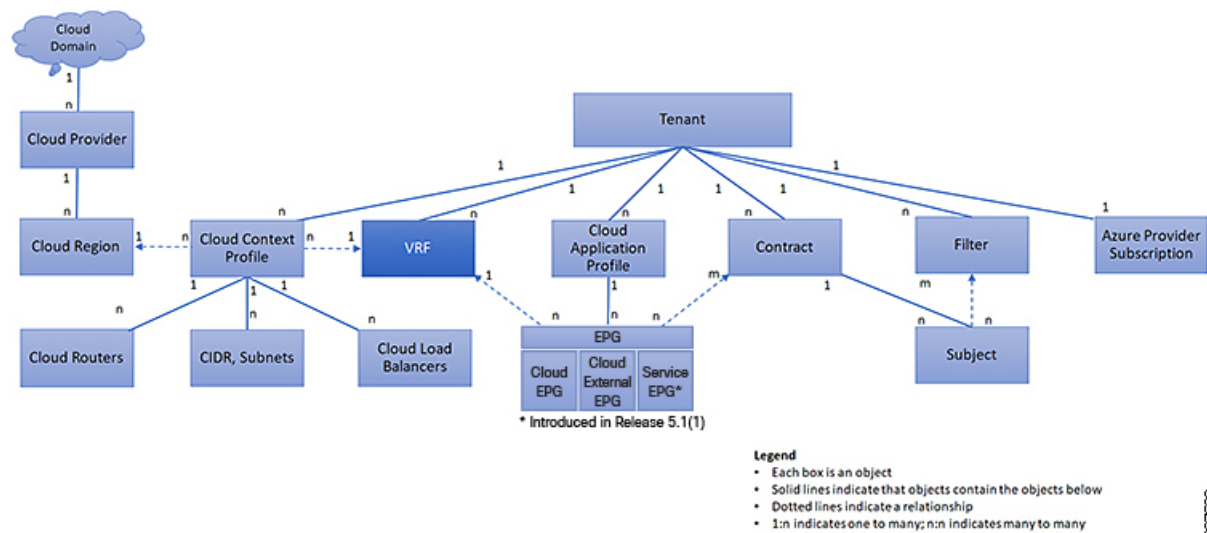
[プライベート IP アドレスを使用した CCR の制限 (Restrictions for CCR with Private IP Address)] :

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

VRF

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

図 4: VRF



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

単一 VNet での複数の VRF のサポート

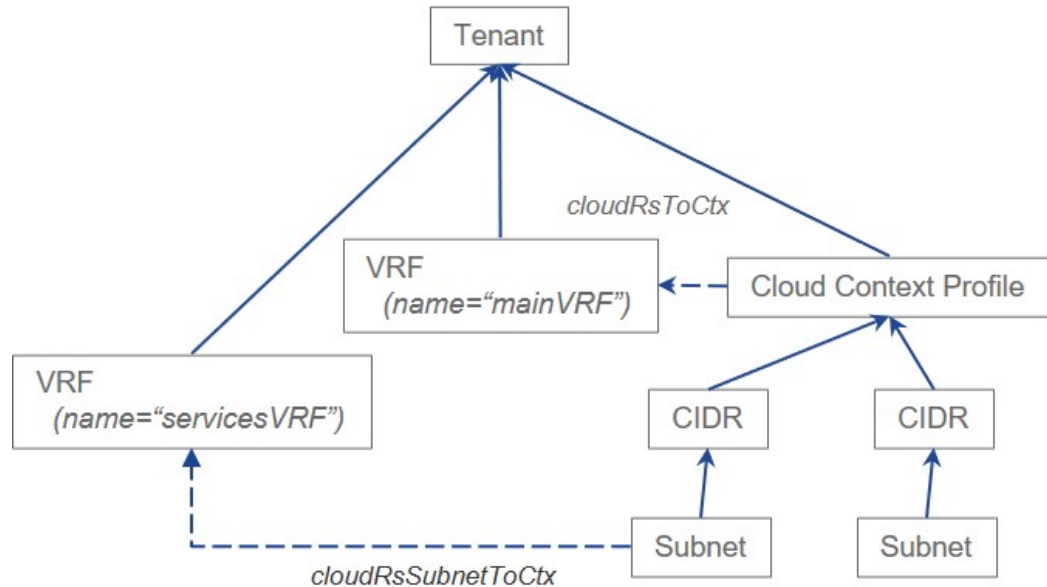
単一 VNet の下で複数の VRF がサポートされるようになりました。

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

また、インフラ VNet を超えて複数の VRF を分割して、単一の VNet に複数の VRF が存在する場合、任意の VNet を同じテナントの下で複数の VRF に分割できるようにすることもできます。これは、クラウドサービスアクセスなど、特定の VNet 内に複数のネットワーク (VRF)

を分割し、クラウドのVNet内の各VRFに固有のルートテーブルを用意することで個別のルーティングを行う必要がある場合に役立ちます。

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



この例では、同じテナント（VNet）の下に2つのVRFが存在します。

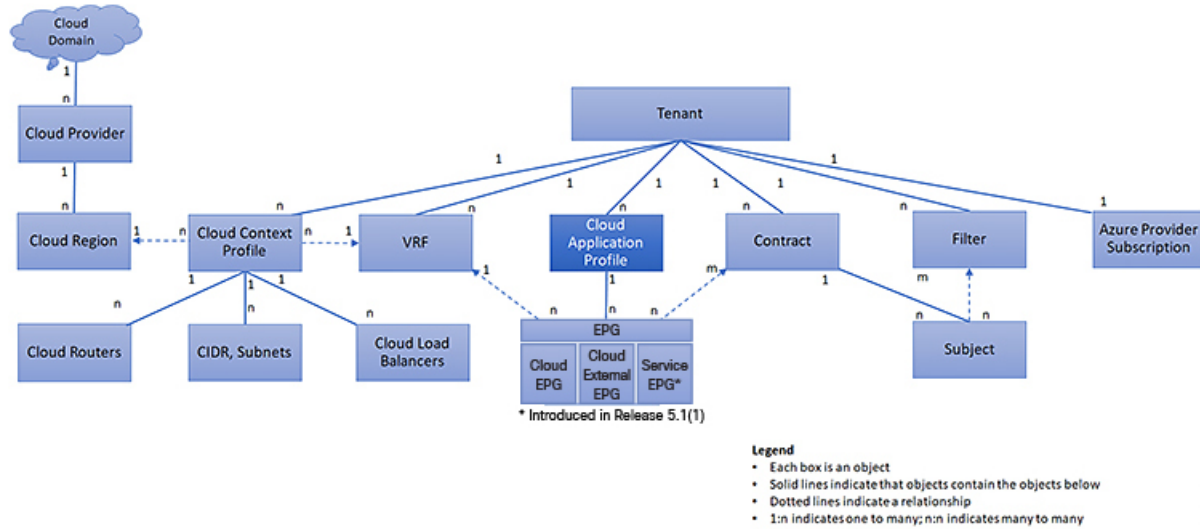
- mainVRF という名前のプライマリ VRF
- servicesVRF という名前のセカンダリ VRF

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

クラウドアプリケーション プロファイル

クラウドアプリケーションプロフィール (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ィールの場所と、テナント内の他のオブジェクトとの関係を示します。

図 5: クラウド アプリケーション プロファイル



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

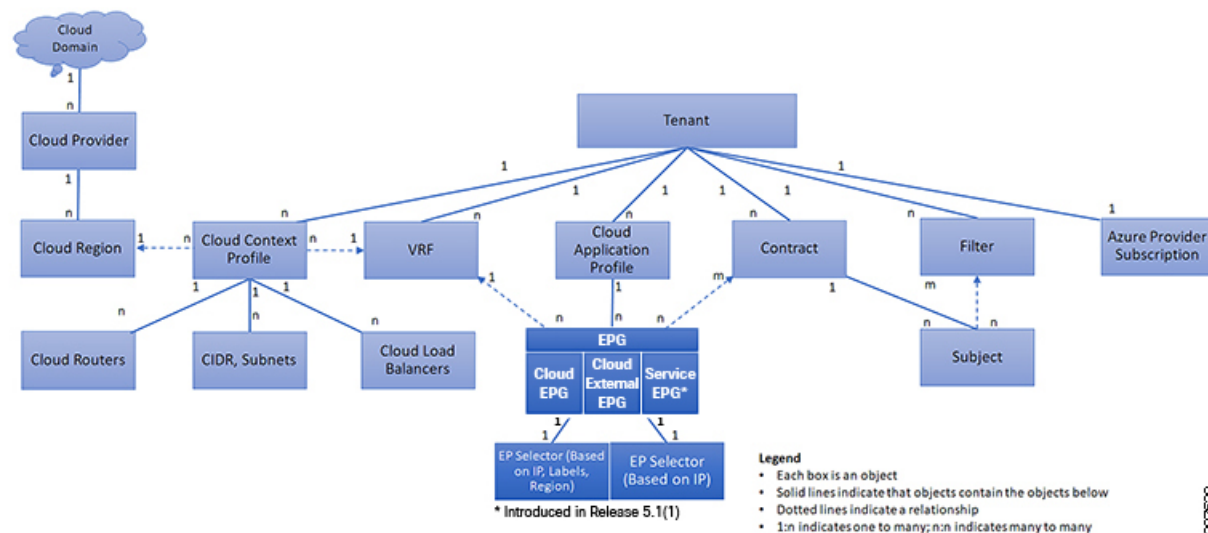
クラウド EPG は次のいずれかに従って組織化できます。

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

クラウドエンドポイントグループ

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

図 6: クラウド エンドポイント グループ



クラウド EPG は、エンドポイントの集合を含む名前付き論理エンティティである管理対象オブジェクトです。エンドポイントは、ネットワークに接続されるデバイスです。エンドポイントは、アドレス (ID)、ロケーション、属性 (バージョンやパッチ レベルなど) を持ち、仮想です。エンドポイントのアドレスを知ること、他のすべての ID の詳細にアクセスすることもできます。クラウド EPG は、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ストレージサービス、またはクライアントが含まれます。クラウド EPG 内のエンドポイント メンバシップは、ダイナミックまたはスタティックにできます。

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 サービスエンドポイント グループ (cloudSvcEPg) : リリース 5.1(2) で導入されました。詳細については、「[クラウド サービスエンドポイント グループ \(35 ページ\)](#)」を参照してください。

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

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

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

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

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

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

クラウド サービスエンドポイント グループ

リリース 5.1(2) で導入されたクラウド サービス EPG は、クラウド ネイティブまたはサードパーティのサービス インスタンスまたはエンドポイントのコレクションを含む名前付き論理構成体である管理対象オブジェクトです。この場合、エンドポイントは特定のサービス インスタンスを指します。たとえば、SQL サーバーはエンドポイントと見なされ、SQL サーバーのコレクションはサービスエンドポイント グループを形成します。サービス EPG の他の例としては、ストレージ アカウントのコレクション、Key Vault のコレクションなどがあります。

サービス EPG には、いくつかの固有の属性があります。

- **サービス タイプ**：この属性は、グループ化されているクラウド サービスのタイプを示します。利用可能なサービスの種類の例には、**Azure SQL**、**Azure Containter Registry**、**Azure ApiManagement Services** などがあります。サービス タイプ **Custom** は、サードパーティ サービス EPG を構成するときに使用されます。
- **展開タイプ**：この属性は、サービスを展開する方法と場所を示します。以下は使用可能な展開タイプです。
 - **クラウド ネイティブ**：このタイプの展開では、サービスはクラウド プロバイダーのネットワークでインスタンス化され、サービスを使用するユーザまたはアプリケーションはサービスを管理します。たとえば、Azure ストレージ アカウントが Azure 独自の VNet 内に存在する場合があります、ストレージ コンテンツにアクセスするための URL があります。
 - **[クラウド ネイティブ管理対象 (Cloud Native Managed)]**：このタイプの展開では、サービスは VNet またはサブネットでインスタンス化されます (Cisco Cloud Network Controller を介して作成されます)。たとえば、Azure Kubernetes クラスタ (AKS) は、Cisco Cloud ネットワーク コントローラによって管理されるサブネットに展開できます。

- **サードパーティ**：これは、サードパーティ（Azure 以外）が市場を通じてサービスを提供している展開です。このサービスへのアクセスは、プライベートリンク機能を通じて提供されます。
- **アクセス タイプ**：サービスへのアクセス方法を示します。使用可能なアクセス タイプは次のとおりです。
 - **パブリック**：サービスには、割り当てられたパブリック IP アドレスを使用してアクセスできます。特定のサービスのパブリック IP アドレス範囲へのアクセスは、NSG ルールの Azure 「サービスタグ」を使用して行います。
 - **プライベート**：割り当てられているプライベート IP アドレスを使用して、サービスにアクセスできます。この割り当ては、展開が **Cloud Native** および **Third Party** の場合、プライベートエンドポイントの作成を通して行われます。**Cloud Native Managed** 展開の場合、プライベート IP はサービスによってサブネット IP スペースから割り当てられます。

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

サービス タイプ (Service Type)	プロバイダー	展開タイプ/アクセス タイプ		
		クラウドネイティブ	クラウドネイティブ管 理対象	サードパーティ製の
Azure Storage Blob	Microsoft.Storage	プライベート	なし	なし
Azure SQL	Microsoft.Sql	<ul style="list-style-type: none"> • パブリック • プライベート 	なし	なし
Azure Cosmos DB	Microsoft.DocumentDB	<ul style="list-style-type: none"> • パブリック • プライベート 	なし	なし
Azure Databricks	Microsoft.Databricks	パブリック	<ul style="list-style-type: none"> • プライベート • パブリックとプライベート 	該当なし
Azure Storage	Microsoft.ストレージ	<ul style="list-style-type: none"> • パブリック • プライベート 	なし	なし
Azure Storage ファイル	Microsoft.Storage	プライベート	なし	なし
Azure Storage キュー	Microsoft.Storage	プライベート	なし	なし

サービス タイプ (Service Type)	プロバイダー	展開タイプ/アクセス タイプ		
		クラウドネイティブ	クラウドネイティブ管 理対象	サードパーティ製の
Azure Storage テーブル	Microsoft.Storage	プライベート	なし	なし
Azure Kubernetes Services (AKS)	Microsoft.ContainerService	プライベート	<ul style="list-style-type: none"> • プライベート • パブリックとプライベート 	該当なし
Azure Active Directory ドメイン サービス	Microsoft.AAD	パブリック	<ul style="list-style-type: none"> • プライベート • パブリックとプライベート 	該当なし
Azure Container レジストリ	Microsoft.ContainerRegistry	<ul style="list-style-type: none"> • パブリック • プライベート 	なし	なし
Azure ApiManagement サービス	Microsoft.ApiManagement	パブリック	<ul style="list-style-type: none"> • プライベート • パブリックとプライベート 	該当なし
Azure Key Vault	Microsoft.KeyVault	<ul style="list-style-type: none"> • パブリック • プライベート 	なし	なし
Redis キャッシュ	Microsoft.Cache	該当なし	<ul style="list-style-type: none"> • プライベート • パブリックとプライベート 	該当なし
カスタムサービス		<ul style="list-style-type: none"> • パブリック • プライベート 	該当なし	プライベート

• **サービスエンドポイントセレクタ**：サービスエンドポイントは、既存のセレクタ（クラウド EPG 選択で使用される）と、以下にリストされている新しいタイプのセレクタを使用して選択できます。

- **リソース名**：サービス リソースの名前
- **リソース ID**：リソースのクラウドプロバイダーの ID

- **URL** : サービスを識別するエイリアスまたは FQDN (プライベートリンク エイリアスは Azure で使用されます)

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



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

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

クラウドサービス EPG の注意事項および制限事項

クラウドサービス EPG を構成している場合は、サブネットごとの NSG 構成を有効にする必要があります。詳細については、「[セキュリティグループ \(43 ページ\)](#)」を参照してください。

サービスタイプについて

特定のサービスタイプに固有の追加情報を以下に示します。

- [Azure Storage \(39 ページ\)](#)
- [Azure ApiManagement サービス \(39 ページ\)](#)
- [Azure Databricks サービス \(40 ページ\)](#)
- [Azure Active Directory ドメイン サービス \(40 ページ\)](#)
- [Azure Kubernetes サービス \(40 ページ\)](#)
- [Azure Redis キャッシュ \(41 ページ\)](#)

Azure Storage

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

- BLOB
- ファイル
- テーブル
- キュー

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

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

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

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

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

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

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

Azure ApiManagement サービス

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

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

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

Azure Databricks サービス

Azure Databricks には、次のものがが必要です。

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

Azure Databricks の場合、次の構成を行います。

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

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

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

Azure Active Directory ドメイン サービス

Azure Active Directory ドメイン サービス (ADDS) には、次のものがが必要です。

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

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

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

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

Azure Kubernetes サービス

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

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

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

AKS サービス EPG の構成例については、[サービス EPG 構成例 \(361 ページ\)](#) を参照してください。

Azure Redis キャッシュ

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

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

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

展開タイプについて

特定の展開タイプに固有の追加情報を以下に示します。

- [クラウドネイティブ \(41 ページ\)](#)
- [クラウド ネイティブ管理対象 \(42 ページ\)](#)

クラウドネイティブ

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

次に、クラウド ネイティブ展開タイプのサービス EPG の例を示します。

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

このサンプル シナリオでは、この順番で次の構成を行います。

1. Cisco Cloud Network Controller GUI で、Azure SQL サービス EPG によって使用されるクラウド コンテキスト プロファイルにプライベート リンク ラベルを作成します。
[Creating a Cloud Context Profile Using the Cisco Cloud Network Controller GUI \(123 ページ\)](#) の手順を実行します。Azure SQL サービス EPG (SQL-PLL など) で使用されるプライベート リンク ラベルを構成します。
2. Cisco Cloud Network Controller GUI で、サービス タイプ Azure SQL のサービス EPG を作成します。

次のパラメータを使用して、[Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#) の手順に従います。

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

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

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

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

別の例として、クラウドプロバイダーのリソース ID

`/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer` を使用して SQL サーバーを選択する場合は、次のように選択します。

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

3. Azure ポータルで、クラウド内の Azure SQL リソースを構成します。

クラウドネイティブ管理対象

このタイプの展開では、サービスはVNetまたはサブネットでインスタンス化されます（Cisco Cloud Network Controller を介して作成されます）。たとえば、Azure ApiManagement Services は、Cisco クラウドネットワークコントローラによって管理されるサブネットに展開できます。

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

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

このサンプルシナリオでは、この順番で次の構成を行います。

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

[Creating a Cloud Context Profile Using the Cisco Cloud Network Controller GUI \(123 ページ\)](#) の手順を実行します。Azure ApiManagement Services service EPG (たとえば、10.50.0.0/16) によって使用されるサブネットを構成します。

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

次のパラメータを使用して、[Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#) の手順に従います。

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

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

たとえば、最初のステップで提供された例を使用して、このサービス EPG に対してこのエンドポイントセレクトラを構成します。

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

3. Azure ポータルで、クラウドの Azure ApiManagement Services リソースを構成します。

セキュリティ グループ

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

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

Cisco クラウドネットワーク コントローラでは、NSG は契約に基づいて自動的に構成されます。

- **アプリケーション セキュリティ グループ** : アプリケーション セキュリティ グループ (ASG) は Azure で使用され、仮想マシン (VM) NIC で実行されるアプリケーションに従って仮想マシン (VM) NIC をグループ化し、それらのグループに基づいてネットワー

クセキュリティポリシーを定義します。ASGはNSG内でこれらのセキュリティポリシーを定義し、ネットワークセキュリティルールを特定のワークロードまたは仮想マシンのグループに適用するために使用されます。

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

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

- リリース 5.1(2) より前のリリース : EPG ごとの NSG 構成 (44 ページ)
- リリース 5.1(2) 以降 : サブネットごとの NSG 構成 (44 ページ)
- リリース 5.1(2g) 以降 : 同じ VNet 内の VRF 間コントラクトの IP ベースのルール (45 ページ)

リリース 5.1(2) より前のリリース : EPG ごとの NSG 構成

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

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

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

リリース 5.1(2) 以降 : サブネットごとの NSG 構成

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

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

- エンドポイント セレクタに基づいて各 EPG のすべてのエンドポイントまたは仮想マシン NIC をグループ化するために使用される ASG [リリース 5.1(2) より前のリリースからの ASG の動作は基本的に変更されません]

- その EPG のセキュリティ ポリシー定義を提供し続けるが、Cisco Cloud Network Controller が管理する VNet のサブネットに関連付けられるようになった NSG

別の視点から見た場合：

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

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

- サブネットごとの NSG 構成を使用すると、VNet 内の NSG の数が減り、共通の共有サービスにアクセスする多数のサブネットがある展開のルール数も減ります。これにより、個々の EPG または ASG にマッピングされた各 NSG ではなく、サブネットの 1 つの NSG ですべてのルールをチェックできるため、管理が容易になります。
- サービス EPG を構成している場合は、サブネットごとの NSG 構成を使用する必要があります。詳細については、「クラウドサービスエンドポイントグループ (35 ページ)」を参照してください。

EPG ごとの NSG またはサブネットごとの NSG 構成を有効または無効にする手順については、[Cisco Cloud Network Controller GUI を使用したネットワークセキュリティグループの構成 \(116 ページ\)](#) を参照してください。

リリース 5.1(2g) 以降：同じ VNet 内の VRF 間コントラクトの IP ベースのルール

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

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

ASG および NSG の注意事項と制限事項

以下は、ASG および NSG の注意事項と制限事項です。

- [5.1\(2\) より前のリリースの注意事項と制限事項 \(46 ページ\)](#)
- [リリース 5.1\(2\) 以降の注意事項と制限事項 \(46 ページ\)](#)

5.1(2) より前のリリースの注意事項と制限事項

リリース 5.1 (2) より前のリリースでは、Cisco Cloud ネットワーク コントローラの NSG から EPG へのマッピングのみがサポートされています。

リリース 5.1(2) 以降の注意事項と制限事項

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

セキュリティ ルール

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

- [EPG ごとの NSG セキュリティ ルール \(46 ページ\)](#)
- [サブネットごとの NSG セキュリティ ルール \(47 ページ\)](#)

EPG ごとの NSG セキュリティ ルール

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

レスを送信元および接続先として使用する NSG セキュリティ ルールがプログラムされます。

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

サブネットごとの NSG セキュリティ ルール

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

ソフトウェア アップグレードまたはダウングレードによる NSG 動作

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

- [ソフトウェア アップグレードによる NSG の動作 \(47 ページ\)](#)
- [ソフトウェア ダウングレードによる NSG の動作 \(48 ページ\)](#)

ソフトウェア アップグレードによる NSG の動作

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

ただし、サブネットごとの NSG 構成には利点があるため、これらの利点を利用するには、EPG ごとの NSG 構成をサブネットごとの NSG に変換することをお勧めします。さまざまな NSG 構成の詳細については [セキュリティ グループ \(43 ページ\)](#) を、EPG ごとの NSG またはサブネットごとの NSG 構成の有効化または無効化に関する指示については [Cisco Cloud Network Controller GUI を使用したネットワーク セキュリティ グループの構成 \(116 ページ\)](#) を参照してください。

アップグレード後は、古い EPG ごとの NSG 構成または新しいサブネットごとの NSG 構成のいずれかを使用できますが、同じ Cisco Cloud Network Controller システムで両方を使用することはできないことに注意してください。詳細については、「[ASG および NSG の注意事項と制限事項 \(45 ページ\)](#)」を参照してください。

ただし、[Cisco Cloud Network Controller GUI を使用したバックアップ構成の作成 \(128 ページ\)](#) の手順を使用して既存の Cisco Cloud Network Controller 構成をバックアップし、アップグレー

ドを実行し、アップグレード後にバックアップされた構成をインポートした場合、サブネットごとの NSG 構成は自動的にオンになり、古い EPG ごとの NSG 構成は新しいサブネットごとの NSG 構成に自動的に変換されます。

ソフトウェア ダウングレードによる NSG の動作

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

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

1. ソフトウェアをリリース 5.1(2) 以降から リリース 5.1(2) より前のリリースにダウングレードする前に、[Cisco Cloud Network Controller GUI を使用したネットワーク セキュリティ グループの構成 \(116 ページ\)](#) で説明されている手順を使用して、サブネットごとの NSG 構成を無効にします。Cisco Cloud APIC ソフトウェアは、サブネットごとの NSG マッピングから EPG ごとの NSG マッピングへの移行を開始します。
2. 移行が完了するまで待ちます。この場合、Cisco Cloud Network Controller ソフトウェアは、サブネットごとの NSG マッピング プロセスの一部として構成されたすべての NSG を削除し、EPG ごとの NSG マッピング構成用に新しい NSG を作成します。移行が完了する前にダウングレードを続行しようとする、エラーメッセージが表示され、Cisco Cloud Network Controller ソフトウェアは、サブネット マッピングごとの NSG から EPG マッピングごとの NSG へのこの移行が完了するまで、ダウングレードを続行することを許可しません。



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

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

```
hcloudReconcileDone
```

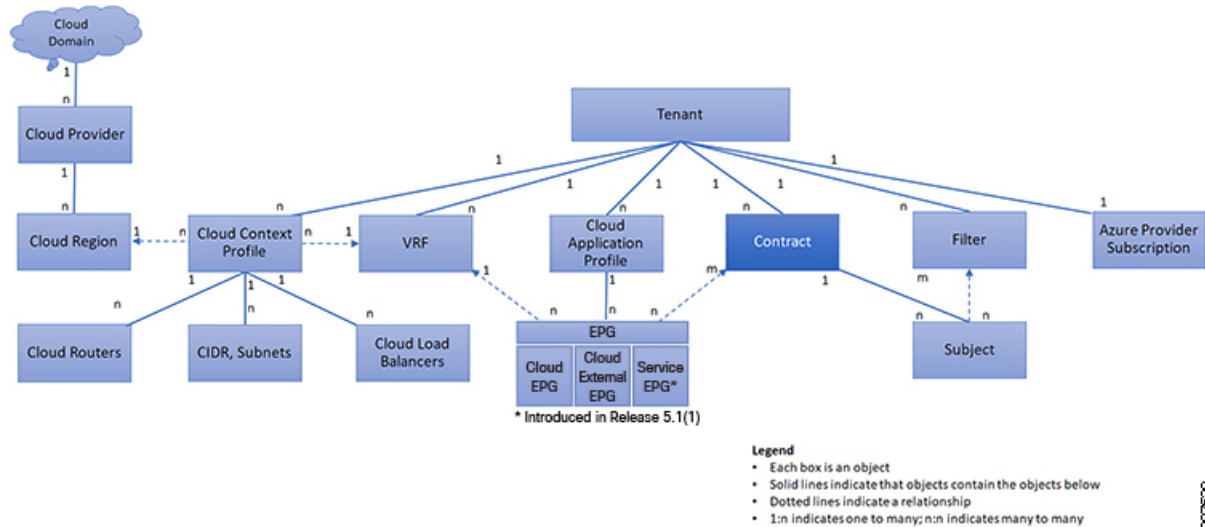
REST API を使用してダウングレードを続行する前に、プロパティ `sgForSubnetModeConverged` が `[yes]` に設定されていることを確認します。

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

コントラクト

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

図 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、そのクラウド EPG 内のクラウド

ドエンドポイントとの通信は、通信が提供されたコントラクトに準拠している限り、他のクラウド EPG 内のクラウドエンドポイントから開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウドエンドポイントは、コントラクトを指定したクラウド EPG のクラウドエンドポイントと通信を開始できます。



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

コントラクトルール統合のためのコンマ区切りフィルタのサポート

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

- ルールは、コントラクト内でのみ統合されます。2 つの異なるコントラクトに起因する 2 つのルールは、Azure に統合されません。
- 送信元/宛先アドレス プレフィックスと宛て先ポートが統合されます。
- 複数のルールを NSG に統合するための条件は次のとおりです。
 - 同一コントラクト
 - 同じプロトコル (UDP、TCP、ICMP)
 - 同じ方向 (インバウンド、アウトバウンド)
 - 同型 (SG、IP)
- 同一コントラクト内の同一プロトコル (TCP/UDP) の重複するポート範囲は 1 つに集約します。

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

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

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

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

```
EPG1 outbound rules:
```

```

EPG1 -> EPG2    TCP    80
EPG1 -> EPG2    TCP    8080
EPG1 -> EPG2    TCP    53
EPG1 -> EPG2    UDP    53
EPG1 -> EPG2    UDP    5000
EPG1 -> 1.1.1.1/32 TCP    80
EPG1 -> 1.1.1.1/32 TCP    8080
EPG1 -> 1.1.1.1/32 TCP    53
EPG1 -> 1.1.1.1/32 UDP    53
EPG1 -> 1.1.1.1/32 UDP    5000
EPG1 -> 2.2.2.2/32 TCP    80
EPG1 -> 2.2.2.2/32 TCP    8080
EPG1 -> 2.2.2.2/32 TCP    53
EPG1 -> 2.2.2.2/32 UDP    53
EPG1 -> 2.2.2.2/32 UDP    5000

```

Rules are consolidated by comma-separated filters (consolidated based on C1 and C2):

```

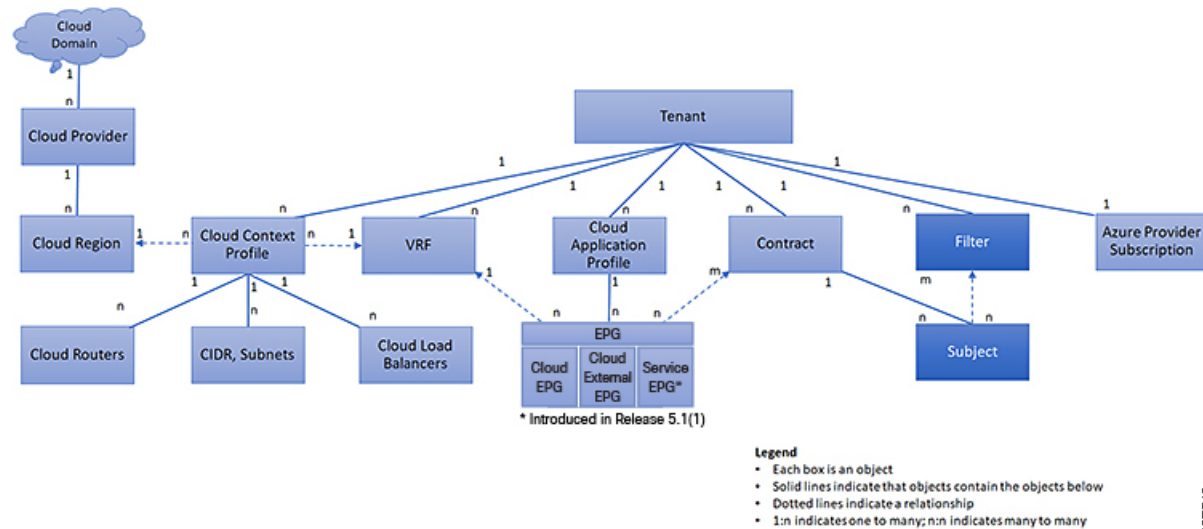
EPG1 -> EPG2    TCP    80,8080
EPG1 -> EPG2    UDP    53,5000
EPG1 -> EPG2    TCP    53
EPG1 -> 1.1.1.1/32, 2.2.2.2/32 TCP    80,8080
EPG1 -> 1.1.1.1/32, 2.2.2.2/32 UDP    53,5000
EPG1 -> 1.1.1.1/32, 2.2.2.2/32 TCP    53

```

クラウド EPG 通信を制御するフィルタおよびサブジェクト

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

図 8: サブジェクトおよびフィルタ



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



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

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

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

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

クラウドテンプレートは、1 つ以上のリージョン名を承認し、それらのリージョンでインフラ VNET の構成全体を生成します。それらはインフラ VNET です。Azure VNET に対応する Cisco Cloud Network Controller 管理対象オブジェクト (MO) は、cloudCtxProfile です。クラウドテンプレートで指定されたすべてのリージョンに対して、cloudCtxProfile 設定が生成されます。cloudCtxProfile は、リージョンに対応するすべての設定の最上位 MO です。その下には、特定の設定をキャプチャするためのツリーとして編成された他の多くの MO があります。インフラ VNet の cloudCtxProfile MO は、クラウドテンプレートにより生成されます。これは

ctxProfileOwner == SYSTEM を伝送します。これは、この MO がシステムによって生成されることを意味します。非インフラストラクチャ ネットワークの場合、cloudCtxProfile を直接設定できます。この場合、cloudCtxProfile は ctxProfileOwner == USER を伝送します。

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

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

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

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

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

詳細については、[Cisco Cloud Network Controller GUI を使用したアプリケーション EPG の作成 \(83 ページ\)](#) を参照してください。

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

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

クラウドテンプレートがない場合は、これらの設定と管理を担当します。

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

表 3:クラウドテンプレートMO

MO	目的
cloudtemplateInfraNetwork	クラウドテンプレート設定のルート。次の属性が含まれます。 numRoutersPerRegion : cloudtemplateIntNetwork で指定された各 cloudRegionName のクラウドルータの数。
cloudtemplateProfile	すべてのクラウドルータの設定プロファイル。次の属性が含まれます。 <ul style="list-style-type: none"> • routerUsername <p>(注)</p> <ul style="list-style-type: none"> • ユーザ名を「admin」にすることはできません。 • Azure からのユーザー名の制限が適用されます。 <ul style="list-style-type: none"> • routerPassword • routerThroughput • routerLicenseToken • routeDataInterfacePublicIP • routerMgmtInterfacePublicIP
cloudtemplateIntNetwork	クラウドルータを展開する場所を指定するリージョンのリストが含まれます。各リージョンは、cloudRegionName 子 MO を介してキャプチャされます。
cloudtemplateExtNetwork	クラウド外部のインフラ ネットワーク設定入力が含まれます。 クラウドルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。 各リージョンは、cloudRegionName 子 MO を介してキャプチャされます。

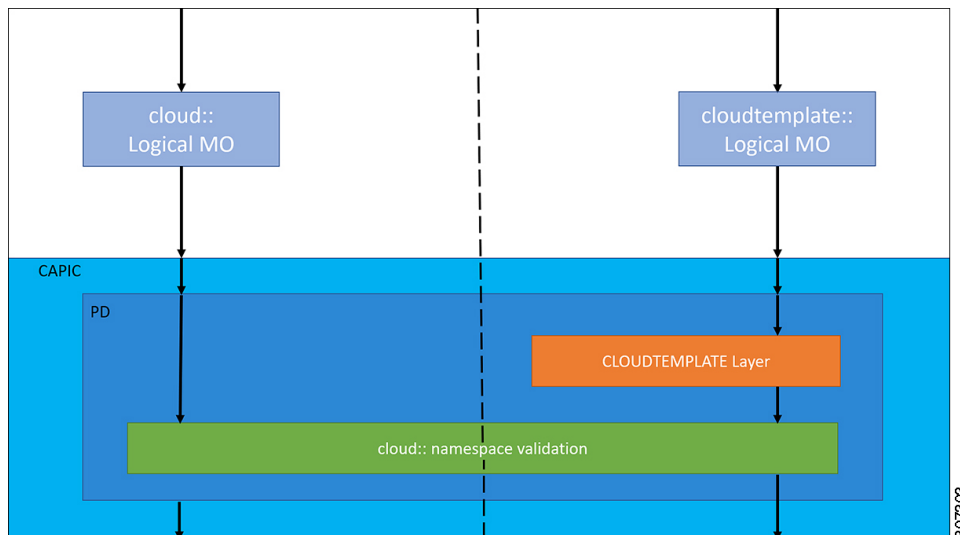
MO	目的
cloudtemplateVpnNetwork	ACI オンプレミス サイトまたは別の Cisco Cloud Network Controller サイトで VPN を設定するための情報が含まれています。
cloudtemplateIpSecTunnel	ACI オンプレミス サイトの IPSec ピアの IP アドレスをキャプチャします。
cloudtemplateOspf	VPN 接続に使用する OSPF エリアをキャプチャします。
cloudtemplateBgpEvpn	オンプレミスサイトとの BGP セッションを設定するために、ピア IP アドレス、ASN などをキャプチャします。

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 \(59 ページ\)](#) を参照してください。

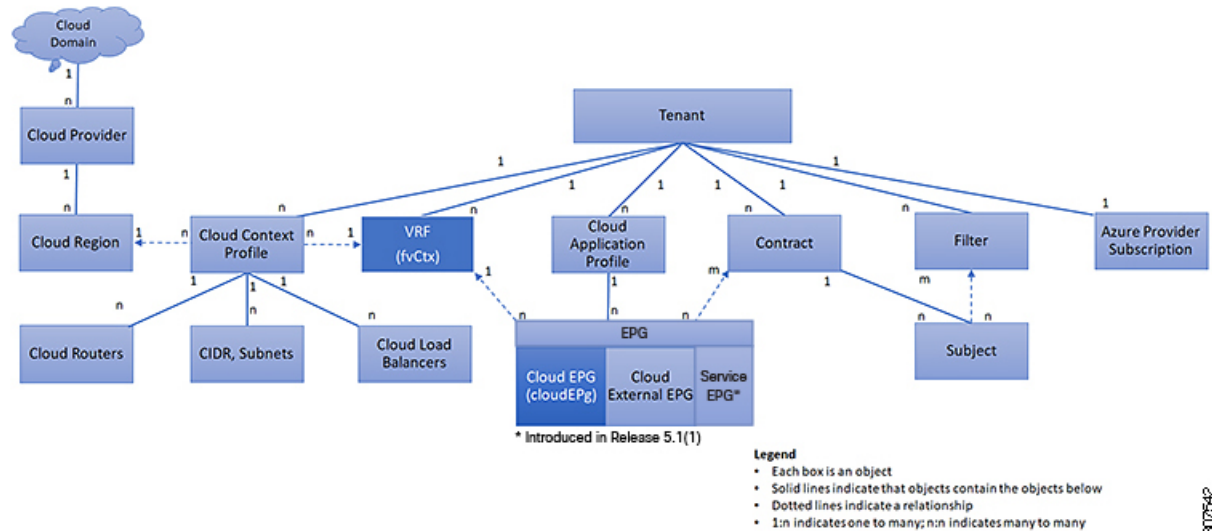
管理対象オブジェクトの関係とポリシー解決

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

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

次の図の点線は、いくつかの一般的な MO の関係を示します。

図 10: MO の関係



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

名前付き関係に基づくポリシー解決の場合は、一致する名前を持つターゲット MO が現在のテナントに見つからない場合、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 プロヴァイル、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 Azure 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。
 - テナント間コントラクトにはグローバル範囲が必要です。



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](#) (59 ページ)
- [GUI を使用した Cisco Cloud Cisco Network Controller の構成](#) (59 ページ)
- [REST API を使用した Cisco Cloud Network Controller の構成](#) (168 ページ)

Cisco Cloud Network Controller の設定について

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



- (注)
- 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](#) (199 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。

始める前に

- Cisco Cloud Network Controller によって管理されるテナント、または管理されていないテナントを作成できます。管理対象テナントを確立するには、最初に Azure portal から Azure サブスクリプション ID を取得する必要があります。テナントの作成時に、Cisco Cloud Network Controller の適切なフィールドにサブスクリプション ID を入力します。管理対象テナントを使用する前に、サブスクリプションを管理するためのアクセス許可を Cisco Cloud Network Controller に明示的に付与する必要があります。これを行うための手順は、テナントの作成中に Cisco Cloud Network Controller GUI に表示されます。ただし、インフラテナントの手順は、インフラテナントの詳細ビューに表示されます。

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



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

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



(注) 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 Azure リソースを妨害しません。自身で作成した Azure リソースのみを管理します。

- 特定のサブスクリプションを管理するための許可を Cisco Cloud Network Controller に明示的に付与するために必要な手順は、Cisco Cloud Network Controller にあります。テナントを作成する場合、クライアントシークレットを入力した後に手順が表示されます。
- 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 Azure サブスクリプション IA1 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 Azure サブスクリプション IA2 に導入されている場合)、これは展開 TA1-R2 の所有者が

現在、IA1-R1 であるため許可されません。つまり、1 つの 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、Azure リソースグループを使用して行われます。リージョン R2 のサブスクリプション TA1 の新しいテナントが Cisco Cloud ネットワーク コントローラ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_eastus2）がサブスクリプションに作成されます。このリソースグループには、値が IA1_R1_TA1_R2 のリソースタグ AciOwnerTag があります（サブスクリプション IA1 の 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。回避策として、他の Cisco Cloud Network Controller が同じテナントとリージョンの組み合わせを管理していないことが確実な場合は、テナントの Azure サブスクリプションにログオンし、影響を受けるリソースグループ（例：CNC_123456789012_eastus2 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。

- インフラ テナントおよびユーザ テナント両方で、認証または資格情報を処理するとき、管理対象 ID と非管理対象 ID/サービス プリンシパルの両方をサポートできます。

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

表 4: テナント ダイアログボックス フィールドの作成

[プロパティ (Properties)]	説明
名前 (Name)	テナント名を入力します。
説明	テナントの説明を入力します。
[設定 (Settings)]	
セキュリティドメインの追加 (Add Security Domain)	<p>テナントのセキュリティドメインを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [セキュリティドメインの追加 (Add Security Domain)] をクリックします。[セキュリティドメインの選択 (Select Security Domains)] ダイアログが表示され、左側のペインにセキュリティドメインのリストが表示されます。 2. セキュリティドメインをクリックして選択します。 3. [選択 (Select)] をクリックして、セキュリティドメインをテナントに追加します。
Azure サブスクリプション	
モード (Mode)	<p>アカウントタイプを選択します。</p> <ul style="list-style-type: none"> • [固有作成 (Create Own)] : 新しいテナントを作成するには、このオプションを選択します。 • [共有を選択 (Select Shared)] : このオプションを選択して、既存のテナントから管理対象または非管理対象の設定を継承します。
Azure サブスクリプション ID	Azure サブスクリプション ID を入力します。

[プロパティ (Properties)]	説明
アクセスタイプ	<p>アクセス タイプを選択します。</p> <ul style="list-style-type: none"> • サービス プリンシパルまたは非管理対象 ID : テナントサブスクリプションが Cisco Cloud ネットワーク コントローラ によって管理されていない場合は、このオプションを選択します。 • [管理対象アイデンティティ (Managed Identity)] : テナントサブスクリプションが Cisco Cloud ネットワーク コントローラ によって管理されている場合は、このオプションを選択します。 <p>(注) インフラテナントに[サービス プリンシパル (Service Principal)]または[管理対象 ID (Managed Identity)]を割り当てることができます。</p> <p>詳細については、テナント、ID、およびサブスクリプションについて (22 ページ) を参照してください。</p>
アプリケーションID	<p>(注) このフィールドは、[サービス プリンシパル (Service Principal)]または[非管理対象 ID (Unmanaged Identity)]アクセス タイプに対してのみ有効です。</p> <p>アプリケーション ID を入力します。</p> <p>(注) アプリケーションIDの取得については、Azure のドキュメントまたはサポートを参照してください。</p>

[プロパティ (Properties)]	説明
クライアントのシークレット (Client Secret)	<p>(注) このフィールドは、[サービス プリンシパル (Service Principal)] または [非管理対象 ID (Unmanaged Identity)] アクセス タイプに対してのみ有効です。</p> <p>クライアントシークレットを入力します。</p> <p>(注)</p> <ul style="list-style-type: none"> • クライアントシークレットの作成については、Azure のドキュメントまたはサポートを参照してください。 • 特定のサブスクリプションを管理するには、Cisco Cloud Network Controller のアクセス許可を明示的に付与する必要があります。Azure ポータルに移動して、次の手順に従います。 <ol style="list-style-type: none"> 1. クラウドシェルをオープンします。 2. 「バッシュ」を選択 3. Cisco Cloud Network Controller GUI に表示されるコマンドをコピーして貼り付けます。
Active Directory ID	<p>(注) このフィールドは、[サービス プリンシパル (Service Principal)] または [非管理対象 ID (Unmanaged Identity)] アクセス タイプに対してのみ有効です。</p> <p>ディレクトリ ID を入力します。</p> <p>(注) Active Directory ID の取得については、Azure のドキュメントまたはサポートを参照してください。</p>

[プロパティ (Properties)]	説明
セキュリティドメインの追加	<p>アカウントのセキュリティドメインを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [セキュリティドメインの追加 (Add Security Domain)]をクリックします。[セキュリティドメインの選択 (Select Security Domains)]ダイアログが表示され、左側のペインにセキュリティドメインのリストが表示されます。 2. セキュリティドメインをクリックして選択します。 3. [選択 (Select)]をクリックして、セキュリティドメインをテナントに追加します。

ステップ5 設定が終わったら [Save] をクリックします。

Cisco Cloud 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 <i>vrfEncoded</i> 値が割り当てられます。テナントと VRF 名の組み合わせが 32 文字を超える場合、VRF 名 (テナント名も含む) は <i>vrfEncoded</i> 値を使用してクラウドルータで識別されます。 <i>vrfEncoded</i> 値を表示するには、[Application Management]>[VRFs] サブタブに移動します。右側のペインで VRF をクリックし、クラウドルータで [Encoded VRF Name] を探します。

[プロパティ (Properties)]	説明
テナント	テナントを選択します。 <ol style="list-style-type: none"> [テナントの選択 (Select Tenant)]をクリックします。[テナントの選択 (Select Tenant)]ダイアログボックスが表示されます。 [テナントの選択 (Select Tenant)]ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)]をクリックします。[VRF の作成 (Create VRF)]ダイアログボックスに戻ります。
説明	VRF の説明を入力します。

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。

[プロパティ (Properties)]	説明
VRF	<p>この 外部 VRF は、外部の非 ACI デバイスとの外部接続に使用されます。この目的で複数の外部 VRF を作成できます。</p> <p>この VRF は、VRF が次の 3 つの特性をすべて備えている場合に 外部 VRF として識別されます。</p> <ul style="list-style-type: none"> • インフラ テナントの下で構成された • 外部ネットワークに関連付けられている • クラウド コンテキスト プロファイルに関連付けられていない <p>外部ネットワークに関連付けられている VRF はすべて 外部 VRF になります。外部 VRF をクラウド コンテキスト プロファイルまたはサブネットに関連付けることはできません。</p> <p>外部 VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [VRF の選択 (Select VRF)] をクリックします。 [VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 2. [VRF の選択 (Select VRF)] ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成 (+ Create VRF)] オプションを使用して VRF を作成することもできます。 3. [選択 (Select)] をクリックします。 [外部ネットワークの作成 (Create External Network)] ダイアログボックスに戻ります。
ホスト ルーター名	このフィールドは編集できません。デフォルトのホスト ルーターが自動的に選択されます。
[設定 (Settings)]	
地域	<p>リージョンを選択するには:</p> <ol style="list-style-type: none"> 1. [地域の追加 (Add Region)] をクリックします。 [地域の選択 (Select Regions)] ダイアログボックスが表示されます。 初回セットアップの一部として選択した地域がここに表示されます。 2. [地域の選択 (Select Regions)] ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)] をクリックします。 [外部ネットワークの作成 (Create External Network)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
VPN ネットワーク	

[プロパティ (Properties)]	説明
	<p>VPN ネットワーク エントリは、外部接続に使用されます。設定されたすべてのVPNネットワークが、選択したすべてのリージョンに適用されます。</p> <p>VPN ネットワークを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [VPNネットワークの追加 (Add VPN Network)] をタップします。 [VPN ネットワークの追加 (Add VPN Network)] ダイアログボックスが表示されます。 2. [名前 (Name)] フィールドに VPN ネットワークの名前を入力します。 3. [+ IPsec ピアの追加 (+ Add IPsec Peer)] をクリックします。 IPsec ピア エントリごとにトンネルが作成されます。 4. 追加する IPsec トンネルの次のフィールドに値を入力します。 <ul style="list-style-type: none"> • IPsec トンネル ピアのパブリック IP • 事前共有キー • IKE Version : IPsec トンネル接続用に ikev1 または ikev2 を選択します。 • BGP ピア ASN • Subnet Pool Name : [サブネット プール名の選択 (Select Subnet Pool Name)] をクリックします。 [サブネット プール名の選択 (Select Subnet Pool Name)] ダイアログボックスが表示されます。リストされている使用可能なサブネット プールのいずれかを選択し、[選択 (Select)] をクリックします。 <p>(注) 必要に応じて、追加の IPsec トンネル サブネット プールを [外部ネットワーク] ページに追加するか、クラウドネットワーク コントローラーの初回セットアップを介して追加できます。詳細については、[Azure 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。</p> <ul style="list-style-type: none"> • [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。 <p>(注) ikev2 は、このフィールドのデフォルト オプションです。IPsec トンネル ソース インターフェイス機能は、IKEv2 構成でのみサポートされます。</p> <p>gig3 は、デフォルトで選択されます。次の中から 1 つまたは複数のインターフェイス</p>

[プロパティ (Properties)]	説明
	<p>を選択します</p> <ul style="list-style-type: none"> • gig2: GigabitEthernet2 インターフェイス • gig3: GigabitEthernet3 インターフェイス • gig4: GigabitEthernet4 インターフェイス <p>(注) この外部ネットワークで IPsec トンネル ソース インターフェイスを構成した後、ルーティング ポリシー: リリース 25.0(2) (9 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。</p> <p>5. この IPSec トンネルを追加するには、チェックマークをクリックします。</p> <p>別の IPSec トンネルを追加する場合は、[+ IPSec トンネルの追加 (+ Add IPSec Tunnel)] をクリックします。</p> <p>6. [VPN ネットワークの追加 (Add VPN Network)] ダイアログボックスで [追加 (Add)] をクリックします。</p> <p>[外部ネットワークの作成 (Create External Network)] ダイアログボックスに戻ります。</p>

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

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

グローバル VRF 間ルート リーク ポリシーの構成

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

始める前に

[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、[内部 VRF 間のルート リーク \(9 ページ\)](#) 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 Configuration)** 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変える必要がある場合は、次の手順に従います：

- **はい設定からいいえ (コントラクトベースのルーティングを無効にする)** : この状況では、現在、コントラクトベースのルーティングが構成されており、ルート マップベースのルーティングにシフト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シフトする前に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)**] 設定に移動する前に、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 VRF 間ルート リークの構成 \(73 ページ\)](#) 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のスイッチをします。

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変更 (契約ベースのルーティングを有効にする)** : この状況では、現在マップベースのルーティングが構成されており、契約ベースのルーティングにシフト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。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)**] 設定にシフト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)] 設定にシフトする前に 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変更します。

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 \(73 ページ\)](#) 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 \(76 ページ\)](#) 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 \(6 ページ\)](#)」を参照してください。

外部宛先は、[Azure サイトから外部デバイスへの接続を有効にする \(79 ページ\)](#) 手順を使用して手動で構成する必要があります。外部の接続先は、別のクラウドサイト、ACI オンプレミス サイト、または分散拠点である可能性があります。



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

- ステップ 1** 左側のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [VRF] に移動します。
設定された VRF が表示されます。
- ステップ 2** [リーク ルート (Leak Routes)] タブをクリックします。
すでに構成されているリーク ルートが表示されます。
- ステップ 3** [アクション (Actions)] をクリックし、[リーク ルートの作成 (Create Leak Route)] を選択します。
[リーク ルートの作成 (Create a Leak Route)] ウィンドウが表示されます。
- ステップ 4** 次の [リーク ルートの作成ダイアログボックスのフィールド (Leak Routes Dialog Box Fields)] テーブルでリストされた各フィールドに該当する値を入力し、続行します。

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

[プロパティ (Properties)]	説明
Source VRF	<p>送信元 VRF を選択するには :</p> <ol style="list-style-type: none"> [送信元 VRF の選択 (Select Source VRF)] をクリックします。 [VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 [VRF の選択 (Select VRF)] ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択しています。 送信元 VRF は、内部または外部 VRF であることに注意してください。 [選択 (Select)] をクリックして、この送信元 VRF を選択します。 [リーク ルートの作成 (Create Leak Route)] ダイアログボックスに戻ります。
宛先 VRF	<p>宛先 VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [宛先の選択 (Select destination)] をクリックします。 [VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 [VRF の選択 (Select VRF)] ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択しています。 送信元 VRF も内部 VRF である場合、接続先 VRF を内部 VRF にすることはできないことに注意してください。 [選択 (Select)] をクリックして、この宛先 VRF を選択します。 [リーク ルートの作成 (Create Leak Route)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
Type	<p>構成するリーク ルートのタイプを選択します。</p> <ul style="list-style-type: none"> • すべてをリーク: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを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 \(74 ページ\)](#) – [ステップ 5 \(75 ページ\)](#) 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 \(74 ページ\)](#) – [ステップ 5 \(75 ページ\)](#) 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 \(74 ページ\)](#) の情報を使用して、必要な情報を入力します。送信元 VRF のエントリーは事前に選択されており、この状況では変更できないことに注意してください。
 - この VRF にリーク ルートを追加するには、[アクション (Actions)] をクリックし、[<VRF_name> にリーク ルートを追加 (Add Leak Route to <VRF_name>)] を選択します。
[リーク ルートの追加 (Add Leak Router)] ウィンドウが表示されます。 [ステップ 4 \(74 ページ\)](#) の情報を使用して、必要な情報を入力します。宛先 VRF のエントリーは事前に選択されており、この状況では変更できないことに注意してください。

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 を使用した外部 EPG の作成 \(89 ページ\)](#) : 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 \(111 ページ\)](#) : 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 \(9 ページ\)](#) で説明されているように、内部 VRF のペア間のルート マップベースのルート リークがサポートされます。この機能は、リリース 25.0(1) で提供されたルーティングとセキュリティの分割更新を拡張したもので、ルーティングとセキュリティ ポリシーが別々に設定されています。

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

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

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

表 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 Dialog Box Fields)

[プロパティ (Properties)]	説明
Source VRF	<p>送信元 VRF を選択するには :</p> <ol style="list-style-type: none"> [送信元 VRF の選択 (Select Source VRF)] をクリックします。 [VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 [VRF の選択 (Select VRF)] ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択しています。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続元 VRF には内部 VRF を選択します。 [選択 (Select)] をクリックして、この送信元 VRF を選択します。 [リーク ルートの作成 (Create Leak Route)] ダイアログボックスに戻ります。
宛先 VRF	<p>宛先 VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [宛先の選択 (Select destination)] をクリックします。 [VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 [VRF の選択 (Select VRF)] ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択しています。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続先 VRF には内部 VRF を選択します。 [選択 (Select)] をクリックして、この宛先 VRF を選択します。 [リーク ルートの作成 (Create Leak Route)] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
Type	<p>構成するリーク ルートのタイプを選択します。</p> <ul style="list-style-type: none"> • すべてをリーク: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを作成することを選択します。 この場合、デフォルトでは、エントリ 0.0.0.0/0 がサブネット IP エリアに自動的に入力されます。 • サブネット IP: 接続元 VRF から接続先 VRF までのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。[サブネット IP (Subnet IP)] ダイアログボックスが表示されます。 [サブネット IP (Subnet IP)] ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。

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

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

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

[リーク ルートの追加 (Add Leak Route)] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、[ステップ 4 \(77 ページ\)](#) ~ [ステップ 5 \(78 ページ\)](#) 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 \(77 ページ\)](#) ~ [ステップ 5 \(78 ページ\)](#) 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 \(77 ページ\)](#) の情報を使用して、必要な情報を入力します。送信元 VRF のエントリは事前を選択されており、この状況では変更できないことに注意してください。
 - この VRF にリークルートを追加するには、[アクション (Actions)] をクリックし、[<VRF_name> にリーク ルートを追加 (Add Leak Route to <VRF_name>)] を選択します。
[リーク ルートの追加 (Add Leak Router)] ウィンドウが表示されます。 [ステップ 4 \(77 ページ\)](#) の情報を使用して、必要な情報を入力します。宛先 VRF のエントリは事前を選択されており、この状況では変更できないことに注意してください。

Azure サイトから外部デバイスへの接続を有効にする

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

外部デバイス構成ファイルのダウンロード

- ステップ 1** Cisco Cloud 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。

Azure サイトから外部デバイスへの接続を有効にする

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

ステップ 2 外部デバイスにログインします。

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

[外部デバイス構成ファイルのダウンロード \(79 ページ\)](#) の手順を使用して外部デバイス構成ファイルをダウンロードした場合、最初のトンネルの構成情報を見つけて、その構成情報を入力します。

最初のトンネルの外部デバイス設定ファイルの例を示します。

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

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

vrf definition infra:externalvrf1
  rd 1:1

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

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

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

crypto ikev2 keyring keyring-ikev2-100
```

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

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

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

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

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

ip route 13.88.168.176 255.255.255.255 GigabitEthernet2 GIG-GATEWAY

router bgp 65015

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

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

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

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

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

Azure サイトから外部デバイスへの接続を有効にする

```

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

```

} VRF Definition

} IPSec Global Configurations

• 次の図に示すフィールドは、これらの領域の構成に使用されます。

- トンネルごとの IPSec および ikev1 構成
- VRF ネイバーの BGP 設定

```

!
crypto keyring Ext-V1-1000-ike
pre-shared-key address <50.18.55.126>[cAPIC CSR Gig3 Public IP] key <abodefg12345>
!
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

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

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

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



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

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ1 インテント アイコンをクリックします。

[インテント (Intent)]メニューが表示されます。

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

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

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

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

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

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

[プロパティ (Properties)]	説明
全般	
名前	EPG の名前を入力します。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [テナントの選択 (Select Tenant)]をクリックします。[テナントの選択 (Select Tenant)]ダイアログボックスが表示されます。 [テナントの選択 (Select Tenant)]ダイアログで、左側の列のテナントをクリックして選択します。 このセクションで前述したように、インフラ テナントを選択し、インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。 [選択 (Select)]をクリックします。[EPG の作成 (Create EPG)]ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
アプリケーションプロファイル	<p>アプリケーションプロファイルを選択します。</p> <ol style="list-style-type: none"> [アプリケーションプロファイルの選択 (Select Application Profile)]をクリックします。[アプリケーションプロファイルの選択 (Select Application Profile)]ダイアログボックスが表示されます。 [アプリケーションプロファイルの選択 (Select Application Profile)]ダイアログで、左側の列のアプリケーションプロファイルをクリックして選択します。 (注) インフラテナントで EPG を作成する場合、アプリケーションプロファイルはオーバーレイ-1 VRF の EPG で使用されるため、クラウド インフラアプリケーションプロファイルを選択しないことを推奨します。異なるアプリケーションプロファイルを選択するか、[アプリケーションプロファイルの作成 (Create Application Profile)]を選択して、新しいプロファイルを作成します。 [選択 (Select)]をクリックします。[EPG の作成 (Create EPG)]ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定 (Settings)]	
タイプ	これはアプリケーション EPG であるため、EPG タイプとして [アプリケーション (Application)] を選択します。
VRF	<p>VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [VRF の選択 (Select VRF)]をクリックします。[VRF の選択 (Select VRF)]ダイアログボックスが表示されます。 [VRF の選択 (Select VRF)]ダイアログで、左側の列の VRF をクリックして選択します。 インフラテナントで EPG を作成している場合は、この手順でセカンダリ VRF を選択します。セカンダリ VRF のクラウド EPG は、他のクラウド EPG およびセカンダリ VRF のクラウド外部 EPG と通信でき、他のユーザテナント VRF のクラウド EPG とも通信できます。 [選択 (Select)]をクリックします。[EPG の作成 (Create EPG)]ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
エンドポイントセクタ	

[プロパティ (Properties)]	説明
	<p>(注) エンドポイントセレクタ構成プロセスの一部として Azure で仮想マシンを構成する手順については、Azureでの仮想マシンの構成 (127ページ) を参照してください。</p> <p>エンドポイントセレクタを追加するには：</p> <ol style="list-style-type: none"> 1. [エンドポイントセレクタの追加 (Add Endpoint Selector)] をクリックして、[エンドポイントセレクタの追加] ダイアログを開きます。 2. [エンドポイントセレクタの追加 (Add Endpoint Selector)] ダイアログの [Name (名前)] フィールドに名前を入力します。 3. [セレクタ式 (Selector Expression)] をクリックします。[キー (Key)]、[演算子 (Operator)]、および [値 (Value)] フィールドが有効になります。 4. [キー (Key)] ドロップダウンリストをクリックしてキーを選択します。次のオプションがあります。 <ul style="list-style-type: none"> • エンドポイントセレクタに IP アドレスまたはサブネットを使用する場合は、[IP] を選択します。 <p>(注) IPv6 は Azure の Cisco Cloud Network Controller ではサポートされていません。このフィールドには有効な IPv4 アドレスを使用する必要があります。</p> <ul style="list-style-type: none"> • エンドポイントセレクタに Azure リージョンを使用する場合は、[リージョン (Region)] を選択します。 • エンドポイントセレクタのカスタムキーを作成する場合は、[カスタム (Custom)] を選択します。 <p>(注) [カスタム (Custom)] オプションを選択すると、ドロップダウンリストがテキストボックスになります。custom: の後にスペースのキーの名前を入力する必要があります (例：custom: Location) 。</p> 5. [演算子 (Operator)] ドロップダウンリストから演算子を選択します。次のオプションがあります。 <ul style="list-style-type: none"> • [等しい (Equals)]: 値フィールドに 1 つの値がある場合に使用します。 • [等しくない (Not Equals)]: 値フィールドに 1 つの値がある場合に使用されます。 • [の中にある (In)]: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。 • [の中にない (Not In)]: 値フィールドに複数のカンマ区切り値がある場合に使用されます。 • [キーを持つ (Has Key)]: 式にキーのみが含まれている場合に使用されます。

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • [キーを持たない (Does Not Have Key)]: 式にキーのみが含まれている場合に使用されます。 <p>6. [値 (Value)] フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。入力する値は、[キー (Key)] フィールドと [演算子 (Operator)] フィールドで選択した内容によって異なります。たとえば、[キー (Key)] フィールドが [IP] に設定され、[演算子 (Operator)] フィールドが [等しい (equals)] に設定されている場合、[値 (Value)] フィールドは IP アドレスまたはサブネットでなければなりません。ただし、[演算子 (Operator)] フィールドが [キー (keys)] に設定されている場合、[値 (Value)] フィールドは無効になります。</p> <p>7. 完了したら、チェックマークをクリックしてセレクトタ式を検証します。</p> <p>8. エンドポイント セレクトタに追加のエンドポイント セレクト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 セレクトタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。</p> <p>たとえば、1つのエンドポイントセレクトタで2つの式セットを作成したとします。</p> <ul style="list-style-type: none"> • エンドポイントセレクトタ 1、式 1: <ul style="list-style-type: none"> • [キー (Key):] Region • 演算子 (Operator) : equals • 値 : westus • エンドポイントセレクトタ1、式 2: <ul style="list-style-type: none"> • [キー (Key):] IP • 演算子 (Operator) : equals • [値 (Value):] 192.0.2.1/24 <p>この場合、これらの式の両方が真になる場合（リージョンが westus で、IP アドレスがサブネット 192.0.2.1/24 に属している場合）に、そのエンドポイントはクラウド EPG に割り当てられます。</p>

[プロパティ (Properties)]	説明
	<p>9. このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックし、終了したら、[追加 (Add)] をクリックします。</p> <p>EPG の下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理ORがあるものとみなされます。たとえば、前のステップで説明したようにエンドポイントセレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイントセレクタを作成したとします。</p> <ul style="list-style-type: none"> • エンドポイントセレクタ 2、式 1: <ul style="list-style-type: none"> • [キー (Key):] Region • 演算子 : in • 値 : eastus、centralus <p>その場合、次のようになります。</p> <ul style="list-style-type: none"> • リージョンが westus で、IP アドレスが 192.0.2.1/24 サブネットに属している (エンドポイントセレクタ 1 の式) <p>OR</p> <ul style="list-style-type: none"> • リージョンが eastus または centralus のどちらかである場合 (エンドポイントセレクタ 2 式) <p>その場合、エンドポイントがクラウド EPG に割り当てられます。</p>

ステップ 5 設定が終わったら [Save] をクリックします。

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

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



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

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 インテント アイコンをクリックします。

[**インテント (Intent)**] メニューが表示されます。

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

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

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

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

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

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

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

[プロパティ (Properties)]	説明
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)]をクリックします。[テナントの選択 (Select Tenant)] ダイアログボックスが表示されます。 2. [テナントの選択 (Select Tenant)] ダイアログで、左側の列のテナントをクリックして選択します。 このセクションで前述したように、インフラ テナントを選択し、インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。 3. [選択 (Select)]をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。
アプリケーションプロファイル	<p>アプリケーション プロファイルを選択します。</p> <ol style="list-style-type: none"> 1. [アプリケーション プロファイルの選択 (Select Application Profile)]をクリックします。[アプリケーション プロファイルの選択 (Select Application Profile)] ダイアログボックスが表示されます。 2. [アプリケーション プロファイルの選択 (Select Application Profile)] ダイアログで、左側の列のアプリケーション プロファイルをクリックして選択します。 (注) インフラ テナントで EPG を作成する場合、アプリケーション プロファイルはオーバーレイ-1 VRF の EPG で使用されるため、クラウド インフラ アプリケーション プロファイルを選択しないことを推奨します。異なるアプリケーション プロファイルを選択するか、[アプリケーション プロファイルの作成 (Create Application Profile)] を選択して、新しいプロファイルを作成します。 3. [選択 (Select)]をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定 (Settings)]	
タイプ	これは外部 EPG であるため、EPG タイプとして [外部 (External)] を選択します。

[プロパティ (Properties)]	説明
VRF	<p>VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [VRF の選択 (Select VRF)] をクリックします。[VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 2. [VRF の選択 (Select VRF)] ダイアログで、左側の列の VRF をクリックして選択します。 インフラテナントで EPG を作成している場合は、この手順でセカンダリ VRF を選択します。セカンダリ VRF のクラウド EPG は、他のクラウド EPG およびセカンダリ VRF のクラウド外部 EPG と通信でき、他のユーザ テナント VRF のクラウド EPG とも通信できます。 3. [選択 (Select)] をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。
ルート到達可能性	<p>外部 EPG のルート到達可能性のタイプを選択します。次のオプションがあります。</p> <ul style="list-style-type: none"> • インターネット • 外部サイト

[プロパティ (Properties)]	説明
エンドポイントセクタ	<p>(注) エンドポイント セクタ構成プロセスの一部として Azure で仮想マシンを構成する手順については、Azureでの仮想マシンの構成 (127ページ) を参照してください。</p> <p>エンドポイント セクタを追加するには：</p> <ol style="list-style-type: none"> 1. [エンドポイントセクタの追加 (Add Endpoint Selector)] をクリックして、エンドポイントセクタを追加します。 2. [名前 (Name)] フィールドに名前を入力します。 3. サブネットにサブネットを入力します。 (注) IPv6 は Azure の Cisco Cloud Network Controller ではサポートされていません。このフィールドには有効なIPv4アドレスを使用する必要があります。 4. 終了したら、チェックマークをクリックしてエンドポイント セクタを検証します。 5. 追加のエンドポイントセクタを作成するかどうかを決定します。 <p>EPG の下で複数のエンドポイントセクタを作成した場合は、それらのエンドポイントセクタの間には論理 OR があるものとみなされます。たとえば、2つのエンドポイントセクタを作成したとします。</p> <ul style="list-style-type: none"> • エンドポイントセクタ 1 : <ul style="list-style-type: none"> • 名前 : EP_Sel_1 • サブネット : 192.1.1.1/24 • エンドポイントセクタ 2 : <ul style="list-style-type: none"> • 名前 : EP_Sel_2 • サブネット : 192.2.2.2/24 <p>その場合、次のようになります。</p> <ul style="list-style-type: none"> • IP アドレスが 192.1.1.1/24 サブネット (エンドポイントセクタ 1) に属する場合 または • IPアドレスが 192.2.2.2/24 サブネット (エンドポイントセクタ 2) に属する場合 <p>その場合、エンドポイントがクラウド EPG に割り当てられます。</p>

ステップ 5 設定が終わったら [Save] をクリックします。

サービス EPG の作成

次のセクションの手順を使用して、サービス EPG を作成します。

Tasks To Perform Prior to Configuring Service EPGs

Before you can configure a service EPG, there are certain tasks that you might have to perform beforehand. If you are using subnets or private link labels with your service EPG, you must first configure the subnets and/or private link label outside of the service EPG.

ステップ 1 Create a VRF, if necessary.

- a) Click the **Intent** icon. The **Intent** menu appears.
- b) Click the drop-down arrow below the **Intent** search box and choose **Application Management**.
A list of **Application Management** options appear in the **Intent** menu.
- c) From the **Application Management** list in the **Intent** menu, click **Create VRF**. The **Create VRF** dialog box appears.
- d) Make the following selections:
 - **Name**: Enter the name for the VRF.
 - **Tenant**: Select a tenant.
- e) Click **Save**.

ステップ 2 Configure a cloud context profile.

- a) Click the **Intent** icon. The **Intent** menu appears.
- b) Click the drop-down arrow below the **Intent** search box and choose **Application Management**.
A list of **Application Management** options appear in the **Intent** menu.
- c) From the **Application Management** list in the **Intent** menu, click **Create Cloud Context Profile**. The **Create Cloud Context Profile** dialog box appears.

ステップ 3 Enter the appropriate values in each field as listed in the following *Cloud Context Profile Dialog Box Fields* table then continue.

Table 11: Create Cloud Context Profile Dialog Box Fields

Properties	Description
Name	Enter the name of the cloud context profile.
Tenant	To choose a tenant: <ol style="list-style-type: none"> a. Click Select Tenant. The Select Tenant dialog box appears. b. From the Select Tenant dialog, click to choose a tenant in the left column then click Select. You return to the Create Cloud Context Profile dialog box.
Description	Enter a description of the cloud context profile.
Settings	

Properties	Description
Region	To choose a region: <ol style="list-style-type: none"><li data-bbox="418 338 1109 369">a. Click Select Region. The Select Region dialog box appears.<li data-bbox="418 390 1498 453">b. From the Select Region dialog, click to choose a region in the left column then click Select. You return to the Create Cloud Context Profile dialog box.
VRF	To choose a VRF: <ol style="list-style-type: none"><li data-bbox="418 543 1060 575">a. Click Select VRF. The Select VRF dialog box appears.<li data-bbox="418 596 1498 659">b. From the Select VRF dialog box, click to choose a VRF in the left column then click Select. You return to the Create Cloud Context Profile dialog box.

Properties	Description
Add CIDR	<p>Note You cannot add, delete, or edit a CIDR when VNet peering is enabled. You must disable VNet peering before adding, deleting or editing a CIDR. To disable VNet peering:</p> <ul style="list-style-type: none"> • For the infra tenant, disable the Hub Network Peering option in the cloud context profile • For a user (non-infra) tenant, disable the VNet Peering option in the cloud context profile <p>Enable VNet peering again after you have made the changes to the CIDR configuration.</p> <p>The following features are supported, depending on the release:</p> <ul style="list-style-type: none"> • You can add additional secondary CIDRs and subnets for infra VNets (cloudCtxProfiles created by the cloud template). You cannot add primary CIDRs or modify the existing CIDRs created by the cloud template. After subnets are created under the user-created CIDRs, the subnets will be implicitly mapped to the secondary VRF. • You can add also additional secondary CIDRs and subnets for VNets other than the infra VNet. <p>See 単一 VNet での複数の VRF のサポート, on page 31 for more information.</p> <p>To add a CIDR:</p> <ol style="list-style-type: none"> a. Click Add CIDR. The Add CIDR dialog box appears. b. Enter the address in the CIDR Block Range field. c. Click to check (enabled) or uncheck (disabled) the Primary check box. If you are adding additional secondary CIDRs and subnets for VNets, leave the Primary box unchecked. d. Click Add Subnet and enter the following information: <ul style="list-style-type: none"> • In the Address field, enter the subnet address. • In the Name field, enter the name for this subnet. • In the Private Link Label field, choose Create New and enter a unique name for the private link label to associate with this subnet. e. In the VRF field, make a selection, if necessary. <ul style="list-style-type: none"> • If you checked the box next to the Primary field, this CIDR is automatically associated with the primary VRF. • If you did not check the box next to the Primary field, you can associate this CIDR with a secondary VRF. Click the X next to the VRF, then click on Select VRF to select the secondary VRF to associate with this CIDR. f. When finished, click Add.
VNet Gateway Router	Click to check (enable) or uncheck (disable) in the VNet Gateway Router check box.

Properties	Description
VNet Peering	Click to check (enable) or uncheck (disable) the Azure VNet peering feature. For more information on the VNet peering feature, see the <i>Configuring VNet Peering for Cisco Cloud Network Controller for Azure</i> document in the Cisco Cloud Network Controller documentation page .

ステップ 4 Click Save.

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

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

始める前に

- [クラウド サービスエンドポイント グループ \(35 ページ\)](#) の情報を確認してください。

- サブネットごとの NSG 構成が有効になっていることを確認します。

クラウド サービス EPG を構成している場合は、サブネットごとの NSG 構成を有効にする必要があります。詳細については、「[セキュリティ グループ \(43 ページ\)](#)」を参照してください。

- アプリケーション プロファイルと VRF を作成します。

ステップ 1 インテント アイコンをクリックします。

[**インテント (Intent)**] メニューが表示されます。

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

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

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

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

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

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

[プロパティ (Properties)]	説明
全般	
名前	EPG の名前を入力します。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログボックスが表示されます。 [テナントの選択 (Select Tenant)] ダイアログで、左側の列のテナントをクリックして選択します。 [選択 (Select)] をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。
アプリケーションプロファイル	<p>アプリケーションプロファイルを選択します。</p> <ol style="list-style-type: none"> [アプリケーションプロファイルの選択 (Select Application Profile)] をクリックします。[アプリケーションプロファイルの選択 (Select Application Profile)] ダイアログボックスが表示されます。 [アプリケーションプロファイルの選択 (Select Application Profile)] ダイアログで、左側の列のアプリケーションプロファイルをクリックして選択します。 <p>(注) インフラテナントでサービス EPG を作成する場合、アプリケーションプロファイルはオーバーレイ-VRF の EPG で使用されるため、cloud-infra アプリケーションプロファイルを選択しないことを推奨します。異なるアプリケーションプロファイルを選択するか、[アプリケーションプロファイルの作成 (Create Application Profile)] を選択して、新しいプロファイルを作成します。</p> <ol style="list-style-type: none"> [選択 (Select)] をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定 (Settings)]	
タイプ	これはサービス EPG であるため、EPG タイプとして [サービス (Service)] を選択します。

[プロパティ (Properties)]	説明
VRF	<p>VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [VRF の選択 (Select VRF)] をクリックします。[VRF の選択 (Select VRF)] ダイアログボックスが表示されます。 2. [VRF の選択 (Select VRF)] ダイアログで、左側の列の VRF をクリックして選択します。 3. [選択 (Select)] をクリックします。[EPG の作成 (Create EPG)] ダイアログボックスに戻ります。
導入タイプ	<p>EPG 展開タイプを選択します。</p> <p>サービスは展開モードによって異なります。</p> <ul style="list-style-type: none"> • [クラウドネイティブ (Cloud Native)] : プロバイダーネットワークに展開されたクラウドネイティブサービス • [クラウドネイティブ管理対象 (Cloud Native Managed)] : ネットワークに展開されたクラウドネイティブサービス • [サードパーティ (Cloud Native Managed)] : 市場からのサードパーティ サービス
アクセスタイプ	<p>EPG 展開のアクセスタイプを選択します。アクセスタイプは、他のサービスまたは VM がサービスに接続する方法を示します。</p> <p>選択肢は、[展開タイプ (Deployment Type)] フィールドで行った選択によって異なります。</p> <ul style="list-style-type: none"> • [クラウドネイティブ (Cloud Native)] 展開タイプ : <ul style="list-style-type: none"> • [パブリック (Public)] : サービスのパブリック IP にアクセスします。 • [プライベート (Private)] : プライベートリンクとプライベートエンドポイントを使用してサービスにアクセスします。 • [クラウドネイティブ管理対象 (Cloud Native Managed)] 展開タイプ : <ul style="list-style-type: none"> • [プライベート (Private)] : 管理対象サブネットに展開されたサービスにプライベート IP アドレスのみがある場合は、このタイプを選択します。 • [パブリックおよびプライベート (Public and Private)] : パブリックエンドポイントとプライベートエンドポイントを使用してサービスにアクセスします。これは、Cisco Cloud Network Controller で管理されたサブネットに展開されたときにパブリック IP アドレスも公開するサービスに使用されます。 • [サードパーティ (Third-Party)] 展開タイプ : [プライベート (Private)] は、アクセスタイプとして使用できる唯一のオプションです。これは、サービスが提供する場合、サービスへのプライベート エンドポイントのみを使用することを意味します。

[プロパティ (Properties)]	説明
サービスの種類	<p>Azure サービス タイプを選択します。</p> <p>特定のサービス タイプは、ある特定の展開タイプでのみサポートされます。特定の展開タイプでサポートされるサービスタイプの詳細については、クラウドサービスエンドポイントグループ (35 ページ) を参照してください。</p> <p>次のオプションがあります。</p> <ul style="list-style-type: none"> • [Azure Storage Blob] (Azure Storage (39 ページ) を参照) • [Azure SQL] • Azure Cosmos DB • [Azure Databricks] (Azure Databricks サービス (40 ページ) を参照) • [Azure Storage] (Azure Storage (39 ページ) を参照) • [Azure Storage ファイル (Azure Storage File)] (Azure Storage (39 ページ) を参照) • [Azure Storage キュー (Azure Storage Queue)] (Azure Storage (39 ページ) を参照) • [Azure Storage テーブル (Azure Storage Table)] (Azure Storage (39 ページ) を参照) • [Azure Kubernetes サービス (AKS) (Azure Kubernetes Services (AKS)] (Azure Kubernetes サービス (40 ページ) を参照) • [Azure Active Directory ドメイン サービス (Azure Active Directory Domain Services)] (Azure Active Directory ドメイン サービス (40 ページ) を参照) • [Azure コンテナ レジストリ (Azure Container Registry)] • [Azure ApiManagement サービス (Azure ApiManagement Services)] (Azure ApiManagement サービス (39 ページ) を参照) • Azure Key Vault • [Redis キャッシュ (Redis Cache)] (Azure Redis キャッシュ (41 ページ) を参照) • [カスタム サービス (Custom Service)] ([展開タイプ (Deployment Type)])として[サードパーティ (Third-Party)]を選択した場合に使用します。)

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

- 展開タイプとして [\[クラウド ネイティブ \(Cloud Native\) \]](#) を選択した場合は、[展開タイプとしてクラウド ネイティブを構成する \(101 ページ\)](#) に進みます。
- 展開タイプとして [\[クラウド ネイティブ管理対象 \(Cloud Native Managed\) \]](#) を選択した場合は、[展開タイプとしてクラウド ネイティブ管理対象を構成する \(104 ページ\)](#) に進みます。

- 展開タイプとして[サードパーティ (Third-Party)]を選択した場合は、[展開の種類としてサードパーティを構成する \(106 ページ\)](#)に進みます。

展開タイプとしてクラウドネイティブを構成する

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

始める前に

[クラウドネイティブ \(41 ページ\)](#) に記載されている情報を確認して、これらの手順を使用する前に実行する必要があるタスクを理解してください。

- ステップ 1** これらの手順を開始する前に、[Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#) の手順を完了していることを確認します。
- これらの手順は、これらの手順で展開タイプを構成する前に、Azure SQL などのサービス タイプを設定する [Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#) で提供される手順の続きです。
- ステップ 2** アクセスタイプとして[プライベート (Private)]を選択した場合、[プライベート リンク ラベルの選択 (Select Private Link Label)] オプションが使用可能になります。
- プライベート リンク ラベルは、サブネットをサービス EPG に関連付けるために使用されます。
- ステップ 3** [プライベート リンク ラベルの選択 (Select Private Link Label)] をクリックします。
- [プライベート リンク ラベルの選択 (Select Private Link Label)] ウィンドウが表示されます。
- ステップ 4** 適切なプライベート リンク ラベルを検索します。
- [Tasks To Perform Prior to Configuring Service EPGs \(94 ページ\)](#) で提供されている手順を使用して作成したプライベート リンク ラベルを検索します。
- ステップ 5** [プライベート リンク ラベルの選択 (Select Private Link Label)] ウィンドウで、適切なプライベート リンク ラベルを選択します。
- [EPG の作成 (Create EPG)] ウィンドウに戻ります。
- 次に、[エンドポイントセクタ (Endpoint Selectors)] フィールドにエンドポイントセクタを追加します。
- ステップ 6** [エンドポイントセクタの追加 (Add Endpoint Selector)] をクリックします。
- [エンドポイントセクタの追加 (Add Endpoint Selector)] ウィンドウが表示されます。
- ステップ 7** [エンドポイントセクタの追加 (Add Endpoint Selector)] ウィンドウの[Name (名前)] フィールドに名前を入力します。
- ステップ 8** [キー (Key)] ドロップダウン リストをクリックしてキーを選択します。

次のオプションがあります。

- カスタム エンドポイント セレクタを作成する場合は、[**カスタム (Custom)**] を選択します。
- エンドポイント セレクタに Azure リージョンを使用する場合は、[**リージョン (Region)**] を選択します。
- エンドポイント セレクタにサービス リソースの名前を使用する場合、[**名前 (Name)**] を選択します。
たとえば、ProdSqlServer という名前の SQL サーバーを選択するには、これらの手順の後半で、[**キー (Key)**] フィールドで [名前 (Name)] を選択し、[**値 (Value)**] フィールドに ProdSqlServer と入力します。
- エンドポイント セレクタにクラウドプロバイダーの ID を使用する場合は、[**リソース ID (Resource ID)**] を選択します。
たとえば、クラウドプロバイダーのリソース ID を使用して SQL サーバーを選択するには、これらの手順の後に [キー] フィールドで [リソース ID (Resource ID)] を選択し、セレクタの値
(/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer など) を [値 (Value)] フィールドに入力します。

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

次のオプションがあります。

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

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

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

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

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

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

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

たとえば、1つのエンドポイントセクタで2つの式セットを作成したとします。

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

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

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

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

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

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

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

その場合、次のようになります。

- リージョンが `westus` であり、リソースに付けられた名前が `ProdSqlServer` である場合（エンドポイントセクタ 1 式）
- OR
- リージョンが `eastus` または `centralus` のどちらかである場合（エンドポイントセクタ 2 式）

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 15 設定が終わったら [Save] をクリックします。

展開タイプとしてクラウドネイティブ管理対象を構成する

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

始める前に

クラウドネイティブ管理対象 (42 ページ) に記載されている情報を確認して、これらの手順を使用する前に実行する必要があるタスクを理解してください。

ステップ 1 これらの手順を開始する前に、Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 (97 ページ) の手順を完了していることを確認します。

これらの手順は、これらの手順で展開タイプを構成する前に、Azure ApiManagement Services などのサービスタイプを設定する Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 (97 ページ) で提供される手順の続きです。

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

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

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

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

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

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

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

次のオプションがあります。

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

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

[Tasks To Perform Prior to Configuring Service EPGs \(94 ページ\)](#) で提供されている手順を使用して作成した IP アドレスまたはサブネットを入力します。

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

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

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

たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイントセレクタ 1、式 1:

- **[キー (Key):]** IP
- **演算子 (Operator)** : equals
- **値** : 192.1.1.1/24

- エンドポイントセレクタ1、式 2:

- **[キー (Key):]** IP
- **演算子** : not equals
- **値** : 192.1.1.2

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

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

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

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

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

- エンドポイントセレクタ 2、式 1:

- **[キー (Key):]** IP
- **演算子 (Operator)** : equals
- **値** : 192.2.2.2/24

その場合、次のようになります。

展開の種類としてサードパーティを構成する

- IP アドレスがサブネット 192.1.1.1/24 に属し、IP アドレスが 192.1.1.2 でない場合（エンドポイントセレクタ 1 式）
- OR
- IP アドレスがサブネット 192.2.2.2/24 に属する場合

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 11 設定が終わったら [Save] をクリックします。

展開の種類としてサードパーティを構成する

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



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

ステップ 1 これらの手順を開始する前に、[Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#) の手順を完了していることを確認します。

これらの手順は、[Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#) で提供されている手順の続きであり、これらの手順で展開タイプを構成する前にサービスタイプを [カスタム サービス (Custom Service)] として設定します。

ステップ 2 [サードパーティ (Third-Party)] の展開タイプのアクセスタイプに必要な選択を行います。

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

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

ステップ 3 適切なプライベートリンクラベルを検索します。

[Tasks To Perform Prior to Configuring Service EPGs \(94 ページ\)](#) で提供されている手順を使用して作成したプライベートリンクラベルを検索します。

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

[EPG の作成 (Create EPG)] ウィンドウに戻ります。

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

- ステップ 5** [エンドポイント セレクタの追加 (Add Endpoint Selector)] をクリックします。
[エンドポイント セレクタの追加 (Add Endpoint Selector)] ウィンドウが表示されます。
- ステップ 6** [エンドポイント セレクタの追加 (Add Endpoint Selector)] ウィンドウの [Name (名前)] フィールドに名前を入力します。
- ステップ 7** [キー (Key)] ドロップダウン リストをクリックしてキーを選択します。
現時点では、このアクセスタイプのキーとして使用できるオプションは [URL] のみであり、エンドポイント セレクタのサービスを識別するエイリアスまたは完全修飾ドメイン名 (FQDN) を使用します。
- ステップ 8** [演算子 (Operator)] ドロップダウン リストから演算子を選択します。
次のオプションがあります。
- [等しい (Equals)] : 値フィールドに 1 つの値がある場合に使用します。
 - [等しくない (Not Equals)] : 値フィールドに 1 つの値がある場合に使用されます。
 - [の中にある (In)] : [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
 - [の中にない (Not In)] : 値フィールドに複数のカンマ区切り値がある場合に使用されます。
 - [キーを持つ (Has Key)] : 式にキーのみが含まれている場合に使用されます。
 - [キーを持たない (Does Not Have Key)] : 式にキーのみが含まれている場合に使用されます。
- ステップ 9** [値 (Value)] フィールドに有効な URL を入力し、チェックマークをクリックしてエントリを検証します。
- ステップ 10** 完了したら、チェックマークをクリックしてセレクタ式を検証し、[追加 (Add)] をクリックします。
[EPG の作成 (Create EPG)] 画面に戻り、新しいエンドポイントセレクタと構成された式が表示されます。
- ステップ 11** 追加のエンドポイント セレクタを作成する場合は、[エンドポイント セレクタの追加 (Add Endpoint Selector)] を再度クリックし、これらの手順を繰り返して追加のエンドポイント セレクタを作成します。
EPG の下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理 OR があるものとみなされます。
たとえば、下で説明しているように 2 つのエンドポイント セレクタを作成したとします。
- エンドポイントセレクタ 1 :
 - キー : URL
 - 演算子 (Operator) : equals
 - 値 : www.acme1.com
 - エンドポイント セレクタ 2 :
 - キー : URL

- 演算子 (Operator) : equals
- 値 : www.acme2.com

その場合、次のようになります。

- URL が www.acme1.com の場合
- OR
- URL が www.acme2.com の場合

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 12 設定が終わったら [Save] をクリックします。

Cisco Cloud 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 Filter)] をクリックします。[フィルタの作成 (Create Filter)] ダイアログボックスが表示されます。

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

表 13: フィルタの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
テナント	テナントを選択します。 <ol style="list-style-type: none"><li data-bbox="911 348 1518 457">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。<li data-bbox="911 478 1518 655">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	<p>フィルタを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [フィルタ エントリの追加 (Add Filter Entry)] をクリックします。[フィルタの追加 (Add Filter)] ダイアログボックスが表示されます。 2. [名前 (Name)] フィールドにフィルタエントリの名前を入力します。 3. [イーサネットタイプ (Ethernet Type)] ドロップダウンリストをクリックして、イーサネットタイプを選択します。次のオプションがあります。 <ul style="list-style-type: none"> • IP • [Unspecified] <p>(注) [指定なし (Unspecified)] を選択すると、IPを含むすべてのトラフィックタイプが許可され、残りのフィールドは無効になります。</p> 4. [IP プロトコル (IP Protocol)] ドロップダウンメニューをクリックして、プロトコルを選択します。次のオプションがあります。 <ul style="list-style-type: none"> • tcp • udp • [Unspecified] <p>(注) 残りのフィールドは、tcp または udp が選択されている場合にのみ有効になります。</p> 5. [宛て先ポート (Destination Port)] フィールドに適切なポート範囲情報を入力します。 6. フィルタエントリ情報の入力完了したら、[追加 (Add)] をクリックします。[フィルタの作成 (Create Filter)] ダイアログボックスに戻り、別のフィルタエントリを追加する手順を繰り返すことができます。

ステップ5 作業が完了したら、[保存 (Save)] をクリックします。

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

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

始める前に

フィルタを作成します。

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

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

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

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

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

表 14: [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	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログボックスが表示されます。 [テナントの選択 (Select Tenant)] ダイアログで、左側の列のテナントをクリックして選択します。 <p>(注) リリース 5.0(2) 以降、インフラテナントでコントラクトを作成できます。共有サービスの使用例では、インフラテナントからコントラクトをエクスポートしたり、インフラテナントにコントラクトをインポートしたりすることもできます。</p> <ol style="list-style-type: none"> [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。

[プロパティ (Properties)]	説明
説明	コントラクトの説明を入力してください。
[設定 (Settings)]	
スコープ	<p>このスコープは、同じアプリケーション プロファイル内、同じ VRF インスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイントグループにコントラクトを制限します。</p> <p>(注) 共有サービスにより、異なるテナントの EPG 間および異なる VRF の EPG 間の通信が可能になります。</p> <p>1つのテナントの EPG が別のテナントの EPG と通信できるようにするには、[グローバル (Global)] スコープを選択します。</p> <p>1つの VRF の EPG が別の VRF の別の EPG と通信できるようにするには、[グローバル (Global)] または [テナント (Tenant)] スコープを選択します。</p> <p>共有サービスの詳細については、共有サービス (58 ページ) を参照してください。</p> <p>ドロップダウン矢印をクリックして、次のスコープ オプションから選択します。</p> <ul style="list-style-type: none"> • アプリケーション プロファイル • VRF • Global • テナント
フィルタの追加	<p>フィルタを選択します。</p> <ol style="list-style-type: none"> 1. [フィルタの追加 (Add Filter)] をクリックします。フィルタ行が表示され、[フィルタの選択 (Select Filter)] オプションが表示されます。 2. [フィルタの選択 (Select Filter)] をクリックします。[フィルタの選択 (Select Filter)] ダイアログボックスが表示されます。 3. [フィルタの選択 (Select Filter)] ダイアログで、左側の列のフィルタをクリックして選択し、[選択 (Select)] をクリックします。[コントラクトの作成 (Create Contract)] ダイアログボックスに戻ります。

ステップ 5 設定が終わったら [Save] をクリックします。

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

このセクションでは、Cisco Cloud Network Controller GUI を使用したテナント間契約の作成方法について説明します。テナント間コントラクトの作成が必要になる状況の詳細については、[共有サービス \(58 ページ\)](#) を参照してください。

始める前に

フィルタを作成します。

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

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

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

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

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

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

[プロパティ (Properties)]	説明
名前 (Name)	契約の名前を入力します。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログボックスが表示されます。 [テナントの選択 (Select Tenant)] ダイアログで、左側の列のテナントをクリックして選択します。 <p>(注) リリース 5.0(2) 以降、インフラテナントでコントラクトを作成できません。共有サービスの使用例では、インフラテナントからコントラクトをエクスポートしたり、インフラテナントにコントラクトをインポートしたりすることもできます。</p> <ol style="list-style-type: none"> [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。

[プロパティ (Properties)]	説明
[設定 (Settings)]	
スコープ	<p>このスコープは、同じアプリケーションプロファイル内、同じ VRF インスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイントグループにコントラクトを制限します。</p> <p>テナント間通信の場合は、まずテナントの1つ（tenant1 など）のグローバルスコープとの契約を作成します。このテナントのEPGは、常にこの契約のプロバイダーになります。</p> <p>このコントラクトは、他のテナント（tenant2 など）にエクスポートされます。この契約をインポートする他のテナントでは、その EPG がインポートされた契約のコンシューマになります。tenant2 の EPG をプロバイダー、tenant1 の EPG をコンシューマにするには、tenant2 でコントラクトを作成し、tenant1 にエクスポートします。</p>
フィルタの追加	<p>フィルタを選択します。</p> <ol style="list-style-type: none"> <li data-bbox="496 867 1477 930">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。 <li data-bbox="496 961 1477 1024">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。 <li data-bbox="496 1056 1477 1161">3. [フィルタの選択 (Select Filter)] ダイアログで、左側の列のフィルタをクリックして選択し、[選択 (Select)] をクリックします。[コントラクトの作成 (Create Contract)] ダイアログボックスに戻ります。

ステップ 5 設定が終わったら [Save] をクリックします。

ステップ 6 作成したコントラクトを別のテナントにエクスポートします。

たとえば、次のようなケースがあるとします。

- 上記の手順で作成したコントラクトの名前は、**tenant tenant1** の **contract1** です。
 - エクスポートするコントラクトは、**exported_contract1** という名前で、テナント **tenant2** にエクスポートします。
- a) [コントラクト (Contracts)] ページ ([アプリケーション管理 (Application Management)] > [コントラクト (Contracts)]) に移動します。
設定されたコントラクトがリストされます。
 - b) 作成したばかりのコントラクトを選択します。
たとえば、コントラクト **contract1** が表示されるまでリストをスクロールし、その横にあるボックスをクリックして選択します。
 - c) [アクション (Actions)] > [コントラクトのエクスポート (Export Contract)] に移動します。

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

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

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

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

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

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

たとえば、**exported_contract1** です。

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

- h) [保存 (**Save**)] をクリックします。

コントラクトのリストが再び表示されます。

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

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

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

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

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

[**選択 (Select)**] ウィンドウが表示されます。

- d) これらの手順の最初に作成したコントラクトを見つけて選択します。

この例では、**contract1** を見つけて選択します。

- e) [選択 (**Select**)] をクリックします。

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

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

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

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

- h) [選択 (**Select**)] をクリックします。

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

- i) [保存 (**Save**)] をクリックします。

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

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

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

- b) [では始めましょう (Let's Get Started)] をクリックします。
- c) [コントラクト (Contract)] 領域で、[コントラクトの選択 (Select Contract)] をクリックします。
[選択 (Select)] ウィンドウが表示されます。
- d) これらの手順の最初に作成したコントラクトを見つけて選択します。
この例では、**exported_contract1** を見つけて選択します。
- e) [選択 (Select)] をクリックします。
[EPG 通信 (EPG Communication)] ウィンドウが表示されます。
- f) [コンシューマー EPG (Consumer EPGs)] 領域で、[コンシューマー EPG の追加 (Add Consumer EPGs)] をクリックします。
[コンシューマー EPG の選択 (Select Consumer EPGs)] ウィンドウが表示されます。
- g) [選択した項目を保持 (Keep selected Items)] チェックボックスをオンのままにして、2 番目のテナント (**tenant2**) の EPG を選択します。
- h) [選択 (Select)] をクリックします。
[EPG 通信 (EPG Communication)] ウィンドウが表示されます。
- i) [保存 (Save)] をクリックします。

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

[セキュリティ グループ \(43 ページ\)](#) で説明されているように、ネットワーク セキュリティ グループの構成方法は、リリースによって異なります。

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



(注) Cisco Cloud Network Controller では、新しい **NSG-per-subnet** 構成 [または (or)] 古い **NSG-per-EPG** 構成を使用できます。同じ Cisco Cloud Network Controller システムに両方の構成を含めることはできません。

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

始める前に

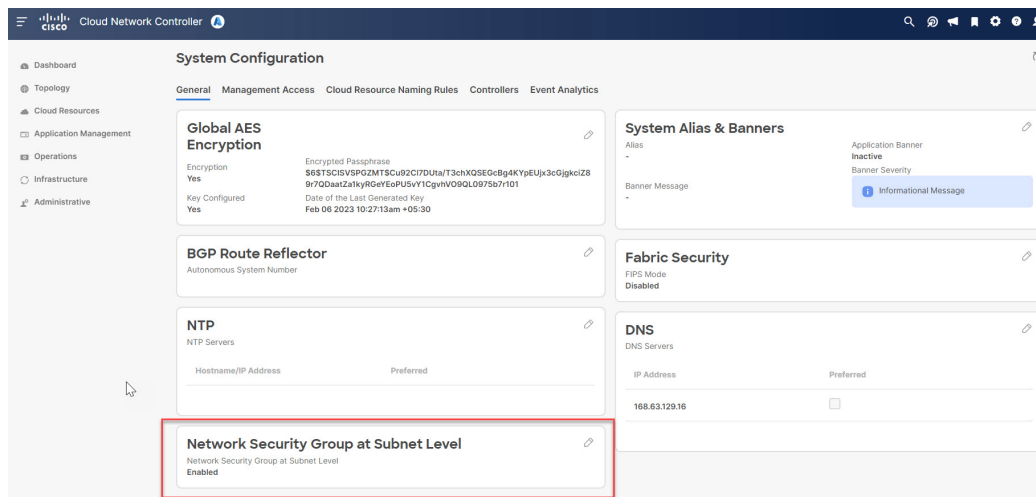
[セキュリティグループ \(43 ページ\)](#) で提供されている情報を確認して、リリースに応じてセキュリティグループがどのように構成されているかを理解し、セキュリティグループのガイドラインと制限を理解してください。

ステップ 1 まだログインしていない場合は、Cisco クラウド ネットワーク コントローラ GUI にログインします。

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

デフォルトでは [全般 (General)] タブが表示されます。

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



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

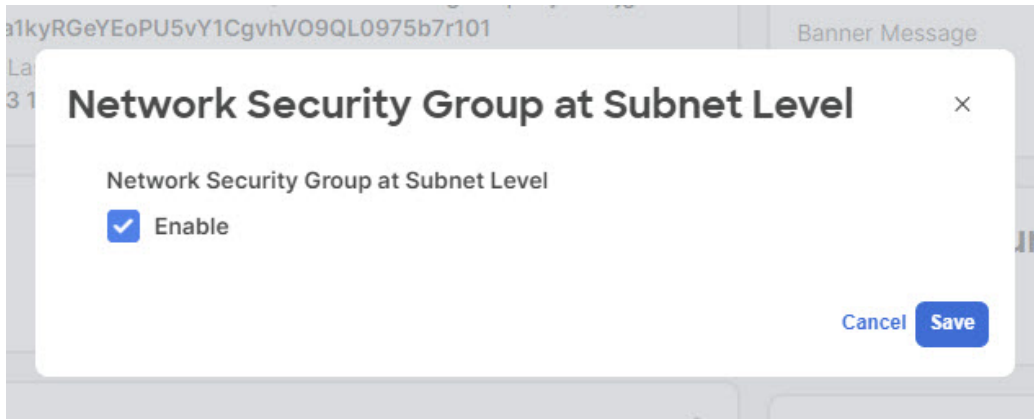
- このフィールドの値として [有効 (Enabled)] が表示されている場合は、Cisco Cloud ネットワーク コントローラの新しい **NSG-per-subnet** 構成があることを意味します。
- このフィールドの値として [無効 (Disabled)] が表示されている場合は、Cisco Cloud ネットワーク コントローラに古い **NSG-per-EPG** 構成があることを意味します。

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

必要な構成	既存の構成	アクション
Cisco Cloud ネットワーク コントローラの新しいNSG-per-subnet 構成が必要な場合、および：	[サブネット レベルのネットワーク セキュリティ グループ (Network Security Group at Subnet Level)] フィールドの値として [有効 (Enabled)] が表示されている場合は、次のようにします。	Cisco Cloud Network Controller は、必要なNSG-per-subnet 構成ですすでにセットアップされています。変更を加える必要はありません。
	[サブネット レベルのネットワーク セキュリティ グループ (Network Security Group at Subnet Level)] フィールドの値として [無効 (Disabled)] が表示されている場合は、次のようにします。	[サブネット レベルのネットワーク セキュリティ グループ (Network Security Group at Subnet Level)] フィールドの設定を変更する必要があります。ステップ 6 (118 ページ) に進みます。
Cisco Cloud ネットワーク コントローラの古いNSG-per-EPG 構成が必要な場合、および：	[サブネット レベルのネットワーク セキュリティ グループ (Network Security Group at Subnet Level)] フィールドの値として [有効 (Enabled)] が表示されている場合は、次のようにします。	[サブネット レベルのネットワーク セキュリティ グループ (Network Security Group at Subnet Level)] フィールドの設定を変更する必要があります。ステップ 6 (118 ページ) に進みます。
	[サブネット レベルのネットワーク セキュリティ グループ (Network Security Group at Subnet Level)] フィールドの値として [無効 (Disabled)] が表示されている場合は、次のようにします。	Cisco Cloud Network Controller は、必要なNSG-per-EPG 構成ですすでにセットアップされています。変更を加える必要はありません。

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

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



ステップ 7 ウィンドウで必要な変更を行います。

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

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

次の点に注意してください。

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

1. [アプリケーション管理 (Application Management)] > [クラウド コンテキスト プロファイル (Cloud Context Profiles)] に移動します。
2. 必要なクラウド コンテキスト プロファイルを見つけて、そのプロファイルをクリックします。
このクラウド コンテキスト プロファイルの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。
3. [詳細 (Details)] アイコンをクリックします (🔍)。
このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。[CIDR] エリアの [サブネット (Subnets)] 列に、テキスト **Private Link Labels** が表示されます。
4. ウィンドウの右上隅の鉛筆アイコンをクリックします。
[クラウド コンテキスト プロファイルの編集 (Edit Cloud Context Profile)] ウィンドウが表示されます。
5. [設定 (Settings)] エリアで、もう一度 [CIDR] エリアを見つけて、その行の鉛筆アイコンをクリックします。
[CIDR の編集 (Edit CIDR)] ウィンドウが表示されます。
6. [サブネット (Subnets)] エリアで、[プライベート リンク ラベル (Private Link Label)] 列にエントリがある行を見つけ、そのサブネットの行の鉛筆アイコンをクリックします。
このサブネット行のエントリが編集可能になります。
7. そのサブネット行の [プライベート リンク ラベル (Private Link Label)] 列のエントリの横にある [X] をクリックします。
これにより、プライベート リンク ラベルが削除されます。

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

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

セキュリティ グループの詳細の表示

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

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

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

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

各タブには、次の情報が表示されます。

• [ネットワーク セキュリティ グループ (Network Security Groups)] タブ :

- **名前** : ネットワーク セキュリティ グループの名前。
- **クラウドプロバイダー ID** : ネットワーク セキュリティ グループに関連付けられているクラウドプロバイダー ID。

[名前 (Name)] および [クラウドプロバイダー ID (Cloud Provider ID)] フィールドに入力されている値は、NSG が新しいサブネットごとの NSG 構成 ([クラウドプロバイダ ID (Cloud Provider ID)] の [subnet-] として表示) で構成されているか、古い EPG ごとの NSG 構成 ([クラウドプロバイダー ID (Cloud Provider ID)] 列の [epg-]) で構成されているかを示します。ソフトウェアリリースに応じて使用できるさまざまなタイプの NSG 構成の詳細については、[セキュリティグループ \(43 ページ\)](#) を参照してください。

- **EPG** : 以前の EPG ごとの NSG 構成を使用している場合、ネットワーク セキュリティグループに関連付けられている EPG。
- **仮想マシン** : ネットワーク セキュリティ グループに関連付けられている仮想マシン。
- **エンドポイント** : ネットワーク セキュリティ グループに関連付けられているエンドポイント。
- **サブネット** : 新しいサブネットごとの NSG 構成を使用している場合、ネットワークセキュリティグループに関連付けられているサブネット。

• [アプリケーション セキュリティ グループ (Application Security Groups)] タブ :

- **正常性** : アプリケーション セキュリティ グループの正常性ステータス。
- **名前** : アプリケーション セキュリティ グループの名前。
- **クラウドプロバイダー ID** : アプリケーション セキュリティ グループに関連付けられているクラウドプロバイダー ID。
- **EPG** : アプリケーション セキュリティ グループに関連付けられている EPG。
- **仮想マシン** : アプリケーション セキュリティ グループに関連付けられている仮想マシン。
- **エンドポイント** : アプリケーション セキュリティ グループに関連付けられているエンドポイント。

ステップ 4 いずれかの列の値をクリックして、詳細情報を取得します。

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

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

Cisco Cloud 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。

(注) テナント内 (契約が作成される) の EPG が表示されます。

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

ステップ 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。

(注) テナント内 (契約が作成される) の EPG が表示されます。

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

- (注) 選択したコントラクトがインポート済みコントラクトの場合、プロバイダー EPG の選択は無効になります。
- c) 完了したら、[**選択 (Select)**] をクリックします。[**プロバイダー EPG の選択 (Select Provider EPGs)**] ダイアログボックスが閉じ、[**EPS コミュニケーション構成 (EPG Communication Configuration)**] ウィンドウに戻ります。
- d) [保存 (Save)] をクリックします。

Creating a Cloud Context Profile Using the Cisco Cloud Network Controller GUI

This section explains how to create a cloud context profile using the Cisco Cloud Network Controller GUI.

Before you begin

Create a VRF.

- ステップ 1** Click the **Intent** icon. The **Intent** menu appears.
- ステップ 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.
A list of **Application Management** options appear in the **Intent** menu.
- ステップ 3** From the **Application Management** list in the **Intent** menu, click **Create Cloud Context Profile**. The **Create Cloud Context Profile** dialog box appears.
- ステップ 4** Enter the appropriate values in each field as listed in the following *Cloud Context Profile Dialog Box Fields* table then continue.

Table 16: Create Cloud Context Profile Dialog Box Fields

Properties	Description
Name	Enter the name of the cloud context profile.
Tenant	To choose a tenant: <ol style="list-style-type: none"> a. Click Select Tenant. The Select Tenant dialog box appears. b. From the Select Tenant dialog, click to choose a tenant in the left column then click Select. You return to the Create Cloud Context Profile dialog box.
Description	Enter a description of the cloud context profile.
Settings	

Properties	Description
Region	To choose a region: <ol style="list-style-type: none"><li data-bbox="496 338 1187 369">a. Click Select Region. The Select Region dialog box appears.<li data-bbox="496 390 1446 453">b. From the Select Region dialog, click to choose a region in the left column then click Select. You return to the Create Cloud Context Profile dialog box.
VRF	To choose a VRF: <ol style="list-style-type: none"><li data-bbox="496 546 1138 577">a. Click Select VRF. The Select VRF dialog box appears.<li data-bbox="496 598 1446 661">b. From the Select VRF dialog box, click to choose a VRF in the left column then click Select. You return to the Create Cloud Context Profile dialog box.

Properties	Description
Add CIDR	

Properties	Description
	<p>Note The following subnet is reserved and should not be used in this Add CIDR field: 192.168.100.0/24 (reserved by the CCR for the bridge domain interface)</p> <p>Note You cannot add, delete, or edit a CIDR when VNet peering is enabled. You must disable VNet peering before adding, deleting or editing a CIDR. To disable VNet peering:</p> <ul style="list-style-type: none"> • For the infra tenant, disable the Hub Network Peering option in the cloud context profile • For a user (non-infra) tenant, disable the VNet Peering option in the cloud context profile <p>Enable VNet peering again after you have made the changes to the CIDR configuration.</p> <p>The following features are supported, depending on the release:</p> <ul style="list-style-type: none"> • You can add additional secondary CIDRs and subnets for infra VNets (cloudCtxProfiles created by the cloud template). You cannot add primary CIDRs or modify the existing CIDRs created by the cloud template. After subnets are created under the user-created CIDRs, the subnets will be implicitly mapped to the secondary VRF. • You can add also additional secondary CIDRs and subnets for VNets other than the infra VNet. <p>See 単一 VNet での複数の VRF のサポート, on page 31 for more information.</p> <p>To add a CIDR:</p> <ol style="list-style-type: none"> a. Click Add CIDR. The Add CIDR dialog box appears. b. Enter the address in the CIDR Block Range field. c. Click to check (enabled) or uncheck (disabled) the Primary check box. If you are adding additional secondary CIDRs and subnets for VNets, leave the Primary box unchecked. d. Click Add Subnet and enter the following information: <ul style="list-style-type: none"> • In the Address field, enter the subnet address. • In the Name field, enter the name for this subnet. • In the Private Link Label field, choose one of the following: <ul style="list-style-type: none"> • Select Existing: Click Select Private Link Label, then choose an existing private link label to associate with this subnet. • Create New: Enter a unique name for the private link label to associate with this subnet. e. In the VRF field, make a selection, if necessary.

Properties	Description
	<ul style="list-style-type: none"> • If you checked the box next to the Primary field, this CIDR is automatically associated with the primary VRF. • If you did not check the box next to the Primary field, you can associate this CIDR with a secondary VRF. Click the X next to the VRF, then click on Select VRF to select the secondary VRF to associate with this CIDR. <p>f. When finished, click Add.</p>
VNet Gateway Router	Click to check (enable) or uncheck (disable) in the VNet Gateway Router check box.
VNet Peering	Click to check (enable) or uncheck (disable) the Azure VNet peering feature. For more information on the VNet peering feature, see the <i>Configuring VNet Peering for Cisco Cloud Network Controller for Azure</i> document in the Cisco Cloud Network Controller documentation page .

ステップ 5 Click **Save** when finished.

Azure での仮想マシンの構成

Cisco クラウド ネットワーク コントローラのためのエンドポイント セレクタを構成するとき Cisco クラウド ネットワーク コントローラを構成するエンドポイントセレクタに対応する Azure で必要なインスタンスについても構成することが必要になります。

このトピックでは、Azure で仮想マシンを設定するための要件について説明します。Cisco Cloud Network Controller のエンドポイント セレクタを設定する前に、または後で、これらの要件を使用して Azure のインスタンスを設定することができます。たとえば、先に Azure のアカウントに移動し、Azure のカスタム タグまたはラベルを作成してから、Cisco Cloud 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、Azure のアカウントに移動し、Azure 以降のカスタム タグまたはラベルを作成することもできます。

始める前に

Azure 仮想マシンの構成プロセスの一環として、クラウド コンテキスト プロファイルを構成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 プロファイルを構成すると、VRF やリージョンの設定などの構成情報は、Azure にプッシュされます。

ステップ 1 クラウド コンテキスト プロファイル設定を確認して、次の情報を取得します。

- VRF 名
- サブネット情報

- サブスクリプション ID
- クラウド コンテキスト プロファイルが展開されている場所に対応するリソース グループ。

(注) 上記の情報に加えて、タグベースのEPGを使用している場合は、タグ名も知っている必要があります。タグ名は、クラウド コンテキスト プロファイル設定では使用できません。

クラウド コンテキスト プロファイル設定情報を取得するには、次の手順を実行します。

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

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。
- b) [クラウド コンテキスト プロファイル (Cloud Context Profiles)] サブタブ オプションを選択します。

Cisco Cloud 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 Azure 仮想マシン構成プロセスの一部として使用するクラウド コンテキスト プロファイルを選択します。

リージョン、VRF、IP アドレス、サブネットなど、このクラウド コンテキスト プロファイルのさまざまな設定パラメータが表示されます。Azure 仮想マシンを構成するときに、このウィンドウに表示される情報を使用します。

ステップ 2 Azure ユーザー テナントの Cisco Cloud Network Controller ポータル アカウントにログインし、クラウド コンテキスト プロファイル構成から収集した情報を使用して Azure VM の作成を開始します。

(注) Azure ポータルで VM を作成する方法の詳細については、Microsoft Azure のマニュアルを参照してください。

Cisco Cloud 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 17: バックアップ構成の作成ダイアログボックスのフィールド

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

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

[プロパティ (Properties)]	説明
	<p>バックアップで考慮するルート階層コンテンツを選択します</p> <ul style="list-style-type: none"> • ポリシー ユニバース • セレクタオブジェクト (Selector Object) : これを選択すると、[オブジェクトタイプ (Object Type)] ドロップダウンリストと [オブジェクト DN (Object DN)] フィールドが追加されます。 <p>1. オブジェクトタイプ (Object Type) ドロップダウンリストで、次のオプションから選択します。</p> <ul style="list-style-type: none"> • テナント (Tenant) : 選択すると、[テナントの選択 (Select Tenant)] オプションが表示されます。 • アプリケーション プロファイル (Application Profile) : 選択すると、[アプリケーションプロファイルの選択 (Select Application Profile)] オプションが表示されます。 • EPG : これを選択すると [EPG の選択 (Select EPG)] オプションが表示されます。 • コントラクト (Contract) : これを選択すると、[コントラクトの選択 (Select Contract)] オプションが表示されます。 • フィルタ (Filter) : これを選択すると、[フィルタの選択 (Select Filter)] オプションが表示されます。 • VRF : これを選択すると、[VRFの選択 (Select VRF)] オプションが表示されます。 • デバイス : [SelectfvcloudLBCtx] プッシュが表示されます。 • サービス グラフ : 選択すると、[Select Service Graph] オプションが表示されます。 • [クラウド コンテキスト プロファイル (Cloud Context Profile)] : これを選

[プロパティ (Properties)]	説明
	<p>択すると、[クラウドコンテキストプロファイルの選択 (Select Cloud Context Profile)]オプションが表示されます。</p> <ol style="list-style-type: none"> 2. Select <object_name> をクリックします。Select <object_name> ダイアログが表示されます。 3. Select <object_name> ダイアログから左側の列のオプションからクリックして選んで、[選択 (Select)] をクリックします。[バックアップ構成の作成 (Create Backup Configuration)] ダイアログ ボックスに戻ります。 <p>(注) [オブジェクトDN (Object DN)] フィールドには、バックアップするオブジェクトツリーのルートとして使用するオブジェクトの DN が自動的に入力されます。</p> <ul style="list-style-type: none"> • DN の入力 (Enter DN) : このオプションを選択すると、[オブジェクト DN (Object DN)] フィールドが表示されます。 <ol style="list-style-type: none"> 1. [オブジェクトDN (Object DN)] フィールドに、バックアップするオブジェクトツリーのルートとして使用する特定のオブジェクトの DN を入力します。
スケジューラ	<ol style="list-style-type: none"> 1. [スケジューラの選択 (Select Scheduler)] をクリックして [スケジューラの選択 (Select Scheduler)] ダイアログを開き、左側の列からスケジューラを選択します。 2. 終了したら、右下隅にある [選択 (Select)] ボタンをクリックします。

[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。 <ul style="list-style-type: none"> • はい (Yes) : (デフォルト) バックアップ設定の作成後にバックアップをトリガーします。 • いいえ (No) : バックアップ設定の作成後にバックアップをトリガーしません。

ステップ 5 設定が終わったら [Save] をクリックします。

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

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

始める前に

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

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

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

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

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

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

表 18: テクニカル サポートの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
エクスポート先	<p>エクスポート先を選択します。</p> <ul style="list-style-type: none"> • コントローラ • [リモート ロケーション (Remote Location)] : 選択すると、[リモート ロケーションの選択 (Select Remote Location)] オプションが表示されます。 <ol style="list-style-type: none"> 1. [リモート ロケーションの選択 (Select Remote Location)] をクリックします。[リモート ロケーションの選択 (Select Remote Location)] ダイアログボックスが表示されます。 2. [[リモート ロケーションの選択 (Select Remote Location)] ダイアログで、左側の列のリモート ロケーションをクリックして選択し、[選択 (Select)] をクリックします。[テクニカル サポートの作成 (Create Tech Support)] ダイアログボックスに戻ります。
アップグレード前のログを含める	<p>テクニカル サポート ポリシーにアップグレード前のログを含める場合は、[有効 (Enabled)] チェックボックスをオンにします。</p>
作成後のトリガー	<p>ポリシーの作成後にテクニカル サポート ポリシーを作成する場合は、[有効] (デフォルト) チェックボックスをクリックしてオンにします。無効にするには、チェックボックスをオフにします。</p>

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud Network Controller GUI を使用したスケジューラの作成

このセクションでは、ユーザーラップトップブラウザのローカル時間で、Cisco Cloud Network Controller のデフォルト UTC 時間に変換されるスケジューラを作成する方法について説明します。

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

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

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

ステップ3 [インテント (Intent)] の [操作 (Operations)] リストから、[スケジューラの作成 (Create Scheduler)] をクリックします。[スケジューラの作成 (Create Scheduler)] ダイアログボックスが表示されます。

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

表 19: スケジューラの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
繰り返しウィンドウ	<p>[繰り返しウィンドウの追加 (Add Recurring Window)] をクリックします。[繰り返しウィンドウの追加 (Add Recurring Window)] ダイアログウィンドウが表示されます。</p> <ol style="list-style-type: none"> [スケジュール (Schedule)] ドロップダウンリストから、次のいずれかを選択します。 <ul style="list-style-type: none"> • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日 [開始時間 (Start Time)] フィールドに、時間を入力します。 [最大同時タスク数 (Maximum Concurrent Tasks)] フィールド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。 [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。 終了したら、[Add] をクリックします。

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

ステップ5 設定が終わったら [Save] をクリックします。

Cisco Cloud 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 20: リモート ロケーションの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	

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

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 21: ログインドメインダイアログボックスの作成のフィールド

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

[プロパティ (Properties)]	説明
プロバイダ	<p>プロバイダーを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)]をクリックします。[プロバイダーの選択 (Select Providers)]ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. クリックしてプロバイダーを選択します。 3. [選択 (Select)] をクリックして、プロバイダを追加します。
詳細設定	<p>[認証タイプ (Authentication Type)]および [LDAP グループマッピングルール (LDAP Group Map Rules)] フィールドを表示します。</p>
認証タイプ	<p>レルムオプションにLDAPを選択した場合は、次のいずれかの認証タイプを選択します。</p> <ul style="list-style-type: none"> • Cisco AV ペア : (デフォルト) • LDAP グループマッピングルール : LDAP グループマッピングルールを追加する必要があります。

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

[プロパティ (Properties)]	説明
	<p>LDAP グループマッピングルールを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [LDAP グループ マッピング ルールの追加 (Add LDAP Group Map Rule)] をクリックします。[LDAP グループ マッピング ルールの追加 (Add LDAP Group Map Rule)] ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. [名前 (Name)] フィールドに、ルールの名前を入力します。 3. [説明 (Description)] フィールドに、ルールの説明を入力します。 4. [グループ DN (Group DN)] フィールドにルールのグループ DN を入力します。 5. セキュリティ ドメインの追加 : <ol style="list-style-type: none"> 1. [セキュリティ ドメインの追加 (Add Security Domain)] をクリックします。[セキュリティ ドメインの追加 (Add Security Domain)] ダイアログ ボックスが表示されます。 2. [セキュリティ ドメインの選択 (Select Security Domain)] をクリックします。[セキュリティ ドメインの選択 (Select Security Domain)] ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。 3. セキュリティ ドメインをクリックして選択します。 4. [選択 (Select)] をクリックして、セキュリティ ドメインを追加します。[セキュリティ ドメインの追加 (Add Security Domain)] ダイアログボックスに戻ります。 5. ユーザー ロールを追加する: <ol style="list-style-type: none"> 1. [セキュリティ ドメインの追加 (Add Security Domain)] ダイアログボックスで、[ロールの選択 (Select Role)] をクリックします。[ロールの選択 (Select Role)] ダイアログボックスが表示され、左側のペインにロールのリストが表

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

ステップ 5 設定が終わったら **[Save]** をクリックします。

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

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

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

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

[Intent] メニューに管理オプションのリストが表示されます。

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

ステップ 4 [名前 (Name)] フィールドに、セキュリティ ドメインの名前を入力します。

ステップ 5 [説明 (Description)] フィールドに、セキュリティ ドメインの説明を入力します。

ステップ 6 [制限付きドメイン (Restricted Domain)] 制御を [はい (Yes)] または [いいえ (No)] に設定します。

セキュリティドメインが制限付きドメインとして構成されている場合 ([はい (Yes)])、このドメインに割り当てられているユーザーは、他のセキュリティドメインで構成されたポリシー、プロファイル、またはユーザーを表示できません。

ステップ 7 設定が終わったら [Save] をクリックします。

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

表 22: ロールの作成ダイアログボックスのフィールド

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

[プロパティ (Properties)]	説明
特権	

[プロパティ (Properties)]	説明
	<p>クリックして、ユーザに割り当てる権限のチェックボックスをオンにします。権限は次のとおりです。</p> <ul style="list-style-type: none"> • aaa : 認証、許可、アカウントिंग、インポート/エクスポート ポリシーの設定に使用されます。 • access-connectivity-l1 インフラの下のレイヤ1設定に使用されます。例: セクタとポートレイヤ1のポリシー設定。 • access-connectivity-l2 : インフラの下のレイヤ2設定に使用されます。例: セクタおよび接続可能なエンティティ設定をカプセル化します。 • access-connectivity : インフラでのレイヤ3の設定、テナントのL3Outでのスタティックルート設定に使用されます。 • access-connectivity-mgmt : 管理インフラ ポリシーに使用されます。 • access-connectivity-util : テナント ERSPAN ポリシーに使用されます。 • access-equipment : アクセスポートの設定に使用されます。 • access-protocol-l1 : インフラのレイヤ1プロトコル設定に使用されます。 • access-protocol-l2 : インフラのレイヤ2プロトコル設定に使用されます。 • access-protocol-l3 : インフラでのレイヤ3プロトコル設定に使用されます。 • access-protocol-mgmt : NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • access-protocol-ops : クラスタ ポリシーやファームウェア ポリシーなどの操作関連のアクセスポリシーに使用されます。 • access-protocol-util : テナント ERSPAN ポリシーに使用されます。 • access-qos : CoPP および QoS に関連するポリシーの変更に使用されます。

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

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • nw-svc-device : レイヤ4からレイヤ7のサービス デバイスを管理するために使用されます。 • nw-svc-devshare : 共有レイヤ4～レイヤ7サービス デバイスの管理に使用されます。 • nw-svc-params : レイヤ4～レイヤ7のサービス ポリシーの管理に使用されます。 • nw-svc-policy : レイヤ4～レイヤ7のネットワーク サービス オーケストレーションの管理に使用されます。 • ops : アトミック カウンタ、SPAN、TSW、技術サポート、トレースルート、分析、コア ポリシーなど、ポリシーのモニタリングとトラブルシューティングを含む動作ポリシーに使用されます。 • tenant-connectivity-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
	<ul style="list-style-type: none"> • tenant-ext-connectivity-mgmt : ファームウェアポリシーの書き込みアクセスとして使用されます。 • tenant-ext-connectivity-util : traceroute、ping、oam、eprk などのデバッグ/監視/観察ポリシーに使用されます。 • tenant-ext-protocol-l1 : テナントの外部レイヤ 1 プロトコルの管理に使用されます。通常、ファームウェアポリシーの書き込みアクセスにのみ使用します。 • tenant-ext-protocol-l2 : テナントの外部レイヤ 2 プロトコルの管理に使用されます。通常、ファームウェアポリシーの書き込みアクセスにのみ使用します。 • tenant-ext-protocol-l3 : BGP、OSPF、PIM、IGMP などのテナントの外部レイヤ 3 プロトコルを管理するために使用されます。 • tenant-ext-protocol-mgmt : ファームウェアポリシーの書き込みアクセスとして使用されます。 • tenant-ext-protocol-util : traceroute、ping、oam、eprk などのデバッグ/監視/観察ポリシーに使用されます。 • tenant-network-profile : ネットワーク プロファイルの削除および作成、エンドポイントグループの削除および作成など、テナント設定の管理に使用されます。 • tenant-protocol-l1 : テナントの下でレイヤ 1 プロトコルの設定を管理するために使用されます。 • tenant-protocol-l2 : テナントの下でレイヤ 2 プロトコルの設定を管理するために使用されます。 • tenant-protocol-l3 : テナントの下でレイヤ 3 プロトコルの設定を管理するために使用されます。 • tenant-protocol-mgmt : ファームウェアポリシーの書き込みアクセスとして使用されます。

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • tenant-protocol-ops : テナント traceroute ポリシーに使用されます。 • tenant-protocol-util — traceroute、ping、oam、eprk 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 23: 証明書認証局の作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	証明書認証局の名前を入力してください。
説明	証明書認証局の説明を入力してください。
用途	次のオプションから選択します。 <ul style="list-style-type: none"> • テナント (Tenant) : 認証局が特定のテナント用かどうかを選択します。選択すると、[テナントの選択 (Select Tenant)] オプションがGUIに表示されます。 • システム (System) : 認証局がシステム用である場合に選択します。
テナントの選択	テナントを選択します。 <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログボックスが表示されます。 2. [テナントの選択 (Select Tenant)] ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)] をクリックします。[証明書認証局の作成 (Create Certificate Authority)] ダイアログボックスが表示されます。
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。 <p>(注) チェーンの証明書を次の順序で追加します。</p> <ol style="list-style-type: none"> 1. CA 2. Sub-CA 3. サブサブCA 4. サーバー

ステップ5 設定が終わったら [Save] をクリックします。

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

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

始める前に

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

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

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

[Intent]メニューに管理オプションのリストが表示されます。

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

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

表 24: キーリングの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	キーリングの名前を入力します。
説明	キーリングの説明を入力します。
用途	<ul style="list-style-type: none"> • System : キーリングはシステム用です。 • Tenant : キーリングは特定のテナント用です。テナントを指定する[テナント (Tenant)]フィールドを表示します。

[プロパティ (Properties)]	説明
テナントの選択	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)]をクリックします。[テナントの選択 (Select Tenant)]ダイアログボックスが表示されます。 2. [テナントの選択 (Select Tenant)]ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)]をクリックします。[キー リングの作成 (Create Key Ring)]ダイアログボックスに戻ります。
Settings	
認証局	<p>認証局を選択するには：</p> <ol style="list-style-type: none"> 1. [認証局の選択 (Select Certificate Authority)]をクリックします。[認証局の選択 (Select Certificate Authority)]ダイアログが表示されます。 2. 左側の列で認証局をクリックして選択します。 3. [選択 (Select)]をクリックします。[キー リングの作成 (Create Key Ring)]ダイアログボックスに戻ります。
秘密キー (Private Key)	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> • [新しいキーの生成 (Generate New Key)]：新しいキーを生成します。 • [既存のキーのインポート (Import Existing Key)]：[秘密キー (Private Key)]テキストボックスが表示され、既存のキーを使用できます。
秘密キー (Private Key)	<p>[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)。</p>

[プロパティ (Properties)]	説明
Modulus	[モジュール (Modulus)] ドロップダウン リストをクリックし、次の項目の中から選択します。 <ul style="list-style-type: none"> • 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 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 25: ローカルユーザーの作成ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	ローカルユーザーのユーザー名を入力します。
Password	ローカルユーザーのパスワードを入力します。
Confirm Password	ローカルユーザーのパスワードを再入力します。
説明	ローカルユーザーの説明を入力します。
Settings	

[プロパティ (Properties)]	説明
アカウント ステータス	アカウントステータスを選択するには、次の手順を実行します。 <ul style="list-style-type: none">• Active : ローカル ユーザー アカウントをアクティブにします。• Inactive : ローカル ユーザー アカウントを非アクティブにします。
[名 (First Name)]	ローカル ユーザーの名を入力します。
姓 (Last Name)	ローカル ユーザーの姓を入力します。
電子メール アドレス (Email Address)	ローカル ユーザーの E メール アドレスを入力します。
Phone Number	ローカル ユーザーの 電話番号を入力します。

[プロパティ (Properties)]	説明
セキュリティドメイン	

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

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

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

表 26: ローカル ユーザーの作成ダイアログボックスのフィールド：高度な設定

プロパティ	説明
Account Expires	[はい (Yes)]を選択すると、アカウントは選択した時点で期限切れになるように設定されます。
パスワードの更新が必要です	[はい (Yes)]を選択した場合、ユーザーは次回ログイン時にパスワードを変更する必要があります。
OTP	ユーザーのワンタイムパスワード機能を有効にするには、チェックボックスをオンにします。
ユーザー証明書	<p>ユーザー証明書を追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [X509 証明書の追加 (Add X509 Certificate)]をクリックします。[X509 証明書の追加 (Add X509 Certificate)]ダイアログボックスが表示されます。 [Name] フィールドに名前を入力します。 [ユーザー X509 証明書 (User X509 Certificate)]テキストボックスに X509 証明書を入力します。 [Add] をクリックします。[ユーザー X509 証明書の X509 証明書]ダイアログボックスが閉じます。[ローカル ユーザー]ダイアログボックスに戻ります。

プロパティ	説明
SSH キー	<p>SSH キーを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [SSH キーを追加 (Add SSG Key)] をクリックします。[SSH キーの追加 (Add SSG Key)] ダイアログボックスが表示されます。 2. [Name] フィールドに名前を入力します。 3. [キー (Key)] テキストボックスに SSH キーを入力します。 4. [Add] をクリックします。[SSH キーの追加 (Add SSG Key)] ダイアログボックスが閉じます。[ローカル ユーザー] ダイアログボックスに戻ります。

ステップ 6 設定が終わったら **[Save]** をクリックします。

Cisco Cloud 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（52 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 **[スマートライセンス (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)]** で、**[構成の編集 (Edit Configuration)]** をクリックします。**[セットアップ - リージョン管理]** ダイアログボックスが表示されます。**セットアップ - リージョン管理** の一連のステップの最初のステップ、**管理するリージョン**が表示され、**管理対象リージョン**のリストが表示されます。

ステップ 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 ~ 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。
- CCR では、サイト間通信のためにパブリック IP アドレスが必要であることに注意してください。
- 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。
- (注) CCR アドレスをパブリック IP アドレスからプライベート IP アドレスに (またはその逆に) 変更すると、中断が発生し、トラフィックが失われる可能性があります。
- 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数を選択するには、[リージョンごとのルータ数 (Number of Routers Per Region)] ドロップダウン リストをクリックし、[2]、[3]、または [4]、[6]、または [8] をクリックします。
- ステップ 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。

(注) Azure クラウドサイトに接続する場合は、CCR のユーザ名として `admin` を使用しないでください。

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、[Cisco Catalyst 8000V について \(26 ページ\)](#) を参照してください。

ステップ 15 必要に応じて、[TCP MSS] フィールドに必要な情報を入力します。

[TCP MSS] オプションを使用すれば TCP 最大セグメントサイズ (MSS) を構成できます。この値は、クラウドへの VPN トンネルとオンプレミス サイトまたは他のクラウドサイトへの外部トンネルを含む、すべてのクラウド ルータ トンネル インターフェイスに適用されます。クラウドへの VPN トンネルの場合、クラウド プロバイダーの MSS 値がこのフィールドに入力した値よりも小さい場合は、低い方の値が使用されます。それ以外の場合は、このフィールドに入力した値が使用されます。

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

ステップ 16 (オプション) ライセンス トークンを指定するには、[ライセンス トークン] テキスト ボックスに製品インスタンスの登録 トークンを入力します。

(注)

- Cisco Catalyst 8000V のライセンス情報については、[Cisco Catalyst 8000V について \(26 ページ\)](#) を参照してください。

- トークンが入力されていない場合、CCR は EVAL モードになります。

- プライベート IP アドレスを [ステップ 10 \(160 ページ\)](#) の CCR に割り当てた場合、プライベート IP アドレスを使用して CCR のスマート ライセンスを登録するときに、**Cisco Smart Software Manager (CSSM)** に直接接続できます ([管理 (Administrative)] > [スマート ライセンス (Smart Licensing)] に移動して使用可能)。この場合、エクスプレ スルート経由で CSSM に到達可能性を提供する必要があります。

ステップ 17 [次へ (Next)] をクリックします。

- これらの手順の前半で [サイト間接続] 領域の [有効] ボックスにチェック マークを付けた場合、**サイト間接続**は、**セットアップ - リージョン管理**の一連のステップの次のステップとして表示されます。[ステップ 18 \(162 ページ\)](#) に進みます。

- これらの手順の前半で [サイト間接続 (Inter-Site Connectivity)] エリアの [有効 (Enabled)] ボックスにチェック マークを付けなかった場合、[クラウド リソース命名規則 (Cloud Resource Naming Rules)] は、[セットアップ - リージョン管理 (Setup - Region Management)] の一連の手順の次の手順として表示されます。[ステップ 22 \(162 ページ\)](#) に進みます。

- ステップ 18** テキストボックスにオンプレミスの IPsec トンネル ピアのピアパブリック IP アドレスを入力するには、**[IPsec トンネル ピアのパブリック IP を追加]** をクリックします。
- ステップ 19** **[エリア ID]** フィールドに OSPF エリア ID を入力します。
- ステップ 20** 外部サブネットプールを追加するには、**[外部サブネットの追加]** をクリックし、テキストボックスにサブネットプールを入力します。
- ステップ 21** すべての接続オプションを設定したら、ページの下部にある**[次へ (Next)]** をクリックします。
[クラウドリソース 命名規則 (Cloud Resource Naming Rules)] ページが表示されます。
- ステップ 22** **[クラウドリソースの命名規則 (Cloud Resource Naming Rules)]** ページで、必要に応じてクラウドリソースの命名規則を構成します。
クラウドリソースの命名規則については、[クラウドリソースの命名 \(163 ページ\)](#) セクションで詳しく説明します。命名規則を変更する必要がない場合は、このページをスキップできます。
- ステップ 23** 終了したら **[Save and Continue (保存して続行)]** ボタンをクリックします。

スマート ライセンスの設定

このタスクでは、Cisco Cloud ネットワーク コントローラでスマート ライセンスを設定する方法を示します。

始める前に

製品インスタンス登録トークンが必要です。

- ステップ 1** インテント アイコンをクリックします。**[インテント (Intent)]** メニューが表示されます。
- ステップ 2** 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、**[クラウドネットワーク コントローラの設定 (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 サーバー (DNS 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** Cisco Cloud Network Controller を Cisco の統合ライセンス管理システムに登録するには、**[スマート ライセンス (Smart Licensing)]** から、**[登録 (Register)]** をクリックします。**[スマート ライセンス (Smart Licensing)]** ダイアログが表示されます。
- ステップ 4** トランスポート設定を選択してください。
- **Cisco Smart Software Manager (CSSM)** に直接接続する
 - トランスポートゲートウェイ/Smart Software Manager サテライト
 - **HTTP/HTTPS プロキシ (HTTP/HTTPS Proxy)**
- (注) **HTTP/HTTPS プロキシ** を選択するときは、IP アドレスが必要です。

ステップ5 指定されたテキスト ボックスで製品インスタンス登録トークンを入力します。

ステップ6 完了したら [登録 (Register)] をクリックします。

クラウドリソースの命名

Cisco Cloud Network Controller でグローバルネーミングポリシーを作成できます。これにより、Cisco Cloud Network Controller から Azure クラウドに展開されたすべてのオブジェクトのカスタムクラウドリソース命名規則を定義できます。Cisco Cloud ネットワーク コントローラ ARM テンプレートの導入に使用される情報技術 グループ名を除き、Cisco Cloud ネットワーク コントローラの初回セットアップ ウィザードで、すべてのクラウドリソースのカスタム命名ルールを定義できます。テンプレートのリソースグループ名は、最初に展開したときに定義され、その後は変更できません。グローバル ポリシーに加えて、REST API を使用して各 Cisco Cloud Network Controller オブジェクトから作成されたクラウドリソースの名前を明示的に定義することもできます。

Cisco Cloud Network Controller リリース 5.1 (2) 以降、レイヤ 4–レイヤ 7 サービスの導入では、ネットワークロードバランサ、アプリケーションロードバランサ、デバイスアプリケーションセキュリティグループなどのクラウドリソースにカスタム名を指定できます。



- (注) カスタム ネーミング ポリシーを使用しても、クラウドリソースが作成されると、名前を変更できないことに注意してください。既存のクラウドリソースの名前を変更する場合は、構成したすべてのクラウドリソースを削除して再作成する必要があります。削除されるクラウドリソースには、セカンダリ CIDR とサブネット、Cisco Cloud Network Controller によって展開された CCR が含まれ、したがって、CCR からすべてのリモートサイトへの IPSec トンネルが含まれます。

命名ルールに使用できる変数

クラウドリソースの命名ポリシーを作成する場合、次の変数を使用して、Cisco Cloud Network Controller オブジェクトに基づいてクラウドリソースの名前を動的に定義できます。

- `{tenant}` –リソースにはテナントの名前が含まれます
- `{ctx}` –リソースにはVRFの名前が含まれます。
- `{ctxprofile}` : リソースにはクラウドコンテキストプロファイルが含まれます。これは、特定のクラウド領域に導入されたVRFです。
- `{subnet}` : リソースには文字列subnetの後にサブネットIPアドレスが含まれます。
- `{app}` : リソースにはアプリケーションプロファイルの名前が含まれます。
- `{epg}` : リソースにはEPGの名前が含まれます。
- `{contract}` –リソースには契約の名前が含まれます

- `{region}` - リソースにはクラウドリージョンの名前が含まれます。
- `{priority}` : リソースにはネットワークセキュリティグループ (NSG) ルールの優先度が含まれます。この番号は、各NSGルール名が一意になるように自動的に割り当てられます。
- `{serviceType}` : リソースにはサービスタイプの省略形が含まれます (プライベートエンドポイントリソースにのみ有効)。
- `{resourceName}` : リソースにはターゲットリソースの名前が含まれます (プライベートエンドポイントリソースにのみ有効)。
- `{device}` : リソースにはレイヤ4-レイヤ7デバイスの名前が含まれます。
- `{interface}` : リソースには、レイヤ4-レイヤ7のデバイスインターフェイスの名前が含まれます。
- `{deviceInterfaceDn}` : リソースには、レイヤ7デバイスインターフェイスのDNが含まれます。

プライベートエンドポイントの場合、`{app}-{svcepg}-{subnet}-{serviceType}-{resourceName}`の組み合わせにより、プライベートエンドポイント名が一意になります。これらの変数のいずれかを削除すると、すでに存在するプライベートエンドポイントの名前になる場合があります。これにより、Cisco Cloud ネットワーク コントローラは障害を発生させます。また、最大長の要件はAzureサービスによって異なります。

1つ以上の上記の変数を使用してグローバル名前付けポリシーを定義すると、Cisco Cloud Network Controller はすべての必須変数が存在し、無効な文字列が指定されていないことを確認するために文字列を検証します。

Azureには名前前の最大長の制限があります。名前前の長さがクラウドプロバイダーでサポートされている長さを超えると、構成が拒否され、Cisco Cloud Network Controller リソースの作成に失敗したというエラーが発生します。その後、障害の詳細を確認し、命名規則を修正できます。Cisco Cloud ネットワーク コントローラ リリース5.0 (2) の時点での最大長の制限を以下に示します。最新の最新情報および長さ制限の変更については、Azure のドキュメントを参照してください。

次の表に、上記の各命名変数をサポートするクラウドリソースの概要を示します。アスタリスク (*) で示されたセルは、そのタイプのクラウドリソースに必須の変数を示します。プラス記号 (+) で示されるセルは、これらの変数の少なくとも1つがそのタイプのクラウドリソースに必須であることを示します。たとえば、VNETリソースの場合、`{ctx}`、`{ctxprofile}`、またはその両方を指定できます。

表 27:クラウドリソースでサポートされる変数

Azure のリソース	<code>\${tenant}</code>	<code>\${ctx}</code>	<code>\${ctxprofile}</code>	<code>\${subnet}</code>	<code>\${app}</code>	<code>\${epg}</code>	<code>\${contract}</code>	<code>\${region}</code>	<code>\${priority}</code>
リソースグループ 最長：90	対応*	対応*	Yes+					対応*	
仮想ネットワーク (VNET) 最長：64	対応	はい+	Yes+					対応	
Subnet 最長：80	はい	はい	はい	対応*				○	
アプリケーションセキュリティグループ (ASG) 最長：80	はい				対応*	対応*		○	
ネットワークセキュリティグループ (NSG) 最長：80	はい				対応*	対応*		○	
ネットワークセキュリティグループルール 最長：80	はい						はい		Yes* (自動)

表 28: クラウドリソースでサポートされる変数 (レイヤ4~レイヤ7デバイスサービス)

Azure のリソース	\${tenant}	\${region}	\${ctxprofile}	\${device}	\${interface}	\${deviceInterfaceID}
インターネットネットワークロードバランサ 最長: 80	はい	はい	はい	対応*		
インターネット側のネットワークロードバランサ 最長: 80	はい	はい	はい	対応*		
インターネットアプリケーションロードバランサ 最長: 80	はい	はい	はい	対応*		
インターネット向け Application Load Balancer 最長: 80	はい	はい	はい	対応*		
デバイス ASG 最長: 80	はい	はい		対応*	対応*	対応*

命名ルールのガイドラインと制限事項

クラウドリソースの命名にカスタムルールを設定する場合、次の制限が適用されます。

- Cisco Cloud Network Controller の初回セットアップ時に、次の2つの命名ルールセットを使用して、グローバル命名ポリシーを定義します。
 - [ハブ リソース命名規則 (Hub Resource Naming Rules)] は、インフラ テナントのハブ リソースグループ、ハブ VNET、オーバーレイ 1 CIDR、セカンダリ 2 CIDR サブネットの名前、およびインフラテナントのシステムによって自動的に作成されるサブネットのサブネットプレフィックスを定義します。
 - クラウドリソース名前付けルールは、ネットワークセキュリティグループ (NSG)、アプリケーションセキュリティグループ (ASG)、ネットワークロードバランサ、アプリケーションロードバランサ、デバイスアプリケーションセキュリティグループ、

およびインフラテナントで作成するサブネットの名前と名前を定義します。ユーザテナント内のすべてのリソース（リソースグループ、仮想ネットワーク、サブネット、NSG、ASG、ネットワークロードバランサ、アプリケーションロードバランサ）。

命名規則を定義したら、それらを確認して確認する必要があります。クラウドリソースを展開する前に、命名規則を確認する必要があることに注意してください。

- クラウドリソースが作成されると、その名前は変更できず、GUIで命名ポリシーを更新できません。Cisco Cloud Network Controller をリリース5.0(2) にアップグレードしたときに、一部のリソースがすでにAzureに導入されていた場合は、グローバルカスタム命名ルールを変更することもできません。

既存のクラウドリソースまたはポリシーの名前を変更する場合は、GUIでグローバル名前付けポリシーを更新する前に、展開されたリソースを削除する必要があります。

このような場合、REST APIを使用して、作成する新しいリソースにカスタム名を明示的に割り当てることができます。

- REST APIを使用してクラウドリソースの命名を更新する場合は、同時に設定をインポートしないことを推奨します。

最初に命名規則を定義することをお勧めします。それからテナント設定も行ってください。

テナント設定の展開後は、命名ポリシーを変更しないことをお勧めします。

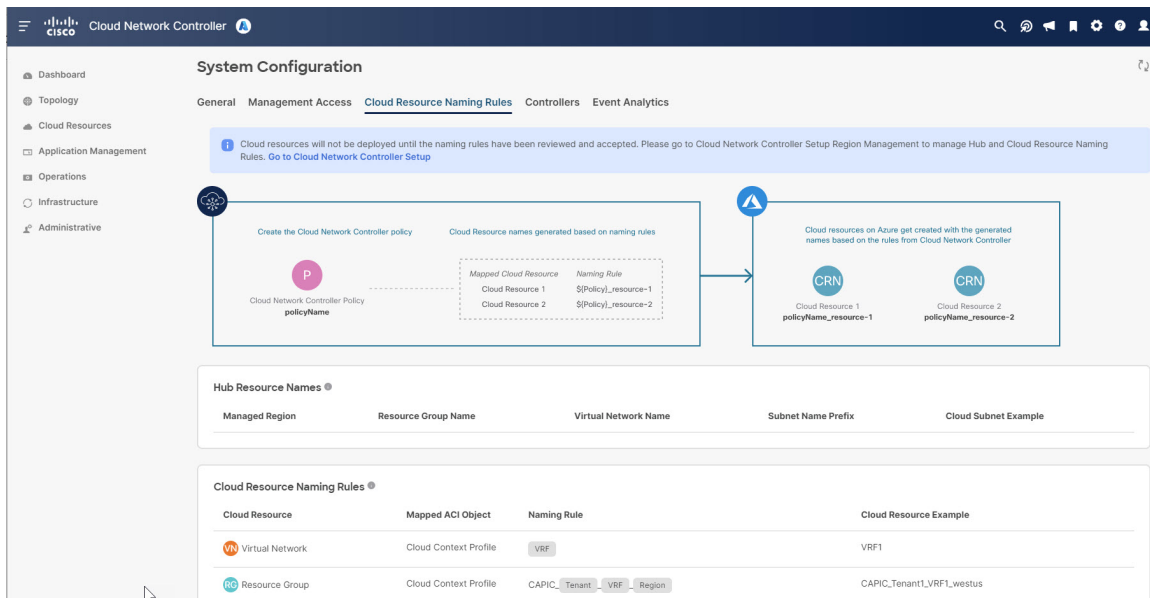
クラウドリソースの命名規則の表示

最初に、Cisco クラウドネットワークコントローラを展開するときに、初回セットアップウィザードのリージョン管理部分でクラウド情報技術の命名規則を定義します。これについては、[Cisco クラウドネットワークコントローラ設置ガイド (Cisco Cloud Network Controller Installation Guide)] で説明されています。初期セットアップの後、このセクションで説明されているように、Cisco Cloud Network Controller GUI の [システム構成 (System Configuration)] 画面で構成した規則を表示できます。

この画面の情報は読み取り専用ビューで表示されます。最初の展開後に規則を変更する場合は、最初のセットアップウィザードを再実行する必要があります。

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

ステップ 2 [クラウドリソースの命名規則 (Cloud Resource Naming Rules)] 画面に移動します。



- [ナビゲーション (Navigation)] サイドバーで、[インフラストラクチャ (Infrastructure)] カテゴリを展開します。
- [インフラストラクチャ (Infrastructure)] カテゴリから、[システム構成 (System Configuration)] を選択します。
- [システム構成 (System Configuration)] 画面で、[クラウドリソースの命名規則 (Cloud Resource Naming Rules)] タブを選択します。

[クラウド情報技術の命名規則 (Cloud Resource Naming Rules)] タブでは、Cisco クラウドネットワークコントローラからクラウドサイトに展開するリソースの名前に対して現在構成されている規則の概要を確認できます。

以前にカスタム命名規則を構成していない場合は、クラウドリソースの Cisco Cloud Network Controller オブジェクト名を使用するデフォルトの規則がここにリストされます。

最初のセットアップ時に定義した命名規則を受け入れなかった場合は、画面の上部に警告バナーが表示されます。

(注) クラウドリソースを展開する前に、命名規則を確認する必要があることに注意してください。

REST API を使用した Cisco Cloud Network Controller の構成

REST API を使用したテナントの作成

サブスクリプションには次の2つのタイプがあります：独自および共有。各サブスクリプションタイプにはプライマリ テナントがあります。新しい管理対象テナントまたは非管理対象テ

テナントを作成するときに、独自のサブスクリプションを選択します。既存のプライマリテナントの管理対象または管理対象外の設定を継承するテナントを作成するときに、共有サブスクリプションを選択します。このセクションでは、独自のタイプのサブスクリプションを使用して管理対象テナントと非管理対象テナントを作成する方法と、共有サブスクリプションを作成する方法を示します。

このセクションでは、Postmanの本文からのサンプルPOST要求を使用して、REST APIを使用してテナントを作成する方法を示します。

ステップ1 独自サブスクリプションの作成。

- a) クライアントシークレットを使用して非管理対象テナントを作成するには：

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

<fvTenant name="{{primary-tenant-name}}">
  <cloudAccount id="{{user-tenant-subscription-id}}" vendor="azure" accessType="credentials"
    status="">
    <cloudRsCredentials tDn="uni/tn-{{primary-tenant-name}}/credentials-{{primary-tenant-name}}"/>
  </cloudAccount>
  <cloudCredentials name="{{primary-tenant-name}}" keyId="{{application_key_id}}"
    key="{{client_secret_key}}">
    <cloudRsAD tDn="uni/tn-{{primary-tenant-name}}/ad-{{active_directory_id}}"/>
  </cloudCredentials>
  <cloudAD name="{{active_directory_name}}" id="{{active_directory_id}}"/>
  <fvRsCloudAccount tDn="uni/tn-{{primary-tenant-name}}/act-[[user-tenant-subscription-id]]-vendor-azure" status="">
</fvTenant>
```

- b) 管理対象テナントを作成するには：

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

<fvTenant name="{{primary-tenant-name}}">
  <cloudAccount id="{{user-tenant-subscription-id}}" vendor="azure" accessType="managed"
    status="" />
  <fvRsCloudAccount tDn="uni/tn-{{primary-tenant-name}}/act-[[user-tenant-subscription-id]]-vendor-azure" status="">
</fvTenant>
```

ステップ2 共有サブスクリプションの作成：

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

<fvTenant name="{{primary-tenant-name}}">
  <fvRsCloudAccount tDn="uni/tn-{{primary-tenant-name}}/act-[[user-tenant-subscription-id]]-vendor-azure" status="">
</fvTenant>
```

REST API を使用したコントラクトの作成

この例では、REST API を使用して Cisco Cloud 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。

ステップ 1 基本的なクラウド コンテキスト プロファイルを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <cloudCtxProfile name="cProfilewestus151">
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
      <cloudRsToCtx tnFvCtxName="ctx151"/>
      <cloudCidr addr="15.151.0.0/16" primary="true" status="">
        <cloudSubnet ip="15.151.1.0/24" name="GatewaySubnet" usage="gateway">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>
```

```

        <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
    </cloudCidr>
</cloudCtxProfile>
</fvTenant>
</polUni>

```

ステップ 2 VNet のセカンダリ VRF、CIDR、およびサブネットを追加するクラウドコンテキストプロファイルを作成するには、次の手順を実行します。

例：

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tenant1" status="">
        <fvCtx name="VRF1" />
        <fvCtx name="VRF2" />
        <cloudCtxProfile name="vpcl" status="">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-centralus" status=""/>

            <cloudRsToCtx tnFvCtxName="VRF1" />
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
            <cloudCidr name="cidr1" addr="192.0.2.0/16" primary="yes" status="">
                <cloudSubnet ip="192.0.3.0/24" usage="gateway" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-centralus/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr name="cidr1" addr="193.0.2.0/16" primary="no" status="">
                <cloudSubnet ip="193.0.3.0/24" usage="" status="">
                    <cloudRsSubnetToCtx tnFvCtxName="VRF2"/>
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-centralus/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
</polUni>

```

REST API を使用したクラウドリージョンの管理

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

クラウドリージョンを作成するには:

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <cloudDomP name="default">
        <cloudProvP vendor="azure">
            <cloudRegion adminSt="managed" name="eastus"><cloudZone name="default"/></cloudRegion>
            <cloudRegion adminSt="managed" name="eastus2"><cloudZone name="default"/></cloudRegion>
            <cloudRegion adminSt="managed" name="westus"><cloudZone name="default"/></cloudRegion>
        </cloudProvP>
    </cloudDomP>
</polUni>

```

```
</cloudDomP>
</polUni>
```

REST API を使用したフィルタの作成

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

フィルタを作成するには、次の手順を実行します。

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="t15">
    <vzFilter name="rule1">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
      <vzEntry etherT="ip" prot="unspecified" name="any"/>
    </vzFilter>
    <vzFilter name="rule2">
      <vzEntry etherT="ip" dToPort="http" prot="tcp" dFromPort="http" name="http"/>
    </vzFilter>
    <vzFilter name="rule3">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
    </vzFilter>
    <vzFilter name='all_rule'>
      <vzEntry etherT="ip" prot="unspecified" name="any"/>
    </vzFilter>

    <vzBrCP name="c1">
      <vzSubj name="c1">
        <vzRsSubjFiltAtt tnVzFilterName="rule2"/>
        <vzRsSubjGraphAtt tnVnsAbsGraphName="c13_g1"/>
        <vzRsSubjFiltAtt tnVzFilterName="rule3"/>
        <vzRsSubjFiltAtt tnVzFilterName="all_rule"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

REST API を使用したアプリケーション プロファイルの作成

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

始める前に

テナントを作成します。

アプリケーション プロファイルを作成する方法 :

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />

    <fvCtx name="ctx151"/>

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

</cloudApp>

  </fvTenant>
</polUni>
```

REST API を使用したネットワーク セキュリティ グループの構成

この例は、REST API を使用して、Cisco Cloud Network Controller の新しいサブネットごとの NSG 構成を設定する方法を示しています。

始める前に

[セキュリティ グループ \(43 ページ\)](#) に記載の情報について、確認してください。

Cisco Cloud Network Controller のサブネットごとの NSG 構成を設定するには、次の手順を実行します。

例 :

```
<polUni>
  <cloudDomP status="">
    <cloudProvP vendor="azure">
      <cloudProvResPolCont><cloudProvSGForSubnetP enableSGForSubnet="true"
status=""/></cloudProvResPolCont>
    </cloudProvP>
  </cloudDomP>
</polUni>
```

REST API を使用した EPG の作成

このセクションの手順を使用して、REST API を使用したアプリケーション EPG、外部 EPG、サービス EPG を作成します。

REST API を使用したクラウド EPG の作成

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

始める前に

アプリケーション プロファイルと VRF を作成します。

クラウド EPG を作成するには、次の手順を実行します。

例 :

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />

    <fvCtx name="ctx151"/>

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

      <cloudEPg name="epg1">
        <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
        <cloudEPSelector matchExpression="custom:tag1=='value1'" name="selector-1"/>
      </cloudEPg>

    </cloudApp>

  </fvTenant>
</polUni>
```

REST API を使用した外部クラウド EPG の作成

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

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 外部クラウド EPG を作成するには、次の手順を実行します。

例 :

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
    <fvCtx name="ctx151"/>
```

```

<cloudVpnGwPol name="VgwPol1"/>
<cloudApp name="a1">
<cloudExtEPg routeReachability="internet" name="extEpg-1">
  <fvRsCons tnVzBrCPName="extEpg-1"/>
  <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
  <cloudExtEPSelector name="extSelector1" subnet="0.0.0.0/0"/>
</cloudExtEPg>
</cloudApp>
</fvTenant>
</polUni>

```

ステップ 2 タイプ **site-external** で外部クラウド EPG を作成するには :

例 :

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="infra">
    <cloudApp name="a1">
      <cloudExtEPg routeReachability="site-ext" name="extEpg-1">
        <fvRsCons tnVzBrCPName="extEpg-1"/>
        <cloudRsCloudEPgCtx tnFvCtxName="overlay-2"/>
        <cloudExtEPSelector name="extSelector1" subnet="10.100.0.0/16"/>
      </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>

```

REST API を使用したサービス EPG の作成

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

始める前に

- [クラウドサービスエンドポイントグループ \(35 ページ\)](#) の情報を確認してください。
- アプリケーションプロファイルと VRF を作成します。

ステップ 1 クラウドネイティブの展開タイプでサービス EPG を作成するには、次の手順を実行します。

例 :

```

<cloudSvcEPg name="Storage" type="Azure-Storage" accessType="Private" deploymentType="CloudNative">
  <cloudPrivateLinkLabel name="ProductionSubnets"/>
  <cloudRsCloudEPgCtx tnFvCtxName="HUB-SERVICES-VRF"/>
  <cloudSvcEPSelector matchExpression="ResourceName=='StorageAcct1'" name="selector-1"/>
  <cloudSvcEPSelector matchExpression="custom:Tag=='ProdStorage'" name="selector-2"/>
</cloudSvcEPg>

```

ステップ 2 クラウドネイティブ管理対象の展開タイプでサービス EPG を作成するには、次の手順を実行します。

例 :

```

<cloudSvcEPg name="APIM" type="Azure-ApiManagement" accessType="Private"

```

```

deploymentType="CloudNativeManaged" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="infra-SvcCtx" />
  <fvRsCons tnVzBrCPName="infra-APIM-Mock"/>
  <fvRsProv tnVzBrCPName="infra-managedAPIM" status=""/>
  <cloudSvcEPSelector matchExpression="IP=='10.21.52.0/28'" name="sel1" status=""/>
</cloudSvcEPg>

```

ステップ 3 サードパーティの展開タイプでサービス EPG を作成するには：

例：

```

<cloudSvcEPg name="SaaS-Hub" type="Custom" accessType="Private" deploymentType="Third-party"
status="">
  <cloudRsCloudEPgCtx tnFvCtxName="infra-SvcCtx" status=""/>
  <cloudSvcEPSelector
matchExpression="URL=='saassvcpg.286b0377-a9b7-40d7-a94f-67abe03ce5f4.centralus.azure.privatelinkservice'"
name="s1" status=""/>
  <cloudPrivateLinkLabel name="saas-hub" status=""/>
  <fvRsProv tnVzBrCPName="SaaS-Hub" status=""/>
</cloudSvcEPg>

```

REST API を使用したクラウド テンプレートの作成

このセクションでは、REST API を使用してクラウドテンプレートを作成する方法を示します。クラウドテンプレートの詳細については、[クラウドテンプレートの概要 \(52 ページ\)](#) 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。

始める前に

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

```

<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2" numRoutersPerRegion="2"
status="" vrfName="overlay-1">
      <cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="250M" routerLicenseToken="thisismysrtoken" />
      </cloudtemplateProfile>
      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
    </cloudtemplateInfraNetwork>
    <cloudtemplateIntNetwork name="default">
      <cloudRegionName provider="azure" region="westus"/>
      <cloudRegionName provider="azure" region="westus2"/>
    </cloudtemplateIntNetwork>
  </fvTenant>
</polUni>

```

```

<cloudtemplateExtNetwork name="default">
  <cloudRegionName provider="azure" region="westus2"/>

  <cloudtemplateVpnNetwork name="default">

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

    <cloudtemplateOspf area="0.0.0.1"/>

  </cloudtemplateVpnNetwork>

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

```

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

```

<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2" numRoutersPerRegion="2"
status="" vrfName="overlay-1">
      <cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="PAYG" vmType="DS2V2" />
      </cloudtemplateProfile>
      <cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="250M" routerLicenseToken="thisismycsrtoken" />
      </cloudtemplateProfile>
      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="westus"/>
        <cloudRegionName provider="azure" region="westus2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="azure" region="westus2"/>

        <cloudtemplateVpnNetwork name="default">

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

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

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

```

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

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

Azure 上の VmName	メモリー	vCPU の数	NetworkBw
DS3V2	14GiB	4	最大 3 ギガビット
DS4V2	28GiB	8	最大 6 ギガビット
F16SV2	32GiB	16	最大 12.5 ギガビット
F32SV2	64GiB	32	最大 16 ギガビット

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 \(9 ページ\)](#) 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一リークします。

```

<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 \(11 ページ\)](#) 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>

```

```

    </cloudtemplateVpnNetwork>
  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>

```

グローバルクラウドリソースの命名規則の定義または特定のオブジェクトの名前のオーバーライド

このセクションでは、クラウドリソースに名前を付けるためのグローバルポリシーを構成したり、特定のクラウドリソースの名前をオーバーライドしたりするために使用できる REST API POST の例を示します。



- (注) カスタム命名規則を確実にサポートできるようにするために、クラウドリソース名をオブジェクトごとに定義できます。これらの明示的な名前のオーバーライドは Cloud Network Controller GUI では使用できず、REST API を使用してのみ実行できます。名前を定義するには、グローバルクラウドリソースの名前付けポリシーを使用することをお勧めします。明示的な名前のオーバーライドは、グローバルな名前付けポリシーを使用して名前付け要件を満たすことができない場合にのみ使用する必要があります。

ステップ1 ハブリソースの命名規則を作成するには：

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2"
      numRoutersPerRegion="2" status="" vrfName="overlay-1">
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="west's" status="">
          <cloudtemplateRegionNameCustomization ctxProfileName="infra-vnet"
            resourceGroupName="infra-rh" subnetNamePrefix="snet-" />
        </cloudRegionName>
      </cloudtemplateIntNetwork>
    </cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>

```

ステップ2 クラウドリソースの命名規則を作成するには：

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <cloudDomP name="default">
    <cloudNaming
      azResourceGroup="{tenant}-network-{$ctx}-{$region}-rg"
      azVirtualNetwork="{tenant}-{$ctxprofile}-vnet"
      azSubnet="{tenant}-{$ctxprofile}-snet-{$subnet}"
      azNetworkSecurityGroup="{app}-{$epg}-nsg"
      azApplicationSecurityGroup="{app}-{$epg}-asg"
      azNetworkSecurityGroupRule="{contract}--{$priority}"
      internetApplicationBalancer="agw-e-{$device}"
    </cloudNaming>
  </cloudDomP>

```



```

    internalApplicationBalancer="agw-i-{$device}"
    internetNetworkBalancer="lbe-{$device}"
    internalNetworkBalancer="lbi-{$device}"
    l4L7DeviceApplicationSecurityGroup="{$deviceInterfaceDn}"
    reviewed="yes" />
  </cloudDomP>
</polUni>

```

ステップ 3 特定の Cisco Cloud Network Controller オブジェクトに対応する Azure クラウドリソース名をオーバーライドするには:

API を使用してカスタム名を指定するときに、同じ変数 (たとえば、`{$tenant}`) を使用できます。

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<fvTenant name="ExampleCorp" status="">
  <fvRsCloudAccount status="" tDn="uni/tn-infra/act-[<infra-subscription>]-vendor-azure"/>
  <fvCtx name="VRF1"/>
  <cloudApp name="App1">
    <cloudEPg name="Db" azNetworkSecurityGroup="db-nsg" azApplicationSecurityGroup="db-asg-{$region}">
      <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
      <cloudEPSelector matchExpression="custom:EPG=='db'" name="100"/>
    </cloudEPg>
  </cloudApp>
  <cloudCtxProfile name="c02" azResourceGroup="custom-tc-rg1" azVirtualNetwork="vnet1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
    <cloudRsToCtx tnFvCtxName="VRF1"/>
    <cloudCidr addr="10.20.20.0/24" name="cidr1" primary="yes" status="">
      <cloudSubnet ip="10.20.20.0/24" name="subnet1" azSubnet="s1" status="">
        <cloudRsZoneAttach status="" tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
      </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>
</fvTenant>

```

ステップ 4 特定の Cloud Network Controller オブジェクトに対応するレイヤ 4 からレイヤ 7 の Azure クラウドリソース名をオーバーライドするには:

API を使用してカスタム名を指定するときに、同じ変数 (たとえば、`{$tenant}`) を使用できます。

ロードバランサのポリシーを上書きします。

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<fvTenant>
  <cloudLB name="ALB" type="application" scheme="internet" size="small" instanceCount="2" status=""
    nativeLBName="ALB" >
    <cloudRsLDevToCloudSubnet
tDn="uni/tn-{$tenantName}/ctxprofile-cl/cidr-[31.10.0.0/16]/subnet-[31.10.80.0/24]" status="" />
  </cloudLB>
</fvTenant>

```

デバイス ASG のオーバーライドポリシー:

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<fvTenant>
  <cloudLDev name="{FWName}" status="" l4L7DeviceApplicationSecurityGroup="Group1" >
    <cloudRsLDevToCtx tDn="uni/tn-{$tenantName}/ctx-VRF1" status="" />
  </cloudLDev>

```

■ グローバルクラウドリソースの命名規則の定義または特定のオブジェクトの名前のオーバーライド

```
</cloudLDev>  
<fvTenant>
```



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 (183 ページ)
- アプリケーション管理詳細の表示 (187 ページ)
- クラウドリソースの詳細の表示 (188 ページ)
- 操作の詳細の表示 (190 ページ)
- インフラストラクチャの詳細の表示 (193 ページ)
- 管理の詳細の表示 (193 ページ)
- Cisco Cloud Network Controller GUI を使用したヘルス詳細の表示 (196 ページ)

VM ホスト メトリックのモニタリング

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

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

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

注意事項と制約事項

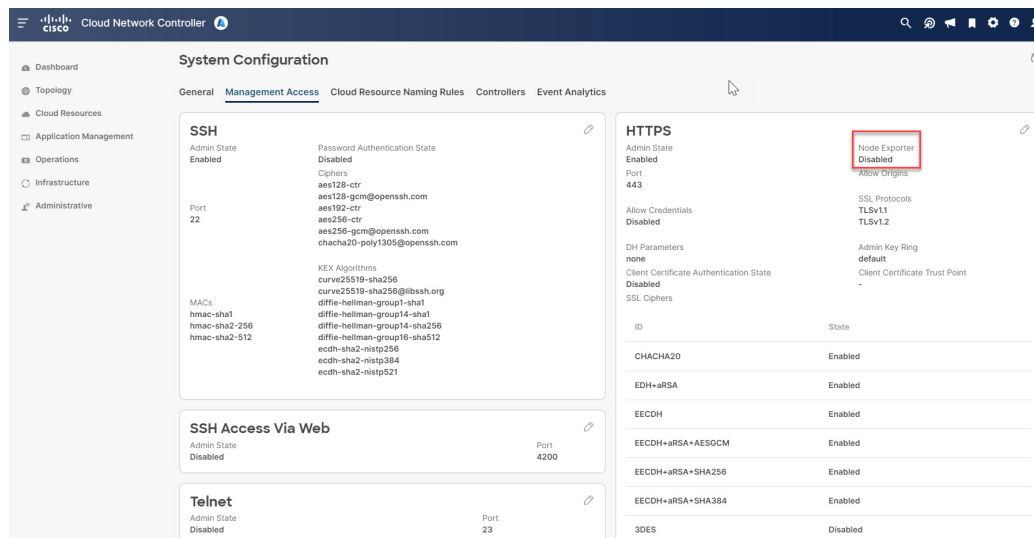
HTTP は、Prometheus Node Exporter を使用したモニタリングメトリックではサポートされていません。Prometheus Node Exporter を使用したメトリックのモニタリングでは、HTTPS のみがサポートされます。

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。

HTTPS Settings

Admin State
 Enable

Node Exporter
 Enable

Port
443

Allow Origins

Allow Credentials
 Enable

SSL Protocols
 TLSv1 TLSv1.1 TLSv1.2

DH Parameter
None

Admin Key Ring
default

Client Certificate Authentication State
 Enable

Client Certificate Trust Point
[Select Client Certificate Trust Point](#)

SSL Ciphers

ID *	State
CHACHA20	Enabled

Cancel Save

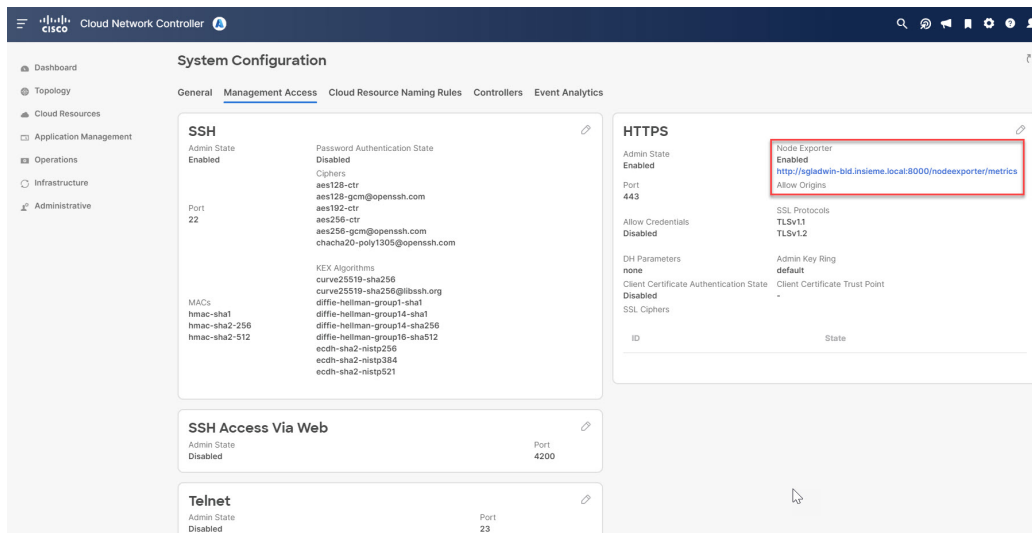
これらの設定を保存すると Web サービスが再起動され、要求への応答が再開されるまで少し時間がかかることを示す警告メッセージが表示されます。[OK] をクリックして、変更内容を確定します。

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

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

REST API を使用した VM ホスト メトリックスの監視

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

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

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

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

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

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

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

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

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

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

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

アプリケーション管理詳細の表示

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

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

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

表 29: アプリケーション管理サブタブ

サブタブ名	説明
テナント	テナントをサマリー テーブルの行として表示します。
アプリケーション プロファイル	サマリー テーブルの行としてアプリケーション プロファイルを表示します。
EPG	EPG をサマリー テーブルの行として表示します。
契約	コントラクトをサマリー テーブルの行として表示します。
フィルタ (Filters)	サマリー テーブルの行としてフィルタを表示します。
VRF	サマリー テーブルの行として VRF を表示します。
サービス (Services)	次の 2 つのサブタブと情報が含まれています。 <ul style="list-style-type: none"> • デバイス : サマリー テーブルの行としてデバイスを表示します。 • サービス グラフ : サービス グラフをサマリー テーブルの行として表示します。

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。

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

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

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

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

(注) 表示されるタブは、コンポーネントと構成が異なるように見えます。

- **概要 (Overview)** : クラウドリソース、設定関係、およびコンポーネントの設定の概要を示します。
- **トポロジ** : オブジェクトと他の関連オブジェクトとの視覚的な関係を提供します。選択したオブジェクトが中央に表示されます。
- **クラウドリソース** : このコンポーネントに関連するクラウドリソース情報を表示するサブタブのリストを含みます。
- **アプリケーション管理** : コンポーネントに関係する ACI 関連情報を表示するサブタブのリストを含みます。
- **統計** : 選択したサンプリング間隔と統計タイプに基づいて統計を表示できるようにします。[統計] タブは表示しているコンポーネントに応じたサブタブを含みます。
- **イベント分析** : 障害、イベント、監査ログを表示するサブタブのリストを含みます。

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

クラウドリソースの詳細の表示

ここでは、Cisco Cloud Network Controller GUI を使用してクラウドリソースの詳細を表示する方法について説明します。クラウドリソースの詳細には、特定のリージョン、VNET、ルータ、セキュリティグループ (アプリケーションセキュリティグループ/ネットワークセキュ

リティグループ)、エンドポイント、VM、およびクラウドサービスに関する情報が含まれます。

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

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

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

表 30:クラウドリソース サブタブ

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

ステップ 2 表示する詳細のコンポーネントを表すタブをクリックします。

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

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

[エンドポイント (Endpoints)]サブタブでは、キーまたは値の用語を入力して、クラウドタグに基づいて検索を絞り込むことができます。両方の用語に基づいて検索する場合は、キーまたは値の用語の上に表示される (+) をクリックします (最初に入力された用語に応じて)。クラウドタグフィルタは編集できま

せん。検索を変更するには、最初にフィルタを削除してから、目的の**キー**または**値**の用語を再度入力します。複数のクラウドタグフィルタに基づく検索がサポートされています。

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

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

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

(注) 表示されるタブは、コンポーネントと構成が異なるように見えます。

- **概要 (Overview)** : クラウドリソース、設定関係、およびコンポーネントの設定の概要を示します。[エンドポイントに関連付けられたクラウドタグも表示されます。(The cloud tags associated with endpoints are also displayed.)]
- **クラウドリソース** : 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 31: [操作 (Operations)]サブタブ

サブタブ名	説明
イベント分析	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [障害 (Faults)]タブ：障害をサマリー テーブルの行として表示します。 • [障害レコード (Fault Records)]タブ：障害レコードをサマリーテーブルの行として表示します。 • [イベント (Events)]タブ：イベントをサマリーテーブルの行として表示します。 • [監査ログ (Audit Logs)]タブ：監査ログをサマリー テーブルの行として表示します。
アクティブセッション	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現用系ユーザーのリストを表示します。
バックアップと復元	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [バックアップ (Backups)]タブ：バックアップをサマリーテーブルの行として表示します。 • [バックアップ ポリシー (Backup Policies)]タブ：バックアップ ポリシーをサマリー テーブルの行として表示します。 • [ジョブステータス (Job Status)]タブ：ジョブのステータスをサマリーテーブルの行として表示します。 • [イベント分析 (Event Analytics)]タブ：次のサブタブが含まれます。 <ul style="list-style-type: none"> • [障害 (Faults)]タブ：サマリー テーブルの行として障害を表示します。 • [イベント (Events)]タブ：イベントをサマリー テーブルの行として表示します。 • [監査ログ (Audit Logs)]タブ：監査ログをサマリー テーブルの行として表示します。

サブタブ名	説明
[Tech Support]	次のサブタブを含みます。 <ul style="list-style-type: none"> • [Tech Support] タブ：テクニカルサポート ポリシーをサマリー テーブルの行として表示します。 • [コア ログ (Core Logs)] タブ：コア ログをサマリー テーブルの行として表示します。
Firmware Management	次のサブタブを含みます。 <ul style="list-style-type: none"> • [全般 (General)] タブ：現在のファームウェアバージョン、アップグレードステータスなどの一般的なファームウェア管理情報が表示されます。 • [イメージ (Images)] タブ：イメージのリストを表示します。 • [イベント分析 (Event Analytics)] タブ：次のサブタブが含まれます。 <ul style="list-style-type: none"> • [障害 (Faults)] タブ：サマリー テーブルの行として障害を表示します。 • [イベント (Events)] タブ：イベントをサマリー テーブルの行として表示します。 • [監査ログ (Audit Logs)] タブ：監査ログをサマリー テーブルの行として表示します。
スケジューラ	スケジューラ ポリシーをサマリー テーブルの行として表示します。
リモート ロケーション	リモート ロケーションをサマリー テーブルの行として表示します。

ステップ 2 表示するコンポーネントを表すタブをクリックします。

サマリー テーブルは、テーブルの行として表示されます。たとえば、**[アクティブ セッション (Active Sessions)]** サブタブを選択した場合、アクティブセッションのリストがサマリー テーブルの行として表示されます。

属性によるフィルタ処理バーをクリックすることにより、行をフィルタ処理できます。属性、演算子、およびフィルタ値を選択します。たとえば、ユーザー名に基づいてフィルタリングするには、`username == user1` を選択します (user1は Cisco Cloud Network Controller にログインしているユーザーです)。

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

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

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

インフラストラクチャの詳細の表示

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

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

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

表 32: インフラストラクチャ サブタブ

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

ステップ2 表示する詳細を含むコンポーネントを表すタブをクリックします。

管理の詳細の表示

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

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

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

表 33: 管理サブタブ

サブタブ名	説明
Authentication	<p>[認証デフォルト設定 (Authentication Default Settings)]、[ログインドメイン (Login Domains)]、[プロバイダー (Providers)]、および[イベント分析 (Event Analytics)] サブタブが表示されます。</p> <ul style="list-style-type: none"> • [認証デフォルト設定 (Authentication Default Settings)] タブ: 設定情報が表示されます。 • [ログインドメイン (Login Domains)] タブ: ログインドメインをサマリーテーブルの行として表示します。 • [プロバイダー (Providers)] タブ: プロバイダーをサマリーテーブルの行として表示します。 • [イベント分析 (Event Analytics)] タブ: [障害 (Faults)]、[イベント (Events)]、および[監査ログ (Audit Logs)] サブタブを表示します。各サブタブには、対応する情報が行としてサマリーテーブルに表示されます。

サブタブ名	説明
セキュリティ	<p>次のサブタブのリストが含まれます。</p> <ul style="list-style-type: none"> • [セキュリティ デフォルト設定 (Security Default Settings)] タブ : デフォルトのセキュリティ設定情報を表示できます。 • [セキュリティ ドメイン (Security Domains)] タブ : サマリー テーブルにセキュリティ ドメイン情報を表示できます。 • [ロール (Roles)] タブ : ロール情報をサマリー テーブルに表示できます。 • [RBAC ルール (RBAC Rules)] タブ : サマリー テーブルに RBAC ルール情報を表示できます。 • [証明書権限 (Certificate Authorities)] タブ : サマリー テーブルの認証局情報を表示できます。 • [キー リング (Key Rings)] タブ : キー リング情報をサマリー テーブルに表示できます。 • [ユーザー アクティビティ (User Activity)] タブ : ユーザーアクティビティを表示できます。
Users	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [ローカル (Local)] タブ : ローカル ユーザーをサマリー テーブルの行として表示します。 • [リモート (Remote)] タブ : リモートユーザーをサマリー テーブルの行として表示します。
スマート ライセンス	<p>次のサブタブを含みます。</p> <ul style="list-style-type: none"> • [一般 (General)] タブ : ライセンスをサマリー テーブルの行として表示します。 • [CCR] タブ : CCR をサマリー テーブルの行として表示します。 • [障害 (Faults)] タブ : 障害をサマリー テーブルの行として表示します。

ステップ 2 表示するコンポーネントを表すタブをクリックします。

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

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

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

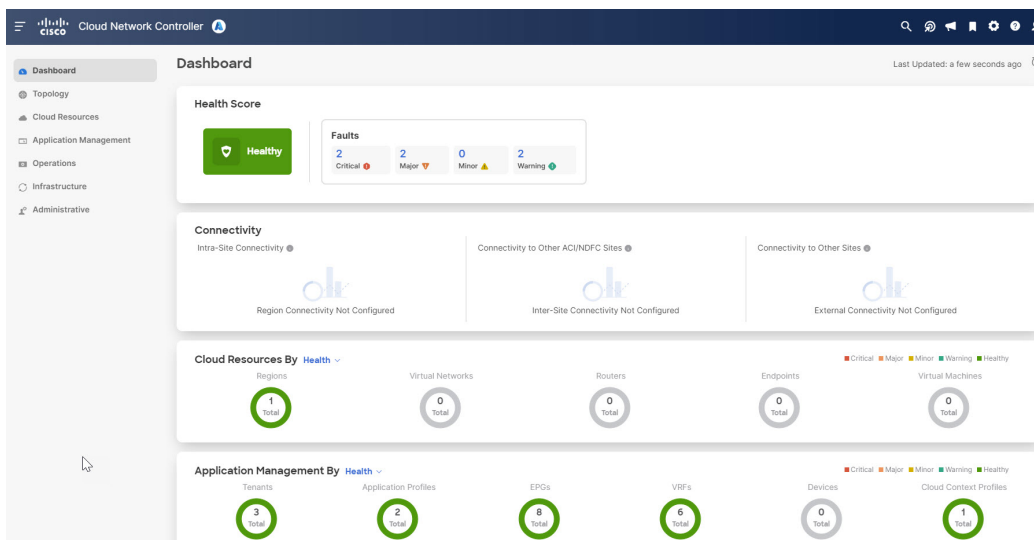
Cisco Cloud Network Controller GUI を使用したヘルス詳細の表示

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

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

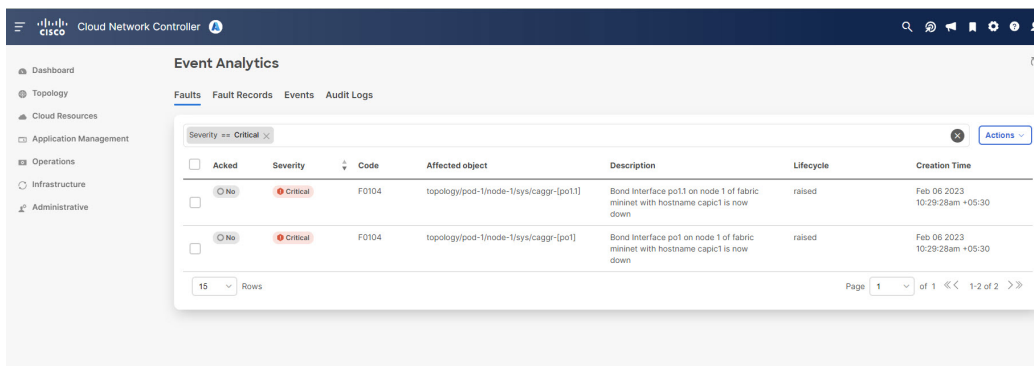
ステップ 1 [ナビゲーション (Navigation)] メニューから [ダッシュボード (Dashboard)] タブを選択します。

Cisco Cloud 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。

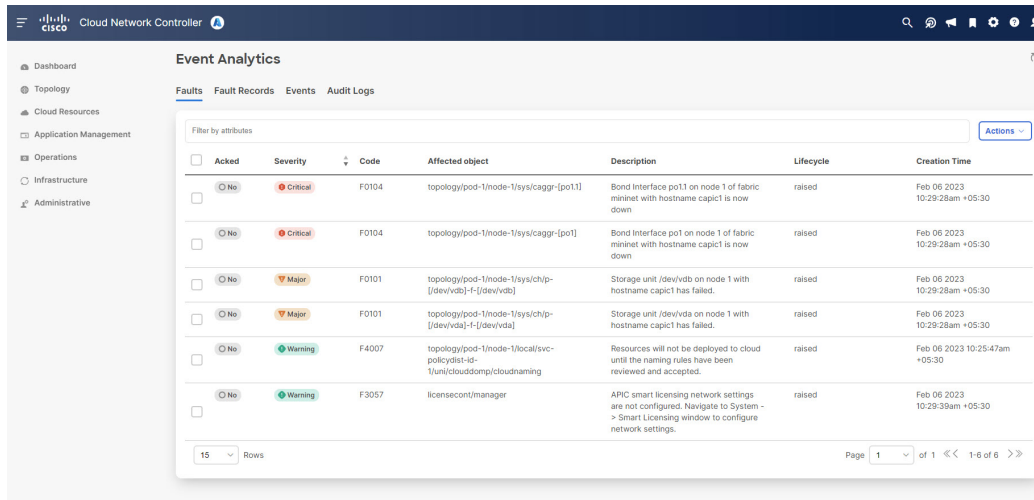
[イベント分析 (Event Analytics)] ウィンドウが表示され、クリックした特定の障害レベルの詳細情報が表示されます。次の画面は、重大度がクリティカルでリストされている障害の [イベント分析 (Event Analytics)] ウィンドウの例を示しています。



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。

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

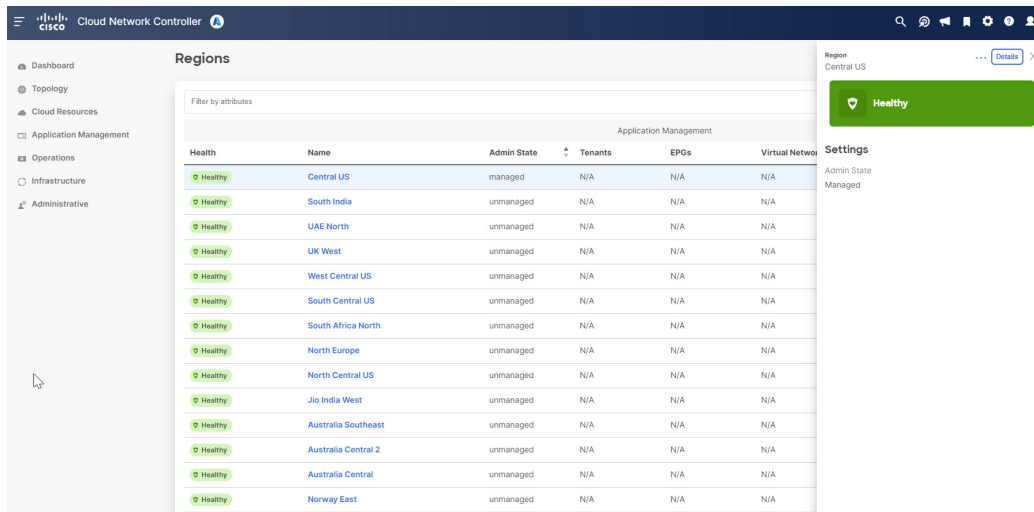


ステップ 4 [ナビゲーション (Navigation)] メニューから、[クラウド リソース (Cloud Resources)] タブを選択します。

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

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

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





第 6 章

レイヤ 4 から レイヤ 7 サービスの展開

- [概要 \(199 ページ\)](#)
- [ユースケースの例 \(212 ページ\)](#)
- [クラウドネイティブおよびサードパーティサービスによるサービス グラフの使用例 \(230 ページ\)](#)
- [リダイレクトの注意事項と制約事項 \(255 ページ\)](#)
- [Cisco Cloud Network Controller GUI を使用したセカンダリ VRF への新しい CIDR の追加 \(257 ページ\)](#)
- [サービス グラフの展開 \(260 ページ\)](#)

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。

Azure での展開では、次の 4 種類のレイヤ 4 からレイヤ 7 サービスがサポートされています。

- ALB は、Azure アプリケーション ゲートウェイまたはアプリケーション ロードバランサを指します。
- NLB は Azure ロードバランサまたはネットワーク ロードバランサを指します。
- サードパーティのファイアウォール
- サードパーティのロードバランサ

サービス グラフについて

サービス グラフは、2 つ以上の EPG ペア間に挿入された一連のレイヤ 4 ~ レイヤ 7 サービス デバイスを表すために使用されます。EPG は、クラウド (Cloud EPG など) またはインターネット (cloudExtEPG) 内で実行されているアプリケーション、または他のサイト (オンプレミスまたはリモート クラウド サイトなど) から実行されているアプリケーションを表すことができます。レイヤ 4 からレイヤ 7 のサービス デバイスは、NLB、ALB、サードパーティの

ファイアウォールのクラスタ、またはサードパーティのロードバランサにすることができます。

サービス グラフとコントラクト（およびフィルタ）は、2つの EPG 間の通信を指定するために使用されます。Cisco Cloud Network Controller は、契約およびサービス グラフで指定されたポリシーに基づいて、セキュリティールール（ネットワーク セキュリティ グループ/NSG および ASG）と転送ルート（UDR）を自動的に導出します。

複数のサービス グラフを指定して、さまざまなトラフィック フローまたはトポロジを表すことができます。

サービス グラフでは、次の組み合わせが可能です。

- 同じデバイスを複数のサービス グラフで使用できます。
- 複数のコンシューマ EPG とプロバイダー EPG の間で同じサービス グラフを使用できます。

サービス グラフを使用することで、ユーザはポリシーを一度指定するだけで、リージョン内またはリージョン間でサービスチェーンを展開できます。グラフを展開するたびに、Cisco ACI は新しい論理トポロジでの転送を行えるように、ネットワーク構成の変更を行います。

サードパーティのファイアウォールの場合、デバイス内の構成は Cisco Cloud Network Controller によって管理されません。

サービス グラフは、次の要素を使ってネットワークを表します。

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

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

クラウドネイティブおよびサードパーティ サービスでのサービス グラフの使用

クラウドネイティブおよびサードパーティ サービスでのサービス グラフの使用ができます。これらの状況では、リダイレクトの有無にかかわらずサービス グラフを使用できます。リダイレクトの有無にかかわらず使用例については [クラウドネイティブおよびサードパーティ サービスによるサービス グラフの使用例 \(230 ページ\)](#) を参照してください。

このタイプのサービス グラフでは、同じくリリース 5.1(2) で導入されたクラウド サービス エンドポイント グループ（サービス EPG）を使用します。サービス EPG、およびサービス EPG で使用できる展開タイプとアクセス タイプの詳細については、[クラウド サービス エンドポイント グループ \(35 ページ\)](#) を参照してください。

この目的でサービス EPG で使用されるサービス グラフでは、次の展開タイプとアクセス タイプがサポートされています。

表 34: プロバイダーサービスの EPG タイプ

導入タイプ	アクセスタイプ
クラウドネイティブ	プライベート
クラウドネイティブ管理対象	パブリックとプライベート
サードパーティ製の	プライベート

表 35: コンシューマサービス EPG タイプ

導入タイプ	アクセスタイプ
クラウドネイティブ管理対象	パブリックとプライベート

注意事項と制約事項

- サービス EPG を使用して、クラウドネイティブおよびサードパーティサービスでサービスグラフを使用するには、新しいサブネットごとの NSG 構成を有効にする必要があります。サブネットごとの NSG 構成の詳細については、[セキュリティグループ \(43 ページ\)](#) を参照してください。
- クラウド EPG とサービスグラフの組み合わせに適用される制限は、サービス EPG とサービスグラフの組み合わせにも適用されます。たとえば、タグベースのコンシューマとプロバイダーが同じリージョンの同じ VRF に存在できないというクラウド EPG/サービスグラフの制限は、サービス EPG とサービスグラフにも適用されます。
- リダイレクトを実行しない 2 つのノードグラフでは、SNAT と DNAT が有効になっています。DNATed アドレスはロードバランサと同等のデバイスであると想定されており、異なるサブネットにある可能性のある異なるターゲット間でトラフィックを分散させることができます。
これらのターゲットが異なるサブネットにある場合、サービスグラフはそれらのターゲットのルート到達可能性ルールを提供しないことに注意してください。この場合、サービス EPG が到達可能性を処理すると想定されます。
- AKS とサービスグラフが関係する場合、サービスグラフは、AKS クラスターのロードバランサのサブネットへのルートの到達可能性のみを確立します。

アプリケーションロードバランサの概要

アプリケーションロードバランサ (Azure Application Gateway または ALB とも呼ばれます) は、HTTP リクエスト、URL フィルタリングなどの属性に基づいて Web トラフィックを分散するレイヤ7ロードバランサです。詳細については、『[Microsoft マニュアル](#)』を参照してください。

Cisco ACI では、2 つのアプリケーションロードバランサを展開する方法があります。

- インターネット向け：アプリケーション ロードバランサを、コンシューマ外部 EPG とプロバイダー クラウド EPG の間のサービスとして挿入します。
- 内部向け：アプリケーション ロードバランサを、コンシューマ クラウド EPG とプロバイダー クラウド EPG 間のサービスとして挿入します。

サービス グラフを使用してアプリケーション ロードバランサを使用できます。一般的な構成には次のものが含まれます。

- アプリケーション ロードバランサとしてのレイヤ4からレイヤ7サービス デバイスの作成
- サービス グラフのノードとして ALB を使用する
- サービス グラフがコントラクトに関連付けられている場合、EPG 通信での1つ以上のリスナーの作成。

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



(注) リスナーは複数の証明書をもつことができます。

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

アプリケーションロードバランサ (ALB) は、他のアプリケーションの展開に使用しない別のサブネットに配置する必要があります。Cisco Cloud Network Controller は、ALB の NSG を作成し、ALB に関連付けられたサブネットに接続します。Cisco Cloud Network Controller は Azure アプリケーション ゲートウェイの標準および Standard_v2 SKUs をサポートします。

ネットワーク ロードバランサについて

ネットワーク ロードバランサ (Azure ロードバランサまたは NLB) は、レイヤ4ポートに基づいてインバウンド フロー パケットを分散するレイヤ4 デバイスです。詳細については、『[Microsoft マニュアル](#)』を参照してください。

ALB と同様に、NLB はサービス グラフを使用して展開できます。1以上のリスナーを構成することで、これらのアクションを指定できます。

リスナーでは、ロードバランサがトラフィックを受け入れて転送するポートおよびプロトコル (TCP または UDP) を指定できます。すべてのリスナーで、少なくとも1つのルール(条件のないデフォルトのルール)を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。アプリケーションゲートウェイとは異なり、ここではルールはバックエンドプールの特定のポートにのみトラフィックを転

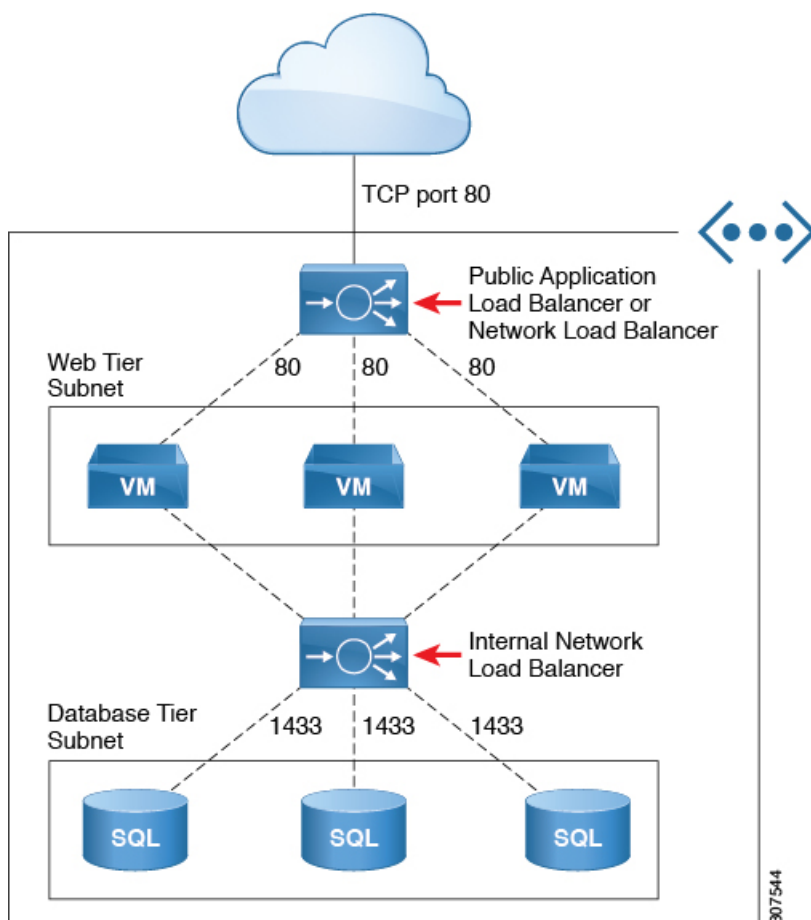
送できます。NLBはALBと同様に別のサブネットにある必要があります。ネットワークロードバランサには、次の2つの動作モードがあります。

- 転送モード：トラフィックは、特定のリスナーポートから指定されたバックエンドポートに転送されます。
- HAポートモード：ネットワークロードバランサは、すべてのポートでTCPフローとUDPフローを同時に負荷分散します。

Cisco Cloud Network Controllerは、標準SKUネットワークロードバランサのみをサポートしています。

図1では、フロントエンドロードバランサ（ALB/NLB）-VMまたはファイアウォール-バックエンドロード（ALB/NLB）バランサがサービスとして、コンシューマの外部EPGとプロバイダーのクラウドEPGの間に挿入されます。

図 11: インターネットおよび内部向け展開



Azure ネットワーク ロードバランサの複数のフロントエンド IP アドレスの構成について

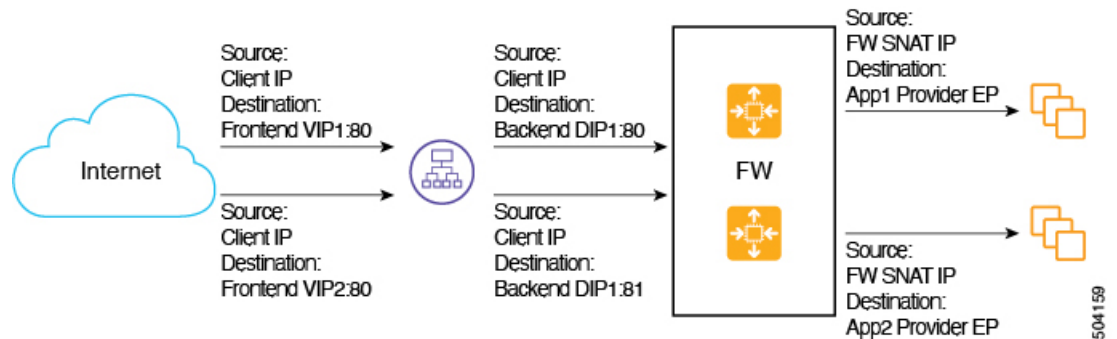
次のセクションでは、Azure ネットワーク ロードバランサでの複数のフロントエンド IP アドレスのサポートに関する情報を提供します。

- [Azure Network Load Balancer の複数のフロントエンド IP アドレスについて \(204 ページ\)](#)
- [注意事項と制約事項 \(204 ページ\)](#)

Azure Network Load Balancer の複数のフロントエンド IP アドレスについて

インターネット向けのネットワーク ロードバランサに対して複数のフロントエンド IP アドレスを構成するためのサポートが利用可能になりました。この機能により、各フロントエンド IP アドレスは、特定のバックエンドプールに対する 1 つ以上のルールにアタッチされます。

次の図は、インターネットに接続するネットワークロードバランサに対して複数のフロントエンド IP アドレスが構成されている構成例を示しています。



この構成例は、次のリスナー ルールのパケット フローを示しています。

	リスナー ルール (フロントエンド構成)	ルール アクション (バックエンド構成)
Rule1	<ul style="list-style-type: none"> • IP: VIP1 • Port: 80 	Port: 80
Rule2	<ul style="list-style-type: none"> • IP: VIP2 • Port: 80 	Port: 81

サービス グラフでは、サービス デバイスでのリスナー ルールとルールアクションの設定を構成できます。ネットワーク ロードバランサで定義されている場合、リスナー ルールとルールアクションの設定は、ロードバランサのフロントエンド構成からバックエンドプールへのマッピングを構築します。インターネットに接続するネットワーク ロードバランサの複数のフロントエンド IP アドレス構成がサポートされ、各フロントエンドがフロントエンド IP アドレス、ポート、およびプロトコルのタプルの組み合わせとして示される複数のフロントエンドでリスナー ルールが構成可能です。

注意事項と制約事項

インターネット向けのネットワーク ロードバランサに複数のフロントエンド IP アドレスを構成するためのサポートに関するガイドラインと制限を次に示します。

- 複数のフロントエンドIPアドレスのサポートは、インターネット向けのネットワーク ロードバランサでのみ使用できます。
- 複数のリスナー ルールでのバックエンド ポートの再利用はサポートされていません。

サードパーティのロードバランサについて

サードパーティ ロードバランサは、非クラウド ネイティブのレイヤ4からレイヤ7のロードバランサです。Cisco Cloud Network Controller は、サードパーティのロードバランサの構成を管理しません。ただし、Cisco Cloud Network Controller は、サードパーティのロードバランサへの接続のためのネットワーク スティッチングを自動化します。

外部インターフェイス サブネットからサードパーティのロードバランサのVIPを構成できます。サードパーティのロードバランサ用の追加のVIPを、外部インターフェイスのセカンダリIPアドレスとして構成することもできます。

Cisco Cloud Network Controller は、ソース NAT が有効になっている2アームモード（外部インターフェイスと内部インターフェイス）で展開されたサードパーティのロードバランサをサポートしています。

サードパーティ ロードバランサの制限事項：

- Cisco Cloud Network Controller は、サードパーティのロードバランサでの Direct Server Return (DSR) 構成をサポートしていません。
- サードパーティのロードバランサは、active/standby の高可用性構成ではサポートされていません。
active/active モードのサードパーティ ロードバランサ VM の詳細については、[ユースケースの例 \(212 ページ\)](#) を参照してください。
- エイリアンVIP範囲は、サードパーティのロードバランサではサポートされていません。

すべてのトラフィックを許可のオプションについて

[すべてのトラフィックを許可 (Allow All Traffic)] オプションは、リダイレクト対応のサービス グラフでパススルー デバイスとして展開されたサードパーティ ファイアウォールおよび Azure network load balancers で使用できます。





- (注) このオプションは、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスを許可します。このオプションを有効にする前に、これがセキュリティ リスクとならないことを確認します。

次のセクションでは、[すべてのトラフィックを許可 (Allow All Traffic)] オプションを有効にする手順について説明します。

- [サードパーティ ファイアウォール \(206 ページ\)](#)

- [Azure ネットワーク ロードバランサ \(207 ページ\)](#)

サードパーティ ファイアウォール


- 新しいサービス グラフ タイプを作成するときこのオプションを有効にするには：
 1. [インテント (Intent)]メニューの[アプリケーション管理 (Application Management)]リストから、[サービス (Services)]>>[デバイス (Devices)]>>[デバイスの作成 (Create Device)]をクリックします。
 2. [サービス タイプ (Service Type)]として[サードパーティ ファイアウォール (Third party firewall)]を選択します。
 3. [インターフェイスの追加 (Add Interface)]をクリックし、[すべてのトラフィックを許可 (Allow All Traffic)]エリアを見つけます。
 4. [すべてのトラフィックを許可 (Allow All Traffic)]エリアの[有効 (Enabled)]フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスを許可します。
 5. 設定が終わったら [Save] をクリックします。
- 既存のサービス グラフ タイプを編集するときこのオプションを有効にするには：
 1. [インテント (Intent)]メニューの[アプリケーション管理 (Application Management)]リストから、[サービス (Services)]をクリックし、[デバイス タイプ (Device Type)]として[サードパーティ ファイアウォール (Third-Party Firewall)]が表示されている既存のサービス デバイスをクリックします。
このサービス デバイス タイプの詳細を示すパネルがウィンドウの右側からスライドします。
 2. [詳細 (Details)]アイコンをクリックします ()。
このサービスデバイス タイプの詳細情報を提供する別のウィンドウが表示されます。
 3. ウィンドウの [インターフェイス (Interfaces)]エリアを見つけ、[インターフェイス セレクタ (Interface Selectors)]列で必要なインターフェイス セレクタをクリックします。
このインターフェイスの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。
 4. [詳細 (Details)]アイコンをクリックします ()。
このインターフェイスの詳細情報を提供する別のウィンドウが表示されます。
 5. 鉛筆アイコンをクリックして、このインターフェイスの構成設定を編集します。
 6. [すべてのトラフィックを許可 (Allow All Traffic)]エリアを見つけ、[すべてのトラフィックを許可 (Allow All Traffic)]エリアの [有効 (Enabled)]フィールドの横に

あるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスを許可します。

7. 設定が終わったら [Save] をクリックします。

Azure ネットワーク ロードバランサ

- 新しいサービス グラフ タイプを作成するときこのオプションを有効にするには：
 1. [インテント (Intent)]メニューの[アプリケーション管理 (Application Management)]リストから、[サービス (Services)]>>[デバイス (Devices)]>>[デバイスの作成 (Create Device)]をクリックします。
 2. [サービス タイプ (Service Type)]として[ネットワーク ロードバランサ (Network Load Balancer)]を選択します。
 3. [設定 (Settings)]エリアで、[すべてのトラフィックを許可 (Allow All Traffic)]エリアの[有効 (Enabled)]フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスを許可します。
 4. 設定が終わったら [Save] をクリックします。
- 既存のサービス グラフ タイプを編集するときこのオプションを有効にするには：
 1. [インテント (Intent)]メニューの[アプリケーション管理 (Application Management)]リストから、[サービス (Services)]をクリックし、[デバイス タイプ (Device Type)]として[ネットワーク ロードバランサ (Network Load Balancer)]が表示されている既存のサービス デバイスをクリックします。

このサービス デバイス タイプの詳細を示すパネルがウィンドウの右側からスライドします。
 2. [詳細 (Details)]アイコンをクリックします ()。

このサービス デバイス タイプの詳細情報を提供する別のウィンドウが表示されます。
 3. 鉛筆アイコンをクリックして、このサービス デバイスの構成設定を編集します。
 4. [設定 (Settings)]エリアで、[すべてのトラフィックを許可 (Allow All Traffic)]エリアを見つけ、[すべてのトラフィックを許可 (Allow All Traffic)]エリアの[有効 (Enabled)]フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスを許可します。
 5. 設定が終わったら [Save] をクリックします。

サーバー プールへのダイナミック サーバーのアタッチ

プロバイダー EPG 内のサーバー、または ALB/NLB の背後にあるサードパーティ ファイアウォールなどのサービス デバイスは、ターゲット グループに動的に追加されます。Azure では、ターゲット グループはバックエンドプールとして参照されます。フロントエンドとバックエンドのプロトコルとポート番号、および負荷分散アクションを定義するリスナーとルール構成は、ユーザによって提供されます。サービスグラフ構成の一部として最後のノードである ALB/NLB でリスナールールを構成する場合、特定のルールに対してプロバイダー EPG を選択できます。その EPG からのエンドポイントは、ロードバランサのターゲット グループに動的に追加されます。サードパーティ ファイアウォールなどの別のノードが ALB/NLB とプロバイダー EPG の間に存在する場合、ファイアウォールエンドポイントはロードバランサのターゲット グループに動的に追加されます。ターゲットのエンドポイントまたは FQDN を指定する必要はありません。

ロードバランサーのバックエンド ターゲットとして VM スケールセットがサポートされるようになりました。



- (注) ファイアウォールに VM スケールセットを使用する場合は、ファイアウォール インターフェイスにサブネット ベースの EP セレクタのみを使用します。Azure は、複数のインターフェイスを持つ VM スケールセットの NIC ごとのタグ付けをサポートしていません。

VNet 間サービスについて

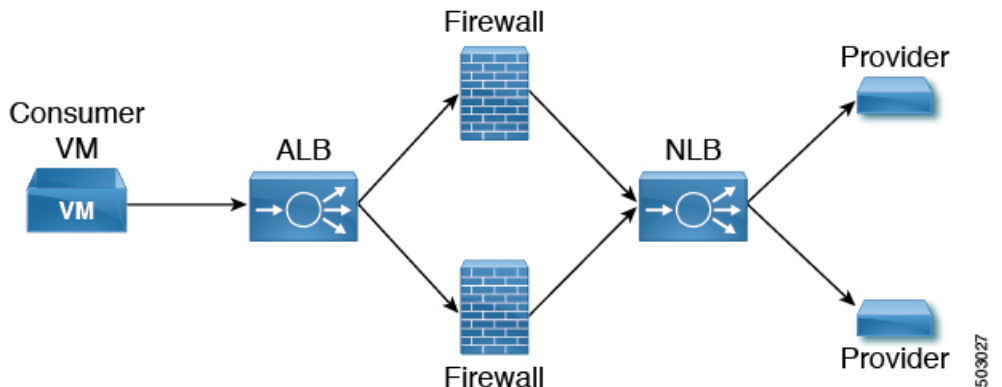
VNet 間サービスの展開と自動化がサポートされています。これは、クラウド内の East-West と North-South の両方のユース ケースに当てはまります。

このサポートについては、以下の点に注意してください。

- VNet ピアリングは、ハブスポーク トポロジ用に構成する必要があります。詳細については、「[Azure 向け Cisco Cloud Network Controller の VNet ピアリングを構成する](#)」を参照してください。
 - リダイレクトを使用したマルチノード サービスの場合：サービス デバイスがインフラ VNet に存在する必要があります。プロバイダーの前にある ALB などのサービス デバイスは、プロバイダー VNet に存在できます。
 - リダイレクトのないマルチノード サービスの場合：サービス デバイスは、プロバイダー VNet 内にあるか、ハブ VNet とプロバイダー VNet にまたがって分散することができます。
- VNet 間トラフィックは、インフラ VNet のアプリケーション ロードバランサまたはネットワーク ロードバランサ、および非インフラ VNet のプロバイダーでサポートされます。VNet は相互にピアリングする必要があり、ロードバランサとプロバイダーは同じリージョンからのもの必要があります。

マルチノードについて

マルチノード サービス グラフはサポートされています。マルチノードにより、サービス グラフを使用した複数の展開シナリオが可能になります。



展開可能なサービス デバイスは、アプリケーション ロードバランサ、ネットワーク ロードバランサ、およびサードパーティ ファイアウォールです。

グラフには2種類のノードが許可されます。

- 非リダイレクト：トラフィックはサービス デバイスに向けられます（ロードバランサ、DNAT と SNAT を備えたサードパーティ ファイアウォール、ネットワーク ロードバランサ）。
- リダイレクト：サービス デバイスはパススルー デバイス（ネットワーク ロードバランサまたはファイアウォール）です。

レイヤ4～レイヤ7サービス リダイレクト

レイヤ4からレイヤ7へのサービスリダイレクト機能は、Cisco Cloud ネットワーク コントローラで使用できます。これは、Cisco APIC で使用可能なポリシーベースのリダイレクト（PBR）機能と同様です。レイヤ4からレイヤ7へのサービスリダイレクト機能は、Cisco Cloud ネットワーク コントローラの [リダイレクト（Redirect）] オプションを使用して構成されます。



- (注) このセクション全体で、「コンシューマからプロバイダーへ」という用語は、ポイントAからポイントBに向かうトラフィックを表す包括的な用語として使用されることがあり、これらの2つのポイントの間にリダイレクトサービスデバイスが挿入される場合があります。ただし、これは、コンシューマからプロバイダーへのトラフィックのみがリダイレクトでサポートされるという意味ではありません。トラフィックは、[スポークツースポーク（215ページ）](#)で説明されているユースケースのように、プロバイダーからコンシューマへの場合もあります。

リダイレクトでは、ポリシーを使用して特定のサービスデバイス経由でトラフィックをリダイレクトします。サービス デバイスは、ネットワーク ロードバランサまたはサードパーティの

ファイアウォールとして展開できます。このトラフィックは、標準のコンシューマからプロバイダーへの構成の一部として、必ずしもサービスデバイスを宛先とするものではありません。むしろ、通常どおりにコンシューマからプロバイダーへのトラフィックを構成し、そのコンシューマからプロバイダーへのトラフィックを特定のサービスデバイスにリダイレクトするようにサービス グラフを構成します。

Cisco Cloud Network Controller のリダイレクトのサポートは、VNet ピアリングで使用されるハブアンドスポーク トポロジを利用して、VNet ピアリング機能と組み合わせてのみ利用できます。VNet ピアリング機能の詳細については、[Configuring VNet Peering for Cisco Cloud Network Controller for Azure](#) ドキュメントを参照してください。

パススルー ルール

リダイレクトを有効にすると、サービス デバイスにアタッチされている NSG（ネットワークセキュリティグループ）のルールが更新され、コンシューマからプロバイダーへのトラフィックが許可されます。これらのルールは「パススルー ルール」と呼ばれます。一般に、パススルー ルールは、コンシューマ IP からプロバイダー IP へのトラフィックを許可することです。接続先 IP がアプリケーションロードバランサ（ALB）VIP の場合、ルールは、コンシューマ IP から ALB VIP へのトラフィックを許可することです。

リダイレクト プログラミング

リダイレクトプログラミングは、接続先 EPG の分類（タグベースまたはサブネットベース）によって異なります。

- サブネットベースの EPG の場合、接続先 EPG のサブネットを使用してリダイレクトをプログラムします。
- タグベースの EPG の場合、接続先 VNet の CIDR を使用してリダイレクトをプログラムします。

この結果、リダイレクトは、EPG がリダイレクトのサービス グラフの一部でない場合でも、リダイレクトで同じ接続先に向かう他の EPG からのトラフィックに影響を与えます。リダイレクトの一部ではない EPG からのトラフィックも、サービス デバイスにリダイレクトされます。

次の表は、さまざまなシナリオでリダイレクトがどのようにプログラムされるかを示しています。

コンシューマ	プロバイダー	コンシューマ VNet でのリダイレクト	プロバイダー VNet でのリダイレクト
タグベース	タグベース	プロバイダーのリダイレクトは、プロバイダーの VNet の CIDR です。	コンシューマのリダイレクトは、コンシューマの VNet の CIDR です。

コンシューマ	プロバイダー	コンシューマ VNet でのリダイレクト	プロバイダー VNet でのリダイレクト
タグベース	サブネットベース	プロバイダーのリダイレクトはプロバイダーのサブネットです	コンシューマのリダイレクトは、コンシューマの VNet の CIDR です。
サブネットベース	タグベース	プロバイダーのリダイレクトは、プロバイダーの VNet の CIDR です。	コンシューマのリダイレクトは、コンシューマのサブネットです
サブネットベース	サブネットベース	プロバイダーのリダイレクトはプロバイダーのサブネットです	コンシューマのリダイレクトは、コンシューマのサブネットです

リダイレクトポリシー

レイヤ4からレイヤ7へのサービスリダイレクト機能をサポートするために、サービスデバイスコネクタで新しいリダイレクトフラグを使用できるようになりました。次の表に、サービスデバイスコネクタの既存のフラグと新しいフラグに関する情報を示します。

接続タイプ	説明
redir	この値は、サービスノードがその接続のリダイレクトノードにあることを意味します。この値は、サードパーティのファイアウォールとネットワークロードバランサでのみ使用可能または有効です。
snat	この値は、サービスノードがトラフィックに対して送信元 NAT を実行していることをサービスグラフに通知します。この値は、サードパーティファイアウォールのプロバイダーコネクタでのみ、ノードのプロバイダーコネクタでのみ使用可能または有効です。
snat_dnat	この値は、サービスノードがトラフィックに対して送信元 NAT と接続先 NAT の両方を実行していることをサービスグラフに伝えます。この値は、サードパーティファイアウォールのプロバイダーコネクタでのみ、ノードのプロバイダーコネクタでのみ使用可能または有効です。
none	デフォルト値。

リダイレクトを構成するためのワークフロー

リダイレクトを構成するための一般的なワークフローは次のとおりです。

1. サービス グラフで使用する 1 つ以上のサービス デバイスを作成します。
 - ネットワーク ロードバランサ (NLB)
 - アプリケーション ロードバランサ (ALB)
 - サードパーティ ファイアウォール
2. サービス グラフを作成し、この特定のサービス グラフに適切なサービス デバイスを選択します。

手順のこの時点でリダイレクトを構成します。

1. ネットワーク ロードバランサ、アプリケーション ロードバランサ、またはファイアウォール アイコンを [デバイスのドロップ (Drop Device)] エリアにドラッグ アンド ドロップして、サービス グラフ用にそのサービス デバイスを選択します。
2. リダイレクト機能を有効にするには、表示される [サービス ノード (Service Node)] ウィンドウで、リダイレクト機能を有効にする場所に応じて、[コンシューマコネクタタイプ (Consumer Connector Type)] または [プロバイダーコネクタタイプ (Provider Connector Type)] エリアの下にある [リダイレクト (Redirect)] オプションの横にあるチェックボックスをオンにします。



(注) サービス グラフにアプリケーション ロードバランサがある場合でも、アプリケーション ロードバランサ サービス デバイスでリダイレクトを有効にすることはできません。

3. [サービス ノード (Service Node)] ウィンドウで残りの構成を完了し、[追加 (Add)] をクリックします。
3. コンシューマとプロバイダーの EPG 間のコントラクトを作成する EPG 通信を構成します。
4. サービス グラフをコントラクトに添付します。
5. サービス デバイスのパラメータを構成します。

ユースケースの例

次に、いくつかのユースケースの例を示します。

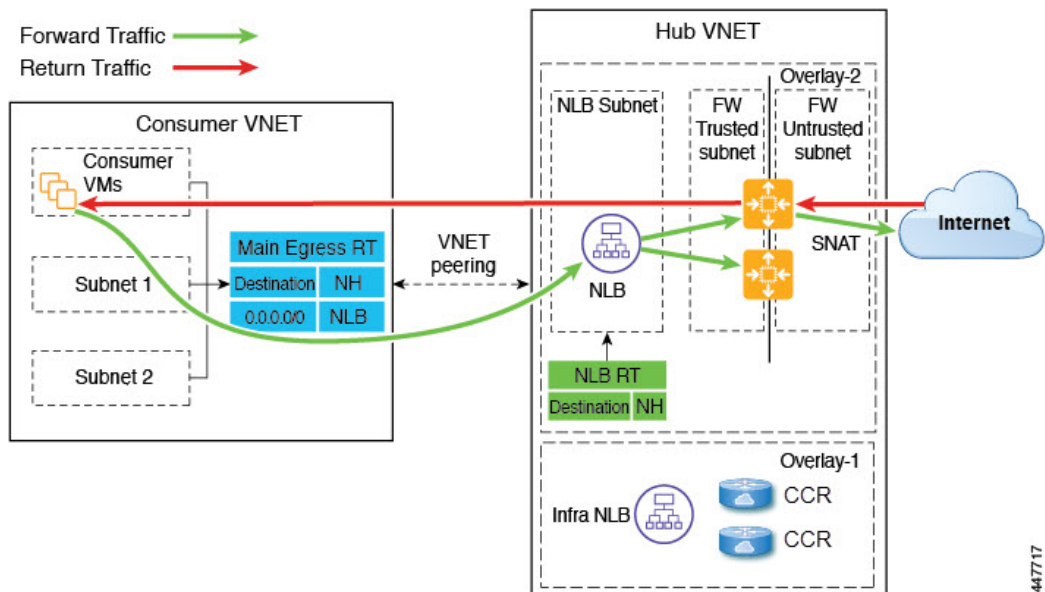
- スポークツーインターネット (213 ページ)
- スポークツースポーク (215 ページ)
- リージョン間スポーク ツー スポーク (218 ページ)

- インターネット ツー スポーク (VRF 間) (221 ページ)
- サードパーティ ロードバランサの高可用性サポート (224 ページ)
- 2つの個別の VNet 内のコンシューマとプロバイダーの EPG (226 ページ)
- 2つの個別の VNet でのコンシューマおよびプロバイダー EPG を使用した VNet のハブ (228 ページ)

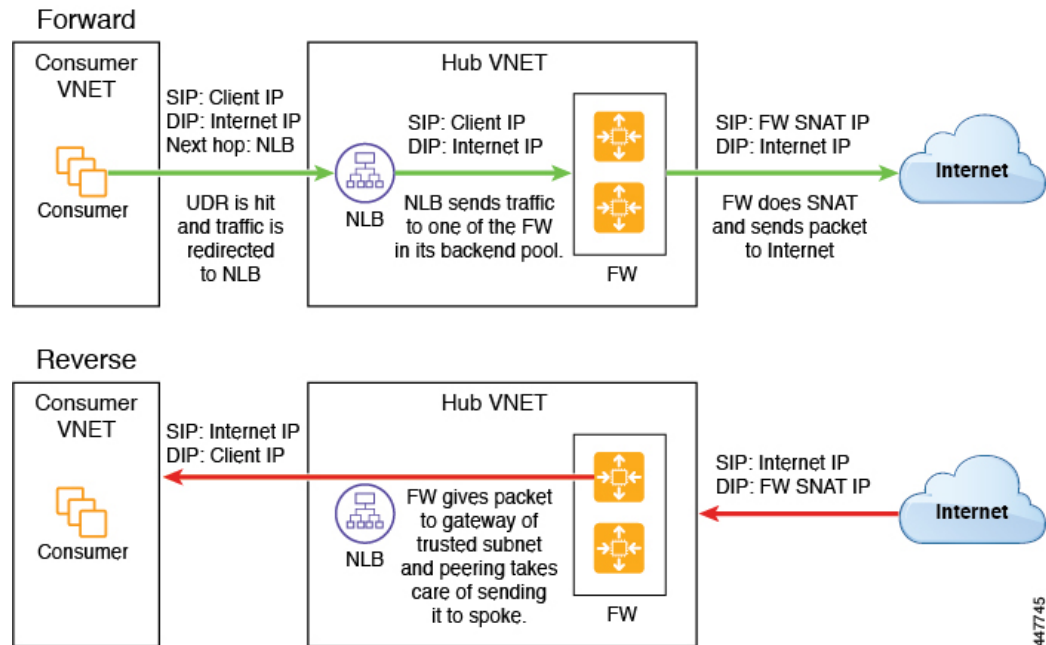
スポークツーインターネット

このユースケースでは、コンシューマ VNet (コンシューマ VM を含む) とハブ VNet は、VNet ピアリングを使用してピアリングされます。ネットワーク ロードバランサも展開され、スケールリングのために2つのファイアウォールに面しています。このユースケースでは、パッチの更新など、特定の理由でコンシューマ VM がインターネットにアクセスする必要があります。この場合、コンシューマ VNet では、インターネットへのリダイレクトを含むようにルートテーブルが変更され、トラフィックはハブ VNet のファイアウォールの前にある NLB にリダイレクトされます。インターネットに向かうサービスグラフの一部であるこのコンシューマからのトラフィックは、すべてネクスト ホップとして NLB に行きます。VNet ピアリングでは、トラフィックは最初に NLB に送られ、次に NLB がトラフィックをバックエンドのファイアウォールの1つに転送します。ファイアウォールは、トラフィックをインターネットに送信するときに、ソース ネットワーク アドレス変換 (SNAT) も実行します。

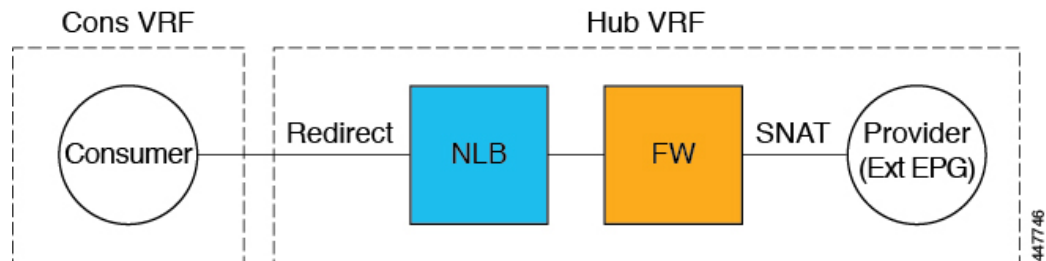
このユースケースで使用されるすべてのレイヤ4からレイヤ7サービスデバイスに専用サブネットがあることを確認します。



次の図は、このユースケースのパケットフローを示しています。



次の図は、このユースケースのサービスグラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

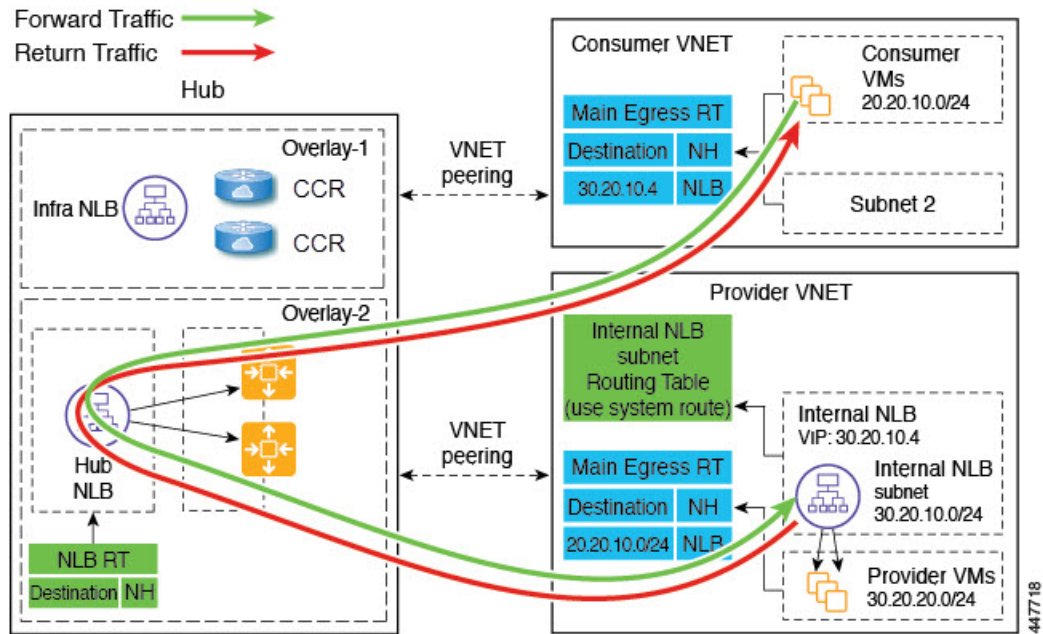
- [デバイス作成 (Create Device)] ウィンドウで
 - [テナント (Tenant)] フィールドで、[インフラ (infra)] テナントを選択します。
 - [サービスタイプ (Service Type)] フィールドでサービスデバイスのタイプを選択します。
 - [サービスタイプ (Service Type)] として [ネットワークロードバランサ (Network Load Balancer)] を選択し、[サブネット (Subnets)] エリアで [サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - [サービスタイプ (Service Type)] として [サードパーティファイアウォール (Third-Party Firewall)] を選択し、[VRF] フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロード バランサ
 - サードパーティ ファイアウォール
- ネットワーク ロードバランサの **[サービス ノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマ コネクタ タイプ (Consumer Connector Type)]** フィールドで、**[リダイレクト (Redirect)]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
 - **[プロバイダ コネクタ タイプ (Provider Connector Type)]** フィールドで、ボックスをオフのままにします。
- サードパーティファイアウォールの **[サービス ノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマ コネクタ タイプ (Consumer Connector Type)]** フィールドで、ボックスをオフのままにします。
 - このユース ケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダ コネクタ タイプ (Provider Connector Type)]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

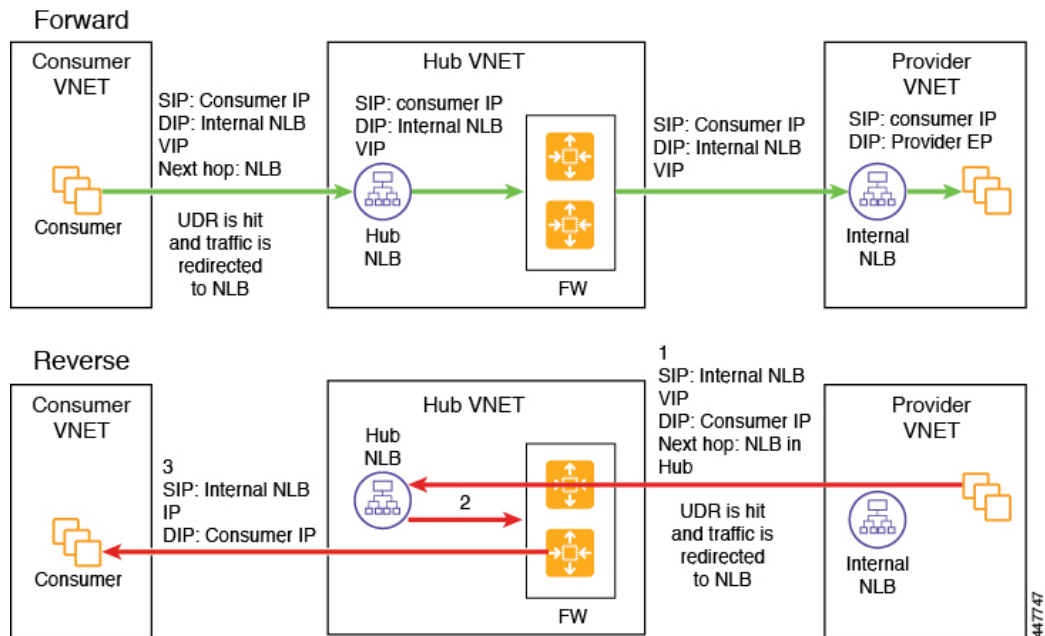
スポークツースポーク

このユースケースでは、トラフィックはスポークからスポークへ、ハブ NLB が前面にあるハブファイアウォールを通過します。コンシューマエンドポイントはコンシューマ VNet 内にあり、プロバイダー VNet には内部 NLB (またはサードパーティ ロードバランサ) が前面にある VM があります。コンシューマとプロバイダーの VNet で出カルートテーブルが変更され、トラフィックが NLB の前にあるファイアウォール デバイスにリダイレクトされるようになります。このユースケースでは、リダイレクトが双方向に適用されます。

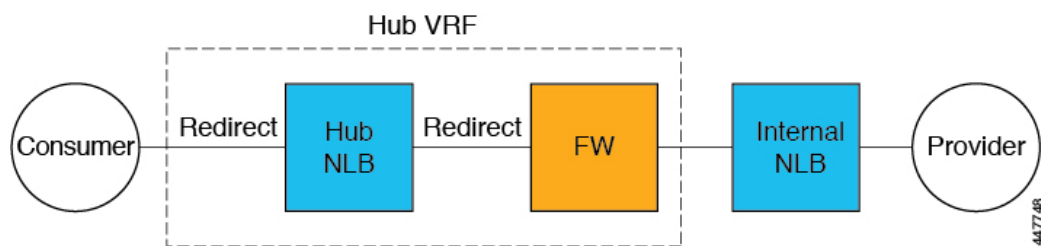
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



次の図は、このユースケースのパケットフローを示しています。



次の図は、このユースケースのサービスグラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- [デバイスの作成 (Create Device)] ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
 - [テナント (Tenant)] フィールドで、[インフラ (infra)] テナントを選択します。
 - [サービス タイプ (Service Type)] フィールドでサービス デバイスのタイプを選択します。
 - [サービス タイプ (Service Type)] として [ネットワーク ロード バランサ (Network Load Balancer)] を選択し、[サブネット (Subnets)] 領域で [サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - [サービス タイプ (Service Type)] として [サードパーティ ファイアウォール (Third-Party Firewall)] を選択し、[VRF] フィールドでセカンダリ VRF を選択します。
- [デバイスの作成 (Create Device)] ウィンドウで、次にプロバイダ VNet のサービス デバイスを作成します。
 - [テナント (Tenant)] フィールドで、プロバイダ テナントを選択します。
 - [サービス タイプ (Service Type)] フィールドで [ネットワーク ロード バランサ (Network Load Balancer)] を選択し、[サブネット (Subnets)] 領域で [サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダ VRF のサブネットを選択します。



(注) 内部 NLB の代わりにサードパーティ ロードバランサを使用できます。[サービス タイプ (Service Type)] として [サードパーティ ロードバランサ (Third Party Load Balancer)] を選択します。[インターフェイスの追加 (Add Interface)] をクリックして、[VRF] を選択し、インターフェイスの詳細を設定します。

- [サービス グラフの作成 (Create Service Graph)] ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロード バランサ (ハブ VNet 用)

- サードパーティ ファイアウォール (ハブ VNet 用)
- ネットワーク ロードバランサまたはサードパーティ ロードバランサ (プロバイダ VNet の場合)
- ハブ VNet のネットワーク ロードバランサの [サービス ノード (Service Node)] ウィンドウで、次のようにします。
 - [コンシューマ コネクタ タイプ (Consumer Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
 - [プロバイダ コネクタ タイプ (Provider Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。
- サードパーティ ファイアウォールの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のボックスをオフのままにします。
- プロバイダ VNet でネットワーク ロードバランサの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のチェックボックスをオフのままにします。

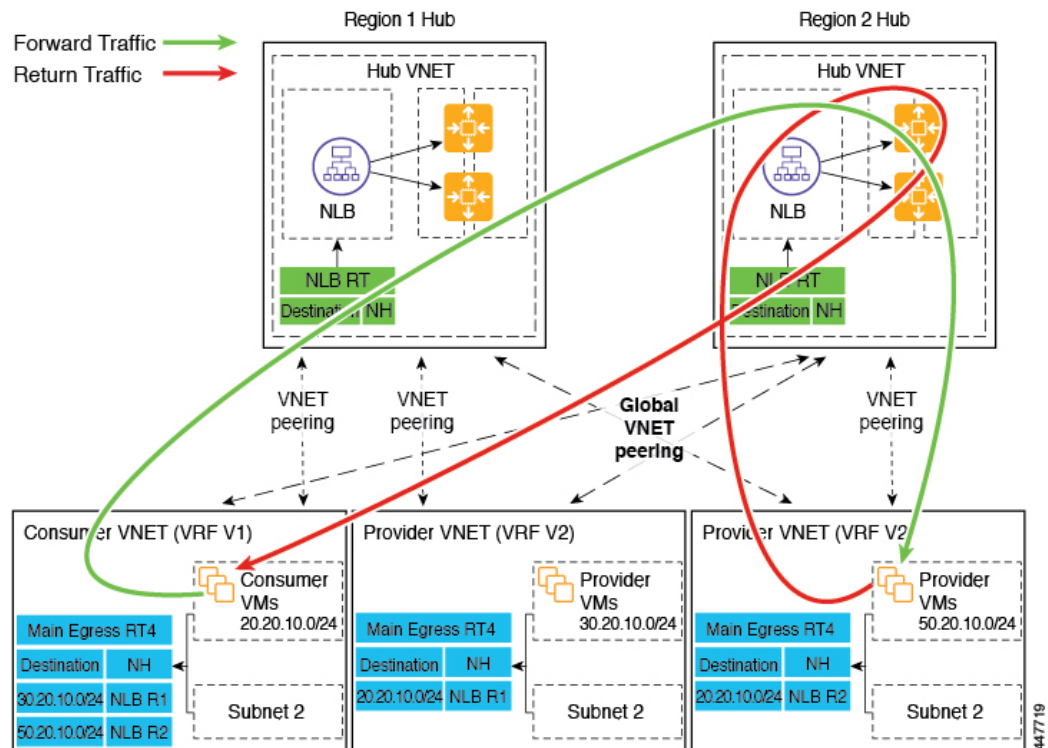


(注) SNAT がサードパーティのロードバランサで構成されていることを確認します。

リージョン間スポーク ツー スポーク

このユースケースでは、両方のリージョンにサービスデバイスが必要です。コンシューマ VNet はリージョン 1 にあり、プロバイダーは両方のリージョン (リージョン 1 と 2) にまたがっており、一部のエンドポイントはリージョン 1 にあり、一部のエンドポイントはリージョン 2 にあります。ローカルプロバイダーエンドポイントとリモートリージョンエンドポイントには、異なるリダイレクトがプログラムされています。この場合、使用されるファイアウォールは、プロバイダーエンドポイント側に最も近いファイアウォールになります。

このユースケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



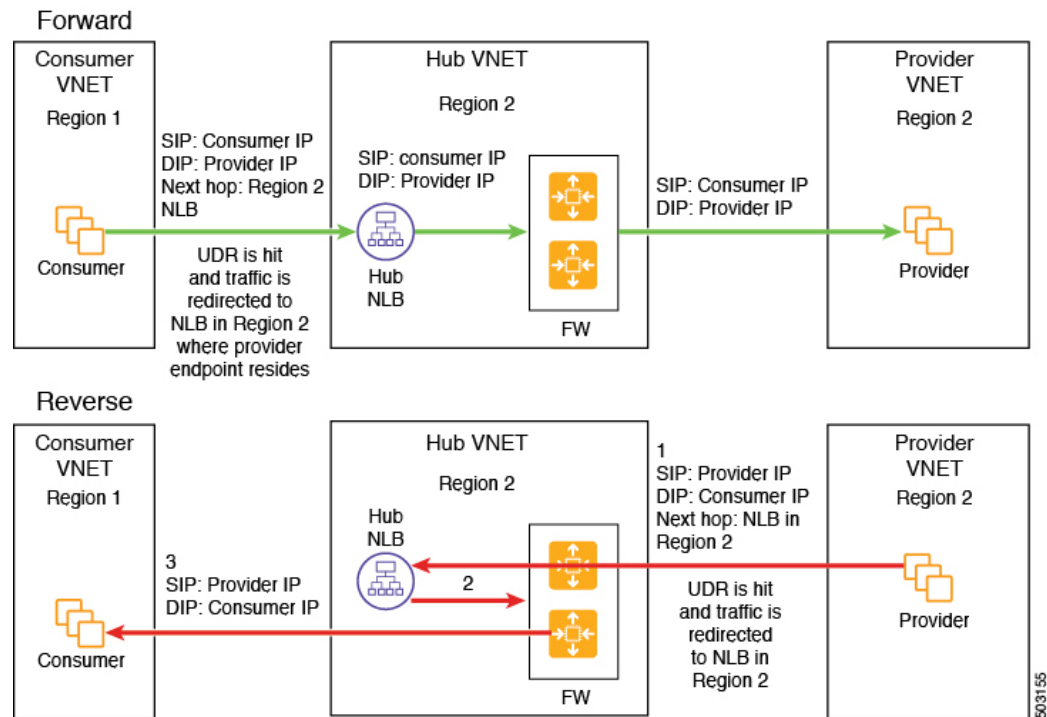
たとえば、コンシューマ VNet (VRF 1) の出カルートテーブル (RT) の 2つのサブネットについて考えてみます。

- 30.20.10.0/24 (リージョン 1 [R1] の NLB)
- 50.20.10.0/24 (リージョン 2 [R2] の NLB)

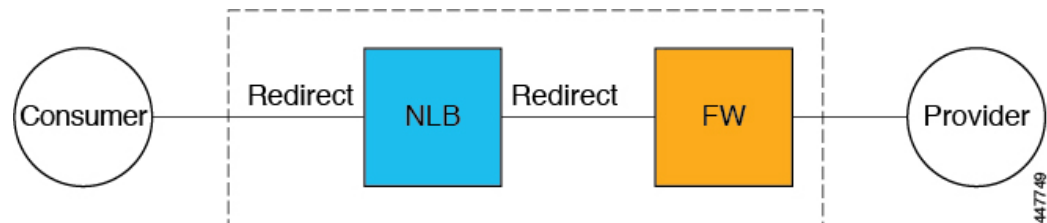
コンシューマが、ローカルにあるプロバイダー VM 30.20.10.0/24 にトラフィックを送信するとします。その場合、トラフィックはリージョン 1 のハブ NLB とファイアウォールにリダイレクトされ、プロバイダーに移動します。

ここで、コンシューマがプロバイダー VM 50.20.10.0/24 にトラフィックを送信するとします。この場合、ファイアウォールはプロバイダーエンドポイントに対してローカルであるため、トラフィックはリージョン 2 のハブ NLB とファイアウォールにリダイレクトされます。

次の図は、このユースケースのパケットフローを示しています。



次の図は、このユースケースのサービスグラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- [デバイス作成 (Create Device)] ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
 - [テナント (Tenant)] フィールドで、[インフラ (infra)] テナントを選択します。
 - [サービスタイプ (Service Type)] フィールドでサービスデバイスのタイプを選択します。
 - [サービスタイプ (Service Type)] として [ネットワークロードバランサ (Network Load Balancer)] を選択し、[サブネット (Subnets)] 領域で [サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - [サービスタイプ (Service Type)] として [サードパーティファイアウォール (Third-Party Firewall)] を選択し、[VRF] フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロード バランサ
 - サードパーティ ファイアウォール
- ハブ NLB の **[サービス ノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマ コネクタ タイプ (Consumer Connector Type)]** フィールドで、**[リダイレクト (Redirect)]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
 - **[プロバイダ コネクタ タイプ (Provider Connector Type)]** フィールドで、**[リダイレクト (Redirect)]** オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。
- サードパーティ ファイアウォールの **[サービス ノード (Service Node)]** ウィンドウで、**[コンシューマ コネクタ タイプ (Consumer Connector Type)]** と **[プロバイダ コネクタ タイプ (Provider Connector Type)]** のボックスをオフのままにします。

上記のユース ケースでは、プロバイダー VM は、クラウド ネイティブまたはサードパーティロードバランサによってフロントエンドにすることもできます。

インターネット ツースポーク (VRF 間)

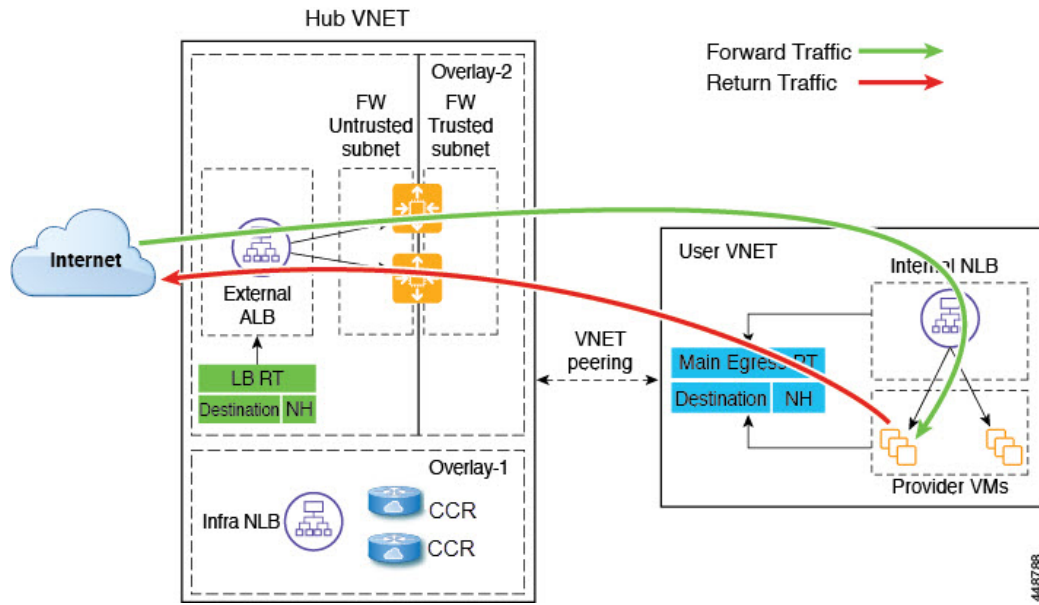
このユース ケースでは、インターネットからのトラフィックは、プロバイダーエンドポイントに到達する前にファイアウォールを通過する必要があります。このユース ケースではリダイレクトは使用されません。



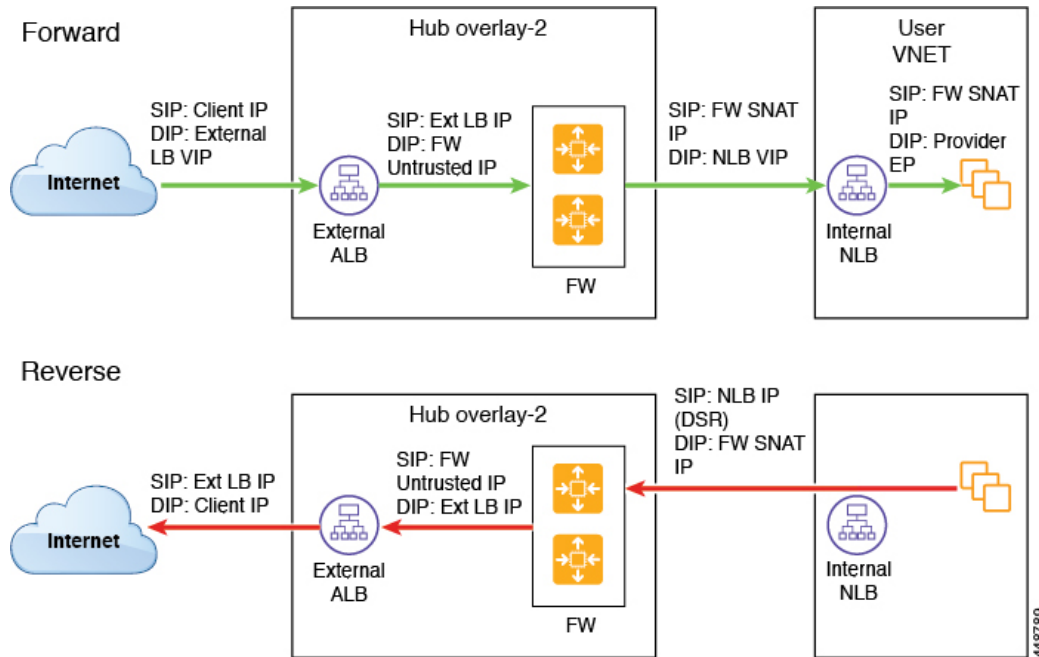
- (注) このセクションでは、一般的な用語「外部ロードバランサ」が使用されています。これは、このユース ケースで外部ロードバランサが NLB、ALB、またはサードパーティロードバランサのいずれかになる可能性があるためです。次の例は、ALBを使用した構成を示していますが、外部ロードバランサは代わりに NLB またはサードパーティロードバランサである可能性があることに注意してください。

外部ロードバランサは、VIP を介してサービスを公開します。インターネットトラフィックはその VIP に送信され、外部ロードバランサはトラフィックをバックエンドプール内のファイアウォールに送信します (外部ロードバランサにはファイアウォールの信頼できないインターフェイスがバックエンドプールとしてあります)。ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP に送られます。次に、内部 NLB はプロバイダーエンドポイントの 1 つにトラフィックを送信します。

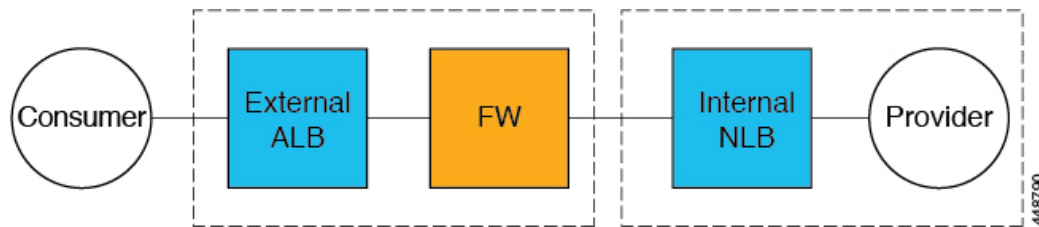
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットワークがあることを確認します。



次の図は、このユースケースのパケットフローを示しています。



次の図は、このユースケースのサービスグラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として **[アプリケーション ロード バランサ (Application Load Balancer)]** または **[ネットワーク ロード バランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** 領域で **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - **[サービス タイプ (Service Type)]** として **[サードパーティ ファイアウォール (Third-Party Firewall)]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
 - **[サービス タイプ (Service Type)]** として **[サードパーティ ロードバランサ (Third Party Load Balancer)]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加 (Add Interface)]** をクリックしてインターフェイスの詳細を設定します。
- **[デバイスの作成 (Create Device)]** ウィンドウで、次にプロバイダ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、プロバイダ テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドで **[ネットワーク ロード バランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** 領域で **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダ VRF のサブネットを選択します。
- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロードバランサまたはアプリケーション ロードバランサ (ハブ VNet 用)
 - サードパーティ ファイアウォール (ハブ VNet 用)
 - ネットワーク ロードバランサまたはサードパーティ ロードバランサ (プロバイダ VNet の場合)
- ハブ VNet のネットワーク ロードバランサまたはアプリケーションロードバランサの **[サービス ノード (Service Node)]** ウィンドウで、**[コンシューマ コネクタ タイプ (Consumer Connector Type)]** と **[プロバイダー コネクタ タイプ (Provider Connector Type)]** のボックスをオフのままにします。

- サードパーティファイアウォールの **[サービスノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマコネクタタイプ (Consumer Connector Type)]** フィールドで、ボックスをオフのままにします。
 - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、**[プロバイダコネクタタイプ (Third-Party Firewall)]** フィールドで、**[SNAT]** および **[DNAT]** オプションの隣のボックスにチェックを入れます。
- プロバイダー VNet でネットワークロードバランサの **[サービスノード (Service Node)]** ウィンドウで、**[コンシューマコネクタタイプ (Consumer Connector Type)]** と **[プロバイダーコネクタタイプ (Provider Connector Type)]** のチェックボックスをオフのままにします。



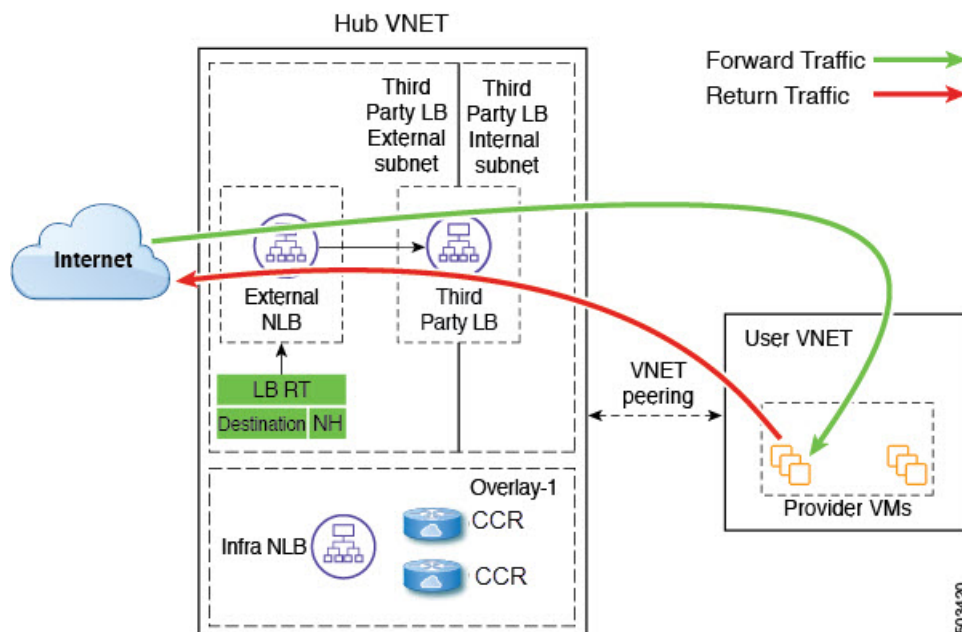
(注) SNAT がサードパーティのロードバランサで構成されていることを確認します。

サードパーティロードバランサの高可用性サポート

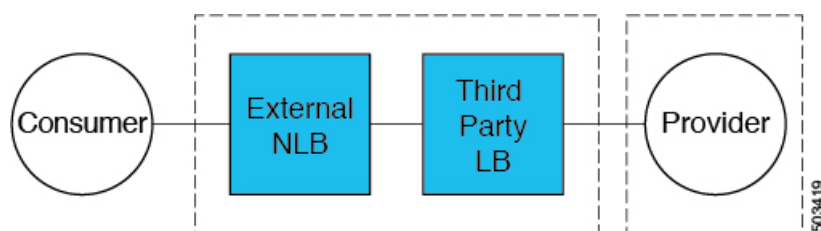
このユースケースでは、インターネットからのトラフィックは、プロバイダーエンドポイントに到達する前にサードパーティロードバランサを通過する必要があります。このユースケースではリダイレクトは使用されません。

サードパーティロードバランサは、NLB のバックエンドプールとして構成されます。デバイスのセカンダリ IP アドレスは、NLB のターゲットとして機能します。NLB のターゲットとして、プライマリまたはセカンダリ IP アドレス (またはその両方) を追加することを選択できます。サードパーティロードバランサ VM は、アクティブ/アクティブモードでのみ展開されます。サードパーティロードバランサは、アクティブ/スタンバイの高可用性構成では使用できません。

サードパーティロードバランサとネットワークロードバランサに専用のサブネットがあることを確認します。



次の図は、このユースケースのサービス グラフを示しています。



このユースケースの構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として**[ネットワーク ロードバランサ (Network Load Balancer)]**を選択し、**[サブネット (Subnets)]**領域で**[サブネットの追加 (Add Subnet)]**をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - **[サービス タイプ (Service Type)]** として**[サードパーティ ロードバランサ (Third Party Load Balancer)]**を選択し、**[VRF]**を選択し、**[インターフェイスの追加 (Add Interface)]**をクリックしてインターフェイスの詳細を設定します。
- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。

- ネットワーク ロード バランサ
- サードパーティ ロードバランサ



(注) ネットワークロードバランサとサードパーティのロードバランサが同じ VNet にあることを確認します。

- ハブ VNet のネットワーク ロードバランサの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダー コネクタ タイプ (Provider Connector Type)] のボックスをオフのままにします。



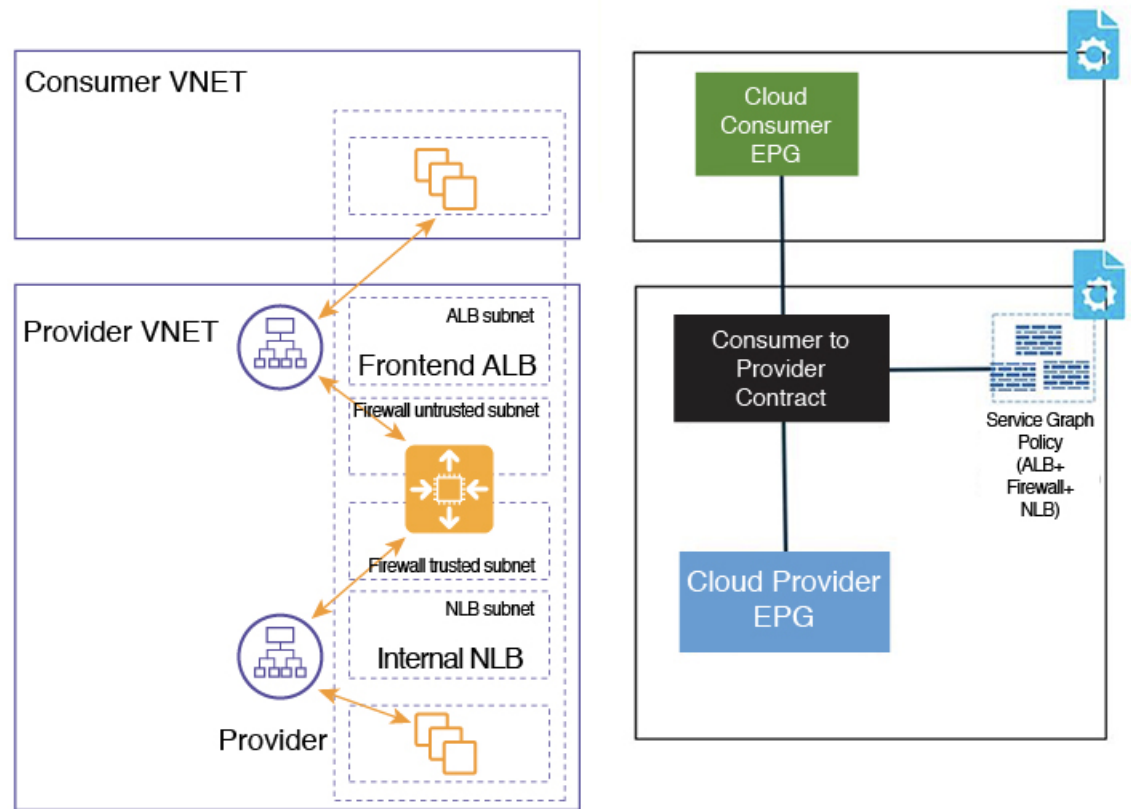
(注) SNAT がサードパーティのロードバランサで構成されていることを確認します。

2つの個別の VNet 内のコンシューマとプロバイダーの EPG

このユースケースは、2つの VNet を使用した構成例であり、コンシューマ EPG とプロバイダー EPG が別々の VNet にあります。

- フロントエンド ALB、ファイアウォール、および内部 NLB は、コンシューマとプロバイダーの EPG の間に挿入されます。
- コンシューマ エンドポイントは、フロントエンドの ALB VIP にトラフィックを送信し、ファイアウォールに転送します。
- ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP にフローが流れます。
- 内部 NLB は、バックエンドプロバイダーエンドポイントへのトラフィックを負荷分散します。

このユースケースでは、フロントエンド ALB または内部 NLB の代わりにサードパーティのロードバランサを使用できます。このユースケースで使用されるすべてのレイヤ4からレイヤ7サービス デバイスに専用サブネットがあることを確認します。

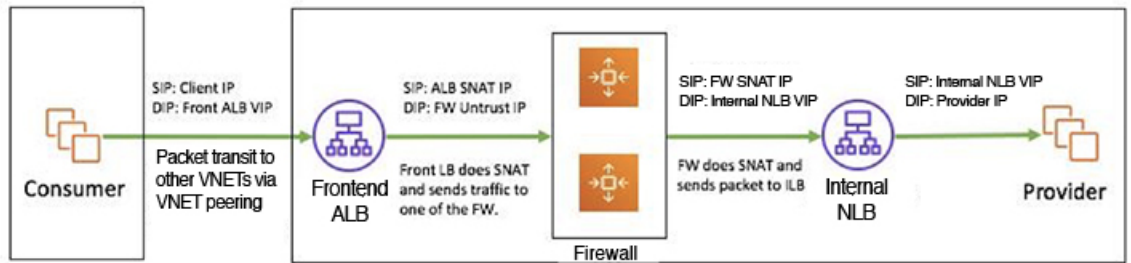


この図では次のようになっています。

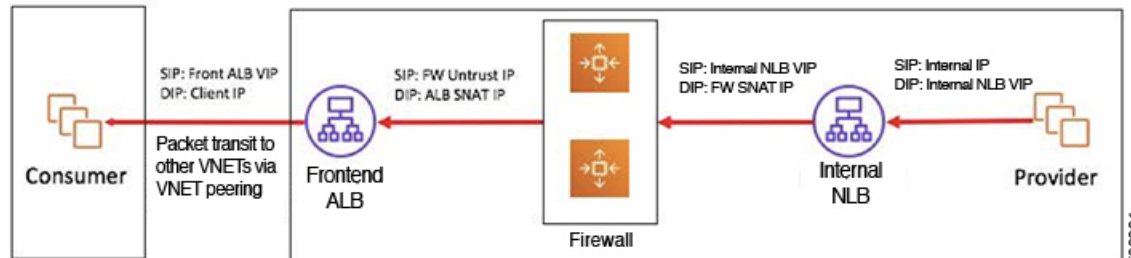
- コンシューマ EPG はコンシューマ VNet にあります。
- プロバイダー EPG とすべてのサービス デバイスはプロバイダー VNet にあります。
- アプリケーションロードバランサ、ネットワークロードバランサ（またはサードパーティのロードバランサ）、およびファイアウォールは、VNet 内に独自のサブネットを持つ必要があります。

両方向のパケットフローを次の図に示します。

Forward



Reverse



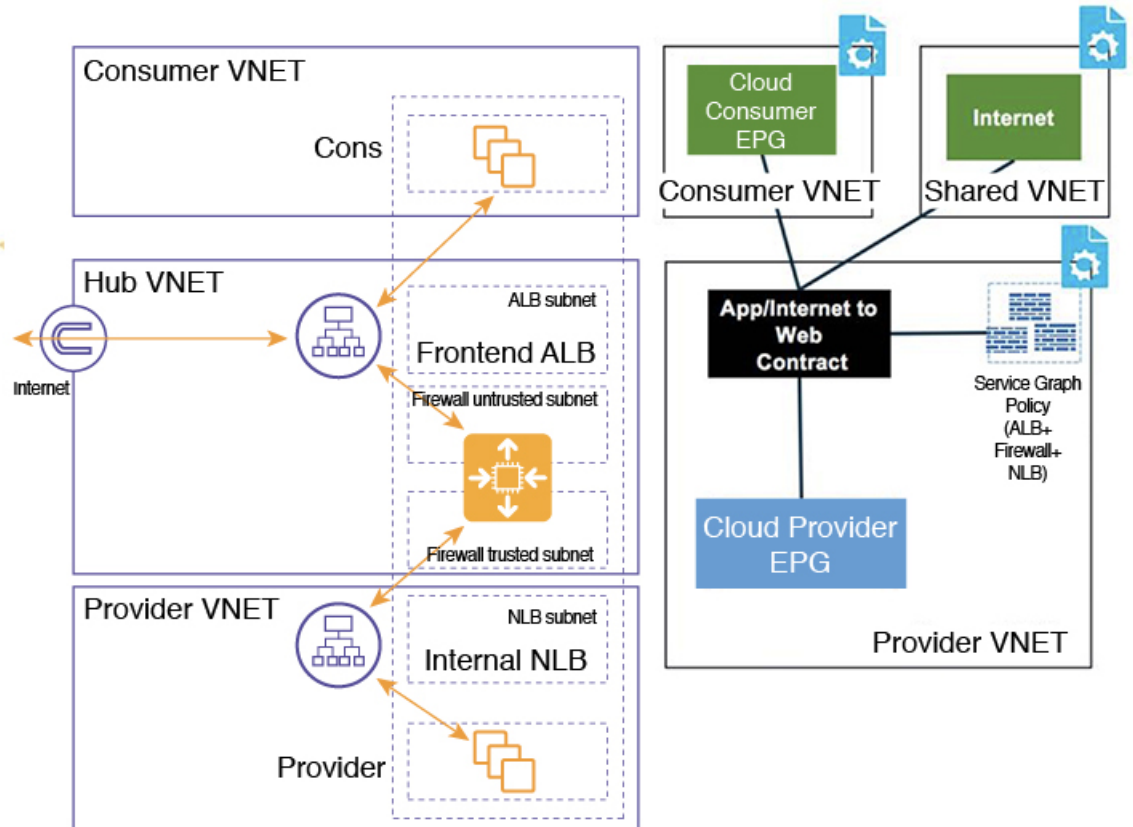
503031

2つの個別のVNetでのコンシューマおよびプロバイダー EPG を使用したVNetのハブ

このユースケースは、ハブ VNet、2つの個別の VNet 内のコンシューマ EPG とプロバイダー EPG の3つの VNet を使用した構成例です。

- フロントエンド ALB とファイアウォールは、コンシューマとプロバイダーの EPG の間にあるハブ VNet 内に挿入されます。
- 内部 NLB はプロバイダー EPG に挿入されます。
- コンシューマ エンドポイントは、フロントエンドの ALB VIP にトラフィックを送信し、ファイアウォールに転送します。
- ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP にフローが流れます。
- 内部 NLB は、バックエンドプロバイダーエンドポイントへのトラフィックを負荷分散します。

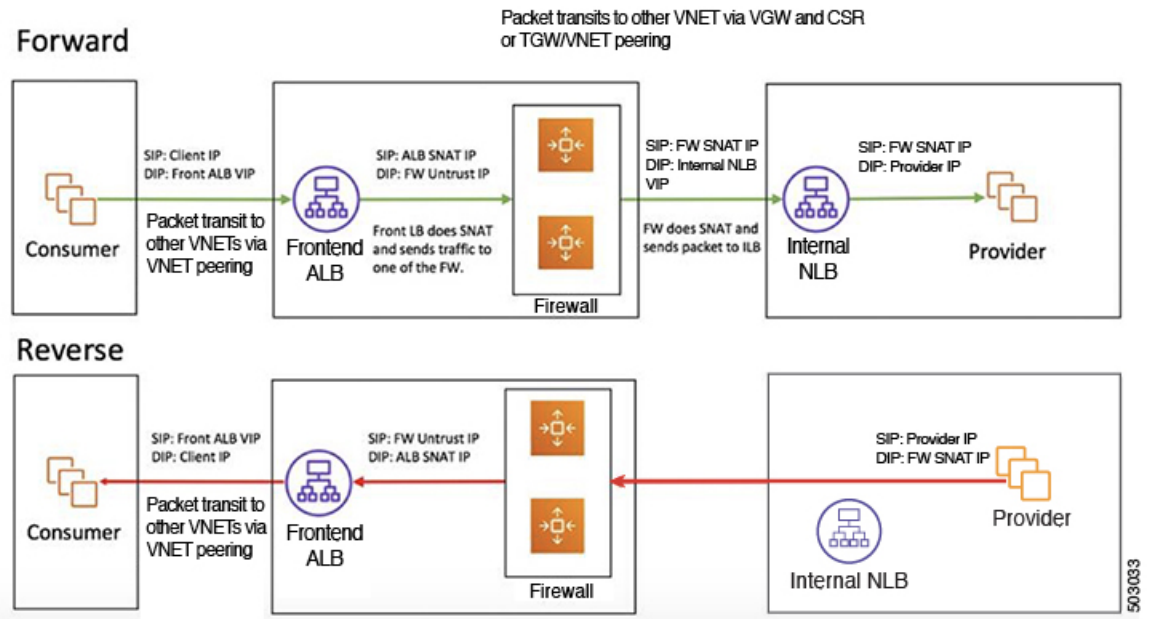
このユースケースでは、フロントエンド ALB または内部 NLB の代わりにサードパーティのロードバランサを使用できます。このユースケースで使用されるすべてのレイヤ4からレイヤ7サービス デバイスに専用サブネットがあることを確認します。



この図では次のようになっています。

- コンシューマ EPG はコンシューマ VNet にあります。
- プロバイダー EPG と内部 NLB はプロバイダー VNet にあります。
- フロントエンド ALB とファイアウォールはハブ VNet にあります
- アプリケーションロードバランサ、ネットワークロードバランサ（またはサードパーティのロードバランサ）、およびファイアウォールは、VNet 内に独自のサブネットを持つ必要があります。

両方向のパケットフローを次の図に示します。



クラウドネイティブおよびサードパーティ サービスによるサービス グラフの使用例

以下は、リダイレクトの有無にかかわらず、クラウドネイティブおよびサードパーティ サービスを使用したサービスグラフのユースケースの例です。詳細、ガイドラインおよび制限事項については、[クラウドネイティブおよびサードパーティ サービスでのサービス グラフの使用 \(200 ページ\)](#) を参照してください。

リダイレクトのないユースケースの例

以下は、リダイレクトのないクラウドネイティブおよびサードパーティのサービスを使用したサービスグラフのユースケースの例です。

これらの各ユースケースのプロセスの一部として、クラウドサービス EPG を構成します。クラウドサービス EPG を構成している場合は、サブネットごとの NSG 構成を有効にする必要があります。詳細については、[セキュリティグループ \(43 ページ\)](#) および [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照してください。

- インターネットインバウンドトラフィックの単一ノードサービスグラフ：プロバイダーとしての非管理サービス EPG (231 ページ)
- インターネットインバウンドトラフィックの単一ノードサービスグラフ：プロバイダーとしてのクラウドネイティブサービス EPG (233 ページ)

- インターネットインバウンドトラフィックの2ノードサービスグラフ：プロバイダーとしてのクラウドネイティブ管理対象サービス EPG (234 ページ)
- インターネットインバウンドトラフィックの3ノードサービスグラフ：プロバイダとしてのクラウドネイティブ管理対象サービス EPG (236 ページ)

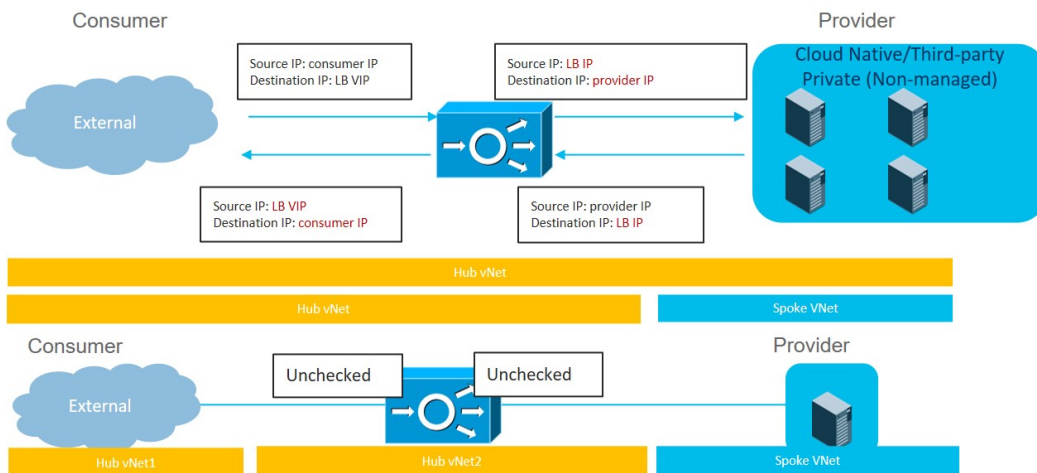


(注) 次の各ユースケースでは、プロバイダーとしてサービス EPG を使用する、単一ノード、2ノード、および3ノードのサービスグラフを使用する同様のトポロジを、クラウドの東西トラフィックに対してサポートできます。これらのユースケースでは、コンシューマはクラウド EPG になり、使用されるロードバランサは内部ロードバランサになります。

インターネットインバウンドトラフィックの単一ノードサービスグラフ：プロバイダーとしての非管理サービス EPG

このユースケースには、サービスノードがロードバランサ（アプリケーションロードバランサ、ネットワークロードバランサ、またはサードパーティのロードバランサ）である単一ノードサービスグラフがあります。

このユースケースでは、サービス EPG はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。サービスエンドポイントは動的に学習され、アプリケーションロードバランサまたはネットワークロードバランサに追加されます。



このユースケースを構成するには：

1. コンシューマー側で外部 EPG を作成します。
これらの手順については、[Cisco Cloud Network Controller GUI を使用した外部 EPG の作成 \(89 ページ\)](#) を参照してください。この外部 EPG の `infra` テナントを選択します。
2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセスタイプをサービス EPG に割り当てます。

これらの手順については、次の設定を使用して [Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#) を参照してください。

- **サービス タイプ** : 展開の種類に応じて、サポートされているサービス タイプ (詳細については [クラウド サービスエンドポイント グループ \(35 ページ\)](#) を参照)。たとえば、Azure Storage は、Cloud Native 展開タイプでサポートされるサービス タイプです。
- **展開タイプ** : Cloud Native またはThird-Party
- **アクセス タイプ** : Private

3. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

次のように選択します。

- **[デバイスの作成 (Create Device)]** ウィンドウで、ハブ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** として **[アプリケーション ロードバランサ (Application Load Balancer)]** または **[ネットワーク ロードバランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** エリアで **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、アプリケーション ロードバランサまたはネットワーク ロードバランサをドラッグアンドドロップします。
- ハブ VNet のアプリケーション ロードバランサまたはネットワーク ロードバランサの **[サービス ノード (Service Node)]** ウィンドウで、**[コンシューマ コネクタ タイプ (Consumer Connector Type)]** と **[プロバイダ コネクタ タイプ (Provider Connector Type)]** のボックスをオフのままにします。

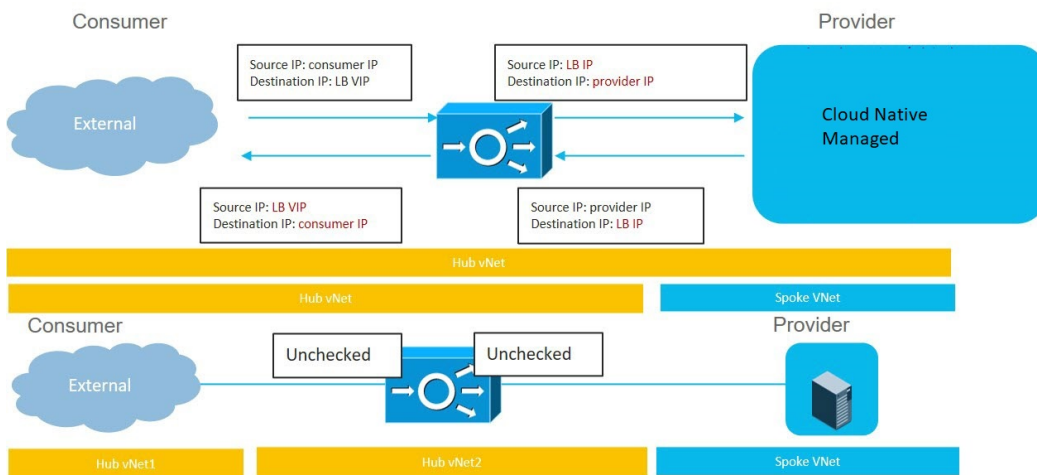
4. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

インターネットインバウンドトラフィックの単一ノードサービスグラフ：プロバイダーとしてのクラウドネイティブサービス EPG

このユースケースには、サービスノードがロードバランサ（アプリケーションロードバランサ、ネットワークロードバランサ、またはサードパーティのロードバランサ）である単一ノードサービスグラフがあります。

このユースケースでは、サービス EPG はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。



このユースケースを構成するには：

1. コンシューマー側で外部 EPG を作成します。

これらの手順については、[Cisco Cloud Network Controller GUI](#) を使用した外部 EPG の作成 (89 ページ) を参照してください。この外部 EPG の infra テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセスタイプをサービス EPG に割り当てます。

これらの手順については、次の設定を使用して [Cisco Cloud Network Controller GUI](#) を使用したサービス EPG の作成 (97 ページ) を参照してください。

- **サービスタイプ**：展開の種類に応じて、サポートされているサービスタイプ（詳細については [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照）。たとえば、Azure ApiManagement Services は、Cloud Native Managed 展開タイプでサポートされるサービスタイプです。
- **展開タイプ**：Cloud Native Managed
- **アクセスタイプ**：Public and Private

3. サービスグラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI](#) を使用したサービスデバイスの作成 (261 ページ) を参照してください。

次のように選択します。

- [デバイスの作成 (Create Device)] ウィンドウで、ハブ VNet のサービス デバイスを作成します。
 - [テナント (Tenant)] フィールドで、[インフラ (infra)] テナントを選択します。
 - [サービス タイプ (Service Type)] として [アプリケーション ロードバランサ (Application Load Balancer)] を選択し、[サブネット (Subnets)] エリアで [サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- [サービス グラフの作成 (Create Service Graph)] ウィンドウで、アプリケーション ロードバランサをドラッグアンドドロップします。
- ハブ VNet のアプリケーション ロードバランサの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のボックスをオフのままにします。

4. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

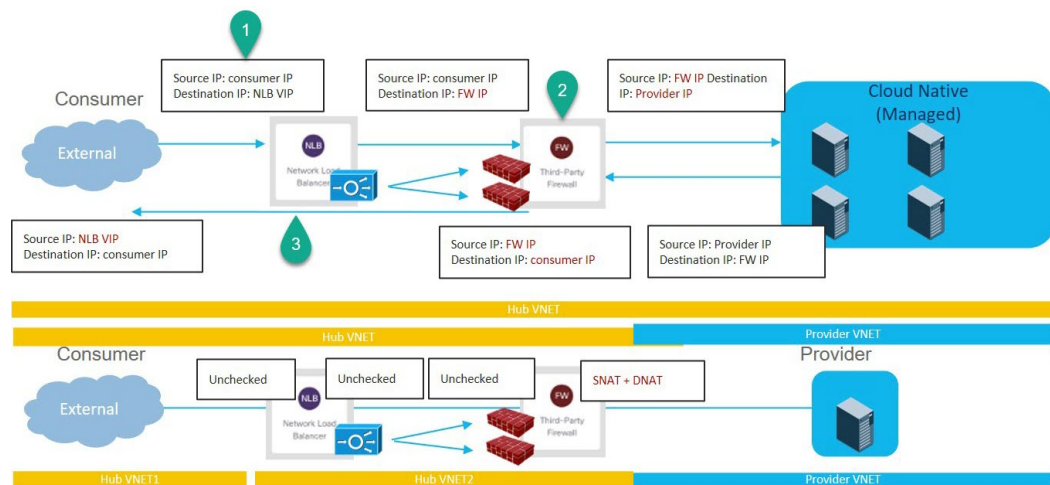
インターネットインバウンドトラフィックの2ノードサービスグラフ：プロバイダーとしてのクラウドネイティブ管理対象サービス EPG

このユースケースには2ノードのサービスグラフがあり、サービスノードはネットワークロードバランサとファイアウォールです。この2ノードサービスグラフはリダイレクトを使用しないため、SNAT+DNATはファイアウォールで実行されます。DNATedアドレスは、ネットワークロードバランサまたは同等のサービスであると想定されます。このユースケースでは、サービスグラフは、ロードバランサのサブネットへのルートの到達可能性のみを確立します。

このユースケースでは、サービス EPG はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックはネットワークロードバランサのパブリックVIPに送信され、ファイアウォール (DNAT) へのトラフィックが負荷分散されます。
2. SNAT+DNAT はファイアウォールで実行されます。
3. リターントラフィックの場合、Azure はソース IP をネットワークロードバランサのパブリックVIPに変換します。



このユースケースを構成するには：

1. コンシューマー側で外部 EPG を作成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用した外部 EPG の作成 \(89 ページ\)](#) を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセスタイプをサービス EPG に割り当てます。

これらの手順については、次の設定を使用して [Cisco Cloud Network Controller GUI を使用したサービス EPG の作成 \(97 ページ\)](#) を参照してください。

- **サービスタイプ**：展開の種類に応じて、サポートされているサービスタイプ（詳細については [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照）。たとえば、Azure Kubernetes Services (AKS) は、Cloud Native Managed 展開タイプでサポートされるサービスタイプです。
- **展開タイプ**：Cloud Native Managed
- **アクセスタイプ**：Private

3. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで

- **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
- **[サービスタイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。

- [サービス タイプ (Service Type)] として [ネットワーク ロードバランサ (Network Load Balancer)] を選択し、[サブネット (Subnets)] エリアで [サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - [サービス タイプ (Service Type)] として [サードパーティ ファイアウォール (Third-Party Firewall)] を選択し、[VRF] フィールドでセカンダリ VRF を選択します。
- [サービス グラフの作成 (Create Service Graph)] ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
- ネットワーク ロード バランサ
 - サードパーティ ファイアウォール
- ネットワーク ロードバランサの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のチェックボックスをオフのままにします。
- サードパーティ ファイアウォールの [サービス ノード (Service Node)] ウィンドウで、次の手順を実行します。
- [コンシューマ コネクタ タイプ (Consumer Connector Type)] フィールドで、ボックスをオフのままにします。
 - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、[プロバイダ コネクタ タイプ (Third-Party Firewall)] フィールドで、[SNAT] および [DNAT] オプションの隣のボックスにチェックを入れます。

4. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

インターネットインバウンドトラフィックの3ノードサービスグラフ：プロバイダとしてのクラウドネイティブ管理対象サービス EPG

このユースケースには3ノードのサービスグラフがあり、サービスノードは次のとおりです。

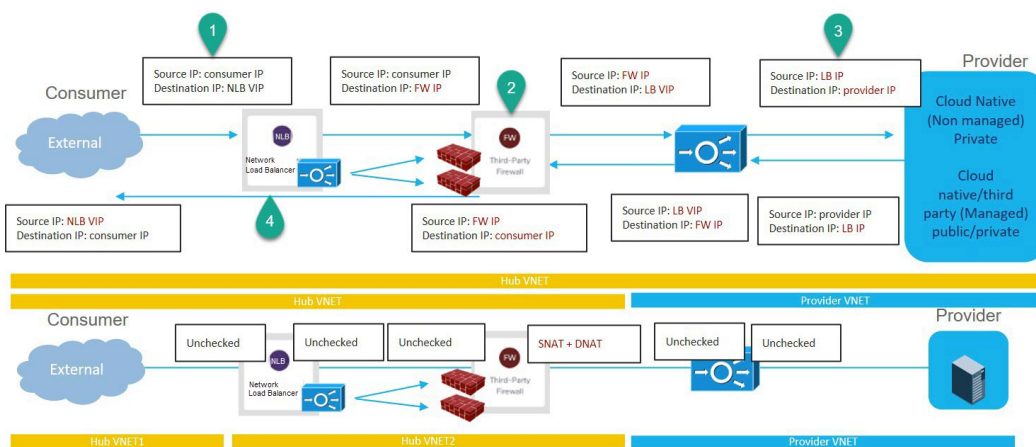
- 最初のサービス デバイス: ハブ VNet のネットワーク ロードバランサ
- 2番目のサービス デバイス: ハブ VNet のファイアウォール
- サードサービス デバイス: ハブ VNet またはスポーク VNet 内のサードパーティのロードバランサ

この3ノードサービスグラフはリダイレクトを使用しないため、SNAT+DNATはファイアウォールで実行されます。DNATedアドレスは、ロードバランサまたは同等のサービスであると想定されます。

このユースケースでは、サービス EPG はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックは最初のサービス デバイスであるネットワーク ロードバランサのパブリック VIP に送信され、次にファイアウォール (DNAT) へのトラフィックの負荷分散が行われます。
2. SNAT+DNAT は、2 番目のサービス デバイスであるファイアウォールで実行されます。
3. トラフィックは、SNAT が構成されているサードパーティのロードバランサであるサードサービス デバイスに移動します。
4. リターン トラフィックの場合、Azure はソース IP をネットワーク ロードバランサのパブリック VIP に変換します。



このユースケースを構成するには：

1. コンシューマー側で外部 EPG を作成します。
これらの手順については、[Cisco Cloud Network Controller GUI](#)を使用した外部 EPG の作成 (89 ページ) を参照してください。この外部 EPG の infra テナントを選択します。
2. プロバイダー側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

次の設定によるこれらの手順については、[Cisco Cloud Network Controller GUI](#)を使用したサービス EPG の作成 (97 ページ) を参照してください。

- **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ (詳細については [クラウドサービスエンドポイントグループ](#) (35 ページ) を参照)。たとえば、Azure ApiManagement Services は、Cloud Native Managed 展開タイプでサポートされるサービス タイプです。

- 展開タイプ : Cloud Native Managed
- アクセスタイプ : Private

3. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

このユース ケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - 最初のデバイスとして、**[サービス タイプ (Service Type)]** として **[アプリケーション ロードバランサ (Application Load Balancer)]** を選択し、**[サブ ネット (Subnets)]** エリアで **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - 2 番目のサービス デバイスについては、**[サービス タイプ (Service Type)]** として **[サードパーティ ファイアウォール (Third-Party Firewall)]** を選択し、**[VRF]** フィールドで、セカンダリ VRF を選択します。
 - 3 番目のサービス デバイスがハブ VNet にある場合は、**[サービス タイプ (Service Type)]** として **[サードパーティ ロードバランサ (Third-Party Load Balancer)]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加 (Add Interface)]** をクリックしてインターフェイスの詳細を設定します。
- **[デバイスの作成 (Create Device)]** ウィンドウで、次に、必要に応じて (3 番目のサービス デバイスがプロバイダ VNet にある場合)、プロバイダー VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、プロバイダ テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドで **[サードパーティ ロードバランサ (Third-Party Load Balancer)]** を選択し、**[サブ ネット (Subnets)]** エリアで **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびプロバイダ VRF のサブネットを選択します。
- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - アプリケーション ロードバランサ (ハブ VNet 用)

- サードパーティ ファイアウォール (ハブ VNet 用)
 - サードパーティのロードバランサ (ハブまたはプロバイダー VNet 用)
 - ハブ VNet のアプリケーション ロードバランサの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のボックスをオフのままにします。
 - サードパーティ ファイアウォールの [サービス ノード (Service Node)] ウィンドウで、次の手順を実行します。
 - [コンシューマ コネクタ タイプ (Consumer Connector Type)] フィールドで、ボックスをオフのままにします。
 - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、[プロバイダ コネクタ タイプ (Third-Party Firewall)] フィールドで、[SNAT] および [DNAT] オプションの隣のボックスにチェックを入れます。
 - SNAT がサードパーティのロードバランサで構成されていることを確認します。
4. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

リダイレクトの使用例

以下は、リダイレクトを備えたクラウド ネイティブ サービスとサードパーティ サービスを使用したサービス グラフのユースケースの例です。

これらの各ユースケースのプロセスの一部として、クラウド サービス EPG を構成します。クラウド サービス EPG を構成している場合は、[サブネットごとの NSG 構成を有効にする必要があります](#)。詳細については、[セキュリティグループ \(43 ページ\)](#) および [クラウド サービス エンドポイント グループ \(35 ページ\)](#) を参照してください。

- [インターネット アウトバウンドの 2 ノード サービス グラフ \(240 ページ\)](#)
- [East-West の 2 ノード サービス グラフ \(242 ページ\)](#)
- [SNAT オプションを使用した East-West の 2 ノード サービス グラフ \(245 ページ\)](#)
- [エクスプレス ルート ゲートウェイ経由の受信トラフィックの 2 ノード サービス グラフ \(247 ページ\)](#)
- [SNAT オプションを使用したエクスプレス ルート ゲートウェイ経由のインバウンドトラフィックの 2 ノード サービス グラフ \(249 ページ\)](#)

- [エクスプレスルート ゲートウェイ経由の受信トラフィックの3 ノード サービス グラフ \(252 ページ\)](#)

インターネットアウトバウンドの2ノードサービスグラフ

このユースケースには2ノードのサービスグラフがあり、サービスノードはネットワークロードバランサとファイアウォールです。このユースケースでは、コンシューマ側でリダイレクトが有効になっており、ファイアウォールでSNATが有効になっています。

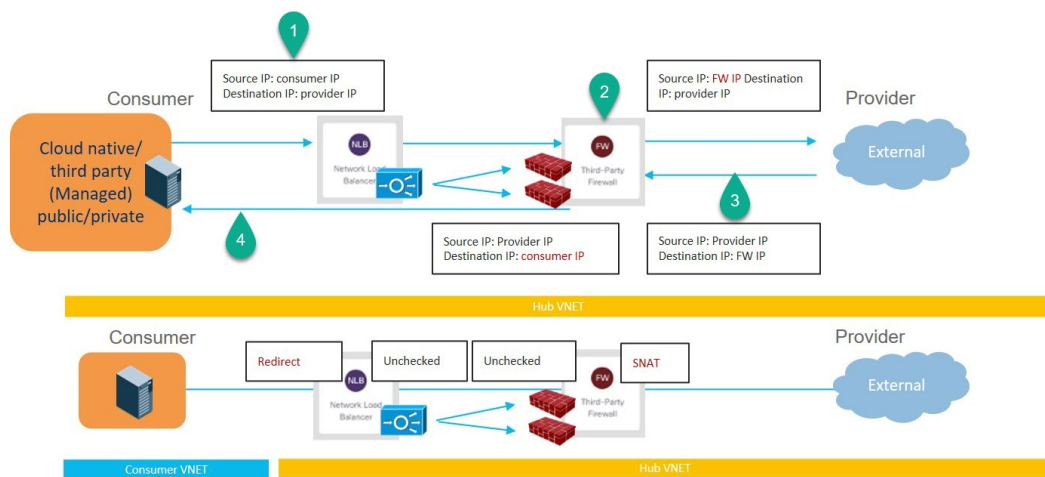
このユースケースでは、サービス EPG はコンシューマであり、外部 EPG はプロバイダー側で構成されます。



- (注) レイヤ4からレイヤ7のサービスグラフが、インターネットの到達可能性のために独自のUDRを使用するPaaSに使用されている場合は、外部EPGで0.0.0.0/0を使用しないことをお勧めします。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターントラフィックは、ファイアウォールのSNAT IPアドレスに戻ります。
4. 戻り方向のこの時点では、リターントラフィックはネットワークロードバランサを通過しません。



このユースケースを構成するには：

1. プロバイダー側で外部 EPG を作成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用した外部 EPG の作成 \(89 ページ\)](#) を参照してください。

- この外部 EPG の `infra` テナントを選択します。
- `0.0.0.0/0` サブネット で外部 EPG を構成しないでください。

2. コンシューマ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

次の設定によるこれらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス EPG の作成 \(97 ページ\)](#) を参照してください。

- **サービス タイプ** : 展開の種類に応じて、サポートされているサービス タイプ (詳細については [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照)。たとえば、Azure Kubernetes Services (AKS) は、Cloud Native Managed 展開タイプでサポートされるサービス タイプです。
- **展開タイプ** : Cloud Native Managed
- **アクセス タイプ** : Private

3. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

このユース ケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として **[ネットワーク ロードバランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** エリアで **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - **[サービス タイプ (Service Type)]** として **[サードパーティ ファイアウォール (Third-Party Firewall)]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロード バランサ

- サードパーティ ファイアウォール
- ネットワーク ロードバランサの [サービス ノード (Service Node)] ウィンドウで、次の手順を実行します。
 - [コンシューマ コネクタ タイプ (Consumer Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
 - [プロバイダ コネクタ タイプ (Provider Connector Type)] フィールドで、ボックスをオフのままにします。
- サードパーティ ファイアウォールの [サービス ノード (Service Node)] ウィンドウで、次の手順を実行します。
 - [コンシューマ コネクタ タイプ (Consumer Connector Type)] フィールドで、ボックスをオフのままにします。
 - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、[プロバイダ コネクタ タイプ (Provider Connector Type)] フィールドで、[SNAT] オプションの隣のボックスにチェックを入れます。

4. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

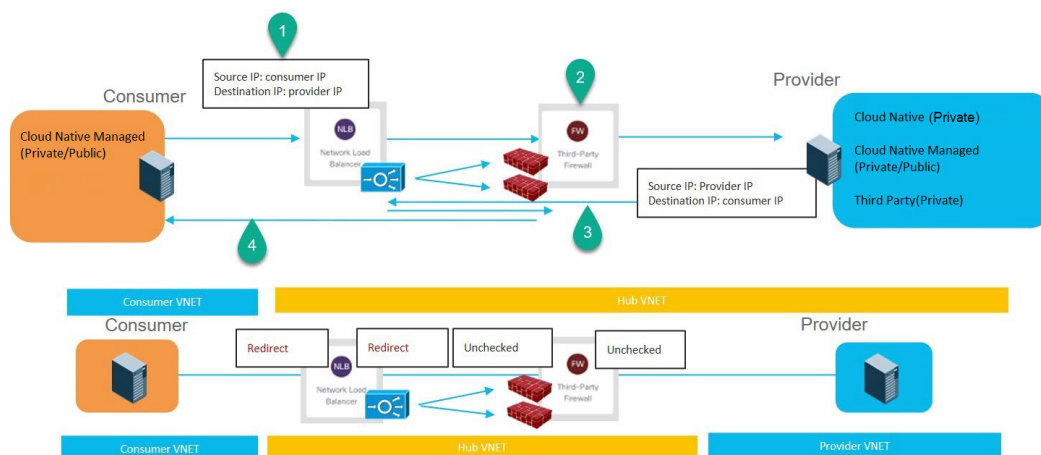
East-West の 2 ノード サービス グラフ

このユースケースには2ノードのサービスグラフがあり、サービスノードはネットワークロードバランサとファイアウォールです。このユースケースでは、コンシューマ側とプロバイダー側の両方でリダイレクトが有効になっています。

このユースケースでは、コンシューマとプロバイダーはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユースケースでは、ファイアウォールで SNAT は実行されません。
3. リターン トラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
4. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユースケースを構成するには：

1. コンシューマまたはプロバイダーのサービス EPG を使用している場合は、サービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

次の設定によるこれらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス EPG の作成 \(97 ページ\)](#) を参照してください。

- コンシューマとしてのサービス EPG には、次の設定があります。
 - **サービスタイプ**：展開の種類に応じて、サポートされているサービスタイプ（詳細については [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照）。たとえば、Azure Kubernetes Services (AKS) は、Cloud Native Managed 展開タイプでサポートされるサービスタイプです。
 - **展開タイプ**：Cloud Native Managed
 - **アクセスタイプ**：Private
- プロバイダーとしてのサービス EPG には、次の設定があります。
 - **サービスタイプ**：展開の種類に応じて、サポートされているサービスタイプ（詳細については [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照）。たとえば、Azure Storage File は、Cloud Native 展開タイプでサポートされるサービスタイプです。
 - **展開タイプ**：Cloud Native
 - **アクセスタイプ**：Private

2. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として **[ネットワーク ロード バランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** 領域で **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - **[サービス タイプ (Service Type)]** として **[サードパーティ ファイアウォール (Third-Party Firewall)]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
 - **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロード バランサ
 - サードパーティ ファイアウォール
 - ハブ NLB の **[サービス ノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマ コネクタ タイプ (Consumer Connector Type)]** フィールドで、**[リダイレクト (Redirect)]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
 - **[プロバイダ コネクタ タイプ (Provider Connector Type)]** フィールドで、**[リダイレクト (Redirect)]** オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。
 - サードパーティ ファイアウォールの **[サービス ノード (Service Node)]** ウィンドウで、**[コンシューマ コネクタ タイプ (Consumer Connector Type)]** と **[プロバイダ コネクタ タイプ (Provider Connector Type)]** のボックスをオフのままにします。
3. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

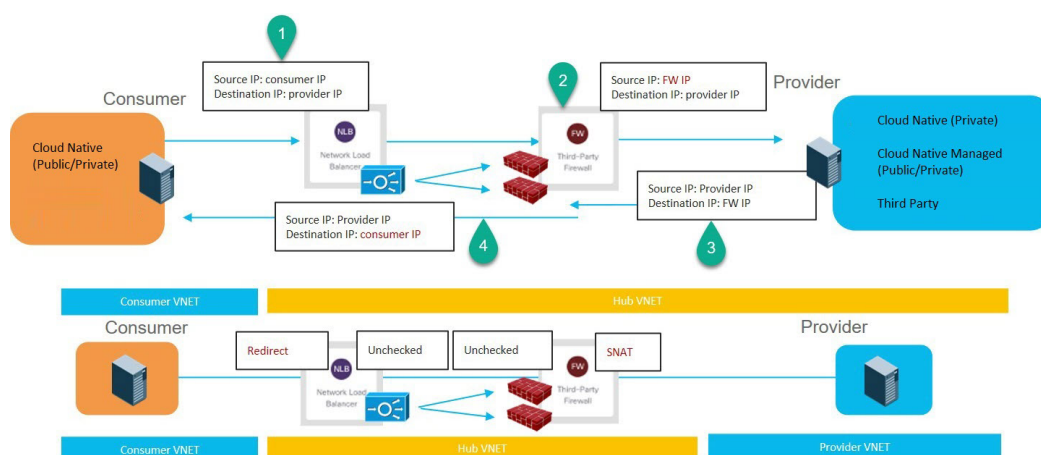
SNAT オプションを使用した East-West の 2 ノード サービス グラフ

このユースケースには2ノードのサービスグラフがあり、サービスノードはネットワークロードバランサとファイアウォールです。このユースケースでは、リダイレクトはコンシューマ側でのみ有効になっており、SNAT はファイアウォールで有効になっています。

このユースケースでは、コンシューマとプロバイダーはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターントラフィックは、ファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、リターントラフィックはネットワークロードバランサを通過しません。



このユースケースを構成するには：

1. コンシューマまたはプロバイダーのサービス EPG を使用している場合は、サービス EPG を作成し、適切な展開タイプとアクセスタイプをサービス EPG に割り当てます。

次の設定によるこれらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス EPG の作成 \(97 ページ\)](#) を参照してください。

- コンシューマとしてのサービス EPG には、次の設定があります。
 - **サービスタイプ**：展開の種類に応じて、サポートされているサービスタイプ（詳細については [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照）。たとえば、Azure Active Directory Domain Services は、Cloud Native Managed 展開タイプでサポートされるサービスタイプです。
 - **展開タイプ**：Cloud Native Managed
 - **アクセスタイプ**：Private

- プロバイダーとしてのサービス EPG には、次の設定があります。
 - **サービス タイプ** : 展開の種類に応じて、サポートされているサービスタイプ（詳細については [クラウド サービスエンドポイント グループ \(35 ページ\)](#) を参照）。たとえば、Azure Storage File は、Cloud Native 展開タイプでサポートされるサービス タイプです。
 - **展開タイプ** : Cloud Native
 - **アクセス タイプ** : Private

2. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

このユース ケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として **[ネットワーク ロードバランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** エリアで **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - **[サービス タイプ (Service Type)]** として **[サードパーティ ファイアウォール (Third-Party Firewall)]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロードバランサ
 - サードパーティ ファイアウォール
- ネットワーク ロードバランサの **[サービス ノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマ コネクタ タイプ (Consumer Connector Type)]** フィールドで、**[リダイレクト (Redirect)]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。

- **[プロバイダコネクタタイプ (Provider Connector Type)]** フィールドで、ボックスをオフのままにします。
- サードパーティファイアウォールの **[サービスノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマコネクタタイプ (Consumer Connector Type)]** フィールドで、ボックスをオフのままにします。
 - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダコネクタタイプ (Provider Connector Type)]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

3. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービスグラフにアタッチします。

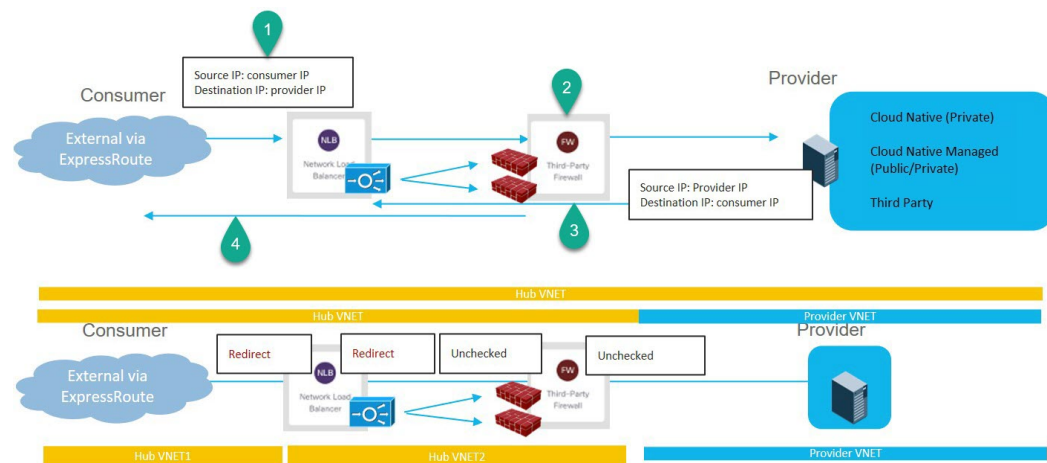
エクスプレスルートゲートウェイ経由の受信トラフィックの2ノードサービスグラフ

このユースケースには2ノードのサービスグラフがあり、サービスノードはネットワークロードバランサとファイアウォールです。このユースケースでは、コンシューマ側とプロバイダー側の両方でリダイレクトが有効になっています。

このユースケースでは、サービス EPG がプロバイダーであり、エクスプレスルートがコンシューマ側にあります。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユースケースでは、ファイアウォールで SNAT は実行されません。
3. リターントラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
4. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユースケースを構成するには：

1. プロバイダー側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

次の設定によるこれらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス EPG の作成 \(97 ページ\)](#) を参照してください。

- **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については [クラウド サービスエンドポイント グループ \(35 ページ\)](#) を参照）。たとえば、Azure Active Directory Domain Services は、Cloud Native Managed 展開タイプでサポートされるサービス タイプです。
- **展開タイプ**：Cloud Native Managed
- **アクセス タイプ**：Private

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

これらの手順については、[#unique_140](#) を参照してください。

3. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として **[ネットワーク ロードバランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** エリアで

[サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。

- [サービス タイプ (Service Type)] として [サードパーティ ファイアウォール (Third-Party Firewall)] を選択し、[VRF] フィールドでセカンダリ VRF を選択します。

- [サービス グラフの作成 (Create Service Graph)] ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。

- ネットワーク ロード バランサ
- サードパーティ ファイアウォール

- ネットワーク ロード バランサの [サービス ノード (Service Node)] ウィンドウで、次の手順を実行します。

- [コンシューマ コネクタ タイプ (Consumer Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。

- [プロバイダ コネクタ タイプ (Provider Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れ、消費者側でリダイレクト機能を有効にします。

- サードパーティ ファイアウォールの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のボックスをオフのままにします。

4. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

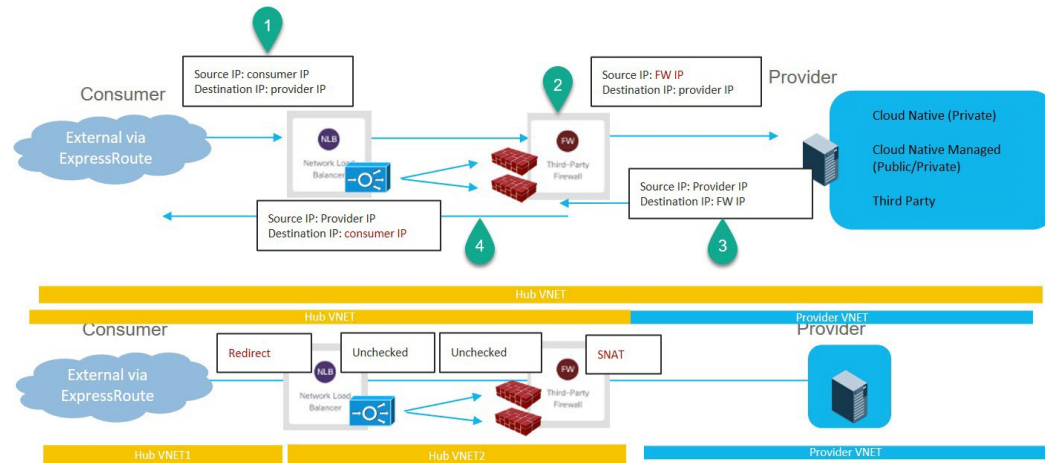
SNATオプションを使用したエクスプレスルートゲートウェイ経由のインバウンドトラフィックの2ノードサービス グラフ

このユースケースには2ノードのサービス グラフがあり、サービス ノードはネットワーク ロード バランサとファイアウォールです。このユースケースでは、リダイレクトはコンシューマ側でのみ有効になっており、SNAT はファイアウォールで有効になっています。

このユースケースでは、サービス EPG はプロバイダーであり、エクスプレス ルートはコンシューマ側にあります。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターントラフィックは、ファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、リターントラフィックはネットワークロードバランサを通過しません。



このユースケースを構成するには：

1. プロバイダー側でサービス EPG を作成し、適切な展開タイプとアクセスタイプをサービス EPG に割り当てます。

次の設定によるこれらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス EPG の作成 \(97 ページ\)](#) を参照してください。

- **サービスタイプ**：展開の種類に応じて、サポートされているサービスタイプ（詳細については [クラウドサービスエンドポイントグループ \(35 ページ\)](#) を参照）。たとえば、Redis Cache は、Cloud Native Managed 展開タイプでサポートされるサービスタイプです。
- **展開タイプ**：Cloud Native Managed
- **アクセスタイプ**：Private

2. コンシューマ側にエクスプレスルートゲートウェイを展開します。

これらの手順については、[#unique_140](#) を参照してください。

3. サービスグラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービスデバイスの作成 \(261 ページ\)](#) を参照してください。

このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として **[ネットワーク ロードバランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** エリアで **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - **[サービス タイプ (Service Type)]** として **[サードパーティ ファイアウォール (Third-Party Firewall)]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
- **[サービス グラフの作成 (Create Service Graph)]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
 - ネットワーク ロード バランサ
 - サードパーティ ファイアウォール
- ネットワーク ロードバランサの **[サービス ノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマ コネクタ タイプ (Consumer Connector Type)]** フィールドで、**[リダイレクト (Redirect)]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
 - **[プロバイダ コネクタ タイプ (Provider Connector Type)]** フィールドで、ボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード (Service Node)]** ウィンドウで、次の手順を実行します。
 - **[コンシューマ コネクタ タイプ (Consumer Connector Type)]** フィールドで、ボックスをオフのままにします。
 - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダ コネクタ タイプ (Provider Connector Type)]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ4～レイヤ7サービスを展開します。

これらの手順については、[Cisco Cloud 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](#)（275ページ）を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

エクスプレスルート ゲートウェイ経由の受信トラフィックの3ノードサービス グラフ

このユースケースには3ノードのサービスグラフがあり、サービスノードは次のとおりです。

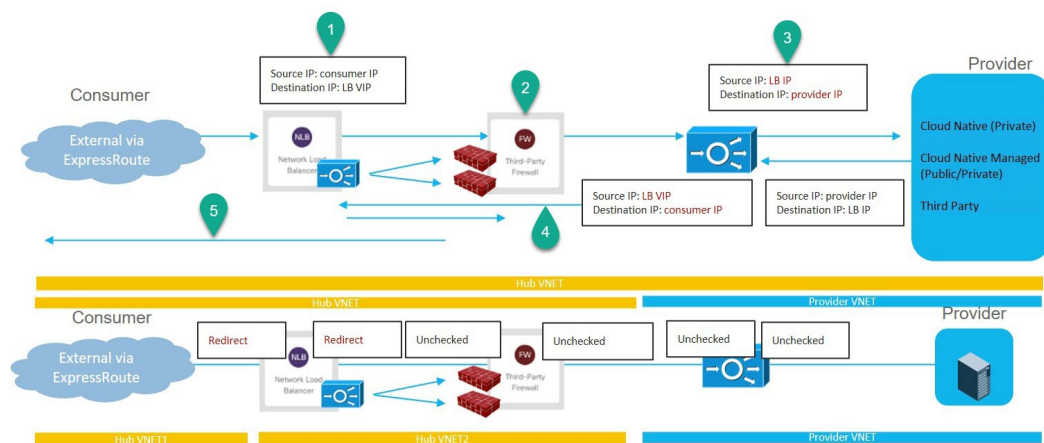
- 最初のサービス デバイス: ハブ VNet のネットワーク ロードバランサ
- 2 番目のサービス デバイス : ハブ VNet のファイアウォール
- 3 番目のサービス デバイス : ハブまたはスポーク VNet のアプリケーション ロードバランサ

このユースケースでは、コンシューマ側とプロバイダー側の両方でリダイレクトが有効になっています。

このユースケースでは、サービス EPG はプロバイダーです。エクスプレスルートはコンシューマ側にあり、コンシューマはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユースケースで実行されます。

1. トラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユースケースでは、ファイアウォールで SNAT は実行されません。
3. トラフィックは、SNAT が構成されている 3 番目のサービス デバイスであるアプリケーションロードバランサに移動します。
4. リターントラフィックはネットワークロードバランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
5. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユースケースを構成するには：

1. プロバイダー側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

次の設定によるこれらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス EPG の作成 \(97 ページ\)](#) を参照してください。

- **サービス タイプ** : 展開の種類に応じて、サポートされているサービス タイプ (詳細については [クラウド サービスエンドポイント グループ \(35 ページ\)](#) を参照)。たとえば、Azure ApiManagement Services は、Cloud Native Managed 展開タイプでサポートされるサービス タイプです。
- **展開タイプ** : Cloud Native Managed
- **アクセス タイプ** : Private

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

これらの手順については、[#unique_140](#) を参照してください。

3. サービス グラフを構成します。

これらの手順については、[Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 \(261 ページ\)](#) を参照してください。

このユース ケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成 (Create Device)]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、**[インフラ (infra)]** テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドでサービス デバイスのタイプを選択します。
 - **[サービス タイプ (Service Type)]** として **[ネットワーク ロード バランサ (Network Load Balancer)]** を選択し、**[サブネット (Subnets)]** 領域で **[サブネットの追加 (Add Subnet)]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
 - **[サービス タイプ (Service Type)]** として **[サードパーティ ファイアウォール (Third-Party Firewall)]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
- **[デバイスの作成 (Create Device)]** ウィンドウで、次にプロバイダ VNet のサービス デバイスを作成します。
 - **[テナント (Tenant)]** フィールドで、プロバイダ テナントを選択します。
 - **[サービス タイプ (Service Type)]** フィールドで **[アプリケーション ロードバランサ (Application Load Balancer)]** を選択し、**[サブネット (Subnets)]** エリアで

[サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびプロバイダー VRF のサブネットを選択します。



(注) 内部 NLB の代わりにサードパーティのロードバランサを使用できます。[サービス タイプ (Service Type)] として [サードパーティ ロードバランサ (Third Party Load Balancer)] を選択します。[インターフェイスの追加 (Add Interface)] をクリックして、[VRF] を選択し、インターフェイスの詳細を設定します。

- [サービス グラフの作成 (Create Service Graph)] ウィンドウで、次のサービス デバイスをこの順序でドラッグアンドドロップします。
 - ネットワーク ロードバランサ (ハブ VNet 用)
 - サードパーティ ファイアウォール (ハブ VNet 用)
 - アプリケーション ロードバランサ (プロバイダー VNet 用)
- ハブ VNet のネットワーク ロードバランサの [サービス ノード (Service Node)] ウィンドウで、次のようにします。
 - [コンシューマ コネクタ タイプ (Consumer Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
 - [プロバイダ コネクタ タイプ (Provider Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。
- サードパーティ ファイアウォールの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のボックスをオフのままにします。
- プロバイダ VNet でネットワーク ロードバランサの [サービス ノード (Service Node)] ウィンドウで、[コンシューマ コネクタ タイプ (Consumer Connector Type)] と [プロバイダ コネクタ タイプ (Provider Connector Type)] のチェックボックスをオフのままにします。



(注) SNAT がサードパーティのロードバランサで構成されていることを確認します。

4. レイヤ 4 ~ レイヤ 7 サービスを展開します。

これらの手順については、[Cisco Cloud 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 \(275 ページ\)](#) を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

リダイレクトの注意事項と制約事項

リダイレクトの注意事項と制約事項は次のとおりです。

- レイヤ4～レイヤ7のすべてのサービス デバイスには、独自の専用サブネットが必要です。
- リージョン内の VRF 内レイヤ4～レイヤ7サービスへのリダイレクション：
 - コンシューマ EPG とプロバイダー EPG が同じ VNet にある場合、レイヤ4～レイヤ7サービスへのリダイレクトは、east-west 展開ではサポートされません。
 - 外部 EPG がプロバイダー EPG である場合、コンシューマ EPG とプロバイダー EPG が同じ VNet にあるかどうかに関係なく、レイヤ4からレイヤ7へのサービス リダイレクトが North-South 展開でサポートされます。
- リージョンでの VRF 間レイヤ4からレイヤ7サービスへのリダイレクト：
 - リージョン間レイヤ4～レイヤ7サービスへのリダイレクトがサポートされています。ただし、コンシューマ EPG とプロバイダー EPG は拡大しないでください。
 - リージョンでは、同じ VRF にコンシューマ EPG とプロバイダー EPG の両方を含めることはできません。たとえば、リージョン1にコンシューマ EPG のみがあり、リージョン2にプロバイダー EPG のみがある場合、これはサポートされますが、リージョン1にコンシューマ EPG とプロバイダー EPG の両方を含めることはできません。
 - コンシューマおよびプロバイダーの EPG は、サブネット ベースの EPG である必要があります。
- レイヤ4～レイヤ7サービスへのリダイレクションを伴うリージョン間サービス グラフの場合、サービス デバイスはプロバイダー EPG のリージョンに展開する必要があります。プロバイダ EPG がリージョン全体に拡張されている場合、サービス デバイスは各リージョンに展開する必要があります。
- プロバイダーとしての外部 EPG の場合、サービス デバイスはコンシューマ EPG に対してローカルなリージョンに展開する必要があります。コンシューマ EPG が複数のリージョンにまたがっている場合は、サービス デバイスを各リージョンに展開する必要があります。
- コンシューマ VNet とプロバイダー EPG の間では、サービス グラフを介して挿入できるリダイレクト デバイスは1つだけです。たとえば、コンシューマ EPG1 とコンシューマ EPG2 がコンシューマ VNet にあり、プロバイダー EPG3 がプロバイダー VNet にある場合、EPG1 と EPG3 間のコントラクト、および EPG2 と EPG3 間のコントラクトに同じリダイレクト デバイスを使用する必要があります。



(注) この制限は、クラウドプロバイダーがユーザ定義ルートの特定の接続先に対して1つのネクストホップのみを許可するためです。

• 次の表に、サポートされている、またはサポートされていない特定のリダイレクト構成に関する情報を示します。

- NLB はネットワーク ロードバランサの略
- ALB はアプリケーション ロードバランサの略
- FWはファイアウォールの略



(注) サードパーティのロードバランサへのリダイレクトはサポートされていません。

サービスチェーンオプション	スポークツースポーク		スポークツェ外部へ (コンシューマが話す)		外部ツースポークへ (コンシューマは外部)	
	VNet 内	VNet 間	VNet 内	VNet 間	VNet 内	VNet 間
NLB/ALB ¹ LB(SNAT) 1	サポート対象	サポート対象	サポート対象外	サポート対象外	サポート対象	サポート対象
FW (SNAT なし) ²	サポート対象外	サポート対象	サポート対象外	サポート対象外	サポート対象外	サポート対象外
FW (SNAT) ³	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象外	サポート対象外
<ul style="list-style-type: none"> • NLB²-FW(no SNAT)¹ • NLB²-FW(no SNAT)¹-NLB/ALB¹ • NLB²-FW(no SNAT)¹-LB(SNAT)¹ 	サポート対象外	サポート対象	サポート対象外	サポート対象外	サポート対象外	サポート対象外
NLB ⁴ -FW(SNAT) ⁵	サポート対象外	サポート対象	サポート対象	サポート対象	サポート対象外	サポート対象外
NLB/ALB ¹ -FW(SNAT+DNAT) ⁶ -NLB/ALB ¹ NLB/ALB ¹ -FW(ANT+DNAT) ⁶ -LB(SNAT) ¹ (リダイレクトなし)	サポート対象	サポート対象	非対応	非対応	サポート対象	サポート対象
NLB ¹ -LB(SNAT) ¹ (リダイレクトなし)	サポート対象	サポート対象	非対応	非対応	サポート対象	サポート対象

¹ Unchecked on both consumer and provider connector or options are not applicable for ALB.

² Redirect is enabled on both consumer and provider connector.

³ リダイレクトは、コンシューマ コネクタで有効になっています。プロバイダ コネクタで SNAT が有効になっています。

⁴ リダイレクトは、コンシューマコネクタで有効になっています。プロバイダーコネクタではオフになっています。

⁵ コンシューマ コネクタではチェックを外します。プロバイダー コネクタで SNAT が有効になっています。

⁶ コンシューマ コネクタではチェックされていません。プロバイダー コネクタで SNAT+DNAT が有効になっています。

Cisco Cloud Network Controller GUI を使用したセカンダリ VRF への新しい CIDR の追加

状況によっては、新しい CIDR を追加したり、セカンダリ VRF で既存の CIDR を編集したりする前に、VNet ピアリングを無効にする必要がある場合があります。これは、アクティブな VNet ピアリングがある場合、VNet 上の CIDR を更新できないという Azure の制限によるものです。CIDR を追加するには、最初にその VNet の VNet ピアリングを削除する必要があります。その後、CIDR を更新できます。CIDR を更新したら、VNet ピアリングを再度有効にすることができます。

これらの手順では、特定のインフラ VNet に関連付けられているすべての VNet ピアリングを削除するハブ ネットワーク ピアリングを無効にする手順について説明します。

- インフラ VNet に追加の CIDR が既に作成されているが、その既存の CIDR にサブネットを追加するだけでよい場合は、それらのサブネットを追加する前に、その特定のインフラ VNet のハブ ネットワーク ピアリングを無効にする必要はありません。既存の CIDR にサブネットを追加するには：
 1. その場合は、適切なクラウド コンテキスト プロファイルに移動します ([**アプリケーション管理 (Application Management)**] > [**クラウド コンテキスト プロファイル (Cloud Context Profiles)**])。
 2. サブネットを既存の CIDR に追加するクラウド コンテキスト プロファイルをダブルクリックし、[ステップ 10 \(259 ページ\)](#) に移動して、新しいサブネットを既存の CIDR に追加します。
- インフラ VNet に新しい CIDR を追加する場合、またはインフラ VNet で CIDR を削除するか、他の方法 (サブネットの追加以外) で CIDR を編集する場合は、その特定のインフラ VNet のハブ ネットワーク ピアリングを無効にする必要があります。CIDR を追加した後、ハブ ネットワーク ピアリングを再度有効にします。以下の手順では、それらの手順について説明します。



(注) 新しい CIDR をセカンダリ VRF に追加しており、次のリリースで実行しているマルチサイト展開がある場合：

- Cisco Cloud Network Controller のリリース 5.2 (1) 以降
- Nexus Dashboard Orchestrator のリリース 3.3 以降

新しい CIDR を追加し、ハブ ネットワーク ピアリングを再度有効にしたら、Nexus Dashboard Orchestrator でサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開する前に、CIDR が起動するまで少なくとも 5 分間待機します。CIDR が Azure に展開されるには時間がかかるため、サイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開する前に少なくとも数分待たないと、新しく追加された CIDR が Nexus Dashboard Orchestrator を介してリモートサイトに伝達されない可能性があります。

Nexus Dashboard Orchestrator からインフラ構成を展開した後に、次のエラー メッセージが表示された場合：

```
Invalid configuration CT_Remotectx_cidr: Remote Site CIDR
```

これは、Nexus Dashboard Orchestrator からインフラ構成を展開する前に十分な時間を待たず、新しく追加された CIDR がリモートサイトに伝達されなかったことを意味します。この場合、次のようになります。

1. Cisco Cloud Network Controller でハブ ネットワーク ピアリングを無効にする
2. Nexus Dashboard Orchestrator でサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開します。
3. Cisco Cloud Network Controller でハブ ネットワーク ピアリングを再度有効にする
4. 少なくとも 5 分（または以前に待機したよりも長い時間）待ってからサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を再度展開します。

-
- ステップ 1** まだログインしていない場合は、Cisco クラウド ネットワーク コントローラ GUI にログインします。
- ステップ 2** 左側のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [クラウド コンテキスト プロファイル (Cloud Context Profiles)] に移動します。
- 既存のクラウドコンテキストプロファイルが表示されます。
- ステップ 3** ハブ ネットワーク ピアリングを無効にするクラウド コンテキスト プロファイルをダブルクリックします。
- そのクラウド コンテキスト プロファイルの概要ウィンドウが表示されます。この概要ウィンドウの [ハブ ネットワーク ピアリング (Hub Network Peeri)] エリアに [有効 (Enabled)] と表示されます。これは、ハブ ネットワーク ピアリングが有効になっていることを示しています。
- ステップ 4** 鉛筆アイコンをクリックして、このクラウド コンテキスト プロファイルを編集します。

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

ステップ 5 [クラウドコンテキスト プロファイルの編集 (Edit Cloud Context Profile)] ウィンドウで、[ハブ ネットワーク ピアリング (Hub Network Peering)] フィールドを見つけ、チェックボックスをクリックして [有効 (Enabled)] フィールドからチェックマークを外します。

[ハブ ネットワーク ピアリング (Hub Network Peering)] オプションを無効にしても、グローバル レベルで VNet ピアリングが削除されるのではなく、この特定のインフラ VNet に関連付けられているすべての VNet ピアリングが削除されます。

ステップ 6 [保存 (Save)] をクリックします。

そのクラウドコンテキスト プロファイルの概要ウィンドウが再び表示されます。この概要ウィンドウの [ハブ ネットワーク ピアリング (Hub Network Peering)] エリアに [無効 (Disabled)] と表示されます。これは、ハブ ネットワーク ピアリングが無効になっていることを示しています。

ステップ 7 新しい CIDR を追加するには、鉛筆アイコンをクリックして、このクラウドコンテキスト プロファイルを再度編集します。

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

ステップ 8 [CIDR の追加 (Add CIDR)] をクリックします。

[CIDR の追加 (Add CIDR)] ダイアログボックスが表示されます。

ステップ 9 [CIDR ブロック範囲 (CIDR Block Range)] フィールドに新しい CIDR を追加します。

[プライマリ (Primary)] フィールドのボックスをクリックしないでください ([プライマリ (Primary)] フィールドの [はい (yes)] の横のボックスにチェックを入れないでください)。

ステップ 10 [サブネットの追加 (Add subnet)] をクリックして、必要なサブネットアドレスを [アドレス (Address)] フィールドに入力します。

必要に応じて、追加のサブネットの [サブネットの追加 (Add Subnet)] をクリックし続けます。

ステップ 11 [CIDR の追加 (Add CIDR)] ウィンドウで必要な情報をすべて追加し終わったら、[追加 (Add)] をクリックします。

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

ステップ 12 [クラウドコンテキスト プロファイルの編集 (Edit Cloud Context Profile)] ウィンドウで情報を確認し、[保存 (Save)] をクリックします。

そのクラウドコンテキスト プロファイルの概要ウィンドウが表示されます。[CIDR ブロック範囲 (CIDR Block Range)] エリアにリストされた新しい CIDR が表示されます。

ステップ 13 これらの手順の最初にハブ ネットワーク ピアリングを無効にした場合は、この時点で再度有効にします。

a) 鉛筆アイコンをクリックして、このクラウドコンテキスト プロファイルを編集します。

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

- b) [クラウド コンテキスト プロファイルの編集 (Edit Cloud Context Profile)] ウィンドウで、[ハブ ネットワーク ピアリング (Hub Network Peering)] フィールドを見つけ、チェックボックスをクリックして [有効 (Enabled)] フィールドにチェックマークを追加し、この特定のインフラ VNet の VNet ピアリングを再度有効にします。
- c) [保存 (Save)] をクリックします。

そのクラウド コンテキスト プロファイルの概要ウィンドウが再び表示されます。この概要ウィンドウの [ハブ ネットワーク ピアリング (Hub Network Peering)] エリアに [有効 (Enabled)] と表示されます。これは、ハブ ネットワーク ピアリングが再び有効になっていることを示しています。

前に説明したように、この時点で Azure portal にアクセスすると、Azure の overlay-1 VNet にてこれらの手順で追加した追加の CIDR とサブネットが表示されます。これは、予期される正しい動作です。

サービス グラフの展開

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

サービス グラフは、次の2つの方法で展開できます。

- 単一ノード サービス グラフ : 1つのデバイスのみが展開されます。
- マルチノード サービス グラフ : 最大3つのノードをサービス チェーンに追加できます。

単一ノードまたはマルチキャストノードのいずれかでサービス グラフを展開可能になる前に、以下を構成する必要があります。

1. テナント
2. アプリケーション プロファイル
3. コンシューマ EPG
4. プロバイダー EPG
5. VRF
6. クラウド コンテキスト プロファイル
7. フィルタとのコントラクト

GUI を使用したサービス グラフの展開

次のセクションでは、GUI を使用してサービス グラフを展開する方法について説明します。

Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成

始める前に

このセクションでは、Cisco Cloud Network Controller GUI を介してサービス グラフで使用できるサービス デバイスを作成する方法について説明します。

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

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

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

ステップ 3 [インテント (Intent)] メニューの[**アプリケーション管理 (Application Management)**] リストから、[**サービス (Services)**] > [**デバイス (Devices)**] > [**デバイスの作成 (Create Device)**] をクリックします。[[**デバイスの作成 (Create Device)**] ダイアログボックスが表示されます。

ステップ 4 次の[**デバイスの作成ダイアログボックスのフィールド (Create Device Dialog Box Fields)**] の表にリストされた各フィールドに該当する値を入力し、続行します。

各タイプのサービス デバイスに固有の情報については、次の表を参照してください。

- アプリケーション ロードバランサについては、[4.a \(261 ページ\)](#) を参照してください。
- ネットワーク ロードバランサについては、[4.b \(263 ページ\)](#) を参照してください。
- サードパーティのロードバランサについては、[4.c \(268 ページ\)](#) を参照してください。
- サードパーティのファイアウォールについては、[4.d \(269 ページ\)](#) を参照してください。

a) アプリケーション ロードバランサに必要な情報を入力します。

[プロパティ (Properties)]	説明
全般	
名前	デバイスの名前を入力します。
テナント	テナントを選択します。 <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択 (Select)] をクリックします。[デバイスの作成 (Create Device)] ダイアログボックスに戻ります。
[設定 (Settings)]	

[プロパティ (Properties)]	説明
サービス タイプ	デバイス タイプを選択します。 <ul style="list-style-type: none"> • アプリケーションロードバランサ
ALB SKU	次から選択します。 <ul style="list-style-type: none"> • 標準 • Standard V2
[VM インスタンス 数 (VM Instance Count)]	[VM インスタンス数 (VM Instance Count)] テキスト ボックスに数値を入力します。 (注) これは、Application Gateway にのみ適用されます。
[VM インスタンス サイズ (VM Instance Size)]	選択する VM インスタンスのサイズ (大、中、または小) のラジオ ボタンをクリックします。 (注) これは、Application Gateway にのみ適用されます。
スキーム	[インターネット向け] または [内部] を選択します。 <ul style="list-style-type: none"> • [インターネット向け (Internet Facing)] : これは、バランサのパブリック IP を構成するために使用されます。これは Azure によって割り当てられます。 • [内部 (Internal)] : クリックして、[IP アドレスの割り当て (IP Address Assignment)] で [動的 (Dynamic)] または [静的 (Static)] を選択します。 <ul style="list-style-type: none"> • [ダイナミック (Dynamic)] : Azure によってダイナミック IP アドレスが割り当てられます。ダイナミック IP アドレスは、VM が起動するたびに変更されます。 • 静的 : クラウドコンテキスト プロファイルで定義されている CIDR に基づいて IP アドレスを入力し、IP アドレスが ALB と同じサブネットにあることを確認します。 ALB SKU Standard は、静的および動的 IP アドレスをサポートします。 ALB SKU Standard V2 は、静的 IP アドレスのみをサポートします。

[プロパティ (Properties)]	説明
サブネット	<p>サブネットを選択するには:</p> <ol style="list-style-type: none"> 1. [リージョンの選択 (Select Region)] をクリックします。[リージョンの選択 (Select Region)] ダイアログボックスが表示されます。[リージョンの選択 (Select Region)] ダイアログで、左側の列のテナントをクリックして選択し、[選択 (Select)] をクリックします。 2. [クラウドコンテキスト プロファイルの選択 (Select Cloud Context Profile)] をクリックします。[クラウド コンテキスト プロファイルの選択 (Select Cloud Context Profile)] ダイアログ ボックスが表示されます。 3. [サブネットの選択 (Select Subnet)] をクリックします。[サブネットの選択] ダイアログボックスが表示されます。静的 IP アドレス テキスト ボックスが表示されます。ロードバランサの IP アドレスを入力します。右の「ティック」マークをクリックして確定します。 4. さらにサブネットを追加するには、手順 a ~ c を繰り返します。

- b) ネットワーク ロードバランサに必要な情報を入力します。

表 36: ネットワーク ロードバランサの [デバイスの作成 (Create Device)] ダイアログ ボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	ロードバランサーの名前を入力します。
[設定 (Settings)]	
サービス タイプ	<p>デバイス タイプを選択します。</p> <ul style="list-style-type: none"> • ネットワーク ロードバランサ

[プロパティ (Properties)]	説明
[すべてのトラフィックを許可 (Allow All Traffic)]	<p>[すべてのトラフィックを許可 (Allow All Traffic)] オプションを有効にするかどうかを決定します。</p> <p>[すべてのトラフィックを許可 (Allow All Traffic)] オプションを有効にすると、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスが許可されます。詳細については、「すべてのトラフィックを許可のオプションについて (205 ページ)」を参照してください。</p> <p>(注) このオプションを有効にする前に、これによってセキュリティリスクが発生しないことを確認してください。</p> <ul style="list-style-type: none"> • すべてのトラフィックを許可する場合は、[すべてのトラフィックを許可 (Allow All Traffic)] エリアで、[有効 (Enabled)] フィールドの横にあるボックスをクリックします。 • すべてのトラフィックを許可しない場合は、[すべてのトラフィックを許可 (Allow All Traffic)] エリアで、[有効 (Enabled)] フィールドの横のボックスをオフ (選択解除) したままにします。
スキーム	<p>[インターネット向け] または [内部] を選択します。</p> <ul style="list-style-type: none"> • [インターネット向け (Internet Facing)]: これは、バランサのパブリック IP を構成するために使用されます。これは Azure によって割り当てられます。 <p>このページの [フロントエンド IP 名 (Frontend IP Names)] フィールドでの選択に応じて、[インターネット向けオプション (Frontend IP Names)] を選択して、単一のデフォルトパブリック フロントエンド IP アドレスまたは複数のパブリック フロントエンド IP アドレスを構成できます。。</p> <ul style="list-style-type: none"> • [内部 (Internal)]: クリックして、[IP アドレスの割り当て (IP Address Assignment)] で [動的 (Dynamic)] または [静的 (Static)] を選択します。 <ul style="list-style-type: none"> • [ダイナミック (Dynamic)]: Azure によってダイナミック IP アドレスが割り当てられます。ダイナミック IP アドレスは、VM が起動するたびに変更されます。 • [静的 (Static)]: クラウド コンテキスト プロファイルで定義されている CIDR に基づいて IP アドレスを入力し、IP アドレスが NLB と同じサブネットにあることを確認します。静的 IP アドレスは、ロードバランサに関連付けられます。 <p>(注) Cisco Cloud Network Controller は、標準 SKU NLB のみを作成します。</p>

[プロパティ (Properties)]	説明
[カスタムリソースグループ (Custom Resource Group)]	必要に応じて、カスタム リソースグループの名前を入力します。
Subnets	<p>サブネットを選択するには:</p> <ol style="list-style-type: none"> 1. [+ サブネットの追加 (+Add Subnet)] をクリックします。 2. [リージョンの選択 (Select Region)] をクリックします。[リージョンの選択 (Select Region)] ダイアログボックスが表示されます。 [リージョンの選択 (Select Region)] ダイアログで、左側の列のリージョンをクリックして選択し、[選択 (Select)] をクリックします。 3. [クラウドコンテキスト プロファイルの選択 (Select Cloud Context Profile)] をクリックします。[クラウドコンテキスト プロファイルの選択 (Select Cloud Context Profile)] ダイアログ ボックスが表示されます。 [クラウドコンテキスト プロファイル (Select Cloud Context Profile)] ダイアログで、左側の列のクラウドコンテキスト プロファイルをクリックして選択し、[選択 (Select)] をクリックします。 4. [サブネットの選択 (Select Subnet)] をクリックします。[サブネットの選択] ダイアログボックスが表示されます。 [サブネットの選択 (Select Subnet)] ダイアログで、左側の列のサブネットをクリックして選択し、[選択 (Select)] をクリックします。 5. 右の「ティック」マークをクリックして確定します。 6. さらにサブネットを追加するには、[+ サブネットの追加 (+ Add Subnet)] を再度クリックして、これらの手順を繰り返します。
詳細設定	下矢印をクリックして、[詳細設定 (Advanced Settings)] エリアを展開します。次のエントリが表示されます。

[プロパティ (Properties)]	説明
[フロントエンド IP 名 (Frontend IP Names)]	

[プロパティ (Properties)]	説明
	<p>インターネット向けのネットワーク ロードバランサに対して複数のフロントエンド IP アドレスを構成するためのサポートが利用可能になりました。</p> <ul style="list-style-type: none"> デフォルトでは、インターネット向けのネットワーク ロード バランサ用に単一のフロントエンド IP アドレスが自動的に作成されます。 インターネット向けネットワーク ロード バランサに追加のフロントエンド IP アドレスが必要な場合は、[+ フロントエンド IP 名の追加 (+ Add Frontend IP Name)] をクリックします。詳細については、Azure ネットワーク ロードバランサの複数のフロントエンド IP アドレスの構成について (203 ページ) を参照してください。 <p>このエリアにフロントエンド IP 名を追加すると、このインターネット向けネットワーク ロードバランサに複数のフロントエンド IP アドレスを割り当てるのが Azure に通知されます。このエリアに入力する各フロントエンド IP 名は、単一の追加フロントエンド IP アドレスになります。</p> <p>このエリアのパブリック フロントエンド IP アドレス (既定のフロントエンド IP アドレスと追加のフロントエンド IP アドレス) は、Azure によって割り当てられます。</p> <ol style="list-style-type: none"> [+ フロントエンド IP 名の追加 (+ Add Frontend IP Name)] をクリックして、Azure でネットワーク ロードバランサに割り当てる追加のフロントエンド IP アドレスの名前を追加します。 追加のフロントエンド IP アドレスの名前を入力し、右側のチェック マークをクリックして新しいフロントエンド IP 名を確認します。 [+ フロントエンド IP 名の追加 (+ Add Frontend IP Name)] を再度クリックして、Azure でネットワーク ロードバランサに割り当てる追加のフロントエンド IP アドレスの名前を追加します。 <p>たとえば、インターネット向けのネットワーク ロードバランサに合計 3 つのフロントエンド IP アドレスが必要だとします。</p> <ul style="list-style-type: none"> 3 つのフロントエンド IP アドレスの最初のアドレスは、デフォルトで自動的に割り当てられます。 次に、[+ フロントエンド IP 名の追加 (+ Add Frontend IP Name)] を 2 回クリックし、2 つの個別のフロントエンド IP 名 (たとえば、frontend2 と frontend3) を入力して、インターネット向けネットワーク ロードバランサに対して合計 3 つのフロントエンド IP アドレスを割り当てることを Azure に通知します。 <p>デフォルトおよび構成済みのフロントエンド IP 名に関連付けられたフロントエンド IP アドレスを表示するには :</p>

[プロパティ (Properties)]	説明
	<ol style="list-style-type: none"> 1. [アプリケーション管理 (Application Management)]>>[サービス (Services)]>>[デバイス (Devices)]に移動します。 2. 構成されたサービス デバイスをダブルクリックして、そのサービス デバイスの [概要 (Overview)] ページを表示します。 3. [クラウドリソース (Cloud Resources)]>[フロントエンド IP 名 (Frontend IP Names)]をクリックします。 デフォルトのフロントエンド IP アドレスは、この詳細ページの [デフォルト (Default)] タグとともに表示されます。

- c) サードパーティ ロードバランサに必要な情報を入力します。

表 37: サードパーティ ロードバランサの [デバイスの作成 (Create Device)] ダイアログ ボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	デバイスの名前を入力します。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)]をクリックします。[テナントの選択 (Select Tenant)] ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択 (Select)]をクリックします。[デバイスの作成 (Create Device)] ダイアログボックスに戻ります。
[設定 (Settings)]	
サービスの種類	<p>デバイス タイプを選択します。</p> <ul style="list-style-type: none"> • サードパーティ ロードバランサ
[作成モード (Creation Mode)]	<p>[セレクタ (Selectors)]を選択します。 [VRF] および [インターフェイス (Interfaces)] フィールドが表示されます。</p>
VRF	<p>[VRF の選択 (Select VRF)]をクリックします。開いている [VRF の選択 (Select VRF)] ダイアログで、クリックして左の列の VRF を選択します。[選択 (Select)] をクリックします。</p>

[プロパティ (Properties)]	説明
[インターフェイス (Interface)]	<p>[インターフェイスの追加 (Add Interface)]をクリックします。[インターフェイス (Interfaces)]ウィンドウが表示されます。</p> <ol style="list-style-type: none"> [インターフェイス設定 (Interface Settings)]フィールドで外部インターフェイスの名前を入力します。 [インターフェイス セレクタの追加 (Add Interface selector)]をクリックします。 [インターフェイス セレクタの設定 (Interface Selector Settings)]ページで、インターフェイスの名前を入力します。 [一致式 (Match Expressions)]フィールドで、[一致式 (Match Expressions)]をクリックして選択します。 <ul style="list-style-type: none"> [キー (Key)]: これは、IP、リージョン、またはカスタム ベースのタグセレクタです。 [演算子 (Operator)]: これは、equal、not equals、in、not in、key あり、または key なしのいずれかです。 [値 (Value)]: サードパーティのロードバランサの外部または内部ネットワークの IP アドレス。 チェック マークをクリックしてインターフェイスを追加し、[保存 (Save)] ([インターフェイス ウィンドウ) をクリックします。 [保存 (Save)] ([デバイスの作成 (Create Device)]ウィンドウ) をクリックします。 <p>[インターフェイスの追加 (Add Interface)]をクリックし、手順 a～e を繰り返して、さらにインターフェイスを追加します。</p> <p>(注) サードパーティのロードバランサインターフェイスは、マルチノードサービスグラフに展開する場合、サブネットベースのセレクタで構成する必要があります。</p>

- d) サードパーティ ファイアウォールに必要な情報を入力します。

表 38: サードパーティ ファイアウォールの [デバイスの作成 (Create Device)]ダイアログ ボックスのフィールド

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

[プロパティ (Properties)]	説明
[設定 (Settings)]	
サービス タイプ	<p>デバイス タイプを選択します。</p> <ul style="list-style-type: none"> • サードパーティ ファイアウォール <p>(注) サードパーティのファイアウォールをマルチノードサービス グラフの最初のデバイスにすることはできません。</p>
VRF	<p>VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [VRF の選択 (Select VRF)]をクリックします。[VRF の選択 (Select VRF)]ダイアログボックスが表示されます。 2. [VRF の選択 (Select VRF)]ダイアログで、左側の列の VRF をクリックして選択し、[選択 (Select)]をクリックします。

[プロパティ (Properties)]	説明
インターフェイス	<p>[インターフェイスの追加 (Add Interface)] をクリックします。</p> <p>[設定] ページが表示されます。</p> <ol style="list-style-type: none"> [名前 (Name)] フィールドに、インターフェイスの名前を入力します。 [すべてのトラフィックを許可 (Allow All Traffic)] オプションを有効にするかどうかを決定します。 <ul style="list-style-type: none"> [すべてのトラフィックを許可 (Allow All Traffic)] オプションを有効にすると、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスが許可されます。詳細については、「すべてのトラフィックを許可のオプションについて (205 ページ)」を参照してください。 (注) このオプションを有効にする前に、これによってセキュリティリスクが発生しないことを確認してください。 すべてのトラフィックを許可する場合は、[すべてのトラフィックを許可 (Allow All Traffic)] エリアで、[有効 (Enabled)] フィールドの横にあるボックスをクリックします。 すべてのトラフィックを許可しない場合は、[すべてのトラフィックを許可 (Allow All Traffic)] エリアで、[有効 (Enabled)] フィールドの横のボックスをオフ (選択解除) したままにします。 [インターフェイス セレクタの追加 (Add Interface Selector)] をクリックします。 インターフェイス セレクタの名前を入力します。 [一致式 (Match Expressions)] をクリックして選択します。 <ul style="list-style-type: none"> [キー (Key)] : これは、IP、リージョン、またはカスタム ベースのタグセレクタです。 [演算子 (Operator)] : これは、equal、notequals、in、not in、key あり、または key なしのいずれかです。 [値 (Value)] : アプリ、Web、内部ネットワーク、管理ネットワーク、または外部ネットワークの IP アドレス。 [追加] をクリックします。 手順 a から f を繰り返して、さらにインターフェイスを追加します。

ステップ5 設定が終わったら [Save] をクリックします。

ステップ6 [サービス グラフの作成 (Create Service Graph)] ダイアログボックスが表示されます。[別のサードパーティファイアウォールを作成 (Create another Third Party Firewall)] をクリックして、別のデバイスを作成します。[[デバイスの作成 (Create Device)] ダイアログボックスが表示されます。

(注) UIは通常、以前に作成したデバイスを作成するように求めます。ただし、それをクリックすると、[デバイスの作成 (Create Device)] ページに戻ります。ここで、作成する必要があるデバイスを選択できます。最初のデバイスは、サードパーティのファイアウォールにしないでください。

Cisco Cloud 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 ネットワーク コントローラ GUI を使用した単一ノードまたはマルチノード向けサービス グラフ テンプレートの作成方法について説明します。

始める前に

デバイスはすでに作成されています。

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

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

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

ステップ3 [インテント (Intent)] メニューの [アプリケーション管理 (Application Management)] リストで、[サービス (Services)] >> [サービス グラフ (Service Graph)] >> [サービス グラフの作成 (Create Service Graph)] をクリックします。[サービス グラフの作成 (Create Service Graph)] ポップアップが表示されます。[さあ、始めましょう (Let's Get Started)] をクリックします。

ステップ4 次の [サービス グラフの作成ダイアログ ボックスのフィールド (Create Service Graph Dialog Box Fields)] の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 39: サービス グラフの作成ダイアログ ボックスのフィールド (単一ノード向け)

[プロパティ (Properties)]	説明
全般	
名前	サービス グラフ テンプレートの名前を入力します。

[プロパティ (Properties)]	説明
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)]をクリックします。[テナントの選択 (Select Tenant)]ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択 (Select)]をクリックします。[サービス グラフの作成 (Create Service Graph)]ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。
[設定 (Settings)]	
デバイスを選択	<p>デバイスを選択します。</p> <ol style="list-style-type: none"> 1. [デバイスの選択 (Select Device)]をクリックします。[デバイスの選択 (Select Device)]ダイアログが表示されます。 2. 左側の列から、デバイスをクリックして選択します。下の[デバイスのドロップ (Drop Device)]スペースにデバイスをドラッグアンドドロップします。これにより、このデバイス タイプの実際のデバイスを選択できる小さなウィンドウが開きます。 3. [選択 (Select)]をクリックします。[サービス グラフの作成 (Create Service Graph)]ダイアログボックスに戻ります。

表 40: サービス グラフの作成ダイアログボックスのフィールド (マルチノード向け)

[プロパティ (Properties)]	説明
全般	
名前	サービス グラフ テンプレートの名前を入力します。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 1. [テナントの選択 (Select Tenant)]をクリックします。[テナントの選択 (Select Tenant)]ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択 (Select)]をクリックします。[サービス グラフの作成 (Create Service Graph)]ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。

[プロパティ (Properties)]	説明
設定：必要なトポロジに基づいて、デバイスを下のボックスにドラッグアンドドロップします。	
[アプリケーション ロードバランサ (Application Load Balancer)]	<ol style="list-style-type: none"> 1. アプリケーションロードバランサ デバイスを下のボックスにドラッグアンドドロップします。 2. [サービス ノード (Service node)] ダイアログ ボックスで、[アプリケーションロードバランサの選択 (Select Application Load Balancer)] をクリックし、左側の列で [アプリケーションロードバランサ (Application Load Balancer)] をクリックして選択し、[追加 (Add)] をクリックします。
[サードパーティの ファイアウォール (Third Party Firewall)]	<ol style="list-style-type: none"> 1. 下のボックスでデバイスの隣にサードパーティファイアウォールをドラッグアンドドロップします。 2. [サービス ノード (Service node)] ダイアログ ボックスで、[サードパーティファイアウォール (Third Party Firewall)] をクリックし、左側の列で [サードパーティファイアウォール (Third Party Firewall)] をクリックして選択し、[追加 (Add)] をクリックします。 (注) サードパーティファイアウォールをサービスグラフの最初のノードにすることはできません。 3. サードパーティファイアウォールのコンシューマ側でユーザーベースのリダイレクト機能を有効にする場合は、[コンシューマコネクタタイプ (Consumer Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れます。 4. サードパーティファイアウォールのプロバイダー側でユーザーベースのリダイレクト機能を有効にする場合は、[プロバイダーコネクタタイプ (Provider Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れます。 5. [プロバイダーコネクタタイプ (Provider Connector Type)] で、該当するオプションの横にチェックを入れます。詳細については、「レイヤ4～レイヤ7サービスリダイレクト」を参照してください。 6. [追加] をクリックします。

[プロパティ (Properties)]	説明
[ネットワーク ロードバランサ (Network Load Balancer)]	<ol style="list-style-type: none"> 1. ネットワーク ロードバランサ デバイスを下のボックスにドラッグアンドドロップします。 2. [サービス ノード (Service node)] ダイアログ ボックスで、[ネットワーク ロードバランサの選択 (Select Network Load Balancer)] をクリックし、左側の列で [ネットワーク ロードバランサ (Network Load Balancer)] をクリックして選択し、[追加 (Add)] をクリックします。 3. ネットワーク ロードバランサのコンシューマ側でユーザベースのリダイレクト機能を有効にする場合は、[コンシューマコネクタタイプ (Consumer Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れます。 4. ネットワーク ロードバランサのプロバイダー側でユーザベースのリダイレクト機能を有効にする場合は、[プロバイダーコネクタタイプ (Provider Connector Type)] フィールドで、[リダイレクト (Redirect)] オプションの隣のボックスにチェックを入れます。 5. [追加] をクリックします。
[サードパーティ ロードバランサ (Third Party Load Balancer)]	<ol style="list-style-type: none"> 1. サードパーティのロードバランサ デバイスを下のボックスにドラッグアンドドロップします。 2. [サービス ノード (Service node)] ダイアログ ボックスで、[サードパーティ ロードバランサの選択 (Select Third Party Load Balancer)] をクリックし、左側の列でサードパーティ ロードバランサをクリックして選択します。 3. [コンシューマ インターフェイスの選択 (Select Consumer Interface)] をクリックします。外部としてマークされたインターフェイスを選択します。 4. [プロバイダー インターフェイスの選択 (Select Provider Interface)] をクリックします。内部としてマークされたインターフェイスを選択します。 5. [追加 (Add)] をクリックします。

ステップ5 設定が終わったら [Save] をクリックします。

ステップ6 [EPG 通信 (EPG Communication)] ダイアログボックスが表示されます。[詳細に移動 (Go to details)] をクリックして、サービス グラフ テンプレートを確認します。

Cisco Cloud 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。この手順は、シングル ノードおよびマルチノードの展開に適用できます。

始める前に

- デバイスを構成しました。
- サービス グラフが構成されました。

-
- ステップ1** インテントアイコンをクリックします。[**インテント (Intent)**]メニューが表示されます。
- ステップ2** [**インテント (Intent)**]検索ボックスの下のドロップダウン□をクリックし、[**構成 (Configuration)**]を選択します。
- [**インテント (Intent)**]の[**構成 (Configuration)**]オプションのリストが表示されます。
- ステップ3** [**インテント (Intent)**]メニューの[**構成 (Configuration)**]リストで、[**EPG Communication**]をクリックします。[**EPG通信 (EPG Communication)**]ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。
- ステップ4** コントラクトを選択します。
- [**コントラクトの選択 (Select Contract)**]をクリックします。[**コントラクトの選択 (Select Contract)**]ダイアログボックスが表示されます。
 - [**コントラクトの選択 (Select Contract)**]ダイアログの左側のペインで、契約をクリックして選択し、[**選択 (Select)**]をクリックします。[**コントラクトの選択 (Select Contract)**]ダイアログボックスが閉じます。
- ステップ5** コンシューマ EPG を追加するには、次の手順を実行します。
- [**コンシューマ EPG の追加 (Add Consumer EPGs)**]をクリックします。[**コンシューマ EPG の選択 (Select Consumer EPGs)**]ダイアログが表示されます。
 - [**コンシューマ EPG の選択 (Select Consumer EPGs)**]ダイアログの左側のペインで、チェックボックスをクリックして、クラウド EPG (内部向けロードバランサの場合) またはクラウド外部 EPG (インターネット向けロードバランサの場合) を選択します。[**選択 (Select)**]をクリックします。[**コンシューマ EPG の選択 (Select Consumer EPGs)**]ダイアログボックスが閉じます。
- ステップ6** プロバイダー EPG を追加するには、次の手順を実行します。
- [**プロバイダー EPG の追加 (Add Provider EPGs)**]をクリックします。[**プロバイダー EPG の選択 (Select Provider EPGs)**]ダイアログが表示されます。
 - [**プロバイダー EPG の選択 (Select Provider EPGs)**]ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダー EPG を選択し、[**選択 (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。
- ステップ7** サービス グラフを選択するには:
- [**EPG 通信の構成 (EPG Communication Configuration)**]ダイアログで、[**サービス グラフの選択 (Select Service Graph)**]をクリックします。[**サービス グラフの選択 (Select Service Graph)**]ダイアログボックスが表示されます。
 - [**サービス グラフの選択 (Select Service Graph)**]ダイアログの左側のペインで、サービス グラフをクリックして選択し、[**選択 (Select)**]をクリックします。[**サービス グラフの選択 (Select Service Graph)**]ダイアログボックスが閉じます。

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

リスナーは、デバイスが動作するポートとプロトコルです。

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

表 41: アプリケーションゲートウェイ用 [クラウドロードバランサリスナーの追加 (Add Cloud Load Balancer Listener)] 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	アプリケーションゲートウェイの場合は、[HTTP] または [HTTPS] をクリックして選択します。
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): <ol style="list-style-type: none"> [SSL 証明書の追加] をクリックします。 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。 キーリングを選択してください: <ol style="list-style-type: none"> [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。 [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。 [証明書ストア] ドロップダウンリストをクリックして、証明書を選択します。 <p>(注) リスナーは複数の証明書を持つことができます。</p>
ルールの追加	ルール設定をデバイスリスナーに追加するには、[ルールの追加] をクリックします。[ルール] リストに新しい行が表示され、[ルール設定] フィールドが有効になります。

[プロパティ (Properties)]	説明
ルール設定	

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

[プロパティ (Properties)]	説明
	<ul style="list-style-type: none"> • リダイレクト プロトコル : [リダイレクト プロトコル (Redirect Protocol)] ドロップダウンリストをクリックして、[HTTP]、[HTTPS]、または [継承 (Inherit)] を選択します。 • リダイレクト クエリ : リダイレクト クエリを入力します。
正常性チェック (Health Checks)	<p>アプリケーションロードバランサは、高可用性のためにバックエンドプールターゲットで正常性チェックを実行します。これは、正常性チェックで構成できます。</p> <ul style="list-style-type: none"> • [プロトコル (Protocol)] : [HTTP] または [HTTPS] をクリックして選択します。 • [パス (Path)]- パスを入力します。 デフォルトは / です • [ポート (Port)] : 正常性チェックを実行するポートを入力します。 • [詳細設定 (Advanced Settings)] <p>[異常なしきい値 (Unhealthy Threshold)] : このしきい値を構成して、バックエンドターゲットが異常であるとアドバタイズされるタイミングを決定します。</p> <ul style="list-style-type: none"> • [タイムアウト (Timeout)]- 正常性チェックのタイムアウトの値を入力します。 • [間隔 (Interval)] : チェックを実行する間隔を決定する時間を秒単位で入力します。 • [成功コード (Success Code)]- 成功コードを入力します。 デフォルトは 200 ~ 399 です。 • [ルールからホストを使用 (Use host from rule)]- ホスト名をルールから選択する必要がある場合は、チェックボックスをクリックします。 • [ホスト (Host)]- [ルールからホストを使用 (Use host from rule)] がチェックされていない場合は、正常性チェックに使用するホスト名を指定します。 <p>完了したら、[ルールの追加] をクリックします。</p>

表 42: ネットワーク ロードバランサ用 [クラウド ロードバランサ リスナーの追加 (Add Cloud Load Balancer Listener)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	リスナーの名前を入力します。

[プロパティ (Properties)]	説明
プロトコル (Protocol)	[TCP] または [UDP] をクリックして選択します。
[ポート (Port)]	デバイスがトラフィックを受け入れるポートを入力します。
[フロントエンド IP 名 (Frontend IP Name)]	<p>クラウドロードバランサリスナーを構成するフロントエンドIPアドレスを選択します。</p> <ul style="list-style-type: none"> • [デフォルト IP を使用 (Use default IP)] : デフォルトのフロントエンド IP アドレスでクラウドロードバランサリスナーを構成するには、このオプションを選択します。 • <frontend_ip_name> : このオプションを選択して、Cisco Cloud Network Controller GUI を使用したサービス デバイスの作成 (261 ページ) でこのインターネット向けネットワークロードバランサのサービスデバイスを作成したときに構成した、フロントエンド IP 名に関連付けられた追加のフロントエンド IP アドレスにクラウドロードバランサーリスナーを構成します。 <p>詳細については、Azure ネットワーク ロードバランサの複数のフロントエンド IP アドレスの構成について (203 ページ) を参照してください。</p>
ルール設定	<p>[ルール設定 (Rule Settings)] ペインで、次のオプションを設定します。</p> <ul style="list-style-type: none"> • 名前 : 規則の名前を入力します。 • [アクションタイプ (Action Type)] : デフォルトで [転送先 (Forward to)] に設定されています。トラフィックは、以下で選択したプロトコルを使用して、選択した EPG のポートに転送されます。 • [ポート (Port)] : バックエンドプールサーバーがロードバランサからのトラフィックを受け入れるポートを入力します。 • [プロトコル (Protocol)] : [TCP] または [UDP] をクリックして選択します。 • [EPG] : Web サーバーがトラフィックを処理する EPG。

[プロパティ (Properties)]	説明
正常性チェック (Health Checks)	<p>ロードバランサは、高可用性のためにバックエンドプール ターゲットで正常性チェックを実行します。ここで構成できます。</p> <ul style="list-style-type: none"> • [プロトコル (Protocol)] : [TCP]、[HTTP] または [HTTPS] をクリックして選択します。 • [ポート (Port)] : 正常性チェックを実行するポートを入力します。 • [詳細設定 (Advanced Settings)] <p>[異常なしきい値 (Unhealthy Threshold)] : このしきい値を構成して、バックエンドターゲットが異常であるとアドバタイズされるタイミングを決定します。</p> <ul style="list-style-type: none"> • [間隔 (Interval)] : チェックを実行する間隔を決定する時間を秒単位で入力します。 <p>終了したら、[Add] をクリックします。</p>

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

REST API を使用したサービス グラフの展開

次のセクションでは、REST API を使用してサービス グラフを展開する方法について説明します。

REST API を使用したインターネット向けロード バランサの作成

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

ステップ1 アプリケーションゲートウェイ (アプリケーションロードバランサ) の内部向けロードバランサを作成するには :

例 :

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
    <cloudLB scheme="internal" type="application" name="alb-151-15" status="">
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
    </cloudLB>
  </fvTenant>
</polUni>
```

```
</polUni>
```

ステップ2 Azure ロードバランシング（ネットワークロードバランサ）の内部向けロードバランサを作成するには：
例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[subscription id]-vendor-azure" />
    <cloudLB scheme="internal" type="network" name="nlb-151-15" status="">
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
    </cloudLB>
  </fvTenant>
</polUni>
```

ステップ3 [すべてのトラフィックを許可のオプションについて（205ページ）](#) で説明されている[すべてのトラフィックを許可（**Allow All Traffic**）] オプションを使用して、Azure ロードバランシング（ネットワークロードバランサ）用の内部向けロードバランサを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[subscription id]-vendor-azure" />
    <cloudLB scheme="internal" type="network" name="nlb-151-15" allowAll="true" status="">
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
    </cloudLB>
  </fvTenant>
</polUni>
```

REST API を使用したインターネット向けロードバランサの構成

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

ステップ1 アプリケーションゲートウェイ（アプリケーションロードバランサ）のインターネット向けロードバランサを作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[subscription id]-vendor-azure" />
```

REST API を使用したサードパーティ ファイアウォールの作成

```

    <cloudLB scheme="internet" type="application" name="alb-151-15" status="">
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
    </cloudLB>

  </fvTenant>
</polUni>

```

ステップ2 インターネット向けネットワーク ロードバランサ :

例 :

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->

<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
    <cloudLB scheme="internet" type="network" name="nlb-151-15" status="">
      <cloudVip name="IP1"/>
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
    </cloudLB>
    </fvTenant>
  </polUni>

```

この例では、以下のようにになっています。

- cloudLB ラインは、単一のデフォルト IP アドレスを持つインターネット向けのネットワーク ロードバランサを作成するために使用されます。
- cloudVip ラインは、インターネットに接続するネットワーク ロードバランサの追加フロントエンド IP アドレスを作成するために使用されます。詳細については、[Azure ネットワーク ロードバランサの複数のフロントエンド IP アドレスの構成について \(203 ページ\)](#) を参照してください。

REST API を使用したサードパーティ ファイアウォールの作成

この例では、REST API を使用したサードパーティ ファイアウォールを作成する方法を示します。

ステップ1 サードパーティ ファイアウォールを作成するには :

例 :

```

<cloudLDev name="HubFW" svcType="FW" status="">
  <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
  <cloudLIif name="provider">
    <cloudEPSelector name="east" matchExpression="IP=='{{eastus_FwUntrustSubnet}}'" status="">

  </cloudLIif>
  <cloudLIif name="consumer">
    <cloudEPSelector name="east" matchExpression="IP=='{{eastus_FwTrustSubnet}}'" status="">
  </cloudLIif>

```



```
</cloudLDev>
```

ステップ 2 [すべてのトラフィックを許可のオプションについて \(205 ページ\)](#) で説明されている [すべてのトラフィックを許可 (Allow All Traffic)] オプションを使用してサードパーティ ファイアウォールを作成するには、次の手順を実行します。

例 :

```
<cloudLDev name="HubFW" svcType="FW" status="">
  <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
  <cloudLIf name="provider" allowAll="true" status="">
    <cloudEPSelector name="1" matchExpression="IP=='10.1.1.0/28'" status=""/>
  </cloudLIf>
  <cloudLIf name="consumer" allowAll="true" status="">
    <cloudEPSelector name="east" matchExpression="IP=='10.1.2.0/28'" status=""/>
  </cloudLIf>
</cloudLDev>
```

REST API を使用したサードパーティ ロードバランサの作成

この例では、REST API を使用してサードパーティ ロードバランサを作成する方法を示します。

この例では、REST API を使用してサードパーティ ロードバランサを作成する方法を示します。

例 :

```
<cloudLDev name="ThirdPartyLB" svcType="ADC" status="">
  <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
  <cloudLIf name="external">
    <cloudEPSelector name="ExtInterfaceSelector" matchExpression="IP=='{{ExtInterfaceSubnet}}'"
    status=""/>
  </cloudLIf>
  <cloudLIf name="internal">
    <cloudEPSelector name="IntInterfaceSelector" matchExpression="IP=='{{IntInterfaceSubnet}}'"
    status=""/>
  </cloudLIf>
</cloudLDev>
```

アプリケーションゲートウェイの REST API を使用したサービス 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。

アプリケーションゲートウェイのサービス グラフを作成するには :

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

```

<fvTenant name="tn15">
  <vnsAbsGraph name="c15_g1" type="cloud" status="">
    <vnsAbsTermNodeProv name="p1">
      <vnsAbsTermConn />
    </vnsAbsTermNodeProv>
    <vnsAbsTermNodeCon name="c1">
      <vnsAbsTermConn />
    </vnsAbsTermNodeCon>
    <vnsAbsNode managed="yes" name="N1" funcType="GoTo">
      <vnsRsNodeToCloudLDev tDn="uni/tn-tn15/clb-alb-151-15"/>
      <vnsAbsFuncConn name="provider"/>
      <vnsAbsFuncConn name="consumer"/>
    </vnsAbsNode>
    <vnsAbsConnection connDir="consumer" connType="external" name="con1">
      <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeCon-c1/AbsTConn"/>
      <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-consumer"/>
    </vnsAbsConnection>
    <vnsAbsConnection connDir="provider" connType="internal" name="con2">
      <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeProv-p1/AbsTConn"/>
      <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-provider"/>
    </vnsAbsConnection>
  </vnsAbsGraph>
</fvTenant>
</polUni>

```

Azure ロードバランサの REST API を使用してサービス グラフを作成する

Azure ロードバランサのサービス グラフを作成するには：

```

<?xml version="1.0" encoding="UTF-8"?>

<!-- api/node/mo/uni/.xml -->

<polUni>

<fvTenant name="tn15">

<vnsAbsGraph name="c15_g1" type="cloud" status="">

<vnsAbsTermNodeProv name="p1">

<vnsAbsTermConn />

</vnsAbsTermNodeProv>

<vnsAbsTermNodeCon name="c1">

<vnsAbsTermConn />

</vnsAbsTermNodeCon>

<vnsAbsNode managed="yes" name="N1" funcType="GoTo">

<vnsRsNodeToCloudLDev tDn="uni/tn-tn15/clb-nlb-151-15" />

<vnsAbsFuncConn name="provider" />

```

```

<vnsAbsFuncConn name="consumer" />
</vnsAbsNode>
<vnsAbsConnection connDir="consumer" connType="external" name="con1">
<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeCon-c1/AbsTConn"
/>
<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-consumer"
/>
</vnsAbsConnection>
<vnsAbsConnection connDir="provider" connType="internal" name="con2">
<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeProv-p1/AbsTConn"
/>
<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-provider"
/>
</vnsAbsConnection>
</vnsAbsGraph>
</fvTenant>
</polUni>

```

サードパーティ ロードバランサの REST API を使用したサービス グラフの作成

サードパーティのロードバランサのサービス グラフを作成するには、次の手順を実行します。

```

<polUni>
<fvTenant name="infra" >
<!-- Abs Graph Creation -->
<vnsAbsGraph name="{graphName}" uiTemplateType="UNSPECIFIED" type="cloud" status="">
<vnsAbsTermNodeProv name="T2">
<vnsOutTerm/>
<vnsInTerm />
<vnsAbsTermConn attNotify="no" name="1" />
</vnsAbsTermNodeProv>
<vnsAbsTermNodeCon name="T1" >
<vnsOutTerm/>
<vnsInTerm />
<vnsAbsTermConn attNotify="no" name="1" />
</vnsAbsTermNodeCon>
<vnsAbsNode funcTemplateType="ADC_TWO_ARM" name="{F5Name}" managed="no">
<vnsRsNodeToCloudLDev tDn="uni/tn-infra/cld-{{F5Name}}"/>
<vnsAbsFuncConn attNotify="no" name="consumer" deviceLifName="external"/>
<vnsAbsFuncConn attNotify="no" name="provider" deviceLifName="internal"/>
</vnsAbsNode>
<vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
name="ConstTermToF5">
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsTermNodeCon-T1/AbsTConn"/>
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsNode-{{F5Name}}/AbsFConn-consumer"/>
</vnsAbsConnection>
<vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
name="F5ToProv">

```

REST API を使用してマルチノード サービス グラフを作成する

```

<vnsRsAbsConnectionConns
  tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsNode-{{F5Name}}/AbsFConn-provider" />
<vnsRsAbsConnectionConns
  tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsTermNodeProv-T2/AbsTConn"/>
</vnsAbsConnection>
</vnsAbsGraph>
</fvTenant>
</polUni>

```

REST API を使用してマルチノード サービス グラフを作成する

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

マルチノード サービス グラフを作成するには、次の例のような投稿を入力します。

```

<polUni>
  <fvTenant name="tn12_iar_iavpc" status="">
    <fvRsCloudAccount tDn="uni/tn-infra/[SubscriptionId]-vendor-azure"/>
    <fvCtx name="vrf50" status=""/>
    <fvCtx name="vrf60" status=""/>
    <cloudVpnGwPol name="VgwPol0"/>
    <cloudCtxProfile name="c50" status="">
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
      <cloudRsToCtx tnFvCtxName="vrf50"/>
      <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
      <cloudCidr addr="12.3.0.0/16" primary="true" status="">
        <cloudSubnet ip="12.3.30.0/24" status="" name="GatewaySubnet" usage="gateway">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="12.3.2.0/24" status="" name="ALBSubnet">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="12.3.1.0/24" status="" name="FwMgmtSubnet">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="12.3.3.0/24" status="" name="FwUntrustSubnet">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="12.3.4.0/24" status="" name="FwTrustSubnet">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="12.3.5.0/24" status="" name="ConsumerSubnet">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
    <cloudCtxProfile name="c60" status="">
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus2"/>
      <cloudRsToCtx tnFvCtxName="vrf60"/>
      <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
      <cloudCidr addr="12.4.0.0/16" primary="true" status="">
        <cloudSubnet ip="12.4.1.0/24" status="" name="ProviderSubnet">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="12.4.2.0/24" status="" name="NLBSubnet">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="12.4.30.0/24" status="" name="GatewaySubnet" usage="gateway">
          <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
        </cloudSubnet>
      </cloudCidr>

```

```

</cloudCtxProfile>
<cloudApp name="ap50" status="">
  <cloudEPg name="ap50vrf50epg1" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
    <fvRsCons tnVzBrCPName="con50"/>
    <fvRsProv tnVzBrCPName="con60"/>
    <cloudEPSelector matchExpression="IP=='12.3.5.0/24'" name="100"/>
  </cloudEPg>
  <cloudEPg name="ap50vrf50epg2" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
    <fvRsProv tnVzBrCPName="con60"/>
    <cloudEPSelector matchExpression="IP=='12.3.1.0/24'" name="100"/>
  </cloudEPg>
  <cloudExtEPg routeReachability="internet" name="ap50extepg1">
    <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
    <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
    <fvRsCons tnVzBrCPName="con60"/>
  </cloudExtEPg>
</cloudApp>
<cloudApp name="ap60" status="">
  <cloudEPg name="ap60vrf60epg1" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="vrf60"/>
    <fvRsProv tnVzBrCPName="con50"/>
    <fvRsProv tnVzBrCPName="con70"/>
    <cloudEPSelector matchExpression="IP=='12.4.1.0/24'" name="100"/>
  </cloudEPg>
  <cloudExtEPg routeReachability="internet" name="ap60extepg1">
    <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
    <cloudRsCloudEPgCtx tnFvCtxName="vrf60"/>
    <fvRsCons tnVzBrCPName="con70"/>
  </cloudExtEPg>
</cloudApp>
<vzBrCP name="con50" scope="tenant" status="">
  <vzSubj name="con50">
    <vzRsSubjFiltAtt tnVzFilterName="f10"/>
    <vzRsSubjGraphAtt tnVnsAbsGraphName="g1" status=""/>
  </vzSubj>
</vzBrCP>
<vzBrCP name="con60" scope="tenant" status="">
  <vzSubj name="con60">
    <vzRsSubjFiltAtt tnVzFilterName="f20"/>
  </vzSubj>
</vzBrCP>
<vzBrCP name="con70" scope="context" status="">
  <vzSubj name="con70">
    <vzRsSubjFiltAtt tnVzFilterName="f20"/>
  </vzSubj>
</vzBrCP>
<vzFilter name="f10" status="">
  <vzEntry etherT="ip" prot="icmp" name="f10entry1" status=""/>
  <vzEntry etherT="ip" prot="udp" dFromPort="1" dToPort="65535" name="f10entry2" status=""/>
  <vzEntry etherT="ip" prot="tcp" dFromPort="1" dToPort="65535" name="f10entry3" status=""/>
</vzFilter>
<vzFilter name="f20" status="">
  <vzEntry etherT="ip" prot="tcp" dFromPort="http" dToPort="http" name="f20entry1" status=""/>
  <vzEntry etherT="ip" prot="tcp" dFromPort="https" dToPort="https" name="f20entry2" status=""/>
  <vzEntry etherT="ip" prot="tcp" dFromPort="22" dToPort="22" name="f20entry3" status=""/>
</vzFilter>
<cloudLB name="FrontALB" type="application" scheme="internal" >
  <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn12_iar_iavpc/ctxprofile-c50/cidr-[12.3.0.0/16]/subnet-[12.3.2.0/24]"/>
</cloudLB>
<cloudLDev name="FW" svcType="FW" status="">
  <cloudRsLDevToCtx tDn="uni/tn-tn12_iar_iavpc/ctx-vrf50" />

```

```

<cloudLif name="provider" >
  <cloudEPSelector name="1" matchExpression="custom:tagp=='trustFW'"/>
</cloudLif>
<cloudLif name="consumer" >
  <cloudEPSelector name="1" matchExpression="custom:tagp=='untrustFW'"/>
</cloudLif>
</cloudLDev>
<cloudLB name="BackNLB" type="network" scheme="internal" >
  <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn12_iar_iavpc/ctxprofile-c60/cidr-[12.4.0.0/16]/subnet-[12.4.2.0/24]"/>
</cloudLB>
<vnsAbsGraph name="g1" type="cloud" status="" >
  <vnsAbsTermNodeProv name="Input1" >
    <vnsAbsTermConn name="C1"/>
  </vnsAbsTermNodeProv>
  <vnsAbsTermNodeCon descr="" name="Output1" nameAlias="" ownerKey="" ownerTag="" >
    <vnsAbsTermConn name="C2" />
  </vnsAbsTermNodeCon>
  <vnsAbsNode funcType="GoTo" name="N1" managed="yes" funcTemplateType="ADC_ONE_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/clb-FrontALB" />
    <vnsAbsFuncConn attNotify="no" descr="" name="provider" nameAlias="" ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" name="consumer" nameAlias="" ownerKey="" ownerTag=""/>
    <cloudSvcPolicy tenantName="tn12_iar_iavpc" contractName="con50" subjectName="con50" >
      <cloudListener name="http_listener1" port="80" protocol="http">
        <cloudListenerRule name="rule1" priority="20" default="yes" >
          <cloudRuleAction type="forward" port="80" protocol="http"/>
        </cloudListenerRule>
      </cloudListener>
    </cloudSvcPolicy>
  </vnsAbsNode>
  <vnsAbsNode funcType="GoTo" name="N2" managed="no" funcTemplateType="ADC_TWO_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/cld-FW" />
    <vnsAbsFuncConn attNotify="no" descr="" connType="snat_dnat" name="provider" nameAlias=""
ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" connType="none" name="consumer" nameAlias="" ownerKey=""
ownerTag=""/>
  </vnsAbsNode>
  <vnsAbsNode funcType="GoTo" name="N3" managed="yes" funcTemplateType="ADC_ONE_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/clb-BackNLB" />
    <vnsAbsFuncConn attNotify="no" descr="" name="provider" nameAlias="" ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" name="consumer" nameAlias="" ownerKey="" ownerTag=""/>
    <cloudSvcPolicy tenantName="tn12_iar_iavpc" contractName="con50" subjectName="con50" >
      <cloudListener name="http_listener1" port="80" protocol="tcp">
        <cloudListenerRule name="rule1" priority="20" default="yes" >
          <cloudRuleAction type="forward" port="80" protocol="tcp"
epgdn="uni/tn-tn12_iar_iavpc/cloudapp-ap60/cloudepg-ap60vrf60epg1"/>
        </cloudListenerRule>
      </cloudListener>
    </cloudSvcPolicy>
  </vnsAbsNode>
  <vnsAbsConnection connDir="provider" connType="external" name="CON4">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N3/AbsFConn-provider"/>
  </vnsAbsConnection>
  <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsTermNodeProv-Input1/AbsTConn"/>
</vnsAbsConnection>
  <vnsAbsConnection connDir="consumer" connType="external" name="CON1">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsTermNodeCon-Output1/AbsTConn"/>
  </vnsAbsConnection>
  <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N1/AbsFConn-consumer"/>
</vnsAbsConnection>
  <vnsAbsConnection connDir="consumer" connType="external" name="CON2">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N1/AbsFConn-provider"/>
  </vnsAbsConnection>

```

```

<vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N2/AbsFConn-consumer"/>
</vnsAbsConnection>
<vnsAbsConnection connDir="consumer" connType="external" name="CON3">
<vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N2/AbsFConn-provider"/>

<vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N3/AbsFConn-consumer"/>

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

```

REST API を使用してリダイレクトでマルチノード サービス グラフを作成する

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

ステップ1 インフラ テナントを設定するには、次の手順を実行します。

```

<polUni>
  <fabricInst>
    <commPol name="default">
      <commSsh name="ssh" adminSt="enabled" passwordAuth="enabled" />
    </commPol>
    <dnsProfile name="default">
      <dnsProv addr="172.23.136.143" preferred="yes" status="" />
    </dnsProfile>
  </fabricInst>
  <fvTenant name="infra">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[[{subscriptionId}]]-vendor-azure"/>
    <cloudAccount name="insbu" id="[[{subscriptionId}]]" vendor="azure" accessType="credentials"
status="">
      <cloudRsCredentials tDn="uni/tn-infra/credentials-CNC-App"/>
    </cloudAccount>
    <cloudCredentials name="CNC-App" keyId="[[{accessKeyId}]]" key="[[{accessKey}]]" httpProxy="">
      <cloudRsAD tDn="uni/tn-infra/ad-[[{adId}]]"/>
    </cloudCredentials>
    <cloudAD name="CiscoINSBUAd" id="[[{adId}]]" />
    <cloudApicSubnetPool subnet="10.10.1.0/24" />
    <cloudtemplateInfraNetwork name="default" numRoutersPerRegion="2" vrfName="overlay-1"
numRemoteSiteSubnetPool="1" status="">
      <cloudtemplateProfile name="default" routerUsername="cisco" routerPassword="ins3965" />
      <cloudtemplateExtSubnetPool subnetpool="11.11.0.0/16" status="" />
      <cloudtemplateExtNetwork name="default" status="">
        <cloudRegionName provider="azure" region="[[{region}]]" />
        <cloudtemplateVpnNetwork name="default">
          <cloudtemplateIpSecTunnel peeraddr="[[{peerAddress}]]"/>
          <cloudtemplateOspf area="0.0.0.1" />
        </cloudtemplateVpnNetwork>
      </cloudtemplateExtNetwork>
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="[[{region}]]"/>
      </cloudtemplateIntNetwork>
    </cloudtemplateInfraNetwork>
  </fvTenant>
  <cloudDomP>
    <cloudBgpAsP asn="1111"/>
  </cloudDomP>

```

```

    <cloudProvP vendor="azure">
      <cloudRegion adminSt="managed" name="{{region}}">
        <cloudZone name="default"/>
      </cloudRegion>
    </cloudProvP>
  </cloudDomP>
</polUni>

```

ステップ2 ハブ VNet でサービス デバイスを構成するには：

```

<polUni>
  <fvTenant name="infra">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[[{subscriptionId}]-vendor-azure"/>
    <cloudCtxProfile name="ct_ctxprofile_{{region}}" status="modified">
      <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

      <cloudCidr name="cidr1" addr="{{HubCidrSvc}}" primary="no" status="">
        <cloudSubnet ip="{{HubNLBSubnet}}" name="HubNLBSubnet" status="">
          <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="{{HubFWSubnetInt}}" name="HubFWSubnetInt" status="">
          <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="{{HubFWSubnetExt}}" name="HubFWSubnetExt" status="">
          <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="{{HubFWMgmtSubnet}}" name="HubFWMgmtSubnet" status="">
          <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="{{ConsHubEPgSubnet}}" name="ConsHubEPgSubnet" status="">
          <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
        </cloudSubnet>
      </cloudCidr>
    </cloudCtxProfile>
    <cloudLDev name="{{FWName}}" status="">
      <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-{{ServicevVNetName}}"/>
      <cloudLIf name="external" >
        <cloudEPSelector matchExpression="custom:EPG=='FwExt'" name="1"/>
      </cloudLIf>
      <cloudLIf name="internal" >
        <cloudEPSelector matchExpression="custom:EPG=='FwInt'" name="1"/>
      </cloudLIf>
    </cloudLDev>
    <cloudLB name="{{NLBName}}" type="network" scheme="internal" size="small" instanceCount="2"
status="">
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-infra/ctxprofile-ct_ctxprofile_{{region}}/cidr-[[{HubCidrSvc}]/subnet-[[{HubNLBSubnet}]]"
status=""/>
    </cloudLB>
  </fvTenant>
</polUni>

```

ステップ3 プロバイダーとスポークのグラフを構成するには：

```

<polUni>
  <fvTenant name="{{tnNameProv}}" status="" >
    <fvRsCloudAccount tDn="uni/tn-infra/act-[[{subscriptionId}]-vendor-azure"/>

```



```

<fvCtx name="{{ProviderVNetName}}"/>
<cloudCtxProfile name="{{ProviderVNetName}}" status="">
  <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
  <cloudRsCtxProfileToRegion status="" tDn="uni/cloudddomp/provp-azure/region-{{region}}"/>

  <cloudRsToCtx tnFvCtxName="{{ProviderVNetName}}"/>
  <cloudCidr name="cidr1" addr="{{VnetCidrProv}}" primary="yes" status="">
    <cloudSubnet ip="{{ProviderSubnet}}" name="ProviderSubnet" status="">
      <cloudRsZoneAttach status=""
tDn="uni/cloudddomp/provp-azure/region-{{region}}/zone-default"/>
    </cloudSubnet>
    <cloudSubnet ip="{{BackALBSubnet}}" name="BackALBSubnet" status="">
      <cloudRsZoneAttach status=""
tDn="uni/cloudddomp/provp-azure/region-{{region}}/zone-default"/>
    </cloudSubnet>
  </cloudCidr>
</cloudCtxProfile>
<!-- contract-->
<vzFilter descr="" name="HttpsFilter" ownerKey="" ownerTag="">
  <vzEntry dFromPort="443" dToPort="443" etherT="ip" name="https" prot="tcp" status=""/>
  <vzEntry dFromPort="80" dToPort="80" etherT="ip" name="http" prot="tcp" status=""/>
  <vzEntry dFromPort="22" dToPort="22" etherT="ip" name="ssh" prot="tcp" status=""/>
</vzFilter>
<vzBrCP name="{{contractName}}" scope="global" status="">
  <vzSubj name="Sub1" revFltPorts="yes">
    <vzRsSubjGraphAtt directives="" tnVnsAbsGraphName="{{graphName}}"/>
    <vzRsSubjFiltAtt tnVzFilterName="HttpsFilter"/>
  </vzSubj>
</vzBrCP>
<!-- cloud App Profile-->
<cloudApp name="provApp" status="">
  <cloudEPg name="App" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="{{ProviderVNetName}}"/>
    <cloudEPSelector matchExpression="custom:EPG=='App'" name="1"/>
    <fvRsProv status="" tnVzBrCPName="{{contractName}}"/>
    <fvRsProv tnVzBrCPName="mgmt_common"/>
  </cloudEPg>
</cloudApp>
<!-- Abs Graph Creation -->
<vnsAbsGraph name="{{graphName}}" uiTemplateType="UNSPECIFIED" type="cloud">
  <vnsAbsTermNodeProv name="T2">
    <vnsOutTerm/>
    <vnsInTerm />
    <vnsAbsTermConn attNotify="no" name="1" />
  </vnsAbsTermNodeProv>
  <vnsAbsTermNodeCon name="T1" >
    <vnsOutTerm/>
    <vnsInTerm />
    <vnsAbsTermConn attNotify="no" name="1" />
  </vnsAbsTermNodeCon>
  <vnsAbsNode name="{{NLBName}}" managed="yes" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-infra/clb-{{NLBName}}" status=""/>
    <cloudSvcPolicy tenantName="{{tnNameProv}}" contractName="{{contractName}}"/>
  </vnsAbsNode>
  <cloudHealthProbe name="http_listener1-rule1" protocol="tcp" port=22 interval=15
unhealthyThreshold=2/>
    <cloudListener name="http_listener1" port="80" protocol="tcp" status="">
      <cloudListenerRule name="rule1" default="true">
        <cloudRuleAction type="haPort" port="80" protocol="tcp"
healthProbe="http_listener1-rule1"/>
      </cloudListenerRule>
    </cloudListener>
  </cloudSvcPolicy>
  <vnsAbsFuncConn attNotify="no" name="provider" connType="redir"/>

```

```

        <vnsAbsFuncConn attNotify="no" name="consumer" connType="redir"/>
    </vnsAbsNode>
    <vnsAbsNode funcTemplateType="FW_ROUTED" name="{{FWName}}" managed="no">
        <vnsRsNodeToCloudLDev tDn="uni/tn-infra/cld-{{FWName}}" />
        <vnsAbsFuncConn attNotify="no" name="consumer" deviceLIIfName="internal"/>
        <vnsAbsFuncConn attNotify="no" name="provider" deviceLIIfName="internal"/>
    </vnsAbsNode>
    <vnsAbsNode name="{{BackALBName}}" managed="yes">
        <vnsRsNodeToCloudLDev tDn="uni/tn-{{tnNameProv}}/clb-{{BackALBName}}"/>
        <cloudSvcPolicy tenantName="{{tnNameProv}}" contractName="{{contractName}}"
subjectName="Sub1" status="">
            <cloudListener name="http_listener1" port="80" protocol="http" status="">
                <cloudListenerRule name="rule1" default="true">
                    <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-{{tnNameProv}}/cloudapp-provApp/cloudepg-App"/>
                </cloudListenerRule>
            </cloudListener>
        </cloudSvcPolicy>
        <vnsAbsFuncConn attNotify="no" name="provider"/>
        <vnsAbsFuncConn attNotify="no" name="consumer"/>
    </vnsAbsNode>
    <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
name="ConstTermToNLB">
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsTermNodeCon-T1/AbsTConn"/>
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{NLBName}}/AbsFConn-consumer"/>
    </vnsAbsConnection>
    <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
name="NLBToFW">
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{NLBName}}/AbsFConn-provider" />
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{FWName}}/AbsFConn-consumer"/>
    </vnsAbsConnection>
    <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
name="FWToBackALB">
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{FWName}}/AbsFConn-provider" />
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{BackALBName}}/AbsFConn-consumer"/>
    </vnsAbsConnection>
    <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
name="BackALBToProv">
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{BackALBName}}/AbsFConn-provider" />
        <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsTermNodeProv-T2/AbsTConn"/>
    </vnsAbsConnection>
</vnsAbsGraph>
    <cloudLB name="{{BackALBName}}" type="application" scheme="internal" size="small"
instanceCount="2">
        <cloudRsLDevToCloudSubnet
tDn="uni/tn-{{tnNameProv}}/ctxprofile-{{ProviderVNetName}}/cidr-{{VnetCidrProv}}/subnet-{{BackALBSubnet}}">
            status="" />
        </cloudLB>
    </fvTenant>
</polUni>

```

ステップ 4 コンシューマを構成し、プロバイダーで定義されたコントラクトをインポートするには：

```

<polUni>
    <fvTenant name="{{tnNameCons}}" >

```

```

<fvRsCloudAccount tDn="uni/tn-infra/act-{{subscriptionId}}-vendor-azure"/>
<fvCtx name="{{ConsumerVNetName}}"/>
<cloudCtxProfile name="{{ConsumerVNetName}}" status="">
  <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
  <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

  <cloudRsToCtx tnFvCtxName="{{ConsumerVNetName}}"/>
  <cloudCidr name="cidr1" addr="{{VnetCidrCons}}" primary="yes" status="">
    <cloudSubnet ip="{{ConsumerSubnet}}" name="ConsumerSubnet" status="">
      <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
    </cloudSubnet>
  </cloudCidr>
</cloudCtxProfile>
<vzCPIf name="imported_{{contractName}}">
  <vzRsIf tDn="uni/tn-{{tnNameProv}}/brc-{{contractName}}"/>
</vzCPIf>
<!-- cloud App Profile-->
<cloudApp name="consApp" status="">
  <cloudEPg name="Web" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="{{ConsumerVNetName}}"/>
    <cloudEPSelector matchExpression="custom:EPG=='Web'" name="1"/>
    <fvRsConsIf tnVzCPIfName="imported_{{contractName}}"/>
    <fvRsProv tnVzBrCPName="mgmt_common"/>
  </cloudEPg>
</cloudApp>
</fvTenant>
</polUni>

```

REST API を使用してサービス グラフを添付する

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

ステップ 1 アプリケーション ゲートウェイのサービス グラフをアタッチするには :

```

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

    <vzBrCP name="c1">
      <vzSubj name="c1">
        <vzRsSubjGraphAtt tnVnsAbsGraphName="c15_g1"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>

```

ステップ 2 Azure ロード バランシングのサービス グラフをアタッチするには :

```

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

<fvTenant name="tn15">

```

```

<vzBrCP name="c1">
<vzSubj name="c1">
<vzRsSubjGraphAtt tnVnsAbsGraphName="c15_g1" />
</vzSubj>
</vzBrCP>
</fvTenant>
</polUni>

```

REST API を使用した HTTPS サービス ポリシーの構成

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

ステップ 1 Application Gateway の HTTP サービス ポリシーを作成するには：

```

<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="http_listener1" port="80" protocol="http" status="">
            <cloudListenerRule name="rule1" priority="10" default="yes" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectRule" priority="20">
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="redirect" RedirectPort="8080"/>
            </cloudListenerRule>
            <cloudListenerRule name="FixedRspRule" priority="30">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleAction type="fixedResponse" FixedResponseCode="200"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectHPRule" priority="40" status="">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
          </cloudListener>
        </cloudSvcPolicy>
      </vnsAbsNode>
    </vnsAbsGraph>
  </fvTenant>
</polUni>

```

ステップ 2 ネットワーク ロードバランサの HTTP サービス ポリシーを作成するには：

```

<?xml version="1.0" encoding="UTF-8"?>
<polUni>

```

```

<fvTenant name="tn15">
  <vnsAbsGraph name="CloudGraph" type="cloud" status="">
    <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
      <cloudSvcPolicy tenantName=" tn15" contractName="httpFamily" subjectName="consubj">

        <cloudListener name="tcp_listener" port="80" protocol="tcp" status="">
          <cloudListenerRule name="rule1" priority="10" default="yes" status="">
            <cloudRsListenerToVip tDn="uni/tn-infra/clb-NLB/vip-IP1" status=""/>
            <cloudRuleAction type="forward" port="80" protocol="tcp" epgdn="uni/tn-
tn15/cloudapp-ap/cloudepg-provEPG" />
          </cloudListenerRule>
        </cloudListener>
        <cloudListener name="udp_listener" port="55" protocol="udp" status="">
          <cloudListenerRule name="rule1" priority="10" default="yes" status="">
            <cloudRsListenerToVip tDn="uni/tn-infra/clb-NLB/vip-IP1" status=""/>
            <cloudRuleAction type="forward" port="55" protocol="udp" epgdn="uni/tn-
tn15/cloudapp-ap/cloudepg-provEPG" />
          </cloudListenerRule>
        </cloudListener>
      </cloudSvcPolicy>
    </vnsAbsNode>
  </vnsAbsGraph>
</fvTenant>
</polUni>

```

このドキュメントで前述したように、ネットワークロードバランサで定義されている場合、リスナールールとルールアクションの設定は、ロードバランサのフロントエンド構成からバックエンドプールへのマッピングを構築します。この例では、以下のようになっています。

- `cloudListenerRule` 行は、単一のフロントエンド IP アドレスを使用してリスナーを構成するために使用されますが、Cisco Cloud Network Controller 上のインターネットに接続されたネットワークロードバランサ用に異なるポートとプロトコルの組み合わせを使用します。
- `cloudRsListenerToVip` 行は、Cisco Cloud Network Controller 上のインターネット向けネットワークロードバランサの複数のフロントエンドでリスナールールを構成するために使用されます。各フロントエンドは、フロントエンド IP アドレス、ポート、およびプロトコルのタプルの組み合わせとして表されます。詳細については、[Azure ネットワークロードバランサの複数のフロントエンド IP アドレスの構成について \(203 ページ\)](#) を参照してください。

REST API を使用したキー リングの設定

この例では、REST API を使用したキー リングのリーク ルートを構成する方法を示します。キー リング構成の詳細については、*Cisco APIC 基本構成ガイド*を参照してください。



(注) この手順は、アプリケーションゲートウェイにのみ適用されます。

キー リングを設定するには:

```

<polUni>
  <fvTenant name="tn15" >
    <cloudCertStore>

```

REST API を使用したキー リングの設定

```

<pkKeyRing status="" name="lbCert" tp="lbTP" key="-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA4DGxaK+RHv/nToHLnmDBq2BfLimgX/zNJQC9bGuzr8Mj7dm0
XuHfQYGV0h1PtL4Pdx5f5qjB0NbHjAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCRE
Ginn/CgF75QPTEd568eScND2Pt/eMeHAuRX/PykKUatWWncGanjvHqc+SOLPF6TD
gQ5nwOHhfVvyM2DY8bfdYWrWmGsO7JqZzbPMptA2QWb1LsSoIrdkIIgf6ZfYy/EN
bh+nYN2rJT8LzYsxs0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8KOfdCZPEq
8takiWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQABAoIBAQQDQqA9IsLrYrdtqN
q6mZ3s2BNfF/4kgb7gn0Dws+9EJLJCJNZVhFEo2ZxxyfPp6HRnjYS50W83/E1anD
+GD1bSucTuxqFWIQVh7rlebYZIWK+NYSjr5yNVxux8U2hCNNV8WWWVqkJjKcUqICB
Bm47FKj53LV46zE0gyCaibFrYxZJ9+farGneyBdnov+3thmez7534KCi0t3J3Eri
lgSY3ql6hPXB2ZXAP4jdAoLgWDU4I1M6OqOiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5G1fV2A4xTBQMCTUZJ9fYAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphED1AoGBAPvlvKfGW46qqRnYovfryxxz4OMlsvSgcJpQTQtBQi2koJ8OweZJ
2s+CX0r+oDqwP23go/QEVYVkcic9RGkJBNGel+dm/bTjzgmQYtqSCNtecTsZD5JN
y1jkciiizznDkjcjReSZ2kh3dGXIBriYk7ezp2z7EKfDrHe5x5ouGMgCnAoGBAOnh
buDEohv8KJaB+DiUfhtoa3aKNPBO+zWPCHP0HFGjPXshJcIYZc1GycmuDKVnNdD
MxhE/yOnQHowl4T9FMLpz5yh5zuCUVqOBgB1P6Mzbc5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCW1OAFJRw3c/OiESwLMzchsl8RnbwOi6kDaGBANV1zmPb07zB3eGTCU0t
KGIqWFLncUkVaDZRFZYPpNwiRkoe73j9brkNbgCqxW+Nlp5UjoeFry0N6y106q/
ZA4I7FnXryLBw2HYuw41Vixl+XOZ/HeO3RmFNlZ717dGmaGbv43aKIB9x+X5n8wF
6z1ntBHmBk7yNwomlIRag1sbAoGAX0p4cJ/tJNXSe7AswHDQCL68uimJdDfZ5nKG
k83nE+Qc0QoZDJAmCiSFmuSNRnSep3FiafjBFXK0X4h+mdbJc7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztZTn+as6xKOUATEezy9DK9zMWzQhhtay
m9yZTp0CgYEALUtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdgJt88ezM1Oej
Pdoab0G2PcfGjZToTSgk7N4XArVKeq7pgZ0kwcYAsh06A2Hal+D1z/bGoZP+kmd/x
Ny82phxYOXCnEc5Vv921U59+j7e067UFLAYJe6fu+oFImvofRnP4DIQ=
-----END RSA PRIVATE KEY-----" cert="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAKGA1UECBMCQ0ExETAPBgNVBACTCFhbiBk3N1M1RiEAYDVQQK
Ew1NeUNvbXBhbnkxDjAMBGNVBAStBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVV0XDE5MTAwMjIwNTMwNVV0Y0xCZAJBgNVBAYTA1VTMQswCQYDVQQIEw
JDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBGNVBAoTCU15Q29tcGFueTEOMAwG
A1UECXMFTXl1PcmcxGDAwBgNVBAMUDyouYW1hem9uYXZzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBQUAA4IBDwAw
ggEKAoIBAQQDgMbFor5Ee/+dOgcueYMGryF8uKaBf/M01AL1sa70vwyPt2bRe4d9B
ga/SHU+Ovg93f/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXv1A8h53nrX5JW0Nk+394x4c5Ff8/KQPrq1Zadwzqe08epz5I4s8XpMOBDMfA
4ccw/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QigB/pl9jL8Q1sf6dg
3aslPyXniZHPRIzHSHfAdOI3Y2INj9lXrflEJd8u2qk1kK4Pwo590Jk8Sry1qSj
YHGJhN8dE+xxYB1ZCyIqAbWtG0RsUD1AgMBAAGjgUwgfIwHQYDVRO0BBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMGbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAKGA1UECBMCQ0ExETAPBgNV
BACTCFhbiBk3N1M1RiEAYDVQQKEw1NeUNvbXBhbnkxDjAMBGNVBAStBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvbmF3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAe/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iUR84mQzhoT
nx5CN109xu5ml5baCYZzsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoelewv+wR10oVRCh1TfKtXO68TUK6vRqpW76hKfOHIA7b2h1IIMdq6VA/
+A5FQ0xqYfKdVd2RaINpzI8mqZiszw+7E6j1PL5k4tftWEaYpFGP1VesFEyJEL
ghBUIPt8TibaMYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjMDL3tpFwg
qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
-----END CERTIFICATE-----">
</pkKeyRing>

```

```

<pkITP status="" name="lbTP" certChain="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAKGA1UECBMCQ0ExETAPBgNVBACTCFhbiBk3N1M1RiEAYDVQQK
Ew1NeUNvbXBhbnkxDjAMBGNVBAStBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVV0XDE5MTAwMjIwNTMwNVV0Y0xCZAJBgNVBAYTA1VTMQswCQYDVQQIEw
JDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBGNVBAoTCU15Q29tcGFueTEOMAwG
A1UECXMFTXl1PcmcxGDAwBgNVBAMUDyouYW1hem9uYXZzLmNvbTEgMB4GCSqGSIb3

```

```

DQEJARYRcmFtc2hhaEBjaXNjby5jb20wgEiMA0GCSqGSIB3DQEBAQUAA4IBDwAw
ggEKAOIBAqDgMbFor5Ee/+dOgcueYMGryF8uKaBf/M01AL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXv1A8h53nrX5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqeO8epz5I4s8XpMOBDMfA
4ccW/IzYNjxt9lhataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/p19jL8Q1sf6dg
3aslPyXNizHPRiZHSHFAdOI3Y2INj91XrfLEJd8uD2qk1kK4Pwo590Jk8Sry1qSj
YHGJHn8dE+xxYB1ZCYiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMegbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BACTCFNhb1Bkb3N1MR1wEAYDVQQKEw1NeUNvbXBhbnkxKjAMBgNVBAsTBu15T3Jn
MRgwFgYDVQDFA8qLmFtYXpvc20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2l2Y28uY29tgkgkApY2On/9qsGwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAE/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5ml5baCYZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiShoeleWv+wRl0oVRChlTfKtXO68TUK6vraqpw76hKfOHIA7b2h1IIMdq6VA/
+A5FQ0xqYfKdVd2RaInpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfGp1VesFEyJEL
gHBUiPt8TIbamiYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjmdL3tpFwg
qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
-----END CERTIFICATE-----"
    </pkiTP>
    </cloudCertStore>
    </fvTenant>
</polUni>

```

REST API を使用した HTTPS サービス ポリシーの作成

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



- (注) リスナーは複数の証明書をもつことができます。証明書のオプションは次のとおりです。
- ELBSecurityPolicy-2016-08 – セキュリティ ポリシーが選択されていない場合のデフォルト。
 - ELBSecurityPolicy-FS-2018-06
 - ELBSecurityPolicy-TLS-1-2-2017-01
 - ELBSecurityPolicy-TLS-1-2-Ext-2018-06
 - ELBSecurityPolicy-TLS-1-1-2017-01
 - ELBSecurityPolicy-2015-05
 - ELBSecurityPolicy-TLS-1-0-2015-04

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

始める前に

キーリング証明書は既に構成されています。



(注) これは、アプリケーション ゲートウェイにのみ適用されます。

HTTPS サービス ポリシーを作成するには:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="https_listener" port="443" protocol="https"
secPolicy="eLBSecurityPolicy-2016-08" status="">
            <cloudRsListenerToCert defaultCert="yes" certStore="default"
tDn="uni/tn-t2/certstore/keyring-lbCert" status=""/>
            <cloudListenerRule name="defaultRule" default="yes" priority="100" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t1/cloudapp-ap/cloudepg-epl">
                </cloudRuleAction>
              </cloudListenerRule>
            </cloudListener>
          </cloudSvcPolicy>
        </vnsAbsNode>
      </vnsAbsGraph>
    </fvTenant>
  </polUni>
```




第 7 章

Cisco Cloud Network Controller のセキュリティ

この章は、次の内容で構成されています。

- [アクセス、認証およびアカウントティング](#) (301 ページ)
- [TACACS+、RADIUS、LDAP、および SAML アクセスの構成](#) (302 ページ)
- [HTTPS Access の構成](#) (311 ページ)

アクセス、認証およびアカウントティング

Cisco Cloud Network Controller ポリシーは、認証、認可、アカウントティング (AAA) 機能を管理します。ユーザ権限、ロール、およびドメインとアクセス権限の継承を組み合わせることにより、管理者は細分化された方法で管理対象オブジェクトレベルで AAA 機能を設定することができます。これらの設定は、REST API または GUI を使用して実行できます。



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

アクセス、認証、およびアカウント構成情報の詳細については、[Cisco Cloud Network Controller Security Configuration Guide](#) をお読みください。

構成

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

ローカルユーザの設定

[Cisco Cloud Network Controller GUI を使用したローカルユーザーの作成](#) (154 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) メニューバーで、**[管理 (Administrative)]** > **[認証 (Authentication)]** を選択します。
- b) 作業ペインで、**[プロバイダー (Providers)]** タブをクリックして、**[アクション (Actions)]** ドロップダウンをクリックして、**[プロバイダーの作成 (Create Provider)]** を選択します。

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

- c) **[ホスト名/IP アドレス (Host name/IP Address)]** フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- d) **[説明 (Description)]** フィールドに、プロバイダーの説明を入力します。
- e) **[タイプ (Type)]** ドロップダウンリストをクリックし、**[TACACS+]** を選択します。
- f) **[設定 (Settings)]** セクションで、**[キー (Key)]**、**[ポート (Port)]**、**[認証プロトコル (Authentication Protocol)]**、**[タイムアウト (Timeout)]**、**[再試行 (Retries)]**、**[管理 EPG (Management EPG)]** を指定します。有効化 (Enabled) または 無効化 (Disabled) のいずれかを **[サーバー監視 (Server Monitoring)]** に対して選択します。

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

- a) **インテント アイコン** をクリックします。

[インテント (Intent)] メニューが表示されます。

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

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから TACACS+ を選択します。
プロバイダ (Providers)	<p>プロバイダーを選択するには :</p> <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成]ダイアログボックスに戻ります。

- e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

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

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

始める前に

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

ステップ 1 Cisco Cloud 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。

- メニューバーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- 作業ペインで、[プロバイダー (Providers)] タブをクリックして、[アクション (Actions)] ドロップダウンをクリックして、[プロバイダーの作成 (Create Provider)] を選択します。
[プロバイダーの作成 (Create Provider)] ダイアログボックスが表示されます。
- [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- [タイプ (Type)] ドロップダウンリストをクリックし、[RADIUS] を選択します。
- [設定 (Settings)] セクションで、[キー (Key)]、[ポート (Port)]、[認証プロトコル (Authentication Protocol)]、[タイムアウト (Timeout)]、[再試行 (Retries)]、[管理 EPG (Management EPG)] を指定します。有効化 (Enabled) または 無効化 (Disabled) のいずれかを [サーバー監視 (Server Monitoring)] に対して選択します。

ステップ 2 RADIUS の [ログイン ドメイン] を作成します。

- 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。
- [インテント (Intent)] 検索ボックスの下にあるドロップダウン矢印をクリックし、[管理 (Administrative)] を選択します。
[Intent] メニューに管理オプションのリストが表示されます。
- [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。
- 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

[プロパティ (Properties)]	説明
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから RADIUS を選択します。
プロバイダ (Providers)	<p>プロバイダーを選択するには :</p> <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

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

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

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

LDAP Access の構成

LDAP 設定には 2 つのオプションがあります。

- Cisco AVPair の設定

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

次のセクションには、両方の構成オプションの手順が含まれています。

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

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

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

始める前に

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

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

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

- (注)
- バインド DN は、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。

- メニューバーで、**[管理 (Administrative)] > [認証 (Authentication)]** を選択します。
- [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。
- 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] を選択します。
プロバイダ (Providers)	<p>プロバイダーを選択するには：</p> <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

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

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

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>/ADFS>/FederationMetadata/2007-06/FederationMetadata.xml` という形式になります。

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

ステップ 2 SAML のログイン ドメインを作成します。

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

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

[プロパティ (Properties)]	説明
プロバイダ (Providers)	プロバイダーを選択するには : <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

d) [保存 (Save)] をクリックして、設定を保存します。

Okta で SAML アプリケーションの設定

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

AD FS で Relying Party Trust の設定

[Cisco Cloud Network Controller Security Configuration Guide](#) の [AD FS での証明書利用者信頼の設定 (Setting Up a Relying Party Trust in AD FS)] セクションを参照してください。

HTTPS Access の構成

ここでは、HTTPS Access を構成する方法について説明します。

HTTPS アクセスについて

この記事は、Cisco ACI を使用する際の HTTPS アクセスのカスタム証明書を設定する方法の例を示します。

詳細については、の『[Cisco Cloud Network Controller Security Configuration Guide](#)』の「*HTTPS Access*」の項を参照してください。

カスタム証明書の構成のガイドライン

- ワイルドカード証明書 (*.cisco.com など。複数のデバイス間で使用) およびそれに関連する他の場所で生成される秘密キーは、Cisco クラウド ネットワーク コントローラではサポートされません。これは、Cisco クラウド ネットワーク コントローラ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ので、メンテナンス時間中のみこのタスクを実行してください。この操作中に Cisco Cloud Network Controller のすべての Web サーバの再起動が予期されます。

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

- ステップ 2 [作業 (Work)] ペインで、[証明書認証局 (Certificate Authorities)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [証明書認証局の作成 (Create Certificate Authorities)] を選択します。
- ステップ 3 [証明書認証局の作成 (Create Certificate Authority)] ダイアログボックスの [名前 (Name)] フィールドに、認証局の名前を入力します。
- ステップ 4 [用途 (Used for)] フィールドで [システム (System)] を選択します。
- ステップ 5 [証明書チェーン (Certificate Chain)] フィールドで、Cisco Cloud Network Controller の証明書署名要求 (CSR) に署名する認証局の中間証明書とルート証明書をコピーします。証明書は、Base64 エンコード X.509 (CER) 形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。
- ```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 メニューバーで、[管理 (Administrative)] > [セキュリティ (Security)] を選択します。
- ステップ 8 [作業 (Work)] ペインで、[キーリング (Key Rings)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [キーリングの作成 (Create Key Ring)] を選択します。
- ステップ 9 [キーリングの作成 (Create Key Ring)] ダイアログボックスで、[名前 (Name)] フィールドにキーリングの名前を入力し、[説明 (Description)] フィールドに説明を入力します。
- ステップ 10 [用途 (Used for)] フィールドで [システム (System)] を選択します。
- ステップ 11 [証明書認証局 (Certificate Authority)] フィールドで、[証明書認証局の選択 (Select Certificate Authority)] をクリックし、以前に作成した認証局を選択します。
- ステップ 12 [秘密キー (Private Key)] フィールドで、[新規キーの生成 (Generate New Key)] または [既存のキーのインポート (Import Existing Key)] を選択します。[既存のキーのインポート (Import Existing Key)] を選択した場合は、[秘密キー (Private Key)] テキストボックスに秘密キーを入力します。
- ステップ 13 [モジュラス (Modulus)] ドロップダウンからモジュラスを選択します。メニュー
- ステップ 14 [Certificate] フィールドには、コンテンツを追加しないでください。
- ステップ 15 [保存 (Save)] をクリックします。
- [Work] ペインの [Key Rings] 領域では、作成したキーリングに対する [Admin State] に [Started] と表示されます。
- ステップ 16 作成したキーリングをダブルクリックして、[作業 (Work)] ペインから [キーリング] [key\_ring\_name] ダイアログボックスを開きます。
- ステップ 17 [作業 (Work)] ペインで、[証明書要求の作成 (Create Certificate Request)] をクリックします。
- ステップ 18 [情報カテゴリ (Subject)] フィールドに、Cisco 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 Cloud 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 8 章

# アクセスの制限

- [ドメイン別にアクセスを制限する \(315 ページ\)](#)
- [RBAC ルール \(316 ページ\)](#)
- [RBACルール \(321 ページ\)](#)
- [制限付きドメインのガイドラインと制限事項 \(321 ページ\)](#)
- [Cisco Cloud Network Controller GUI を使用した RBAC ルールの作成 \(322 ページ\)](#)

## ドメイン別にアクセスを制限する

制限付きセキュリティ ドメインを使用すると、テナント A などのファブリック管理者は、両方のグループのユーザーに同じ権限が割り当てられている場合、あるユーザーグループがテナント B などの別のセキュリティ ドメインのユーザーグループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、テナント A の制限付きセキュリティ ドメインのテナント管理者は、テナント B のセキュリティ ドメインで構成されたポリシー、プロファイル、またはユーザーを表示できません。テナント B のセキュリティ ドメインも制限されていない限り、テナント B は、テナント A で設定されたポリシー、プロファイル、またはユーザーを表示できます。ユーザーが適切な権限を持つシステム作成の設定に対して、ユーザーは常に読み取り専用で閲覧可能であることに注意してください。

たとえば、制限付きセキュリティ ドメインのユーザがテナント A に関連付けられているとします。テナント A には、ユーザが作成したアプリケーション プロファイル 1 と管理者が作成したアプリケーション プロファイル 2 の 2 つのアプリケーション プロファイルが含まれています。アプリケーション プロファイル 2 も同じテナントのもですが、ユーザはアプリケーション プロファイル 1 しか表示できません。ユーザが制限付きセキュリティ ドメインにいる場合、管理者によって作成されたプロファイルも表示されません。

上記の例では、アプリケーション プロファイル 2 は別のユーザ（管理者）によって作成されていますが、制限のないユーザ（制限付きのセキュリティ ドメインに属していないユーザ）は、アプリケーション プロファイル 1 とアプリケーション プロファイル 2 の両方を表示できます。

# RBAC ルール

Cloud Network Controller では、ロールベース アクセス コントロール (RBAC) を介してユーザのロールに従ってアクセスが提供されます。ファブリック ユーザは以下に関連付けられています。

- ロールのセット
- ロールごとの権限タイプ : アクセスなし、読み取り専用、または読み取り/書き込み
- ユーザがアクセスできる管理情報ツリー (MIT) の一部を識別する 1 つ以上のセキュリティ ドメイン タグ

Cisco Cloud Network Controller は、管理対象オブジェクト (MO) レベルでアクセス権限を管理します。権限は、システム内の特定の機能に対するアクセスを許可または制限する MO です。たとえば、ファブリック機器は権限ビットです。このビットは、物理ファブリックの機器に対応するすべてのオブジェクト上で Cisco Cloud Network Controller によって設定されます。

ロールは権限ビットの集合です。たとえば、「管理者」ロールが「ファブリック機器」と「テナントセキュリティ」に対する権限ビットに設定されていると、「管理者」ロールにはファブリックの機器とテナントセキュリティに対応するすべてのオブジェクトへのアクセス権があります。

セキュリティ ドメインは、Cisco Cloud Network Controller オブジェクト階層の特定のサブツリーに関連付けられたタグです。たとえば、デフォルトのテナント「common」にはドメイン タグ common が付いています。同様に、特殊なドメイン タグ all の場合、MIT オブジェクト ツリー全体が含まれます。管理者は、MIT オブジェクト階層にカスタム ドメイン タグを割り当てることができます。

ユーザを作成してロールを割り当てても、アクセス権は有効になりません。1 つ以上のセキュリティ ドメインにそのユーザを割り当てることも必要です。デフォルトでは、Cloud Network Controller ファブリックには事前作成された次の 2 つの特殊なドメインが含まれています。

- All : MIT 全体へのアクセスを許可
- インフラ : ファブリック アクセス ポリシーなどの、ファブリック インフラストラクチャのオブジェクトおよびサブツリーへのアクセスを許可

Cisco Cloud Network Controller は、次の AAA ロールと権限をサポートしています。

| 特権       | 説明                                                              |
|----------|-----------------------------------------------------------------|
| ロール : 管理 |                                                                 |
| admin    | すべてのファブリックの機能へのフル アクセスを提供します。管理者権限は、その他のすべての権限を組み合わせたものとみなされます。 |



| 特権                        | 説明                                                                                                                                   |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>ロール : aaa</b>          |                                                                                                                                      |
| aaa                       | ポリシーの認証、許可、アカウントティング、インポート/エクスポートの設定に使用されます。                                                                                         |
| <b>Role: access-admin</b> |                                                                                                                                      |
| access-connectivity       | インフラでのレイヤ 1～3 の構成、テナントの L3Out での静的ルート構成、管理インフラポリシー、テナント ERSPAN ポリシーに使用されます。                                                          |
| access-equipment          | アクセス ポート設定に使用されます。                                                                                                                   |
| access-protocol           | インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタ ポリシーやファームウェア ポリシーなどの操作関連のアクセスポリシーでレイヤ 1～3 のプロトコル構成に使用されます。                  |
| access-qos                | CoPP および QoS に関連するポリシーの変更に使用されます。                                                                                                    |
| <b>ロール : fabric-admin</b> |                                                                                                                                      |
| fabric-connectivity       | ファブリック、ファームウェア、および導入ポリシーのレイヤ 1～3 の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーを生成します。                |
| fabric-equipment          | リーフスイッチおよびスパインスイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。                                                                               |
| fabric-protocol           | ファブリックでのレイヤ 1～3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN および正常性スコア ポリシー、およびファームウェア管理のトレースルートおよびエンドポイントトラッキングポリシーに使用されます。 |
| <b>ロール : nw-svc-admin</b> |                                                                                                                                      |

| 特権                         | 説明                                                                                                                                  |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| nw-svc-policy              | レイヤ4～レイヤ7ネットワークサービスオーケストレーションの管理に使用されます。                                                                                            |
| <b>ロール : nw-svc-params</b> |                                                                                                                                     |
| 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。                                                                                                       |
| <b>Role: ops</b>           |                                                                                                                                     |
| ops                        | 設定されているポリシーの表示に使用されま<br>す（ポリシーのトラブルシューティングな<br>ど）。                                                                                  |
| <b>ロール : port-mgmt</b>     |                                                                                                                                     |
| port-mgmt                  | ノードをセキュリティドメインに割り当てる<br>ために使用されます。また、ノードルールを<br>持つセキュリティドメインのユーザーは、<br>port-mgmt のロールを持つドメイン all に割り<br>当てる必要があります。                 |
| <b>Role: tenant-admin</b>  |                                                                                                                                     |
| aaa                        | ポリシーの認証、許可、アカウントिंग、<br>インポート/エクスポートの設定に使用されま<br>す。                                                                                 |
| access-connectivity        | インフラでのレイヤ1～3の構成、テナント<br>の L3Out での静的ルート構成、管理インフラ<br>ポリシー、テナント ERSPAN ポリシーに使用<br>されます。                                               |
| access-equipment           | アクセスポート設定に使用されます。                                                                                                                   |
| access-protocol            | インフラストラクチャ、NTP、SNMP、DNS、<br>およびイメージ管理用のファブリック全体の<br>ポリシー、およびクラスタポリシーやファーム<br>ウェアポリシーなどの操作関連のアクセス<br>ポリシーでレイヤ1～3のプロトコル構成に<br>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<br>に使用されます。                                                                                               |

| 特権                            | 説明                                                                                                                                   |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| fabric-connectivity           | ファブリック、ファームウェア、および導入ポリシーのレイヤ1～3の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。                   |
| fabric-equipment              | リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーに使用されます。                                                                                |
| fabric-protocol               | ファブリックでのレイヤ1～3のprotocols構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPANおよび正常性スコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイントトラッキングポリシーに使用されます。 |
| nw-svc-policy                 | レイヤ4～レイヤ7ネットワークサービスオーケストレーションの管理に使用されます。                                                                                             |
| tenant-network-profile        | ネットワークプロファイルの削除および作成、エンドポイントグループの削除および作成など、テナント設定の管理に使用されます。                                                                         |
| tenant-protocol               | テナント下のレイヤ1～3protocolsの構成、テナントトレースルートポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。                                                             |
| tenant-qos                    | テナントのQoSに関連する設定に使用されます。                                                                                                              |
| tenant-security               | テナントのコントラクトに関連する設定に使用されます。                                                                                                           |
| <b>Role: tenant-ext-admin</b> |                                                                                                                                      |

| 特権                      | 説明                                                                                                                                                                        |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tenant-connectivity     | ブリッジドメイン、サブネット、および VRF などの レイヤ 1～3 の接続変更で使用されます。これには、リーフスイッチおよびスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシー、テナントのインバンドおよびアウトオブバンド管理接続構成。アトミックカウンタや正常性スコアなどのデバッグ/モニタリングポリシーなどがあります。 |
| tenant-epg              | エンドポイントグループ、VRF、ブリッジドメインの削除/作成など、テナント設定の管理に使用されます。                                                                                                                        |
| tenant-ext-connectivity | 書き込みアクセスファームウェアポリシーに使用されます。テナント L2Out および L3Out 設定の管理。デバッグ/モニタリング/オブザーバポリシー。                                                                                              |
| tenant-ext-protocol     | BGP、OSPF、PIM、IGMP などのテナント外部レイヤ 1～3 プロトコルの管理、およびトレースルート、ping、oam、eprk などのデバッグ/モニタリング/オブザーバポリシーに使用されます。通常、ファームウェアポリシーの書き込みアクセスにのみ使用します。                                     |
| tenant-network-profile  | ネットワークプロファイルの削除および作成、エンドポイントグループの削除および作成など、テナント設定の管理に使用されます。                                                                                                              |
| tenant-protocol         | テナント下のレイヤ 1～3 プロトコルの構成、テナント トレースルート ポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。                                                                                                  |
| tenant-qos              | テナントの QoS に関連する設定に使用されます。                                                                                                                                                 |
| tenant-security         | テナントのコントラクトに関連する設定に使用されます。                                                                                                                                                |

カスタム権限は、任意の MO クラスに割り当てることができます。22 個のカスタム権限が Cisco Cloud Network Controller GUI に表示されます。これらのカスタム権限のいずれかがクラスに割り当てられている場合、その MO のアクセスには、新しく追加されたカスタム権限が含まれます。1 つのカスタム権限を 1 つ以上の MO クラスに関連付けることができます。



- (注) カスタム権限は Cisco Cloud Network Controller GUI で表示されますが、現在サポートされていません。

事前に定義された一連の管理対象オブジェクトクラスをドメインに関連付けることができます。これらのクラスがオーバーラップすることはできません。ドメインの関連付けをサポートするクラスの例：

- レイヤ 2 およびレイヤ 3 のネットワークで管理されたオブジェクト
- ネットワーク プロファイル (物理、レイヤ 2、レイヤ 3、管理など)
- Quality of Service (QoS) ポリシー

ドメインに関連付けることができるオブジェクトが作成されると、ユーザは、ユーザのアクセス権の範囲内でオブジェクトにドメインを割り当てる必要があります。ドメインの割り当てはいつでも変更できます。

## RBACルール

RBACルールは、リソース (アプリケーションプロファイル、EPG、コントラクトなど) を、別のセキュリティドメインにいるためにアクセスできないユーザに選択的に公開します。RBACルールは、アクセスされるオブジェクトを特定する識別名 (DN) と、オブジェクトにアクセスするユーザを含むセキュリティドメインの名前の 2 つの部分で構成されます。

RBACルールには 2 つのタイプがあります。

- 暗黙的：ユーザは、RBAC 階層に基づいてルールまたは権限を継承します
- 明示的：ルールは特定のポリシーに基づいてユーザに直接割り当てられます

制限付きおよび制限なしの両方のセキュリティドメインがサポートされています。



- (注) 管理情報ツリー内の異なる部分に存在するユーザに対し、RBAC規則によりオブジェクトを公開することは可能ですが、CLIの使用によってツリーの構造を横断することでそのようなオブジェクトに移動することはできません。ただし、RBAC規則に含まれるオブジェクトのDNをユーザが把握していれば、ユーザはMO検索コマンドにより、CLIを使用してそれを見つけることができます。

## 制限付きドメインのガイドラインと制限事項

制限付きドメインのユーザに対するガイドラインと制限は次のとおりです。

- あるセキュリティ ドメインのユーザに別のセキュリティ ドメインが割り当てられている場合、そのユーザは新しいドメインに関連付けられた構成にアクセスできます。
- ユーザは、「制限付き」とマークされた1つ以上のセキュリティ ドメインの一部になることができます。
- 制限付きドメイン ユーザは、システムで作成された構成への読み取り専用アクセス権を持っています。
- 複数のセキュリティ ドメインを持つユーザの場合、すべてのセキュリティ ドメインを合わせた長さが 1024 文字を超えることはできません。長さが 1024 を超えると、ユーザはポリシーの作成に問題が発生します。
- Cisco Cloud Network Controller の制限付きドメインは、クラウドリソースではサポートされていません。つまり、ある制限付きドメインのユーザは、別の制限付きドメインのユーザによって作成されたクラウドリソースを表示できません。

## 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。



(注) RBAC ルールを構成できますが、Cisco Cloud Network Controller GUI は構成をサポートしていません。この手順 (手順 4) を使用して構成された DN は、API を使用して照会できます。

### 始める前に

セキュリティ ドメインの作成詳細なタスクについては、「[Cisco Cloud Network Controller GUI を使用したセキュリティ ドメインの作成](#)」を参照してください。

- ステップ 1 インテント アイコンをクリックします。[**インテント (Intent)**] メニューが表示されます。
- ステップ 2 [Intent] 検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative] を選択します。  
[**インテント (Intent)**] メニューに**管理オプション**のリストが表示されます。
- ステップ 3 [インテント (**Intent**)] メニューの [**管理 (Administrative)**] リストから、[**セキュリティ (Security)**] > [**RBAC ルール (RBAC Rules)**] > [**RBAC ルールの作成 (Create RBAC Rule)**] をクリックします。[**RBAC ルールの作成 (Create RBAC Rule)**] ダイアログボックスが表示されます。
- ステップ 4 DN フィールドに、ルールの DN を入力します。  
明示的な RBAC ルールを作成するには、ObjectStore でアプリケーションの DN を見つけます。ここでその DN 値を使用します。
- ステップ 5 セキュリティ ドメインを選択します。

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

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

**ステップ 7** 設定が終わったら [Save] をクリックします。

(注) 明示的な RBAC ルールを作成した後、セキュリティドメインに割り当てられたユーザは、以前に (ObjectStore から) 定義されたアプリケーションとその子のみを表示できます。

---







## 第 9 章

# 設定のばらつき

- [構成のばらつき通知と障害 \(325 ページ\)](#)
- [構成ドリフトのメインページにアクセスする \(326 ページ\)](#)
- [欠落しているコントラクト構成の確認 \(329 ページ\)](#)
- [欠落している EPG 構成の確認 \(331 ページ\)](#)
- [欠落している VRF 構成の確認 \(332 ページ\)](#)
- [構成のばらつきのトラブルシューティング \(334 ページ\)](#)

## 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 Controller 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。

構成ドリフト情報は、[クラウド リソース (Cloud Resources)] >> [ドリフト (Drifts)] にある 1 つのページに統合されました。

**Drifts**

**Detection Summary**

|                   |                     |                               |
|-------------------|---------------------|-------------------------------|
| Unmanaged Objects | Objects with Drifts | Last Drift Check              |
| 236               | 3                   | Feb 16 2023 04:14:55pm +08:00 |

Filter by attributes

| Object                              | Status    | Drift Type   | Last Configuration Update     |
|-------------------------------------|-----------|--------------|-------------------------------|
| brown2                              | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| brown3                              | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| context-[vrf2]-addr-[10.119.0.0/16] | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| ctxcidr-[10.119.0.0/16]             | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| ctxcidr-[10.129.0.0/16]             | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| ctxcidr-[10.198.2.0/24]             | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| ctxcidr-[10.198.3.0/24]             | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| egress-[-1]-[0]-[0]-[0.0.0.0/0]     | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| egress-[-1]-[0]-[0]-[0.0.0.0/0]     | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| egress-[-1]-[0]-[0]-[0.0.0.0/0]     | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| egress-[-1]-[0]-[0]-[0.0.0.0/0]     | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |

詳細については、「[構成ドリフトのメインページにアクセスする \(326ページ\)](#)」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

- 存在する必要があるものが正しく表示されていることを確認するには

**ステップ 1** Cloud 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。

| Object                              | Status    | Drift Type   | Last Configuration Update     |
|-------------------------------------|-----------|--------------|-------------------------------|
| brown2                              | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| brown3                              | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| context-[vrf2]-addr-[10.119.0.0/16] | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| ctxcidr-[10.119.0.0/16]             | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| ctxcidr-[10.129.0.0/16]             | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| ctxcidr-[10.198.2.0/24]             | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| ctxcidr-[10.198.3.0/24]             | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| egress-[1]-[0]-[0]-[0.0.0.0/0]      | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| egress-[1]-[0]-[0]-[0.0.0.0/0]      | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |
| egress-[1]-[0]-[0]-[0.0.0.0/0]      | Unmanaged | Extra Object | Feb 15 2023 04:55:39pm +08:00 |
| egress-[1]-[0]-[0]-[0.0.0.0/0]      | Unmanaged | Extra Object | Feb 15 2023 04:57:13pm +08:00 |

[ドリフト (Drifts)] ページでは、ファブリック内の構成の問題の概要を確認できます。

[検出の概要 (Detection Summary)] のエリアには、管理対象または管理対象外のオブジェクトとして検出された構成ドリフトの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある [更新] アイコンをクリックして情報を更新できます。

**ステップ 3** [検出の概要 (Detection Summary)] エリア下の表の情報を使用して、構成のドリフトを見つけます。

- **オブジェクト** : 構成ドリフトに関連するオブジェクトに関する情報を提供します。
- **ステータス** : [ステータス (Status)] 列に表示される可能性のあるさまざまな値を次に示します。
  - **Transient (低)** : 最近の構成変更が原因である可能性が高いドリフト。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。
  - **Presumed (中)** : 一時的である場合とそうでない場合があるドリフト。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。
  - **Raised (高)** : クリティカルなドリフト。Cloud 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 \(329 ページ\)](#)
- [欠落している EPG 構成の確認 \(331 ページ\)](#)
- [欠落している VRF 構成の確認 \(332 ページ\)](#)

## 欠落しているコントラクト構成の確認

このセクションでは、Cloud 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。

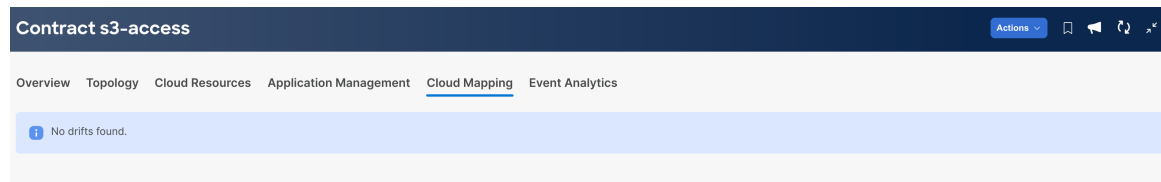
**ステップ 3** 適切なコントラクトをダブルクリックして、そのコントラクトの [概要 (Overview)] ページを表示します。

**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 \(199 ページ\)](#)」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 \(326 ページ\)](#)」を参照してください。

画面は、[検出の概要 (Detection Summary)]、[関連オブジェクト (Related Objects)]、[構成ドリフト (Configuration Drifts)] および [提示されたクラウドリソース (Presented Cloud Resources)] の4つのセクションに分かれています。各セクションには、選択したコントラクトに関するそれぞれの情報をリストした表が含まれています。

- [検出の概要 (Detection Summary)] の表には、検出された構成ドリフトの数、構成された意図された実際のクラウドリソースの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある [更新] アイコンをクリックして情報を更新できます。
- [関連オブジェクト (Related Objects)] エリアには、コントラクトに関連するその他のオブジェクト (コンシューマーやプロバイダーの EPG、フィルタなど) が表示されます。
- 構成のばらつきテーブルには、コントラクトルールに関するすべての問題が一覧表示されます。具体的には、展開することを意図していたが、実際のファブリック構成に欠落しているすべてのコントラクトルール。

この表には、使用されるプロトコル、ポート範囲、送信元と宛先の IP またはグループ、コンシューマーとプロバイダーの EPG、問題の説明、問題を解決するための推奨アクションなどの詳細情報が含まれています。構成ののばらつきごとに、[ステータス] フィールドに重大度と推奨されるアクションが示されます。

- **Transient (低)** : 最近の構成変更が原因である可能性が高いドリフト。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。
  - **Presumed (中)** : 一時的である場合とそうでない場合があるドリフト。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。
  - **Raised (高)** : クリティカルなドリフト。Cloud 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。

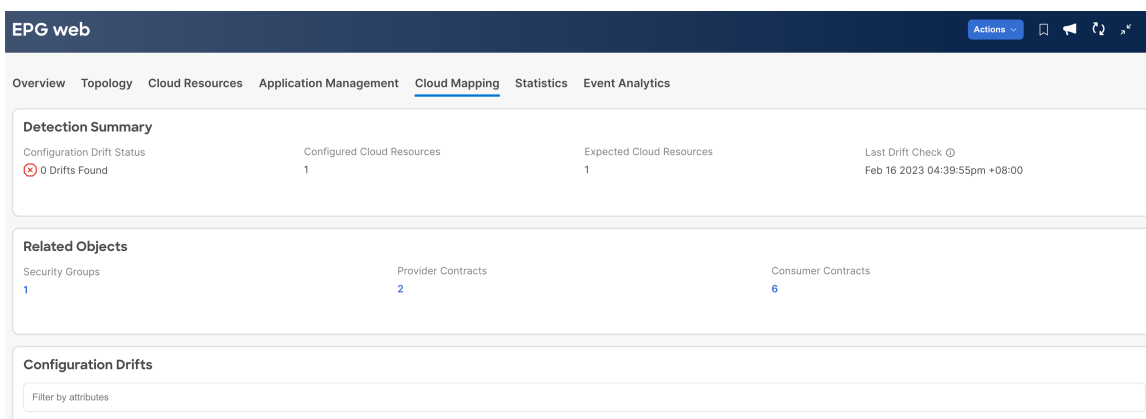
**ステップ 1** Cloud Network Controller GUI にログインします。

**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 \(326 ページ\)](#)」を参照してください。

画面は、[検出の概要 (Detection Summary)]、[関連オブジェクト (Related Objects)]、[構成ドリフト (Configuration Drifts)] および [提示されたクラウドリソース (Presented Cloud Resources)] の4つのセクションに分かれています。各セクションには、選択した EPG に関するそれぞれの情報をリストした表が含まれています。

- [検出の概要 (Detection Summary)] の表には、検出された構成ドリフトの数、構成された意図された実際のクラウドリソースの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある [更新] アイコンをクリックして情報を更新できます。
- [関連オブジェクト (Related Objects)] エリアには、セキュリティグループ、コントラクトなど、EPG に関連するその他のオブジェクトが表示されます。

- **[構成ドリフト (Configuration Drifts)]** テーブルには、EPG に関連付けられたセキュリティグループに関するすべての問題が一覧表示されます。具体的には、展開することを意図していたが、実際のファブリック構成に欠落しているすべてのセキュリティグループ。

この表には、論理 DN、クラウドプロバイダー ID、ドリフトタイプ、問題の説明、問題を解決するための推奨アクションなどの詳細情報が含まれています。構成ののばらつきごとに、[ステータス]フィールドに重大度と推奨されるアクションが示されます。

- **Transient (低)** : 最近の構成変更が原因である可能性が高いドリフト。ファブリックが安定するまで待つことをお勧めします。ばらつきは、次の構成の更新後に自然に解決する可能性があります。
  - **Presumed (中)** : 一時的である場合とそうでない場合があるドリフト。状態を監視し、ばらつきが続く場合は構成のトラブルシューティングを行うことをお勧めします。
  - **Raised (高)** : クリティカルなドリフト。Cloud 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。



The screenshot shows the VRF vrf1 configuration page. The top navigation bar includes Overview, Topology, Cloud Resources, Application Management, Cloud Mapping (selected), Statistics, and Event Analytics. The main content area is divided into three sections:
 

- Detection Summary:** Configuration Drift Status shows 0 Drifts Found. Configured Cloud Resources and Expected Cloud Resources are both 8. The Last Drift Check is Feb 16 2023 04:14:55pm +08:00.
- Related Objects:** Security Groups: 3, CIDRs: 1, Subnets: 6.
- Configuration Drifts:** A table with a filter by attributes input field. The table is currently empty.

- (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 \(326 ページ\)](#)」を参照してください。

画面は、[検出の概要 (Detection Summary)]、[関連オブジェクト (Related Objects)]、[構成ドリフト (Configuration Drifts)] および [提示されたクラウドリソース (Presented Cloud Resources)] の 4 つのセクションに分かれています。各セクションには、選択した VRF に関するそれぞれの情報をリストした表が含まれています。

- [検出の概要 (Detection Summary)] の表には、検出された構成ドリフトの数、構成された意図された実際のクラウドリソースの数、およびこの情報が最後に更新された時刻の概要が表示されます。在庫更新のタイムスタンプが古い場合は、この画面の右上隅にある [更新] アイコンをクリックして情報を更新できます。
- [関連オブジェクト (Related Objects)] 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、構成のばらつきプロセスが Cisco 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 CApiDrift
ACI-Cloud-Fabric-1# trigger techsupport controllers application CApiDrift 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\_CApiDrift 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 クラウドネットワークコントローラ で管理されたクラウドサイトと非 ACI リ モート サイト間の接続の設定

この章のセクションでは、エクスプレスルート ゲートウェイを使用して、またはエクスプレ  
スルート ゲートウェイを使用せずに、Cisco Cloud ネットワーク コントローラで管理されたク  
ラウドサイトと非 ACI リモート サイト間の接続を構成する方法について説明します。

- [エクスプレスルート ゲートウェイを使用して接続を構成する \(337 ページ\)](#)
- [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成 \(344 ページ\)](#)

## エクスプレスルートゲートウェイを使用して接続を構成 する

エクスプレスルートゲートウェイはリダイレクトを使用してまたは、リダイレクトを使用せ  
ずに、ハブ VNet の中でのエクスプレスルートゲートウェイの展開と一緒にサポートされま  
す。エクスプレスルートゲートウェイは、Cisco Cloud Network Controller が管理するクラウド  
サイトと非 ACI リモートサイト間の接続を提供するために使用されます。非 ACI リモートサ  
イト (この場合、エクスプレスルートゲートウェイによって接続されている) の外部 EPG に  
は、ハブまたはスポーク VNet 内のクラウド EPG とのコントラクトがあります。

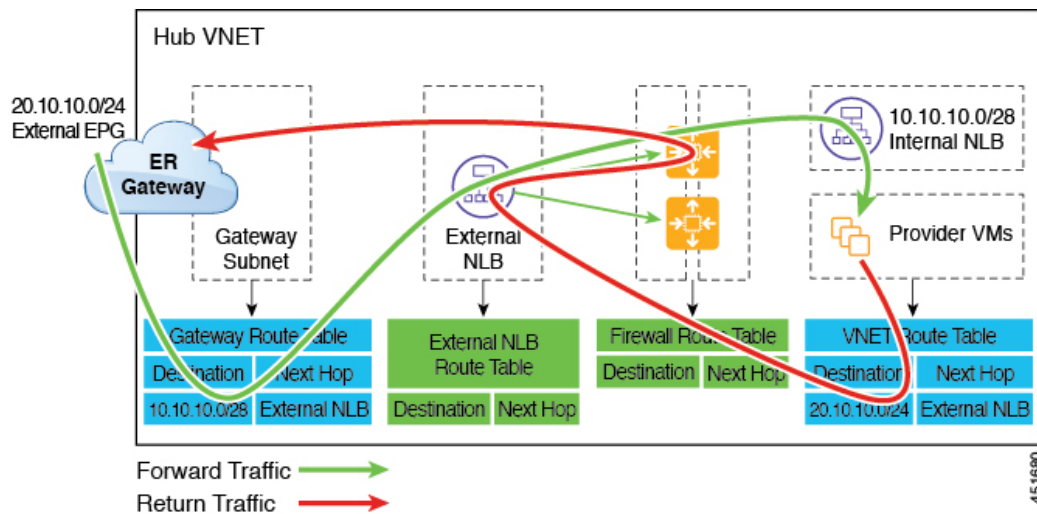
## リダイレクトを使用してエクスプレスルートゲートウェイを展開す ることについて

エクスプレスルートゲートウェイを介してクラウドエンドポイントと外部ネットワーク間の  
接続を展開している状況では、リダイレクトを使用してそれらの間にサービスデバイスを挿入  
できます。

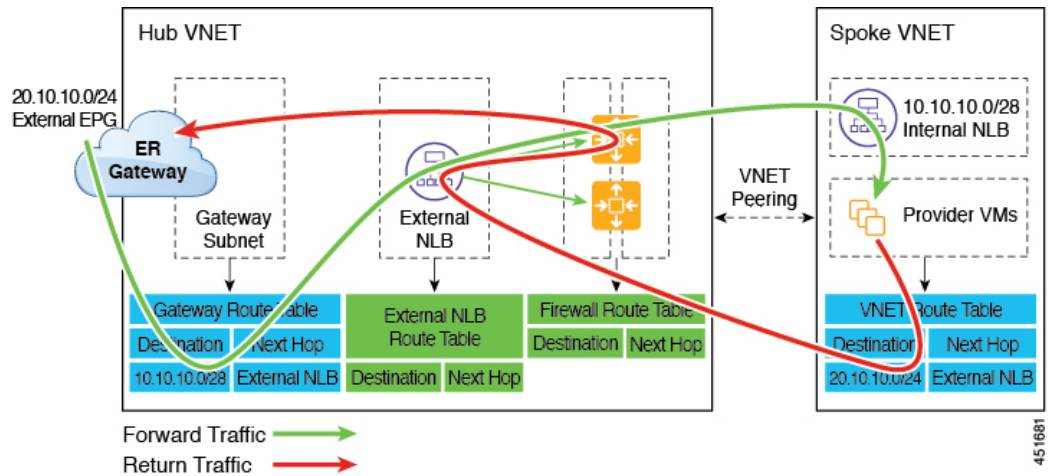
このユース ケースでは、エクスプレス ルート ゲートウェイによって接続された外部 EPG は、ハブまたはスポーク VNet のいずれかでクラウド EPG とコントラクトがあります。このケースから得られた結果を以下に示します。

- リダイレクトは、Cisco Cloud Network Controller によってゲートウェイ サブネット ルート テーブルで構成されます。プロバイダー クラウド EPG 宛てのトラフィックは、ハブ VNet に展開されたサービス デバイスにネクスト ホップとしてリダイレクトされます。
- リダイレクトで使用されるサービス デバイスは、エクスプレス ルート ゲートウェイ（この場合はハブ VNet）によって接続された外部 EPG と同じ VNet にある必要があります。
- この場合、プロバイダー クラウド EPG をリージョン全体に拡張することがサポートされています。

次の図は、ハブ VNet のプロバイダー EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の図は、スポーク VNet 内のプロバイダー EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の表は、リダイレクトがどのようにプログラムされるかを示しています。

| コンシューマ                         | プロバイダー                           | ゲートウェイサブネットルートテーブルでのリダイレクト                     | プロバイダー VNet でのリダイレクト                            |
|--------------------------------|----------------------------------|------------------------------------------------|-------------------------------------------------|
| エクスプレスルートゲートウェイによって接続された外部 EPG | サブネットベースのエンドポイントセレクタを備えたクラウド EPG | プロバイダーのサブネットを使用したコンシューマからプロバイダーへのトラフィックのリダイレクト | 外部 EPG のサブネットを使用したプロバイダーからコンシューマへのトラフィックのリダイレクト |

## リダイレクトを使用してエクスプレスルートゲートウェイを展開することについて

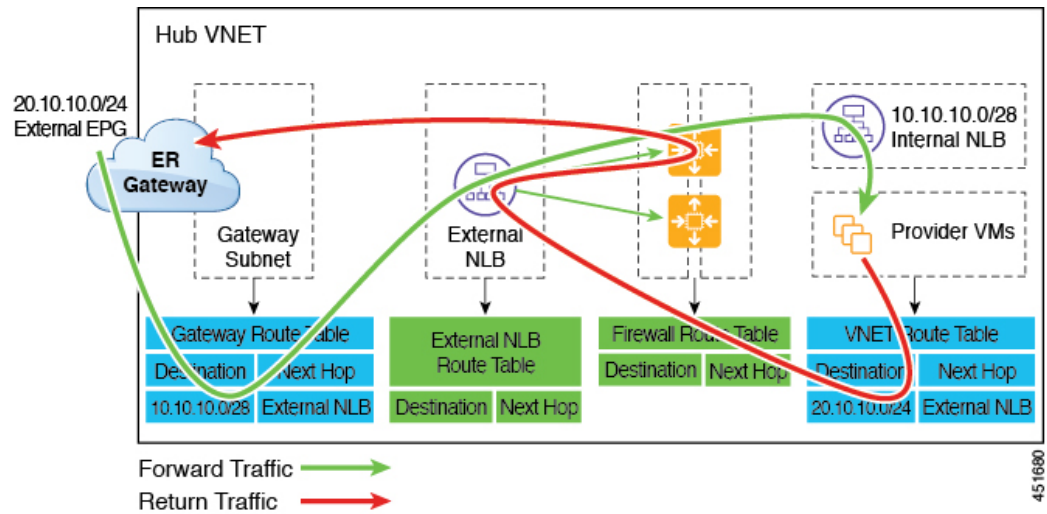
エクスプレスルートゲートウェイを介してクラウドエンドポイントと外部ネットワーク間の接続を展開している状況では、リダイレクトを使用してそれらの間にサービスデバイスを挿入できます。

このユースケースでは、エクスプレスルートゲートウェイによって接続された外部 EPG は、ハブまたはスポーク VNet のいずれかでクラウド EPG とコントラクトがあります。このケースから得られた結果を以下に示します。

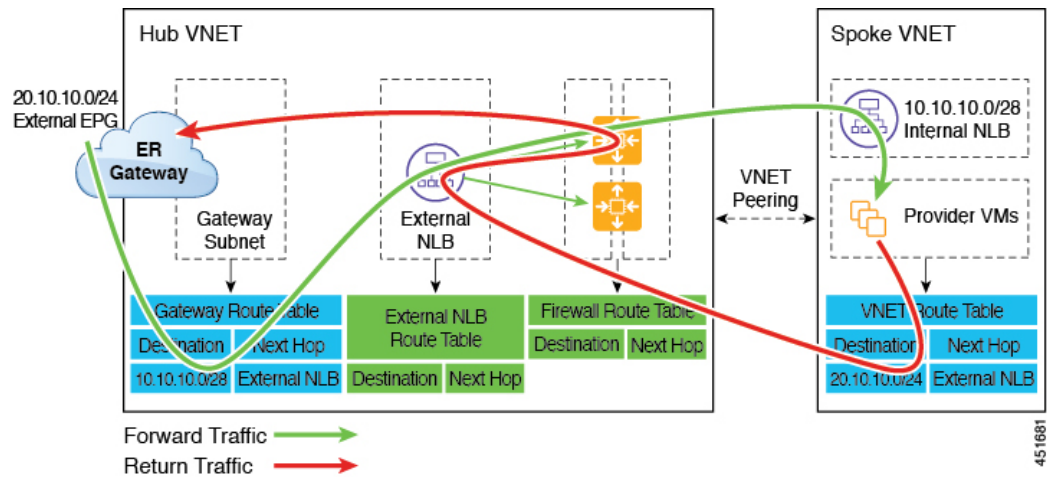
- リダイレクトは、Cisco Cloud Network Controller によってゲートウェイサブネットルートテーブルで構成されます。プロバイダークラウド EPG 宛てのトラフィックは、ハブ VNet に展開されたサービスデバイスにネクストホップとしてリダイレクトされます。
- リダイレクトで使用されるサービスデバイスは、エクスプレスルートゲートウェイ（この場合はハブ VNet）によって接続された外部 EPG と同じ VNet にある必要があります。
- この場合、プロバイダークラウド EPG をリージョン全体に拡張することがサポートされています。

次の図は、ハブ VNet のプロバイダー EPG へのエクスプレスルートゲートウェイのリダイレクトの例を示しています。

リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて



次の図は、スポーク VNet 内のプロバイダー EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の表は、リダイレクトがどのようにプログラムされるかを示しています。

| コンシューマ                           | プロバイダー                          | ゲートウェイサブネット ルートテーブルでのリダイレクト                    | プロバイダー VNet でのリダイレクト                            |
|----------------------------------|---------------------------------|------------------------------------------------|-------------------------------------------------|
| エクスプレス ルート ゲートウェイによって接続された外部 EPG | サブネットベースのエンドポイントセクタを備えたクラウド EPG | プロバイダーのサブネットを使用したコンシューマからプロバイダーへのトラフィックのリダイレクト | 外部 EPG のサブネットを使用したプロバイダーからコンシューマへのトラフィックのリダイレクト |



## リダイレクトなしの Express Route ゲートウェイの展開について

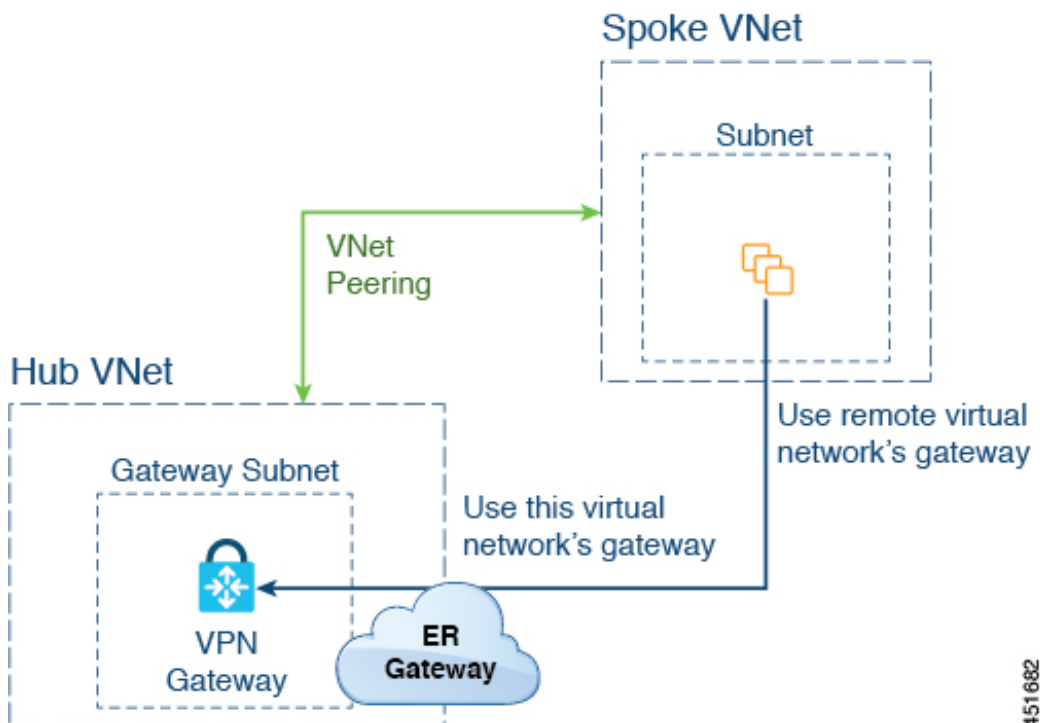
このタイプの展開では、スポーク VNet へのルート伝達が Cisco Cloud Network Controller によって自動的に有効になります。これにより、ゲートウェイ移行を使用した VNet ピアリング（移行ピアリングとも呼ばれます）を使用して、ハブ VNet を介してスポーク VNet で非 ACI リモートサイトサブネットルートを使用できるようになります。ゲートウェイトランジットを使用した VNet ピアリングは、この場合 Cisco Cloud Network Controller によって自動的に有効になります。

この構成の一部として、ハブ VNet にエクスプレスルートゲートウェイを展開します。Cisco Cloud Network Controller は、エクスプレスルートゲートウェイがハブ VNet で構成されていることを検出すると、Azure portal で移行ピアリングプロパティを自動的に設定します。1 つはハブ → スポーク ピアリング用、もう 1 つはスポーク → ハブ ピアリング用です。

- **Hub VNet** : [この仮想ネットワークのゲートウェイを使用する (Use this virtual network's gateway) ] に自動的に設定されます。
- **スポーク VNet** : Cisco Cloud Network Controller によって管理されるスポーク VNet で [リモート仮想ネットワークのゲートウェイを使用する (Use remote virtual network's gateway) ] に自動的に設定されます。

スポーク VNet の出カールートテーブルに対してルート伝達を有効にするには、スポーク VNet のクラウド EPG と、非 ACI リモートサイトに接続する外部 EPG との間のコントラクトを構成する必要があります。

次の図に、この展開タイプの例を示します。



451682

この例では、以下のようにになっています。

- 次の構成は、Cisco Cloud Network Controller によって自動的に行われます。
  - スポーク VNet は、ゲートウェイ トランジット (トランジット ピアリング) で VNet ピアリングを使用する
  - ハブ VNet の VPN ゲートウェイがオンプレミスの非 ACI リモートサイトに接続されている
  - エクスプレス ルート ゲートウェイがハブ VNet に展開されていることを Cisco Cloud Network Controller が検出すると、移行ピアリング プロパティがピアリングの各側で自動的に設定されます (ハブ → スポークおよびスポーク → ハブ)。
    - **Hub VNet** : [この仮想ネットワークのゲートウェイを使用する (Use this virtual network's gateway) ] に自動的に設定されます。
    - **スポーク VNet** : Cisco Cloud Network Controller によって管理されるスポーク VNet で [リモート仮想ネットワークのゲートウェイを使用する (Use remote virtual network's gateway) ] に自動的に設定されます。
  - スポーク VNet の EPG が外部 EPG とコントラクトしている場合、VPN ゲートウェイによって学習されたオンプレミスの非 ACI ルートは、スポーク VNet で使用できます。
  - ハブ VNet は、VPN ゲートウェイを介してオンプレミスの非 ACI リモートサイトを宛先としたスポーク VNet 内の EPG からのトラフィックを許可します。

## リダイレクトなしのエクスプレス ルート ゲートウェイの展開

### 始める前に

これらの手順を続行する前に、[リダイレクトなしの Express Route ゲートウェイの展開について \(341 ページ\)](#) の情報を確認します。

**ステップ 1** Cisco Cloud Network Controller で VNet ピアリングを有効にします。

これらの指示については、「[Azure 向け Cisco Cloud Network Controller の VNET ピアリングを構成する](#)」を参照してください。

エクスプレス ルート ゲートウェイに必要なハブ VNet のゲートウェイ サブネットは、VNet ピアリングが有効な場合 Cisco Cloud Network Controller で展開されます。これは、エクスプレス ルート ゲートウェイの展開用にハブ VNet を準備するために行われます。

**ステップ 2** 非 ACI リモートサイトのネットワークを表すハブ VNet に外部 EPG を作成します。

- GUI を使用して外部 EPG を作成するには、[Cisco Cloud Network Controller GUI を使用した外部 EPG の作成 \(89 ページ\)](#) を参照してください。

外部 EPG の [ルート到達可能性 (Route Reachability) ] で、[外部サイト (External-Site) ] を選択します。

- REST API を使用して外部 EPG を作成するには、[REST API を使用した外部クラウド EPG の作成 \(174 ページ\)](#) を参照してください。

タイプ **site-external** の外部クラウド EPG を作成します。

**ステップ 3** Azure ポータルを通じて、[ステップ 1 \(342 ページ\)](#) で構成したゲートウェイ サブネットを使用してハブ VNet でエクスプレスルートゲートウェイを展開します。

[ステップ 1 \(342 ページ\)](#) で VNet ピアリングを有効にするときに選択したリージョンの数に応じて、Cisco Cloud Network Controller が管理する複数のリージョンでエクスプレスルートゲートウェイアクセスが必要な場合は、それらの各リージョンにエクスプレスルートゲートウェイを個別に展開します。

- a) Azure ポータルで、仮想ネットワークゲートウェイを作成する Resource Manager 仮想ネットワークに移動します。
- b) 左側で、[リソースの作成 (Create a resource)] を選択し、検索に仮想ネットワークゲートウェイと入力します。
- c) 検索結果で [仮想ネットワークゲートウェイ (Virtual network gateway)] を見つけて、エントリーをクリックします。
- d) [仮想ネットワークゲートウェイ (Virtual network gateway)] ページで、[作成 (Create)] を選択します。
- e) [仮想ネットワークゲートウェイの作成 (Create virtual network gateway)] ページで、次のフィールドに適切な情報を入力します。
  - サブスクリプション：適切なサブスクリプションが選択されていることを確認します。
  - リソースグループ：仮想ネットワークを選択すると、リソースグループが自動的に選択されます。
  - 名前：エクスプレスルートゲートウェイの名前。
  - リージョン：仮想ネットワークが配置されている場所を指すように [リージョン (Region)] フィールドを変更します。場所が仮想ネットワークのあるリージョンを指していない場合、仮想ネットワークは [仮想ネットワークの選択 (Choose a virtual network)] ドロップダウンに表示されません。
  - ゲートウェイの種類：ExpressRoute を選択します。
  - SKU：ドロップダウンからゲートウェイ SKU を選択します。
  - 仮想ネットワーク：[ステップ 1 \(342 ページ\)](#) で Cisco Cloud Network Controller によって作成された仮想ネットワークを選択します。
  - パブリック IP アドレス：[新規作成 (Create new)] を選択します。
  - パブリック IP アドレス名：パブリック IP アドレスの名前を指定します。
- f) [確認 + 作成 (Review + Create)] を選択し、[作成 (Create)] でゲートウェイの作成を開始します。設定が確認され、ゲートウェイが展開します。仮想ネットワークゲートウェイの作成には、完了までに最長 45 分かかります。

エクスプレス ルート ゲートウェイが正常に展開されたことを確認するには、Azure ポータルのネットワーク ゲートウェイ ページに移動し、タイプ **エクスプレス ルート** のネットワーク ゲートウェイが作成されたことを確認します。

追加のリージョンでエクスプレス ルート ゲートウェイ アクセスが必要な場合、それらのリージョンそれぞれにこれらの手順を繰り返します。

**ステップ 4** エクスプレス ルート ゲートウェイで接続したクラウド EPG および外部 EPG 間のコントラクトを構成します。

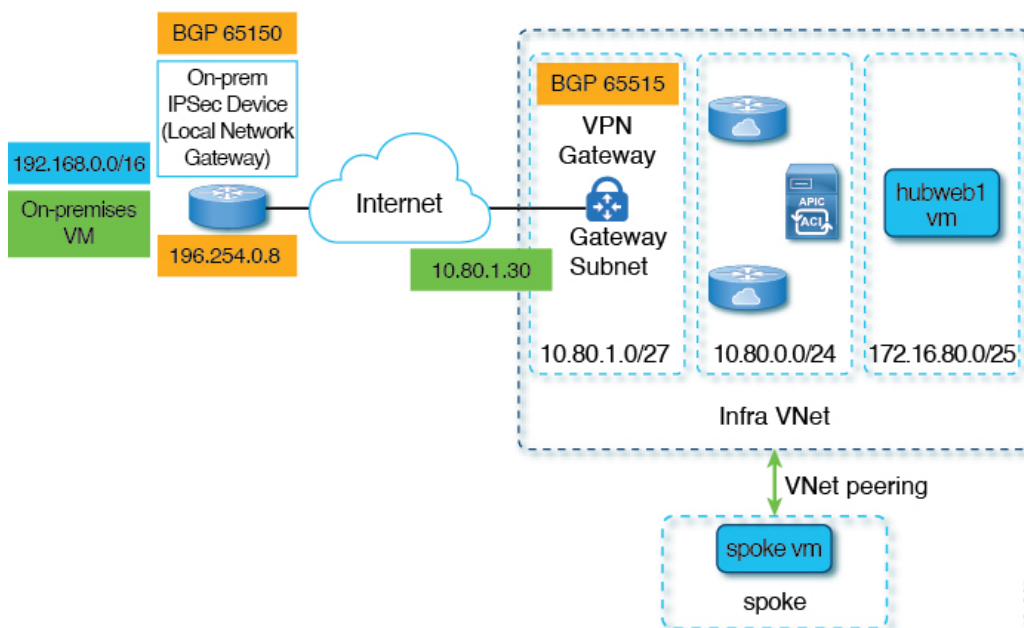
- GUI を使用して契約を作成するには、[Cisco Cloud Network Controller GUI を使用したコントラクトの作成（111 ページ）](#) を参照してください。
- REST API を使用して契約を構成するには、[REST API を使用したコントラクトの作成（170 ページ）](#) を参照してください。

---

## VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成

VPN ゲートウェイを使用して、Cisco Cloud Network Controller で管理されたクラウド サイトと非 ACI リモート サイト間の接続を提供するためのサポートを利用できます。このタイプの接続では、仮想ネットワーク ゲートウェイ（VNG）がインフラ（ハブ）VNet に展開され、Cisco Cloud Network Controller で管理されたクラウド サイトから非 ACI リモート ブランチ サイトに接続できるようにします。BGP は、インフラ VNet の CCR ルータと VNG と、非 ACI リモート ブランチ サイトのオンプレミス IPsec デバイス（ローカル ネットワーク ゲートウェイ）との間のルーティング プロトコルとして IPsec トンネル上で実行されます。

次の図では、このタイプの接続による構成例を示します。




次の手順では、このタイプの接続を構成する方法について説明します。最終的には、192.168.20.0/24 サブネットにあるオンプレミスの仮想マシンと、172.16.80.0/25 サブネットにある hubweb 仮想マシンの間で到達可能です。

## Configuring Connectivity Using VPN Gateway

### Before you begin

Review the information provided in [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成](#), on page 344 before proceeding with these procedures.

- ステップ 1** Enable VNet peering on your Cisco Cloud Network Controller, if necessary.  
Refer to [Configuring VNET Peering for Cisco Cloud Network Controller for Azure](#) for those instructions.
- ステップ 2** Add the second subnet for the VPN gateway subnet.
- In the Cisco Cloud Network Controller GUI, click the Intent icon (  ) and select **Cisco Cloud Network Controller Setup**.
  - In the **Region Management** area, click **Edit Configuration**.
  - In the **Regions to Manage** window, click **Next**.  
The **General Connectivity** window appears.
  - Under the **General** area, in the **Subnet Pools for Cloud Routers** field, click **Add Subnet Pool for Cloud Routers**.
  - Enter the information for the second subnet for the VPN gateway router.

For example, using the example configuration in [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成, on page 344](#), you would add 10.80.1.0/24 for the second subnet for the VPN gateway router in this field.

- f) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

Cisco Cloud Network Controller will create the subnet for the VPN gateway router after you have completed the **Cisco Cloud Network Controller Setup** process. You can verify that the configuration for the subnet for the VPN gateway router was pushed to Azure successfully by navigating to the **Subnets** page in the Azure portal and locating the **GatewaySubnet** entry.

### ステップ 3 Create an infra-hosted VRF and use that VRF for the site-external EPG.

You will create an infra-hosted VRF, where you have a VRF that is hosted within the parent infra VNet, and you will use that VRF for the site-external EPG that you will create in the next step.

- a) In the Cisco Cloud Network Controller GUI, navigate to **Application Management > VRFs**.
- b) Click **Actions > Create VRF**.  
The **Create VRF** window appears.
- c) Enter a name for this infra-hosted VRF, then click **Select Tenant** and select **infra** for the tenant and click **Select**.
- d) Enter a description if necessary, then click **Save**.

### ステップ 4 Create an external EPG in the hub VNet that represents the network for the non-ACI remote site.

- To create an external EPG using the GUI, see [Cisco Cloud Network Controller GUI を使用した外部 EPG の作成, on page 89](#).
  - In the **VRF** field for the external EPG, select the infra-hosted VRF that you just created for this external EPG.
  - In the **Route Reachability** field for the external EPG, select **External-Site**.
- To create an external EPG using the REST API, see [REST API を使用した外部クラウド EPG の作成, on page 174](#).
  - Use the infra-hosted VRF for this site-external EPG.
  - Create an external cloud EPG with the type **site-external**.

### ステップ 5 Through the Azure portal, create the virtual network gateway in the infra VNet for the VPN gateway subnet that you configured in [ステップ 2, on page 345](#).

In these steps, you will build the IPsec and BGP connections from the on-premises site to the Azure VPN gateway. For more information, see the following article in the Azure site:

<https://docs.microsoft.com/en-gb/azure/virtual-network/virtual-network-configure-vnet-connections>

- a) In the Azure portal, create the virtual network gateways by navigating to the Resource Manager virtual network where you want to create a virtual network gateway.
- b) On the left side, select **Create a resource**, and type **Virtual Network Gateway** in search.
- c) Locate **Virtual network gateway** in the search return and click the entry.
- d) On the **Virtual network gateway** page, choose **Create**.
- e) On the **Create virtual network gateway** page, enter the appropriate information for these fields:
  - **Subscription**: Verify that the correct subscription is selected.

- **Resource Group**: The resource group will automatically be chosen once you choose the virtual network.
  - **Name**: The name of your virtual network gateway.
  - **Region**: Change the **Region** field to point to the location where your virtual network is located. If the location isn't pointing to the region where your virtual network is, the virtual network won't appear in the **Choose a virtual network** dropdown.
  - **Gateway type**: Choose **VPN**.
  - **VPN type**: Choose **Route-based**.
  - **SKU**: Choose **VpnGw1**.
  - **Generation**: Choose **Generation1**.
  - **Virtual network**: Choose **overlay-1**.
  - **Public IP address**: Choose **Create new**.
  - **Public IP address name**: Provide a name for the public IP address.
  - **Enable active-active mode**: Set to **Disabled**.
  - **Configure BGP**: Set to **Enabled**.
  - **Autonomous system number (ASN)**: Enter the appropriate BGP ASN value for the VPN gateway. By default, Azure uses an ASN value of 65515.
- f) Select **Review + Create**, and then **Create** to begin creating the gateway.

The settings are validated and the gateway deploys. Creating a virtual network gateway can take up to 45 minutes to complete.

To verify that the virtual network gateway was deployed successfully, navigate to the virtual network gateways page and select the virtual network gateway that you just created, then click on **Settings: Configuration** to view and verify the configuration settings for the virtual network gateway.

## ステップ 6 Create the local network gateway.

For this configuration, the local network gateway is an object that represents the on-premises IPsec device. Prepare the following parameters before creating the local network gateway:

- BGP autonomous system number (ASN)
  - Public IP address
  - An appropriate address space for the on-premises subnet that needs to be advertised to the virtual network gateway
- a) In the Azure portal, create the local network gateway by navigating to the Resource Manager local network where you want to create a local network gateway.
  - b) On the left side, select **Create a resource**, and type **Local Network Gateway** in search.
  - c) Locate **Local network gateway** in the search return and click the entry.
  - d) On the **Local network gateway** page, choose **Create**.
  - e) On the **Create local network gateway** page, enter the appropriate information for these fields:
    - **Name**: The name of your local network gateway.
    - **Endpoint**: Choose **IP address**.

- **IP address:** Enter the appropriate IP address for the local network gateway.
- **Address space:** Enter the appropriate value for the address space. For example, using the example configuration in [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成, on page 344](#), you would add 192.168.0.0/16 in this field.
- **Configure BGP settings:** Click the checkbox to enable this setting.
- **Autonomous system number (ASN):** Enter the appropriate BGP ASN value for the local network gateway. This is the ASN value of the remote device. For example, using the example configuration in [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成, on page 344](#), you would add 65150 in this field.
- **BGP peer IP address:** Enter the BGP peer IP address that you will use for the on-premises device in this field (not the Azure virtual network gateway). For example, using the example configuration in [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成, on page 344](#), you would add 196.254.0.8 in this field.
- **Subscription:** Choose the same subscription that you used for the virtual network gateway in [ステップ 5, on page 346](#).
- **Resource group:** Choose the same resource group that you used for the virtual network gateway in [ステップ 5, on page 346](#).
- **Location:** Choose the same location (region) that you used for the virtual network gateway in [ステップ 5, on page 346](#).

- f) Select **Review + Create**, and then **Create** to begin creating the gateway.

The settings are validated and the gateway deploys.

To verify that the local network gateway was deployed successfully, navigate to the local network gateways page and select the local network gateway that you just created, then click on **Settings: Configuration** to view and verify the configuration settings for the local network gateway.

**ステップ 7** Create the VPN connection from the Azure virtual network gateway to the local network gateway (the on-premises IPsec device).

- a) In the Azure portal, navigate to the virtual network gateway page and locate the Azure virtual network gateway that you created in [ステップ 5, on page 346](#).
- b) Select the virtual network gateway that you created and click on **Settings: Connections**.
- c) Click **Add**.

The **Add connection** window appears.

- d) Fill in the necessary information to add this VPN connection from the Azure virtual network gateway to the local network gateway (the on-premises IPsec device).
  - In the **Connection type** field, select `Site-to-site (IPsec)`.
  - In the **Virtual network gateway** field, select the Azure virtual network gateway that you created in [ステップ 5, on page 346](#).
  - In the **Local network gateway** field, select the local network gateway that you created in [ステップ 6, on page 347](#).



- In the **Enable BGP** field, click the checkbox to enable BGP for this connection.
- In the **IKE Protocol** field, select `IKEv2`.

e) Click **OK** when you have finished entering the configuration information for this VPN connection.

**ステップ 8** Download the VPN configuration template from Azure.

- a) In the Azure portal, navigate to the virtual network gateway page and locate the Azure virtual network gateway that you created in [ステップ 5, on page 346](#).
- b) Select the virtual network gateway that you created and click on **Settings: Connections**.
- c) Select the name of the VPN connection that you just configured.

The overview page for that VPN connection appears.

d) Click **Download configuration**.

The **Download configuration** page appears.

e) Make the following selections in the **Download configuration** page:

- In the **Device vendor** field, select `Cisco`.
- In the **Device family** field, select `IOS (ISR, ASR)`.
- In the **Firmware version** field, select `15.x (IKEv2)`.

f) Click **Download configuration**.

**ステップ 9** Open the downloaded configuration template file in a text editor and make the necessary edits using the instructions in the configuration template.

Typically, the only changes needed in the configuration template are the following fields in the BGP configuration:

- **LOCAL\_ROUTE**: Must be the network that needs to be advertised to Azure. For example, using the example configuration in [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成, on page 344](#), you would enter `192.168.0.0` in this field.
- **LOCAL\_MASK**: Must be `255.255.255.0`

**ステップ 10** Save and close the edited configuration template.

**ステップ 11** Apply the edited configuration template to the on-premises IPsec device.

Following is an example edited configuration template based on the example configuration in [VPN ゲートウェイ \(仮想ネットワーク ゲートウェイ\) を使用した接続の構成, on page 344](#):

```
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.0.0 0.0.0.127
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.0.128 0.0.0.127
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.1.0 0.0.0.127
access-list 101 permit esp host 52.152.235.192 host 173.39.125.130
access-list 101 permit udp host 52.152.235.192 eq isakmp host 173.39.125.130
access-list 101 permit udp host 52.152.235.192 eq non500-isakmp host 173.39.125.130
!
crypto ikev2 proposal Azure-Ikev2-Proposal
 encryption aes-cbc-256
 integrity sha1
 group 2
 exit
!
```

```
crypto ikev2 policy Azure-Ikev2-Policy
 proposal Azure-Ikev2-Proposal
 match address local 173.39.125.130
 exit
!
crypto ikev2 keyring singaporeisr-keyring
 peer 52.152.235.192
 address 52.152.235.192
 pre-shared-key 0123456789cisco
 exit
exit

crypto ikev2 profile Azure-Ikev2-Profile
 match address local 173.39.125.130
 match identity remote address 52.152.235.192 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 lifetime 28800
 dpd 10 5 on-demand
 keyring local singaporeisr-keyring
 exit
!
crypto ipsec transform-set Azure-TransformSet esp-aes 256 esp-sha256-hmac
 mode tunnel
 exit
!
crypto ipsec profile Azure-IPsecProfile
 set transform-set Azure-TransformSet
 set ikev2-profile Azure-Ikev2-Profile
 set security-association lifetime seconds 3600
 ! Note: PFS (perfect-forward-secrecy) is an optional feature (commented out)
 !set pfs None
 exit
!
int tunnel 11
 ip address 169.254.0.1 255.255.255.255
 tunnel mode ipsec ipv4
 ip tcp adjust-mss 1350
 tunnel source 173.39.125.130
 tunnel destination 52.152.235.192
 tunnel protection ipsec profile Azure-IPsecProfile
 exit

interface Loopback 11
 ip address 196.254.0.8 255.255.255.255
 exit
!
router bgp 65150
 bgp log-neighbor-changes
 neighbor 10.80.1.30 remote-as 65515
 neighbor 10.80.1.30 ebgp-multihop 255
 neighbor 10.80.1.30 update-source loopback 11

 address-family ipv4
 network 192.168.0.0 mask 255.255.0.0
 neighbor 10.80.1.30 activate
 exit
exit
!
ip route 10.80.0.0 255.255.255.128 Tunnel 11
ip route 10.80.0.128 255.255.255.128 Tunnel 11
ip route 10.80.1.0 255.255.255.128 Tunnel 11
ip route 10.80.1.30 255.255.255.255 Tunnel 11
```

- ステップ 12** Verify the VPN connections.
- In the Azure portal, navigate to the virtual network gateway page and locate the Azure virtual network gateway that you created in [ステップ 5, on page 346](#).
  - Select the virtual network gateway that you created and click on **Settings: Connections**.
  - Verify that the VPN connection that you created is shown as `Connected` in the **Status** column.
- ステップ 13** Determine if you are deploying the virtual network gateway with or without redirect.
- If you are deploying the virtual network gateway without redirect, go to [ステップ 14, on page 351](#).
  - If you are deploying the virtual network gateway with redirect, configure the service device for the redirect.  
To configure a service device for redirect using the GUI or REST API, see [レイヤ 4 から レイヤ 7 サービスの展開, on page 199](#).
- ステップ 14** Configure a contract between the cloud EPG and the external EPG connected by the virtual network gateway.
- To create a contract using the GUI, see [Cisco Cloud Network Controller GUI を使用したコントラクトの作成, on page 111](#).
  - To configure a contract using the REST API, see [REST API を使用したコントラクトの作成, on page 170](#).
-





## 付録 **A**

# Cisco Cloud Network Controller エラーコード

- [Cisco Cloud Network Controller エラーコード \(353 ページ\)](#)

## 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 43: 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の数は最大 1 です。                              |
| cloud-template | CT_INFRANETWORK_VRF                         | cloudtemplateInfraNetwork MOでは、vrfName を overlay-1 にする必要があります。       |
| cloud-template | CT_INFRANETWORK_PARENT                      | cloudtemplateInfraNetworkMO の場合、親 MO は uni/tn-infra である必要があります。      |
| cloud-template | CT_INFRANETWORK_NUMROUTERSPERREGION_MINIMUM | cloudtemplateInfraNetwork MO では、属性 numRoutersPerRegion の最小許容値は 2 です。 |
| cloud-template | CT_INFRANETWORK_NUMROUTERSPERREGION_MAXIMUM | cloudtemplateInfraNetwork MO では、属性 numRoutersPerRegion の最大許容値は 4 です。 |
| cloud-template | CT_INTNETWORK_COUNT                         | cloudtemplateIntNetwork MO の数は最大 1 です                                |

| コンポーネント        | エラー コード (Error Code)                 | 制約                                                                                                                          |
|----------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| cloud-template | CT_EXTNETWORK_COUNT                  | cloudtemplateExtNetwork MO の数は最大 1 です                                                                                       |
| cloud-template | CT_VPNNETWORK_COUNT                  | cloudtemplateVpnNetwork MO の数は最大 1 です                                                                                       |
| cloud-template | CT_OSPF_COUNT                        | cloudtemplateOspf MO の数は最大 1 です                                                                                             |
| cloud-template | CT_INTNETWORK_REGION_MATCH           | cloudtemplateIntNetwork で cloudRegionName によって指定されたリージョンには、cloudProvP で対応する cloudRegion が必要です。                              |
| cloud-template | CT_INTNETWORK_REGION_MANAGED         | cloudtemplateIntNetwork の cloudRegionName の子によって指定されたリージョンには、adminSt が管理対象の対応する cloudRegion が必要です。                          |
| cloud-template | CT_INTNETWORK_REGION_MAXIMUM         | cloudtemplateIntNetwork で指定されるリージョンの最大数 (cloudRegionName) は 4 です                                                            |
| cloud-template | CT_EXTNETWORK_REGION_SUBSET          | cloudtemplateExtNetwork の cloudRegionName の子によって指定されたリージョンは、cloudtemplateIntNetwork の下の cloudRegionName の子によっても指定する必要があります。 |
| cloud-template | CT_EXTNETWORK_REQUIRES_EXTSUBNETPOOL | cloudtemplateExtNetwork の存在には、cloudtemplateExtSubnetPool の存在が必要です。                                                          |
| cloud-template | CT_EXTSUBNETPOOL_COUNT               | cloudtemplateExtSubnetPool の数は最大 1 です                                                                                       |
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_ADDRESS  | cloudtemplateExtSubnetPool では、サブネットプールにネットワーク アドレスが含まれている必要があります。                                                           |

| コンポーネント        | エラー コード (Error Code)                     | 制約                                                                                                                                                                                                                                             |
|----------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_IP_VERSION   | cloudtemplateExtSubnetPool では、サブネットプールに IPv4 アドレスが含まれている必要があります                                                                                                                                                                                |
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_ADDRESS_TYPE | cloudtemplateExtSubnetPool では、サブネットプールの IP アドレスはマルチキャストまたはループバックアドレス空間からのものであってはなりません                                                                                                                                                          |
| cloud-template | CT_EXTSUBNETPOOL_SUBNETPOOL_MINIMUM_SIZE | cloudtemplateExtSubnetPool では、サブネットプールは /22 以上である必要があります (ネットマスクは 22 以下である必要があります)。                                                                                                                                                            |
| cloud-template | CT_EXTSUBNETPOOL_AND_REMOTESITE          | cloudtemplateExtSubnetPool は、cloudtemplateRemoteSite ごとに少なくとも 1 つの cloudtemplateRemoteSiteSubnetPool を持つのに十分な大きさである必要があります。                                                                                                                    |
| cloud-template | CT_INTNETWORK_MISSING_HOME               | cloudtemplateIntNetwork の下に cloudRegionName がある場合は、cloudRegionName の 1 つを Cisco Cloud Network Controller のホーム リージョン (capicDeployed) に関連付ける必要があります。                                                                                             |
| cloud-template | CT_CLOUD_APICSUBNETPOOL_INSUFFICIENT     | cloudApicSubnetPool MO は、cloudApicSubnet MO を生成するために十分な数である必要があります。これにより、cloudtemplateIntNetwork で指定されたすべての cloudRegionName MO を一意の cloudApicSubnet MO に関連付けることができます。cloudApicSubnet MO からのサブネットは、対応するリージョンの cloudCtxProfile で CIDR として使用されます。 |

| コンポーネント        | エラー コード (Error Code)                     | 制約                                                                                                                                                                     |
|----------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cloud-template | CT_IPSECTUNNEL_PEERADDR_IP_VERSION       | cloudtemplateIpSecTunnel では、peeraddr に IPv4 アドレスを含める必要があります。                                                                                                           |
| cloud-template | CT_IPSECTUNNEL_PEERADDR_IS_HOST          | cloudtemplateIpSecTunnel では、peeraddr はホストアドレス (/32 など) である必要があります。                                                                                                     |
| cloud-template | CT_PROFILE_COUNT                         | cloudtemplateProfile MO のカウントは最大 1 です                                                                                                                                  |
| cloud-template | CT_PROFILE_DELETE                        | cloudtemplateProfile MO は、親の cloudtemplateInfraNetwork も削除されない限り、削除できません。                                                                                              |
| cloud-template | CT_AZURE_PROFILE_ROUTERUSERNAME_INVALID  | Azure では、一部のユーザー名 (admin、root など) が無効であり、ピリオドで終わらないようにしてください。                                                                                                          |
| cloud-template | CT_AZURE_PROFILE_ROUTERUSERNAME_TOO_LONG | Azure では、ユーザー名は最大 20 文字に制限されています。                                                                                                                                      |
| cloud-template | CT_PROFILE_ROUTERUSERNAME_NONEMPTY       | cloudtemplateProfile では、routerUsername は空でない必要があります。                                                                                                                   |
| cloud-template | CT_PROFILE_ROUTERPASSWORD_NONEMPTY       | cloudtemplateProfile では、routerLicenseToken に無効な文字を含めることはできません。                                                                                                         |
| cloud-template | CT_PROFILE_ROUTERTHROUGHPUT_MODIFY       | cloudtemplateProfile では、routerThroughput は、いずれかのリージョン (つまり、cloudtemplateIntNetwork の下にある cloudRegionName) にルータが展開されている場合は変更できません。(どのリージョンにもルータが導入されていない場合は、変更が許可されます)。 |



| コンポーネント        | エラー コード (Error Code)                            | 制約                                                                          |
|----------------|-------------------------------------------------|-----------------------------------------------------------------------------|
| cloud-template | CT_PROFILE_ROUTERLICENSETOKEN_INVALID_CHARACTER | cloudtemplateProfile では、routerPassword は空でない必要があります。                        |
| cloud-template | CT_APICSUBNET_INVALID_HOME_REGION               | cloudApicSubnet MO では、captiveDeployed としてマークされたリージョンは有効なリージョンである必要があります。    |
| cloud-template | CT_APICSUBNET_REPEATED_REGION                   | cloudApicSubnet MO では、リージョンを最大1つのサブネットに関連付けることができます。                        |
| cloud-template | CT_APICSUBNET_MULTIPLE_HOME_REGION              | cloudApicSubnet MO では、最大で1つのリージョンがcaptiveDeployedを true に設定できます。            |
| cloud-template | CT_HUBNETWORK_COUNT                             | cloudtemplateHubNetwork MO の数は最大1です                                         |
| クラウド           | CLOUD_APICSUBNETPOOL_CREATEDBY_USER             | cloudApicSubnetPool では、createdBy 属性は USER である必要があります                        |
| クラウド           | CLOUD_APICSUBNETPOOL_SUBNET_IP_VERSION          | cloudApicSubnetPool では、サブネットに IPv4 アドレスが含まれている必要があります。                      |
| クラウド           | CLOUD_APICSUBNETPOOL_SUBNET_SIZE                | cloudApicSubnetPoolでは、サブネットは /24 である必要があります。                                |
| クラウド           | CLOUD_APICSUBNETPOOL_DELETE_USAGE               | cloudApicSubnetPool は、その cloudApicSubnet 子の少なくとも1つがリージョンで使用されている場合は削除できません。 |
| クラウド           | CLOUD_APICSUBNETPOOL_DELETE_CREATEDBY           | createdBy 属性が USER ではない cloudApicSubnetPool は削除できません。                       |
| クラウド           | CLOUD_AZURE_CTXPROFILE_SUBNET_RENAME            | cloudSubnet 名は変更できません                                                       |

| コンポーネント | エラーコード (Error Code)                     | 制約                                                                                         |
|---------|-----------------------------------------|--------------------------------------------------------------------------------------------|
| クラウド    | CLOUD_AZURE_CTXPROFILE_SUBNET_DUPLICATE | 同じ cloudCtxProfile 内の 2 つの cloudSubnet に同じ名前を付けることはできません                                   |
| クラウド    | CLOUD_CAPIC_IP_EXT_EPG_SELECTOR_MAXIMUM | Cisco Cloud Network Controller IP に対応する cloudExtEpg には最大1つの cloudExtEpSelector があります       |
| クラウド    | CLOUD_AZURE_ACCOUNT_IN_USE              | アカウントが使用中で、コンテキスト プロファイルが展開されている間は、アカウントとテナント間の関連付けを更新または削除することはできません。                     |
| クラウド    | CLOUD_AZURE_INFRA_ACCOUNT_CHANGE        | テナント インフラのアカウントは変更または削除できません                                                               |
| クラウド    | CLOUD_SOURCE_PORT_NOT_SUPPORTED         | 送信元ポート範囲は Cisco Cloud Network Controller では許可されていません                                       |
| クラウド    | CLOUD_ONLY_PERMIT_ACTION_SUPPORTED      | 「許可」とは異なるアクションは Cisco Cloud Network Controller ではサポートされていません                               |
| クラウド    | CLOUD_CIDR_OVERLAP                      | cloudCidr のサブネットはオーバーラップできません                                                              |
| クラウド    | CLOUD_SUBNET_USAGE                      | 特定のゾーンには最大で1つのゲートウェイ サブネットが存在でき、各ユーザー サブネットは同じユーザー サブネットのゾーンに正確に1つのゲートウェイ サブネットを持つ必要があります。 |
| クラウド    | CLOUD_AZURE_ACCOUNT_CRED_CROSS_TENANT   | cloudAccount によって使用される cloudCredentials は、同じテナントにある必要があります                                 |

| コンポーネント        | エラー コード (Error Code)                            | 制約                                                                                                                                                                                                                                                                                                                                                  |
|----------------|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| クラウド           | CLOUD_AZURE_ACCOUNT_AD_CROSS_TENANT             | cloudAccount によって使用される cloudAd は、同じテナントにある必要があります                                                                                                                                                                                                                                                                                                   |
| cloud-template | CT_CLOUD_APICSUBNETPOOL_INSUFFICIENT_HUBNETWORK | cloudApicSubnetPool MO は、cloudApicSubnet MO を生成するために十分な数である必要があります。これにより、cloudtemplateIntNetwork で指定されたすべての cloudRegionName MO を一意の cloudApicSubnet MO に関連付けることができます。cloudApicSubnet MO からのサブネットは、対応するリージョンの cloudCtxProfile で CIDR として使用されます。HubNetworking を有効にすると、cloudtemplateIntNetwork の下の cloudRegionName と同じ数の cloudApicSubnetPool が必要になります。 |
| クラウド           | CLOUD_SYSTEM_MO_IS_IMMUTABLE                    | システムによって作成されたインスタンスは不変です                                                                                                                                                                                                                                                                                                                            |
| cloud-template | CT_BGPEVPN_PEERADDR_IP_VERSION                  | cloudtemplateBgpEvpn では、peeraddr に IPv4 アドレスを含める必要があります。                                                                                                                                                                                                                                                                                            |
| cloud-template | CT_BGPEVPN_PEERADDR_ADDRESS_TYPE                | cloudtemplateBgpEvpn では、peeraddr IP アドレスはホストアドレスである必要があります                                                                                                                                                                                                                                                                                          |
| クラウド           | CLOUD_APICSUBNETPOOL_SUBNET_HOST_PART           | cloudApicSubnetPool サブネットでは、ホスト部分は 0 である必要があります。                                                                                                                                                                                                                                                                                                    |
| cloud-template | CT_EXTSUBNETPOOL_CLOUD_APICSUBNETPOOL_OVERLAP   | cloudtemplateExtSubnetPool と cloudApicSubnetPool の間にサブネットのオーバーラップがあります。                                                                                                                                                                                                                                                                             |





## 付録 **B**

# サービス EPG 構成例

サービス EPG の詳細については、以下を参照してください。

- [クラウド サービスエンドポイント グループ \(35 ページ\)](#)
- [Cisco Cloud Network Controller GUI を使用した サービス EPG の作成 \(97 ページ\)](#)
- [REST API を使用したサービス EPG の作成 \(175 ページ\)](#)

次のセクションにサービス EPG の構成例を示します。

- [Azure Kubernetes Services \(AKS\) サービス EPG 構成例 \(361 ページ\)](#)

## Azure Kubernetes Services (AKS) サービス EPG 構成例

このセクションでは、次の設定を持つサービス EPG 例を構成する手順を説明します。

- **サービス タイプ** : Azure Kubernetes Services (AKS)
  - Azure Kubernetes Services (AKS) には、他のサービスへのアクセスが必要です。
  - Cisco Cloud Network Controller は、[\[ルールプログラミング \(programming of the rules\)\]](#) を自動化します。
- **展開タイプ** : 管理対象クラウド ネイティブこのタイプの展開では、サービスは VNet またはサブネットにインスタンス化されます (Cisco Cloud Network Controller を介して作成されます)。たとえば、Azure Kubernetes サービス (AKS) サービスは、Cisco Cloud ネットワーク コントローラによって管理されるサブネットに展開できます。
- **アクセス タイプ** : プライベート

AKS のこのサンプル サービス EPG を構成する手順は、次のセクションで提供されます。

## クラウドコンテキストプロファイルでサブネットの作成

これらの手順では、Azure Kubernetes Services (AKS) サービス EPG によって使用されるクラウドコンテキストプロファイルにサブネットを作成する方法について説明します。これらの手順では、Cisco Cloud Network Controller GUI を使用して構成を行います。

### 始める前に

- 1つのブラウザウィンドウで、Cisco Cloud Network Controller GUI にログインします。
- 別のブラウザウィンドウで、Cisco Cloud Network Controller インフラテナントの Azure アカウントにログインし、Azure 管理ポータルに移動します。

<https://portal.azure.com/#home>

**ステップ 1** Cisco Cloud Network Controller GUI で、[**インテント (Intent)**] アイコンをクリックします。

[**インテント (Intent)**] メニューが表示されます。

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

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

**ステップ 3** [**インテント (Intent)**] メニューの [**アプリケーション管理 (Application Management)**] リストで、[**クラウドコントラクトプロファイルの作成 (Create Cloud Context Profile)**] をクリックします。

[**クラウドコンテキストプロファイルの作成 (Create Cloud Context Profile)**] ウィンドウが表示されます。

The screenshot shows the 'Create Cloud Context Profile' window with the following fields and options:

- General:** Name (text input), Tenant (dropdown menu), Description (text input).
- Settings:** Region (dropdown menu), VRF (dropdown menu), CIDRs (table with columns: CIDR Block Range, Primary, VRF, Subnets, Private Link Label, Cloud Access Privilege), Advanced Settings (dropdown menu).
- VNet Peering Settings:** VNet Gateway Router (checkbox with 'Enable' text), VNet Peering (checkbox with 'Enable' text).

**ステップ 4** [**クラウドコンテキストプロファイルの作成 (Create Cloud Context Profile)**] ウィンドウに次の情報を入力します。

- **名前:** クラウドコンテキストプロファイルの名前を入力します。たとえば、**ct\_ctxprofile\_eastus** です。

- **テナント** : [テナントの選択 (**Select Tenant**) ] をクリックし、このユース ケースのクラウド コンテキスト プロファイルのテナントを選択して、[選択 (**Select**) ] をクリックします。
- **リージョン** : [リージョンの選択 (**Select Region**) ] をクリックし、リージョン (例 : **eastus**) を選択し、[選択 (**Select**) ] をクリックします。
- **VRF** : [VRF の選択 (**Select VRF**) ] をクリックし、適切な VRF を選択し、[選択 (**Select**) ] をクリックします。
- **CIDR の追加** : CIDR 情報を入力します。
  1. [CIDR の追加 (**Add CIDR**) ] をクリックします。
  2. [CIDR ブロック範囲 (**CIDR Block Range**) ] フィールドにアドレスを入力します。  
たとえば、30.1.0.0/16 です。
  3. [プライマリ (**Primary**) ] チェックボックスをオフ (無効) にします。
  4. [サブネットの追加 (**Add subnet**) ] をクリックして、サブネットアドレスを [アドレス (**Address**) ] に入力します。  
たとえば、30.1.0.0/17 です。AKS クラスタには 338 個のアドレスが必要であることに注意してください。
  5. [追加] をクリックします。
- **VNet ゲートウェイ ルータ** : このフィールドのボックスをオフ (選択解除) したままにします。
- **VNet ピアリング** : VNet ピアリングを有効にするには、このボックスをオンにします。

**ステップ 5** 設定が終わったら [Save] をクリックします。

#### 次のタスク

[「AKS のクラウド サービス EPG の作成 \(363 ページ\)」](#) に進みます。

## AKS のクラウド サービス EPG の作成

これらの手順では、Azure Kubernetes Services (AKS) サービス タイプでクラウド サービス EPG を作成する方法について説明します。これらの手順では、Cisco Cloud Network Controller GUI を使用して構成を行います。

#### 始める前に

これらの手順に進む前に、[クラウド コンテキスト プロファイルでサブネットの作成 \(362 ページ\)](#) の手順を完了してください。

**ステップ 1** Cisco Cloud Network Controller GUI で、[インテント (**Intent**) ] アイコンをクリックします。

[**インテント (Intent)**] メニューが表示されます。

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

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

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

[**EPG の作成 (Create EPG)**] ウィンドウが表示されます。

**ステップ 4** [**EPG の作成 (Create EPG)**] ウィンドウに次の情報を入力します。

- **名前** : クラウドサービス EPG の名前を入力します。たとえば、**svc-Hub-AzureAKS** などです。
- **テナント** : [テナントの選択 (**Select Tenant**)] をクリックし、このユースケースのクラウドサービス EPG のテナントを選択してから、[**選択 (Select)**] をクリックします。
- **アプリケーションプロファイル** : [アプリケーションプロファイルの選択 (**Select Application Profile**)] をクリックし、アプリケーションプロファイルを選択してから、[**選択 (Select)**] をクリックします。
- **タイプ** : EPG タイプとして [サービス (**Service**)] を選択します。
- **VRF** : [VRF の選択 (**Select VRF**)] をクリックし、適切な VRF を選択し、[**選択 (Select)**] をクリックします。
- **サービス タイプ** : [Azure Kubernetes Services (**AKS**)] サービス タイプを選択します。
- **展開タイプ** : [クラウドネイティブ管理対象 (**Cloud Native Managed**)] の展開タイプを選択します。
- **アクセス タイプ** : [プライベート (**Private**)] アクセス タイプを選択します。



- ステップ5 [エンドポイントセクタの追加 (Add Endpoint Selector)] をクリックします。  
[エンドポイントセクタの追加 (Add Endpoint Selector)] ウィンドウが表示されます。  
このユースケースでは、IP アドレスが前のステップで構成されたサブネット情報 30.1.0.0/17 と一致するエンドポイントセクタを作成します。エンドポイントセクタの IP アドレスが前の手順のサブネットと一致することで、Cisco Cloud Network Controller は NSG をプログラムして、このサービスタイプに必要なすべてのルールを許可するようになります。
- ステップ6 [エンドポイントセクタの追加 (Add Endpoint Selector)] ウィンドウの [Name (名前)] フィールドに名前を入力します。
- ステップ7 [キー (Key)] ドロップダウンリストをクリックしてキーを選択します。  
現時点では、このアクセスタイプのキーとして使用できるオプションは [IP] のみです。
- ステップ8 [演算子 (Operator)] ドロップダウンリストをクリックし、[等しい (equals)] を選択します。
- ステップ9 [値 (Value)] フィールドに 30.1.0.0/17 と入力し、チェックマークをクリックしてエントリを検証します。
- ステップ10 [Add] をクリックします。
- ステップ11 設定が終わったら [Save] をクリックします。

#### 次のタスク

[[アウトバウンドセキュリティルールの確認 \(365 ページ\)](#)] に進みます。

## アウトバウンドセキュリティルールの確認

これらの手順では、必要なアウトバウンドセキュリティルールが正しく構成されていることを確認する方法について説明します。Cisco Cloud Network Controller は、AKS を Azure ポータルに展開するために必要なすべてのアウトバウンドセキュリティルールを Azure で構成します。

#### 始める前に

これらの手順に進む前に、[AKS のクラウドサービス EPG の作成 \(363 ページ\)](#) の手順を完了してください。

- ステップ1 Azure ポータルで、自動的に作成されたサブネットのネットワークセキュリティグループに移動します。
- 適切なリソースグループに移動します。
  - AKS サービス EPG に使用されたサブネットを選択します。
  - 必要なアウトバウンドセキュリティグループを見つけます。
- ステップ2 ページで [アウトバウンドセキュリティルール (Outbound security rules)] エリアを見つけ、NSG のアウトバウンドセキュリティルールが正しく構成されていることを確認します。  
アウトバウンドセキュリティルールの詳細については、次を参照してください。

<https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic>

---

### 次のタスク

「[Kubernetes サービスの作成 \(366 ページ\)](#)」に進みます。

## Kubernetes サービスの作成

これらの手順では、Kubernetes サービスを作成する方法について説明します。これらの手順では、Azure ポータルを使用して構成を行います。



(注) 次の手順では、Azure ポータルを使用して Kubernetes サービスを作成する方法について説明します。Kubernetes サービスを作成するための代替方法も、[\[Cisco Cloud Network Controller での Azure Kubernetes サービスの使用 \(Using Azure Kubernetes Service with Cisco Cloud Network Controller\)\]](#)に関するドキュメントで提供されています。

---

### 始める前に

これらの手順に進む前に、[アウトバウンドセキュリティ ルールの確認 \(365 ページ\)](#) の手順を完了してください。

---

**ステップ 1** Azure ポータルで、「[Kubernetes Service by Microsoft](#)」というワード検索を行い、検索結果をクリックします。

**[Kubernetes サービス (Kubernetes Service)]** ページが表示されます。

**ステップ 2** **[Kubernetes サービス (Kubernetes Service)]** ページで **[作成 (Create)]** をクリックします。

**[Kubernetes クラスターの作成 (Create Kubernetes cluster)]** ページが表示されます。

[Home](#) > [Kubernetes services](#) >

## Create Kubernetes cluster

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ

[Create new](#)

### Cluster details

Kubernetes cluster name \* ⓘ

Region \* ⓘ

Availability zones ⓘ

Kubernetes version \* ⓘ

### Primary node pool

The number and size of nodes in the primary node pool in your cluster. For production workloads, at least 3 nodes are recommended for resiliency. For development or test workloads, only one node is required. If you would like to add additional node pools or to see additional configuration options for this node pool, go to the 'Node pools' tab above. You will be able to add additional node pools after creating your cluster. [Learn more about node pools in Azure Kubernetes Service](#)

Node size \* ⓘ

[Change size](#)

Node count \* ⓘ

**ステップ 3** [基本 (Basics)] タブで、次のエリアを構成します。

- サブスクリプション：適切なサブスクリプションを選択します。
- リソースグループ：適切なリソースグループを選択します。
- **Kubernetes クラスタ名**：この Kubernetes クラスタの一意の名前を入力します。
- リージョン：適切なリージョンを選択します。
- **Kubernetes バージョン**：デフォルトの選択をそのままにします。
- **ノード サイズ**：デフォルトの選択をそのままにします。
- **ノード数**：このフィールドのエントリが 1 になるように、スクロールバーが左端にあることを確認します。

**ステップ 4** [次へ：ノードプール (Next: Node pools)] をクリックします。デフォルトのエントリをそのままにして、[次へ：認証 (Next: Authentication)] をクリックして [認証 (Authentication)] タブに進みます。

The screenshot shows the 'Create Kubernetes cluster' wizard in the Azure portal. The 'Authentication' tab is active. Under 'Authentication method', 'Service principal' is selected. Below it, a 'Service principal' dropdown menu is open, showing a 'Configure service principal' link. A modal dialog titled 'Configure service principal' is displayed, with 'Use existing' selected. It contains two input fields: 'Service principal client ID' and 'Service principal client secret'. At the bottom of the dialog is an 'Ok' button. The main page has navigation buttons for '< Previous' and 'Next: Networking >', and a 'Review + create' button.

ステップ 5 [認証 (Authentication)] タブで、次のエリアを構成します。

- 認証方法 : [サービス プリンシパル (Service principal)] を選択します。  
[サービス プリンシパル (Service principal)] フィールドが表示されます。
- サービス プリンシパル : [サービス プリンシパルの構成 (Configure service principal)] をクリックします。

[サービス プリンシパルの構成 (Configure service principal)] ウィンドウで、次のエリアを構成します。

- サービス プリンシパル : [新規作成 (Create new)] または [既存のものを使用 (Use existing)] を選択します。

[既存のものを使用 (Use existing)] を選択した場合は、既存のサービス プリンシパルについての情報を入力します。

- サービス プリンシパルのクライアント ID
- サービス プリンシパルのクライアント シークレット

(注) これら 2 つのフィールドに入力するエントリをメモします。これらのフィールドのエントリは、これらの手順の後半で使用します。

[OK] をクリックして、[Kubernetes クラスタの作成 (Create Kubernetes cluster)] ウィンドウの [認証 (Authentication)] タブに戻ります。

- 役割別アクセス コントロール (RBAC) : [有効 (Enabled)] を選択します。
- AKS で管理される Azure Active Directory : [無効 (Disabled)] を選択します。
- 暗号化タイプ : デフォルトの選択をそのままにします。

ステップ 6 [次へ : ネットワーキング (Next: Networking)] をクリックして、[ネットワーキング (Networking)] タブに進みます。

[Home](#) > [Kubernetes services](#) >

## Create Kubernetes cluster

[Basics](#) [Node pools](#) [Authentication](#) **[Networking](#)** [Integrations](#) [Tags](#) [Review + create](#)

You can change networking settings for your cluster, including enabling HTTP application routing and configuring your network using either the 'Kubenet' or 'Azure CNI' options:

- The **kubenet** networking plug-in creates a new VNet for your cluster using default values.
- The **Azure CNI** networking plug-in allows clusters to use a new or existing VNet with customizable addresses. Application pods are connected directly to the VNet, which allows for native integration with VNet features.

[Learn more about networking in Azure Kubernetes Service](#)

Network configuration ⓘ

Kubenet

Azure CNI

**i** The Azure CNI plugin requires an IP address from the subnet below for each pod on a node, which can more quickly exhaust available IP addresses if a high value is set for pods per node. Consider modifying the default values for pods per node for each node pool on the "Node pools" tab. [Learn more](#) ↗

Virtual network \* ⓘ  ▼  
[Create new](#)

Cluster subnet \* ⓘ  ▼  
[Manage subnet configuration](#)

Kubernetes service address range \* ⓘ  ✓

Kubernetes DNS service IP address \* ⓘ  ✓

Docker Bridge address \* ⓘ  ✓

DNS name prefix \* ⓘ  ✓

---

Traffic routing

[Review + create](#) [< Previous](#) [Next : Integrations >](#)

ステップ7 [ネットワーキング (Networking)] タブで、次のエリアを構成します。

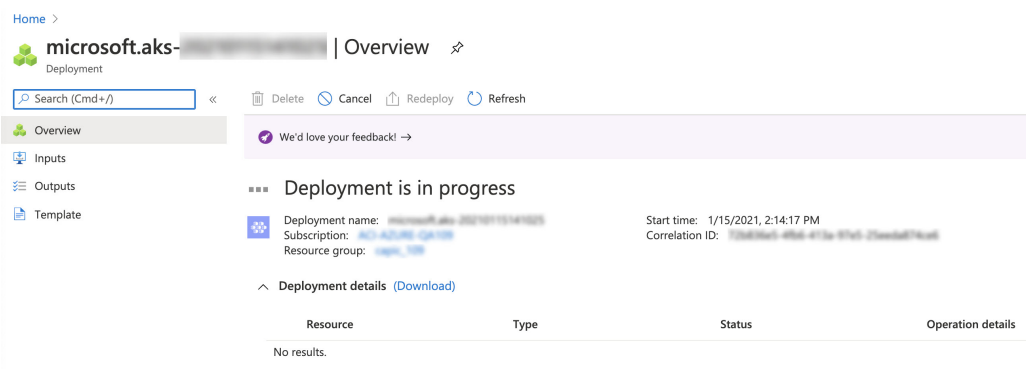
- ネットワーク構成：[**Azure CNI**] を選択します。
- 仮想ネットワーク：対応する仮想ネットワークを選択します。
- クラスタ サブネット：Cisco Cloud Network Controller で管理されるサブネットを選択します。
- **Kubernetes** サービスのアドレス範囲：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **Kubernetes DNS** サービスの IP アドレス：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **Docker Bridge** アドレス：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **DNS** 名のプレフィックス：デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- ロードバランサ：標準規格

- **HTTP アプリケーションルーティングを有効にする**：デフォルトの選択をそのままにするか（有効にしない）、必要に応じてエントリを変更します。
- **プライベート クラスタを有効にする**：必要に応じて、デフォルトの選択をそのまま（無効）にするか、エントリを変更します。

**ステップ 8** [次へ：統合 (Next: Integration)]、[次へ：タグ (Next: Tags)] の順にクリックして、デフォルトのエントリを変更せずにこれらの画面を進め、[次へ：確認 + 作成 (Next: Review+Create)] をクリックします。

**ステップ 9** [確認 + 作成 (Review+Create)] ウィンドウで [作成 (Create)] をクリックし、検証に合格した後もう一度 [作成 (Create)] をクリックして Kubernetes クラスタを作成します。

「Deployment is in progress」というメッセージが表示され、Kubernetes サービスの [概要 (Overview)] 画面が表示されます。



先に進む前に、Kubernetes サービスが正常に展開されるまで待ちます（展開にかかる時間は異なります）。このプロセスが完了すると、メインの AKS サービスは元のリソースグループに含まれます。Azure はすべての agentpools VM スケールセットを使用して、Kubernetes サービス専用の追加のリソースグループも作成します。

### 次のタスク

「[新しい Kubernetes サービスの確認 \(370 ページ\)](#)」に進みます。

## 新しい Kubernetes サービスの確認

これらの手順では、新しい Kubernetes サービスが、Kubernetes サービス専用で作成されたリソースグループにあることを確認する方法について説明します。

### 始める前に

これらの手順に進む前に、[Kubernetes サービスの作成 \(366 ページ\)](#) の手順を完了してください。

**ステップ 1** Azure ポータルで、左側のナビゲーションバーの [リソースグループ (Resource groups)] をクリックして、リソースグループ ページに移動します。

**ステップ 2** [リソースグループ (Resource groups)] ページで、Kubernetes サービス専用で作成されたリソースグループを見つけ、そのリソースグループのリンクをクリックします。

Kubernetes サービス専用で作成されたリソースグループは、次の形式になります。

`MC_resourcegroupname_clustername_region`

それぞれの説明は次のとおりです。

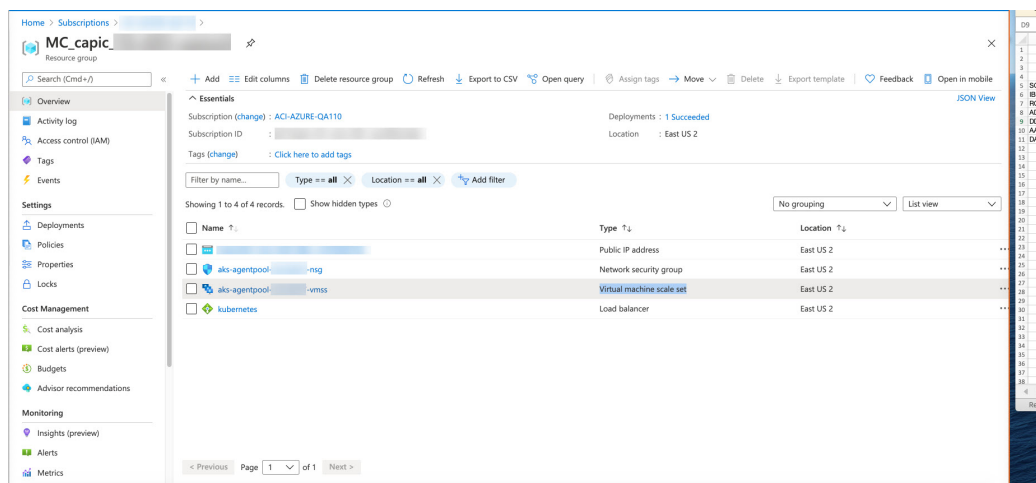
- `resourcegroupname` は、Kubernetes サービス専用で作成されたリソースグループの名前です (MC\_aks は、Azure によってデフォルトで使用されるリソースグループ名です)。
- `clustername` は、[ステップ 3 \(367 ページ\)](#) の [Kubernetes サービスの作成 \(366 ページ\)](#) で指定した Kubernetes クラスタ名です。
- `region` は、[ステップ 3 \(367 ページ\)](#) の [Kubernetes サービスの作成 \(366 ページ\)](#) で選択した地域です。

例：

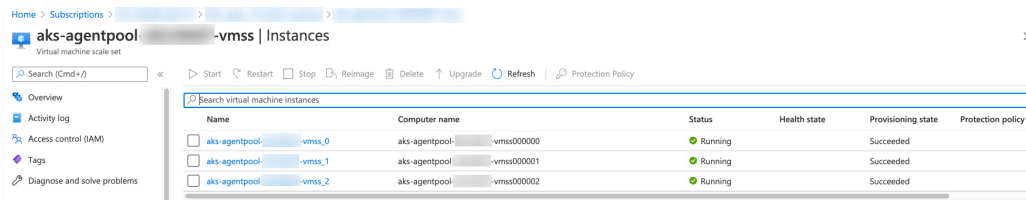
`MC_aks_acme-aks-cluster_centralus`

Kubernetes サービス リソースグループの概要ページが表示されます。

**ステップ 3** [仮想マシンスケールセット (Virtual machine scale set)] の行を見つけて、そのリンクをクリックします。これは、AKS エージェントが実行されている場所です。

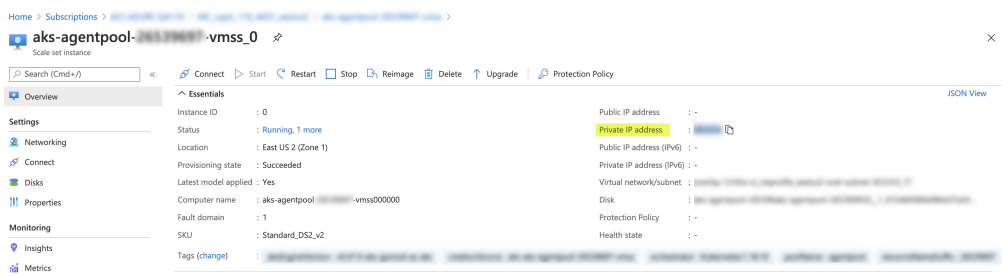


**ステップ 4** 左側のナビゲーションバーで [インスタンス (Instances)] をクリックして、この Kubernetes サービス リソースグループの仮想マシン インスタンスを表示します。



**ステップ 5** このウィンドウで3つのインスタンスのいずれかをクリックし、[プライベート IP アドレス (Private IP address)] フィールドに表示されている IP アドレスがハブ サブネットの IP アドレスと一致することを確認します。

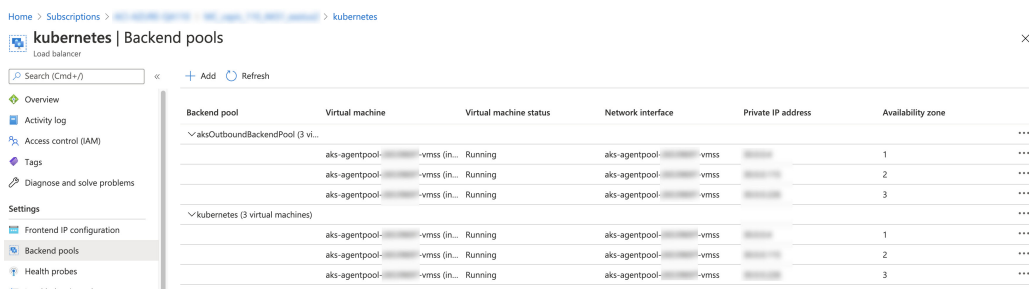
このウィンドウに表示される3つのインスタンスはすべて、[ステップ 7 \(369 ページ\)](#) の **Kubernetes サービスの作成 (366 ページ)** で選択したサブネットからの IP アドレスを持っている必要があります。



**ステップ 6** Kubernetes サービス リソースグループの概要ページに戻り、タイプとして Load balancer が表示されている kubernetes エントリを見つけて、そのリンクをクリックします。

Kubernetes ロードバランサの概要ページが表示されます。

**ステップ 7** 左側のナビゲーションバーで [バックエンド プール (Backend pools)] をクリックして、AKS エージェントを表示します。



**ステップ 8** コントラクトを構成するプロセスの一部として仮想マシンが作成された場合 (たとえば、仮想マシンがコンシューマ用に作成された場合)、プロバイダーとして AKS がある場合は、ルールが正しく構成されていることを確認します。

- Azure ポータルで、インフラ リソースグループに戻ります。
- インフラ リソースグループの [概要 (Overview)] ページに表示されるレコードの [タイプ別にグループ化 (Group by type)] を選択します。
- [仮想マシン (Virtual machine)] エリアが表示されるまで下にスクロールし、コントラクトのコンシューマの仮想マシンをクリックします。



その仮想マシンの [概要 (Overview)] ウィンドウが表示されます。

- d) 左側のナビゲーションバーの [設定 (Settings)] で、[ネットワーク (Networking)] をクリックします。

その仮想マシンの [ネットワーク (Networking)] ウィンドウが表示され、インバウンドおよびアウトバウンドのポートルールに関する情報が示されます。

- e) [アウトバウンド ポートのルール (outbound port rules)] タブをクリックし、表にリストされているアウトバウンド ポートのルールのいずれかをクリックします。

ウィンドウが右からスライドして表示され、これらのアウトバウンドポートルールに関する追加情報が表示されます。たとえば、[宛先 IP アドレス/CIDR 範囲 (Destination IP addresses/CIDR ranges)] エリアのエントリは、AKS クラスタに関連付けられているアドレスに関する情報を提供します。

---

### 次のタスク

「[Azure および AKS CLI のインストール \(373 ページ\)](#)」に進みます。

## Azure および AKS CLI のインストール

これらの手順では、Azure と AKS CLI をインストールする方法について説明します。

### 始める前に

これらの手順に進む前に、[新しい Kubernetes サービスの確認 \(370 ページ\)](#) の手順を完了してください。

---

**ステップ 1** インターネットにアクセスできるコンシューマ VM に、Azure CLI をインストールします。

詳細については、以下を参照してください。

<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-linux>

たとえば、Azure の Ubuntu Linux VM に Azure CLI をインストールするには、次のようにします。

```
curl -sL https://aka.ms/InstallAzureCliDeb | sudo bash
```

**ステップ 2** Kubernetes コマンドライン ツールである **kubect1** と、azure 認証を実装する **client-go** 資格情報 (exec) プラグインである **kubelogin** をダウンロードしてインストールします。

```
az aks install-cli
```

**ステップ 3** 次の手順で [ステップ 5 \(368 ページ\)](#) の [Kubernetes サービスの作成 \(366 ページ\)](#) に入力したサービス プリンシパル情報でログインします。

```
az login --service-principal --username <service_principal_client_id>
--password '<service_principal_client_secret>' --tenant <tenant_ID>
```

それぞれの説明は次のとおりです。

- `<service_principal_client_id>` は、[ステップ 5 \(368 ページ\)](#) の **Kubernetes サービスの作成 (366 ページ)** で **[サービス プリンシパル クライアント ID (Service principal client ID)]** フィールドからのエントリです。
- `<service_principal_client_secret>` は、[ステップ 5 \(368 ページ\)](#) の **Kubernetes サービスの作成 (366 ページ)** で **[サービス プリンシパル クライアントシークレット (Service principal client secret)]** フィールドからのエントリです。
- `<tenant_ID>` は、サービス プリンシパル (Azure Active Directory テナント ID) に関連付けられたテナントです。このコマンドのテナント ID 情報を見つけるには：

1. Azure ポータルにサインインします。
2. **[Azure Active Directory]** を選択します。
3. **[プロパティ (Properties)]** を選択します。
4. **[テナント ID (Tenant ID)]** フィールドまで下にスクロールします。ボックスにテナント ID が表示されます。

詳細については、以下を参照してください。

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant>

例：

```
az login --service-principal --username 12a3b456-7c89-1234-5de6-7f89012gh3i4
--password 'secretkey12341234!' --tenant 98765zy4-xwv-3ut2-1uts-rq0pon98m765
```

**ステップ 4** サブスクリプションを現在アクティブなサブスクリプションに設定します。

```
az account set --subscription <AKS_rg_subscription_ID>
```

`<AKS_rg_subscription_ID>` は、Azure が **新しい Kubernetes サービスの確認 (370 ページ)** の Kubernetes サービス用に作成したリソースグループのサブスクリプション ID です。

例：

```
az account set --subscription 56klm789n-o0p1-234q-5r6s-7t890123u4v5
```

**ステップ 5** コンシューマ VM から次のように入力してログインし、AKS に接続します。

```
root@hub-vm:/home/CNC# az aks get-credentials --resource-group <resource_group> --name
<AKS_cluster_name> --admin
```

それぞれの説明は次のとおりです。

- `<resource_group>` インフラ リソースグループの名前です。
- `<AKS_cluster_name>` は、[ステップ 3 \(367 ページ\)](#) の **Kubernetes サービスの作成 (366 ページ)** に入力された Kubernetes クラスタの名前です。

例：

```
root@hub-vm:/home/CNC# az aks get-credentials --resource-group CNC_infra_westus --name azureaksclus
--admin
```

次のようなメッセージが表示されます。

```
Merged "azureaksclus-admin" as current context in /root/.kube/config
```

**ステップ 6** 各ノードの内部 IP アドレスを確認してください。

```
root@hub-vm:/home/CNC# kubectl get nodes -o wide
```

次のような出力が表示されます。

| NAME                              | STATUS | ROLES | AGE | VERSION | INTERNAL-IP | EXTERNAL-IP | OS-IMAGE           | KERNAL-VERSION    | CONTAINER-RUNTIME |
|-----------------------------------|--------|-------|-----|---------|-------------|-------------|--------------------|-------------------|-------------------|
| aks-agentpool-12345678-vmss000000 | Ready  | agent | 14h | v1.17.9 | 30.1.1.1    | <none>      | Ubuntu 16.04.7 LTS | 4.15.0-1092-azure | docker://19.3.12  |
| aks-agentpool-12345678-vmss000001 | Ready  | agent | 14h | v1.17.9 | 30.1.1.21   | <none>      | Ubuntu 16.04.7 LTS | 4.15.0-1092-azure | docker://19.3.12  |
| aks-agentpool-12345678-vmss000002 | Ready  | agent | 14h | v1.17.9 | 30.1.1.31   | <none>      | Ubuntu 16.04.7 LTS | 4.15.0-1092-azure | docker://19.3.12  |

[INTERNAL-IP] 列にリストされている IP アドレスは、ハブサブネットにあります。

(注) 上記の出力例では、EXTERNAL-IP 列のエントリは <none> と表示されます。これは、[アクセスタイプ (Access Type)] が **ステップ 4 (364 ページ) の AKS のクラウドサービス EPG の作成 (363 ページ)** で Private に設定されていたためです。[アクセスタイプ (Access Type)] が **Public and Private** に設定されている場合、IP アドレスは EXTERNAL-IP 列に表示されます。

**ステップ 7** (任意) 必要に応じて、新しいユーザに管理者ロールを割り当てます。

- Azure ポータルで、インフラ リソースグループに戻ります。
- ページのレコードエリアで、[Kubernetes サービス (Kubernetes service)] エントリが見つかるまで下にスクロールします。
- 構成した Kubernetes サービスをクリックします。

Kubernetes サービスの [概要 (Overview)] ページが表示されます。

- 左側のナビゲーションバーで、[アクセス制御 (IAM) (Access Control (IAM))] をクリックします。その Kubernetes サービスのアクセス制御 (IAM) が表示されます。
- [+ Add] をクリックし、ドロップダウンメニューから [Add role Assignment] を選択します。
- [ロール割り当ての追加 (Add role Assignment)] ページで、次の選択を行います。
  - [ロール (Role)] フィールドで、ドロップダウンメニューから [Azure Kubernetes Service Cluster 管理者ロール (Azure Kubernetes Service Cluster Admin Role)] を選択します。
  - [アクセス先の割り当て (Assign access to)] フィールドで、[ユーザ、グループ、またはサービスプリンシパル (User, group, or service principal)] を選択します。
  - 適切なキーを選択します。
- 画面の下部にある [保存 (Save)] をクリックします。



## 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。