



## 既存のブラウフィールド Azure クラウド VNets の Cisco Cloud APIC へのインポート

[新機能および変更された機能に関する情報 2](#)

[既存の Azure ブラウフィールドクラウド VNet を Cisco Cloud APIC にインポートする利点 2](#)

[このドキュメントで使用される用語 3](#)

[管理対象外（ブラウフィールド）VNets の VNet ピアリングの概要 4](#)

[Cisco Cloud APIC がブラウフィールド VNet で行うことと行わないこと 5](#)

[ガイドラインと制限 7](#)

[既存のブラウフィールドクラウド VNet を Cisco Cloud APIC にインポートするためのワークフロー 8](#)

[読み取り専用アカウントの設定 9](#)

[管理対象外（ブラウフィールド）クラウド コンテキスト プロファイルの作成 11](#)

[Azure での管理対象外 VNet からインフラ VNet へのピアリングの追加 17](#)

[ブラウフィールドクラウド コンテキスト プロファイルに関連付けられた EPG の作成 19](#)

[Azure でのブラウフィールド VNet の残りの構成の完了 26](#)

[設定の確認 32](#)

改訂：2022年1月5日、

## 新機能および変更された機能に関する情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

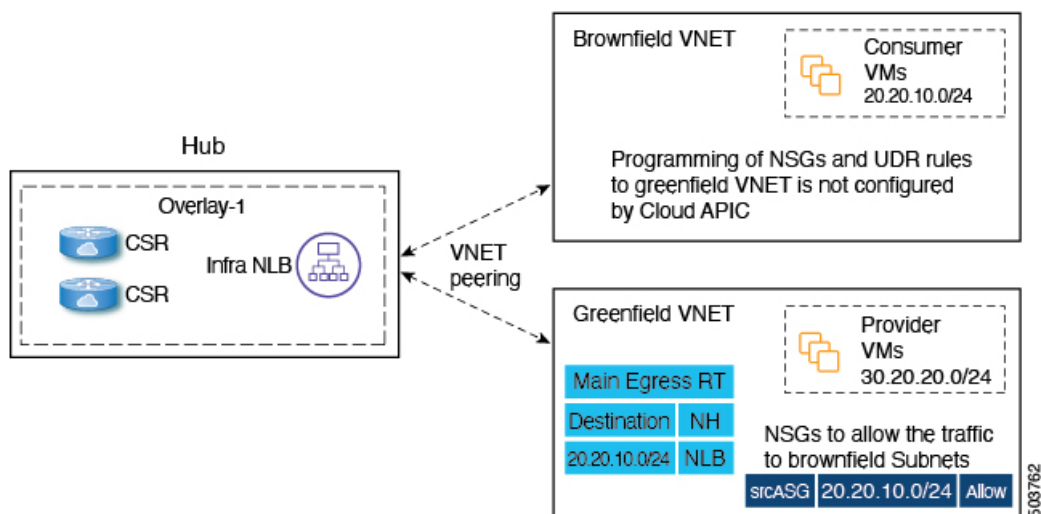
Cisco APIC のリリース バージョン	特長	説明
5.2(1)	Cisco Cloud APIC への既存のブラウнフィールドクラウド VNet のインポートのサポート	このリリースでは、既存のブラウнフィールドクラウド VNet を Cisco Cloud APIC に指定します

## 既存の Azure ブラウнフィールドクラウド VNet を Cisco Cloud APIC にインポートする利点

リリース 5.2(1) より前では、Cisco Cloud APIC を通じたクラウド導入はグリーンフィールド導入と見なされ、必要なコンポーネント（リソースグループ、VNet、CIDR、サブネットなど）の設定は Cisco Cloud APIC を通じて行われます。次に、Cisco Cloud APIC で作成したこれらのリソースグループの下にサービスを展開し、アプリケーションを起動します。

データセンター拡張に Microsoft Azure Cloud を採用した多くのユーザは、すでにクラウドに導入された数百の VNet とインスタンスを持っています。これにより、Azure の Cisco Cloud APIC を通じた新しいグリーンフィールド設定と既存のブラウнフィールド設定の2つの異なる環境ができます。Cisco Cloud APIC ソリューションを導入した後、既存のクラウドリソースに個別のコントロールポイントが必要ない場合、これは理想的ではありません。

リリース 5.2(1) よりも前では、リソースグループと VNet が Cisco Cloud APIC を使用せずに作成された既存のブラウнフィールド環境は、Cisco Cloud APIC のマネージドサイトで共存できませんでした。リリース 5.2(1) 以降では、既存のブラウнフィールド VNet を Cisco Cloud APIC にインポートできるようになりました。この拡張機能では、VNet ピアリングを使用して、Cisco Cloud APIC を通じて設定されたグリーンフィールド VNet と Cisco Cloud APIC の外部で設定されたブラウнフィールド VNet 間の通信を提供します。



上図では、次のことが言えます。

- ハブ VNet とグリーンフィールド VNet が作成され、Cisco Cloud APIC を通じて管理されます。
- ブラウンフィールド VNet は Azure 経由で作成され、Cisco Cloud APIC の外部で管理されます

この機能を使用すると、Cisco Cloud APIC は既存のブラウンフィールドリソースグループで何も設定またはプロビジョニングされないことに注意してください。通常のリートテーブル、UDR ルール、NSG、および ASG は、これらのブラウンフィールドリソースグループでは Cisco Cloud APIC を通じて作成されません。Cisco Cloud APIC は、これらの既存のブラウンフィールド展開のセキュリティルールとルーティングを管理しないため、Cisco Cloud APIC の外部の既存のブラウンフィールド展開のセキュリティルールとルーティングを引き続き管理します。

このブラウンフィールド機能を使用すると、ブラウンフィールド VNet を Cisco Cloud APIC にインポートできます。

- インフラテナントに関連付けられたものと同じ Azure AD を指すサブスクリプションに属するブラウンフィールド VNet、または
- インフラテナントに関連付けられた Azure AD とは異なる Azure AD を指すサブスクリプションに属するブラウンフィールド VNet。これは、リリース 5.2 (1) で利用可能な Azure AD 間の VNet ピアリングのサポートを使用して実現されます。詳細については、「[Configuring VNet Peering for Cloud APIC for Azure](#)」を参照してください。

## このドキュメントで使用される用語

このセクションでは、このドキュメントで使用される主要な用語と概念の一部を紹介します。

### グリーンフィールド VNet

クラウドコンテキストプロファイルの Cloud APIC に基づいて作成される Azure 上の仮想ネットワーク。

### ブラウンフィールドまたはアンマネージド VNet

Cloud APIC を通じたポリシーを使用せずに作成された Azure 上の仮想ネットワーク。

### グリーンフィールド リソース グループ

クラウドコンテキストプロファイルの Cloud APIC に基づいて作成された Azure 上のリソースグループ。

## ブラウンフィールドまたはアンマネージド リソース グループ

Cloud APIC を通じたポリシーを使用せずに作成された Azure 上のリソース グループ。

### アクセス ポリシー

Cloud APIC で作成されたポリシーは、それぞれの権限を示します。現在、ポリシーは次のとおりです。

- デフォルト
- Unmanaged
- 読み取り専用

### 読み取り専用クラウド コンテキスト プロファイル

読み取り専用アクセス ポリシーに関連するクラウド コンテキスト プロファイル。

### 読み取り専用アカウント

読み取り専用アクセス ポリシーに関連するクラウド アカウント。

### グリーンフィールドクラウド コンテキスト プロファイル

アクセス ポリシーと関係がない、またはデフォルト アクセス ポリシーと関係がないクラウド コンテキスト プロファイル。

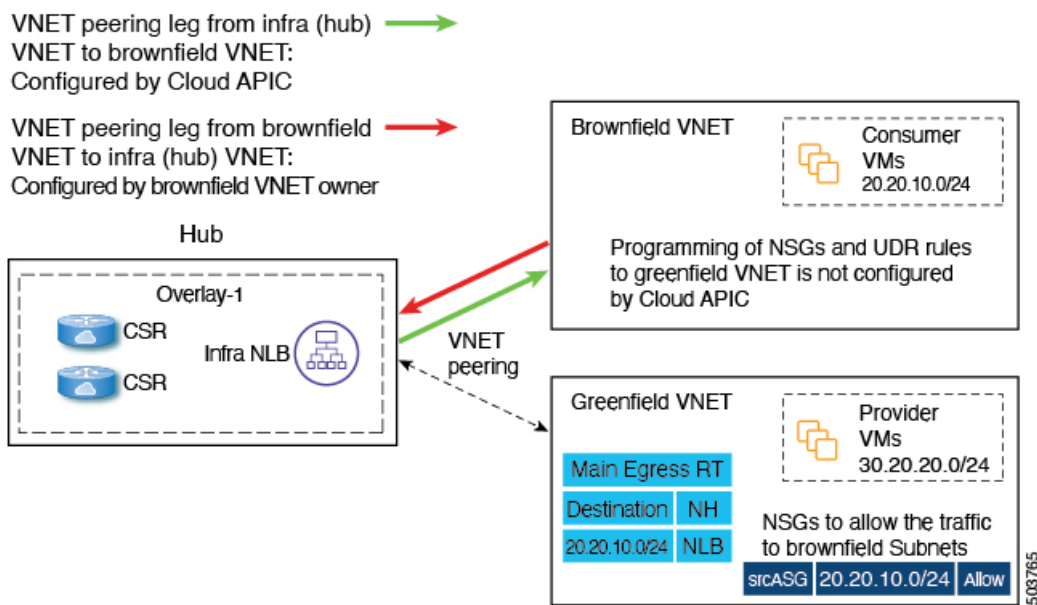
## 管理対象外（ブラウンフィールド）VNet の VNet ピアリングの概要

通常、Cisco Cloud APIC はクラウド上でグリーンフィールド VNet を作成すると、このスポーク VNet からすべてのインフラ（ハブ）VNet への双方向 VNet ピアリング設定を作成します。グリーンフィールド VNet を使用した VNet ピアリング設定の場合、Cisco Cloud APIC ではこのピアリング設定の両方のレッグを設定します。

- Cisco Cloud APIC はインフラ（ハブ）VNet からスポーク VNet への最初のレッグを設定します。
- Cisco Cloud APIC は次に、スポーク VNet からインフラ VNet への他のレッグを設定します。

ただし、アンマネージド（ブラウンフィールド）VNet を使用して VNet ピアリングを設定する場合、VNet ピアリング設定の一部は Cisco Cloud APIC によって行われ、他の VNet ピアリング設定は手動で行う必要があります。

- **インフラ（ハブ）VNet からアンマネージド VNet への最初のレッグ**：Cisco Cloud APIC によって設定されます。ここで、Cisco Cloud APIC は Cisco Cloud APIC が管理するリソース グループのグリーンフィールド NSG の UDR および NSG ルールのプログラミングを処理します。
- **管理対象外 VNet からインフラ VNet への他のレッグ**：管理対象外（ブラウンフィールド）VNet の所有者として、この VNet ピアリング設定のレッグを手動で設定する必要があります。VNet ピアリング設定のこのレッグは Cisco Cloud APIC により実行されません。グリーンフィールド VNet と通信するには、ブラウンフィールド VNet で UDR および NSG ルールを設定する必要があります。



グリーンフィールド VNet とブラウンフィールド VNet の間で通信を行うには、アンマネージド VNet からすべてのインフラ VNet へのシングルレッグ VNet ピアリングを作成する必要があります。これがないと、グリーンフィールド VNet とブラウンフィールド VNet の間でパケットフローが発生しません。

また、リリース 5.2(1) 以降では、Azure Active Directory 間での VNet ピアリングのサポートも利用できます。この拡張機能がないと、同じ Azure Active Directory に制限されます。この拡張機能では、インフラ VNet と同じ Azure Active Directory からブラウンフィールド VNet をインポートすることに制限されません。インフラストラクチャの Azure Active Directory とは異なる Azure Active Directory に存在するブラウンフィールド VNet は、Azure Active Directory 全体で VNet ピアリングのこの拡張機能を使用して Cisco Cloud APIC にインポートできます。

詳細については、「[Configuring VNet Peering for Cloud APIC for Azure](#)」を参照してください。

## Cisco Cloud APIC がブラウンフィールド VNet で行うことと行わないこと

リリース 5.2(1) の一部としてのこの拡張により、Cisco Cloud APIC はブラウンフィールド VNet とパケットを送受信できるように、グリーンフィールドリソースグループ/VNet 側で必要なネットワーク接続とセキュリティを調整できます。

Cisco Cloud APIC は、プロビジョニングに関する次の情報を提供します。

- Cisco Cloud APIC は、すべてのインフラ VNet からブラウンフィールド VNet への VNet ピアリングをプロビジョニングします。
- グリーンフィールド VNet 側から：
  - Cisco Cloud APIC はインフラ VNet でネットワークロードバランサとしてネクストホップを使用して、ブラウンフィールド VNet CIDR のルートテーブルエントリをプロビジョニングします。

- Cisco Cloud APIC は設定されたコントラクトに応じて、ブラウフィールド VNet エンドポイントまたはサブネットのサブネットまたは IP アドレスでのパケットの着信または発信を許可するセキュリティグループルールをプロビジョニングします。

ブラウフィールド VNet を Cisco Cloud APIC で登録すると、次の設定が行われます。

- インベントリ プルは、ブラウフィールドリソース グループまたは VNet で実行されます。
- Cisco Cloud APIC は、すべてのインフラ VNet からブラウフィールド VNet への単方向 VNet ピアリングを自動的に設定します。詳細については、「[管理対象外 \(ブラウフィールド\) VNets の VNet ピアリングの概要 \(4 ページ\)](#)」を参照してください。
- 既存のグリーンフィールド EPG とのコントラクトに基づいて、UDR および NSG ルールは、Cisco Cloud APIC によって管理されるリソース グループのグリーンフィールド NSG にのみ設定されます。
- コントラクトがグリーンフィールド VNet に関連付けられた EPG とブラウフィールドクラウド コンテキスト プロファイルに関連付けられた EPG の間で定義されると、Cisco Cloud APIC はスタティック ルートで CSR を自動的にプログラムします。また、Cisco Cloud APIC は CSR のブラウフィールド VNet CIDR に対応するルート リークも設定します。
- Cisco Cloud APIC は、EPG 間のコントラクトに基づいて、グリーンフィールド VNet のブラウフィールド VNet CIDR に対応するすべてのルート エントリを自動的にプログラムします。

VRF を介したブラウフィールドクラウド コンテキスト プロファイルに関連付けられているクラウド EPG には、サブネット ベースのエンドポイント セレクタが必要です (タグベースの EPG はブラウフィールドクラウド コンテキスト プロファイルには適用されません)。

リリース 5.2(1) の場合、Cisco Cloud APIC はアンマネージドリソース グループでは何も設定またはプロビジョニングしません。Cisco Cloud APIC は、通常のルート テーブル、UDR ルール、NSG およびこれらのアンマネージドリソース グループの ASG を作成しません。これらのアンマネージドリソース グループのセキュリティとルーティングは、Cisco Cloud APIC がそれらをマネージしないため、お客様が責任を負います。

次の設定は、ブラウフィールド VNet の Cisco Cloud APIC での登録時に行われなかったため、これらのポリシーを作成して適用する必要があります。

- Cisco Cloud APIC は、グリーンフィールド EPG とのコントラクトに基づいて、インフラ NLB を指す UDR を含むルート テーブルを作成しません。外部サイトのサブネットからパケットを送受信するように、ルート テーブルの UDR ルールをプログラムする必要があります。これらの外部サブネットは、ハブ VNet 内のインフラ NLB の 1 つのプライベート IP を指すネクスト ホップでプログラムする必要があります。
- Cisco Cloud APIC は、ブラウフィールドリソース グループに NSG または ASG を作成しません。セキュリティ ルールが外部サイトのエンドポイントまたはサブネットからパケットを送受信できるように、NSG または ASG ルールをプログラムする必要があります。詳細については、[Azure サイトの次のページを参照してください](#)。

<https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group#work-with-application-security-groups>

- Cisco Cloud APIC は、ブラウフィールド VNet からインフラ VNet への VNet ピアリングをプログラムしません。ブラウフィールド VNet からインフラ VNet への VNet ピアリングをプログラムする必要があります。詳細については、「[管理対象外 \(ブラウフィールド\) VNets の VNet ピアリングの概要 \(4 ページ\)](#)」を参照してください。

- これらのブラウフィールドリソースグループのエンドポイントに対して行われたエンドポイント検出はありません。

さらに、ブラウフィールド VNet を Cisco Cloud APIC に登録すると、次の Cisco Cloud APIC コンポーネントが影響を受けるか、影響を受けません。

- ブラウフィールド VRF の CSR プログラミングに変更はありません。CSR の観点からは、ブラウフィールド VRF は他の VRF と同様に動作します。CSR では、ブラウフィールド VRF は CIDR（アンマネージドクラウドコンテキストプロファイルに存在する CIDR）とともにプログラムされます。アクセスリストはギガビット 1 インターフェイスでプログラムされ、これらのアンマネージド VNet CIDR からのトラフィックを許可します。コントラクトに基づいて、必要に応じて異なる VRF 間でルートリークが発生します。

## ガイドラインと制限

次に、既存のブラウフィールドクラウド設定を Cloud APIC にインポートする際の注意事項と制約事項を示します。



(注) 次の箇条書きでは、「インフラ NLB」という用語は、インフラ VNet のリソースグループ内の NLB を指します。

- 既存のブラウフィールドクラウド設定を Cloud APIC にインポートするプロセスの一環として、次の設定を行います。
  - ブラウフィールドリソースグループに属するルートテーブル内のグリーンフィールド CIDR のルートエントリ（ネクストホップがインフラ NLB に設定されている）
  - グリーンフィールド EPG との間のトラフィックを許可するセキュリティルール
  - ブラウフィールド VNet とインフラ VNet 間の VNet ピアリング。

一般的な Cloud APIC マルチハブ展開では、通常、1 つのリージョンでのインフラ NLB 障害が自動的に検出されます。その結果、UDR はルートプレーンのネクストホップとして使用可能な別のインフラ NLB で自動的に更新されます。ただし、上記のように既存のブラウフィールドクラウド設定を Cloud APIC にインポートするようにシステムを設定すると、このインフラ NLB 障害検出と UDR の更新は通常のように自動的に行われません。

この状況では、インフラ NLB 障害を検出し、ネクストホップとして動作中のインフラ NLB IP アドレスを使用してブラウフィールドルートテーブルを手動で更新する必要があります。

- アンマネージド（ブラウフィールド）クラウドコンテキストプロファイルには、特に次の注意事項と制約事項が適用されます。
  - アンマネージド VNet の特定の VNet ID は、Cisco Cloud APIC 上の 2 つの異なるアンマネージドクラウドコンテキストプロファイルにマッピングできません。特定の VNet ID は、Cisco Cloud APIC で 1 つのアンマネージドクラウドコンテキストプロファイルのみを作成するために使用できます。
  - クラウドコンテキストプロファイルにマッピングされたアンマネージド VNet は、この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テナントと同じアカウント（サブスクリプション）に存在する必要がある

あります。Cisco Cloud APIC でこれらのアンマネージドクラウド コンテキスト プロファイルを定義している間は、ランダムな VNet ID を指定できません。

- ホスト VRF は、ブラウフィールド VNet のインポートには使用できません。

## 既存のブラウフィールドクラウド VNet を Cisco Cloud APIC にインポートするためのワークフロー

次に、既存のブラウフィールドクラウド VNet を Cisco Cloud APIC にインポートするための一般的なワークフローを示します。

1. 必要な場合は、アンマネージド（ブラウフィールド）クラウド コンテキスト プロファイルで使用する新しいテナントを作成します。

アンマネージド（ブラウフィールド）VNet が別のサブスクリプションにある場合、新しいテナントを作成する必要があります。

アンマネージドテナントの下で作成されたこの新しいアカウントは、これらのサブスクリプションでイベント収集または統計収集リソースの作成をトリガーしない読み取り専用ポリシーにも関連付けられます。これらのサブスクリプションでは、インベントリ プルのみが実行されます。

新しいテナントの作成方法については、『[Cisco Cloud APIC for Azure User Guide、リリース 5.2 以降](#)』を参照してください。

- 「テナント、ID、およびサブスクリプションについて」
- 「Cisco Cloud APIC GUI を使用したテナントの作成」

2. Cisco Cloud APIC に既存のブラウフィールド VNet、CIDR、およびサブネット設定をインポートします。

これを行うには、ブラウフィールド VNet に対応するクラウド コンテキスト プロファイルを作成します。これにより、ブラウフィールド VNet と VRF の間に関連付けが作成されます。Cisco Cloud APIC のクラウド コンテキスト プロファイルは、ブラウフィールド VNet と VRF 間のリンクに使用されるオブジェクトです。ブラウフィールド VNet をインポートするには、最初に VRF オブジェクトを作成する必要があります。これは、後でブラウフィールド VNet をインポートするときに使用されるクラウド コンテキスト プロファイル関連付けのプレースホルダです。

これらの手順については、[管理対象外（ブラウフィールド）クラウド コンテキスト プロファイルの作成（11 ページ）](#) を参照してください。

3. ブラウフィールド VNet の VNet ピアリングを設定します。

- アンマネージド（ブラウフィールド）VNet の所有者として、VNet ピアリング設定の一部、つまりアンマネージド VNet からインフラ VNet へのレッグを手動で設定する必要があります。Cisco Cloud APIC は、VNet ピアリング設定の他の部分、インフラ VNet からアンマネージド VNet へのレッグを自動的に設定します。

詳細については、[管理対象外（ブラウフィールド）VNets の VNet ピアリングの概要（4 ページ）](#) を参照してください。



- Azure AD 間で VNet ピアリングが必要な場合は、個別に設定する必要があります。  
詳細については、「[Configuring VNet Peering for Cloud APIC for Azure](#)」を参照してください。

#### 4. ブラウンフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成します。

これらの手順については、[ブラウンフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成 \(19 ページ\)](#) を参照してください。

## 読み取り専用アカウントの設定

次のセクションでは、読み取り専用アカウントの設定に関して説明します。

### 読み取り専用アカウントの概要

アンマネージド VNet のみを含むアカウント（サブスクリプション）があり、Azure でこのサブスクリプションの VNet を管理するために Cisco Cloud APIC を使用しない場合は、このアカウントを読み取り専用アカウントとして定義できます。読み取り専用アカウント（ポリシー）は、これらのサブスクリプションでイベント収集/統計収集リソースの作成をトリガーしません。この読み取り専用ポリシーに関連するサブスクリプションに対しては、インベントリ プルのみが実行されます。

テナントの下で読み取り専用アカウントとしてアカウントを設定する場合、そのテナントのすべてのクラウドコンテキストプロファイルは読み取り専用である必要があります。そのテナントでは、通常のグリーンフィールド（Cisco Cloud APIC が作成）クラウドコンテキストプロファイルを使用できません。Cisco Cloud APIC は、クラウドのこのサブスクリプションにリソースを作成しません。また、このサブスクリプションのイベントまたは統計に関連する項目はクラウドに表示されません。このアカウントはクラウド上で読み取り専用アクセスを持ちますが、アクセスタイプはマネージド ID またはサービスプリンシパル（アンマネージド）ID のいずれかです。

### GUI を使用した読み取り専用のアカウントの設定

#### 始める前に

読み取り専用のアカウントを作成する前に、[読み取り専用アカウントの概要 \(9 ページ\)](#) に示された情報をレビューします。

#### 手順

- 
- ステップ 1** 左のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [テナント (Tenants)] に移動します。  
設定済みのテナントが [テナント (Tenants)] ページに表示されます。
  - ステップ 2** [アクション (Actions)] をクリックし、[テナントの作成 (Create Tenant)] を選択します。  
[テナントの作成 (Create Tenant)] ダイアログ ボックスが表示されます。
  - ステップ 3** このテナントを設定するために必要な予備情報を入力します。

- [モード (Mode) ]フィールドで、[個別作成 (Create Own) ]を選択して新しいテナントを読み取り専用アカウントで設定するか、共有する既存のテナントがすでに読み取り専用アカウントで作成されている場合は [共有 (Shared) ]を選択します。
- [アクセス タイプ (Access Type) ]フィールドでは、[読み取り専用アカウントの概要 \(9 ページ\)](#) の説明に従って、[サービス プリンシパル (Service Principal) ]または[マネージド アイデンティティ (Managed Identity) ]を選択できます。

**ステップ 4** [クラウドアクセス権限 (Cloud Access Privilege) ]フィールドで、[読み取り専用 (Read Only) ]を選択します。

このフィールドは、クラウドアカウントを読み取り専用を設定します。

**ステップ 5** このテナントの残りの設定を完了し、完了したら [保存 (Save) ]をクリックします。

## REST API を使用した読み取り専用アカウントの設定

### 始める前に

読み取り専用のアカウントを作成する前に、[読み取り専用アカウントの概要 \(9 ページ\)](#) に示された情報をレビューします。

### 手順

**ステップ 1** クライアントシークレットを使用して読み取り専用アカウントでアンマネージドテナントを作成するには、以下を投稿します。

太字のテキストは、クラウドアカウントを読み取り専用を設定する行を示しています。

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

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

**ステップ 2** 読み取り専用アカウントでマネージドテナントを作成するには、以下を投稿します。

太字のテキストは、クラウドアカウントを読み取り専用を設定する行を示しています。

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

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

---

## 管理対象外（ブラウフィールド）クラウドコンテキスト プロファイルの作成

次のトピックでは、アンマネージド（ブラウフィールド）クラウドコンテキストプロファイルを作成する方法について説明します。

### アンマネージド（ブラウフィールド）クラウドコンテキスト プロファイルの概要

アンマネージド（ブラウフィールド）クラウドコンテキスト プロファイルは、アンマネージド（ブラウフィールド）VNetに関連付けられているCisco Cloud APIC ポストされた設定を参照します。

- アンマネージド（ブラウフィールド）クラウドコンテキストプロファイルは、グリーンフィールド（Cisco Cloud APIC マネージド）アカウントに関連付けられているかどうか、またはアンマネージドアカウントであるかどうかに関係なく、任意のテナントで定義できます。
- すでにVNetがCisco Cloud APIC 設定されているグリーンフィールドアカウントがあり、同じサブスクリプションにアンマネージドVNetもある場合は、グリーンフィールドアカウントに関連付けられたテナントでアンマネージドクラウドコンテキストプロファイルを定義できます。つまり、グリーンフィールドクラウドコンテキストプロファイルで使用されているテナントがすでに作成されている場合、その同じテナントをブラウフィールドクラウドコンテキストプロファイル（アンマネージドVNetインポート）の作成にも使用できます。

アンマネージド（ブラウフィールド）クラウドコンテキストプロファイルに設定する必要があるパラメータは次のとおりです。

- **VRF** : アンマネージドVNetを関連付けるCisco Cloud APIC のVRF
- **リージョン** : アンマネージドVNetがクラウド上に存在するリージョン
- **VNet ID** : クラウド上のこのアンマネージドVNetのクラウドプロバイダーID
- **CIDR** : Cisco Cloud APIC で参照する必要があるCIDR

Cisco Cloud APICはこれらのパラメータを使用して、ブラウフィールドクラウドコンテキストプロファイルをクラウド上の特定のVNetにマッピングします。

## GUIを使用したアンマネージド（ブラウフィールド）クラウドコンテキストプロファイルの作成

### 始める前に

これらの手順を実行する前に、[アンマネージド（ブラウフィールド）クラウドコンテキストプロファイルの概要（11 ページ）](#)に記載されている情報を確認してください。

### 手順

---

**ステップ 1** 必要な場合は、アンマネージド（ブラウフィールド）クラウドコンテキストプロファイルで使用する新しいテナントを作成します。

アンマネージド（ブラウフィールド）VNetが別のサブスクリプションにある場合、新しいテナントを作成する必要があります。

ブラウフィールド VNet で使用される新しいテナントには、次の特性があります。

- クラウド上にアンマネージドの VNet のみを持つアカウント（サブスクリプション）があり、Azure でこのサブスクリプションの VNet を管理するために Cisco Cloud APIC を使用しない場合は、読み取り専用アカウントとして設定できます。読み取り専用アカウントの詳細については、[読み取り専用アカウントの概要（9 ページ）](#)を参照してください。
- 読み取り専用アクセス権を持つアンマネージドテナントは、次のいずれかのモードで設定できます。
  - マネージドアイデンティティ モード
  - サービス プリンシパル モード

新しいテナントの作成方法については、『[Cisco Cloud APIC for Azure User Guide、リリース 5.2 以降](#)』を参照してください。

- 「テナント、ID、およびサブスクリプションについて」
- 「Cisco Cloud APIC GUI を使用したテナントの作成」

このテナントは、Azure のアンマネージド（ブラウフィールド）VNet と同じ Azure サブスクリプション ID を使用する必要があります。

**ステップ 2** ブラウフィールド VNet のクラウドコンテキストプロファイルに関連付ける VRF を作成します。

a) Cisco Cloud APIC GUI の左側のナビゲーションバーで、**[Application Management] > [VRF]** をクリックします。

設定されている VRF リストが表示されます。

b) **[アクション (Actions)] > [VRF の作成 (Create VRF)]** をクリックします。

**[VRF の作成 (Create VRF)]** ページが表示されます。

- c) 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 1: [VRFの作成 (Create VRF) ] ダイアログボックスのフィールド

[プロパティ (Properties) ]	説明
全般	
名前	[Name] フィールドに、VRF の表示名を入力します。 すべての VRF に <i>vrfEncoded</i> 値が割り当てられます。テナントと VRF 名の組み合わせが 32 文字を超える場合、VRF 名 (テナント名も含む) は <i>vrfEncoded</i> 値を使用してクラウドルータで識別されます。 <i>vrfEncoded</i> 値を表示するには、[Application Management]>[VRFs] サブタブに移動します。右側のペインで VRF をクリックし、クラウドルータで [Encoded VRF Name] を探します。
テナント	テナントを選択します。 <b>1.</b> [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>2.</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。[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。

- d) 作業が完了したら、[保存 (Save) ] をクリックします。

- ステップ 3** Cisco Cloud APIC GUI で、[Intent] アイコン (🔗) をクリックします。  
ウィンドウの右側に、何をしますかを尋ねるスライドインペインが表示されます。
- ステップ 4** [アンマネージド仮想ネットワーク (Unmanaged Virtual Network) ] オプションをクリックします。  
アンマネージドクラウドコンテキストプロファイルを作成するためのセットアップウィザードが表示されます。
- ステップ 5** [アンマネージド仮想ネットワーク関連付けのインポート (Import Unmanaged Virtual Network Association) ] ウィンドウの [設定 (Settings) ] 領域で、[アンマネージド仮想ネットワーク (Unmanaged Virtual Network) ] フィールドの下の [アンマネージド仮想ネットワークの選択 (Select Unmanaged Virtual Network) ] をクリックします。  
[アンマネージド仮想ネットワークの選択 (Select Unmanaged Virtual Network) ] ウィンドウが表示され、テナントを作成したサブスクリプションで Azure で使用可能なすべてのブラウザーフィールド VNet (Cisco Cloud APIC によって管理されていない VNet) が表示されます。このウィンドウに入力される VNet のリストは、このサブスクリプションのインベントリプルに基づいています。

**ステップ 6** インポートするアンマネージド VNet をリストから探し、アンマネージドクラウドコンテキストプロファイルに関連付けます。

Cisco Cloud APIC GUI のこのウィンドウでは、このリストのアンマネージド VNet が次の形式で表示されます。

**AZURE > {Azure\_subscription\_ID} > {Azure\_resource\_group}**

Cisco Cloud APIC GUI ページの **[Name]** 列のブラウフィールド VNet の名前。

Azure ポータルに戻り、Azure ページでアンマネージド VNet をクリックし、このブラウフィールド VNet の **[リソース グループ (Resource Group)]**、**[サブスクリプション (Subscription ID)]**、および **[名前 (Name)]** フィールドを見つけて、情報が Cisco Cloud APIC GUI ページに表示される情報と一致することを確認します。

**ステップ 7** リストから適切なアンマネージド VNet をクリックします。

ウィンドウの右側のペインに、このアンマネージド VNet に関する追加情報が表示されます。

**ステップ 8** **[選択 (Select)]** をクリックします。

**[アンマネージド仮想ネットワーク関連付けのインポート (Import Unmanaged Virtual Network Association)]** のメイン ウィンドウに戻ります。

**ステップ 9** **[テナント (Tenant)]** フィールドで、このアンマネージドクラウドコンテキストプロファイルに関連付ける、このサブスクリプションの下テナントを選択します。

このアンマネージドクラウドコンテキストプロファイルは、このテナントの下に作成されます。

**ステップ 10** **[関連付けられた VRF (Associated VRF)]** フィールドで、このアンマネージドクラウドコンテキストプロファイルに関連付ける VRF を選択します。

**ステップ 11** **[名前 (Name)]** フィールドに、プロファイルの名前を入力します。

**ステップ 12** **[VNet ピアリング (VNet Peering)]** フィールドで、**[Enable]** の横にあるボックスをクリックして、このアンマネージドクラウドコンテキストプロファイルの VNet ピアリングを有効にします。

この VNet ピアリングフィールドを有効にすると、Cisco Cloud APIC がインフラ VNet からクラウド上のアンマネージド VNet へのピアリングを作成できます。詳細については、「[Azure Active Cloudies の VNet ピアリングの設定](#)」の「Azure Active Directory の VNet ピアリングのサポート」を参照してください。

**ステップ 13** **[インポートするリソース (Resources to Import)]** フィールドで、このアンマネージドクラウドコンテキストプロファイルにインポートするアンマネージド VNet 内で使用可能な CIDR を選択します。

この領域にリストされているすべての CIDR を選択するか、このアンマネージドクラウドコンテキストプロファイルにインポートする特定の CIDR を選択できます。選択したすべての CIDR について、対応するサブネットもインポートされます。

最初に選択した CIDR が自動的にプライマリ CIDR としてマークされますが、その CIDR と他の選択した CIDR に違いはないことに注意してください。

**ステップ 14** **[アンマネージド仮想ネットワーク関連付けのインポート (Import Unmanaged Virtual Network Association)]** ウィンドウで **[保存 (Save)]** 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保存します。

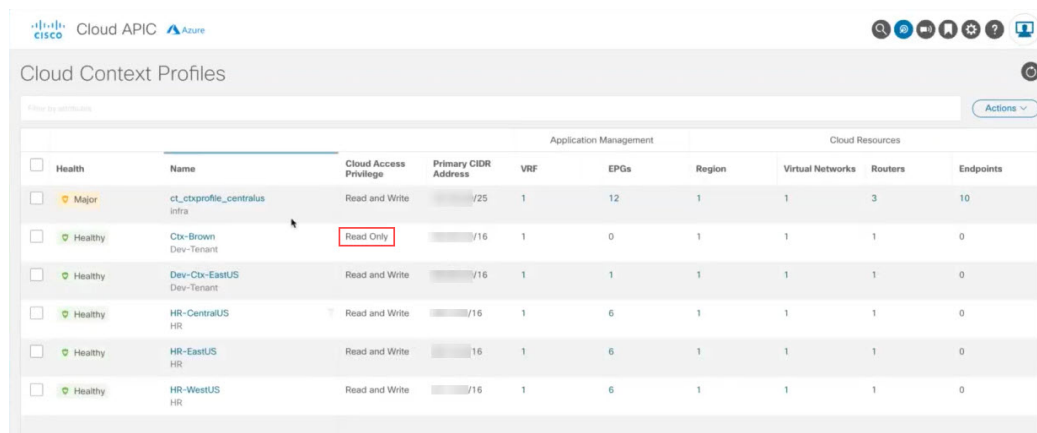
[What's Next] ページが表示されます。

**ステップ 15** ウィンドウの右下にある[クラウドコンテキストプロファイルの詳細に移動 (Go to Cloud Context Profile Details)] をクリックします。

メインの[クラウドコンテキストプロファイル (Cloud Context Profiles)] ページに戻り、設定されているすべてのクラウドコンテキストプロファイルが一覧表示されます。

**ステップ 16** 作成したアンマネージドクラウドコンテキストプロファイルを見つけます。

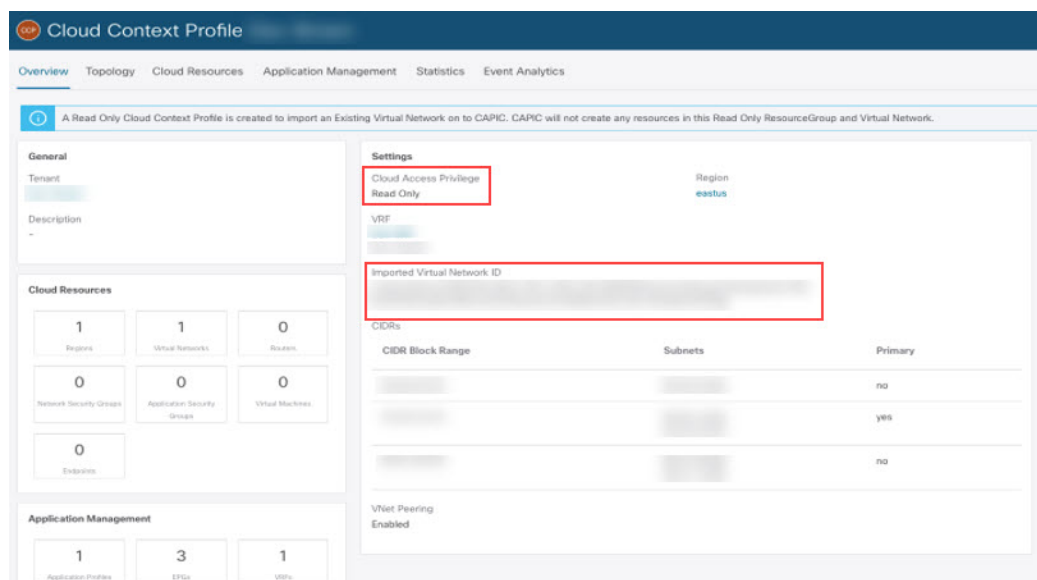
アンマネージドのクラウドコンテキストプロファイルでは、[クラウドアクセス権限 (Cloud Access Privilege)] 列に[読み取り専用 (Read Only)] と表示されます。これは、インベントリを読み取るだけで、Azure には何も書き込まないことを示します。



Health	Name	Cloud Access Privilege	Primary CIDR Address	VRF	EPGs	Region	Virtual Networks	Routers	Endpoints
Major	ct_ctxprofile_centralus_infra	Read and Write	/25	1	12	1	1	3	10
Healthy	Ctx-Brown Dev-Tenant	Read Only	/16	1	0	1	1	1	0
Healthy	Dev-Ctx-EastUS Dev-Tenant	Read and Write	/16	1	1	1	1	1	0
Healthy	HR-CentraUS HR	Read and Write	/16	1	6	1	1	1	0
Healthy	HR-EastUS HR	Read and Write	/16	1	6	1	1	1	0
Healthy	HR-WestUS HR	Read and Write	/16	1	6	1	1	1	0

**ステップ 17** このプロファイルの追加情報を表示するには、作成したアンマネージドクラウドコンテキストプロファイルをクリックします。

次の図は、読み取り専用フラグが有効になっており、関連付けられているクラウドプロバイダー ID が設定されたアンマネージドクラウドコンテキストプロファイルを示しています。



Cloud Context Profile

Overview | Topology | Cloud Resources | Application Management | Statistics | Event Analytics

A Read Only Cloud Context Profile is created to import an Existing Virtual Network on to CAPIC. CAPIC will not create any resources in this Read Only ResourceGroup and Virtual Network.

**General**

Tenant: [redacted]  
Description: -

**Cloud Resources**

1	1	0
Regions	Virtual Networks	Routers
0	0	0
Network Security Groups	Application Security Groups	Virtual Machines
0		
Endpoints		

**Application Management**

1	3	1
Application Profiles	EPGs	VRFs

**Settings**

Cloud Access Privilege: Read Only  
Region: eastus  
VRF: [redacted]  
Imported Virtual Network ID: [redacted]

CIDR Block Range	Subnets	Primary
[redacted]	[redacted]	no
[redacted]	[redacted]	yes
[redacted]	[redacted]	no

Visit Peering: Enabled

**ステップ 18** Cisco Cloud APIC GUIの左側のナビゲーション バーで、[Application Management]> [VRF] をクリックします。

設定されている VRF リストが表示されます。

**ステップ 19** ブラウンフィールド VNet のクラウド コンテキスト プロファイルに関連付けられるこれらの手順で以前に作成した VRF を見つけ、その VRF をクリックします。

VRF がインポートされたブラウンフィールド VNet に関連付けられていることを確認します。

**ステップ 20** Azure ポータルで、インフラ VNet の [仮想ネットワーク (Virtual network)] ページの [ピアリング (Peerings)] 領域に移動し、インフラ (ハブ) VNet からアンマネージド (ブラウンフィールド) VNet への VNet ピアリングが設定されていることを確認します。

管理対象外 (ブラウンフィールド) VNets の VNet ピアリングの概要 (4 ページ) で説明したように、VNet ピアリングの最初のレッグのみが (インフラ VNet からアンマネージド VNet に) Cisco Cloud APIC により設定され、他のレッグはまだ設定されていないため (アンマネージド VNet からインフラ VNet に)、ピアリング ステータスはこの VNet ピアリングの開始として表示され、非管理 (ブラウンフィールド) VNet は [ピア (Peer)] 列に表示されます。

Name	Peering status	Peer	Gateway transit
klab_vrf1_eastus	Connected	vrf1	Disabled
klab_vrf2_centralus	Connected	vrf2	Disabled
klab_ninja1_eastus	Initiated	ninja1	Disabled

## 次のタスク

Azure での管理対象外 VNet からインフラ VNet へのピアリングの追加 (17 ページ) に示す手順を使用して、Azure で VNet ピアリングのもう一方のレッグ (アンマネージド VNet からインフラ VNet へ) を設定します。

## REST API を使用したアンマネージド (ブラウンフィールド) クラウド コンテキスト プロファイルの作成

### 始める前に

これらの手順を実行する前に、アンマネージド (ブラウンフィールド) クラウド コンテキスト プロファイルの概要 (11 ページ) に記載されている情報を確認してください。



## 手順

アンマネージド（ブラウフィールド）のクラウドコンテキストプロファイルを作成するには、以下を投稿します。

太字のテキストは、アンマネージドクラウドコンテキストプロファイルの作成に固有の行を示しています。

- `cloudRsCtxProfileToAccessPolicy` 行は、クラウドコンテキストプロファイルを読み取り専用を設定します（詳細については、[読み取り専用アカウントの概要（9 ページ）](#) を参照してください）。
- `cloudBrownfield` 行は、クラウドプロバイダーの ID を使用してブラウフィールド VNet をクラウドにインポートするために使用されます。

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

```
<fvTenant name="tn15">
  <cloudCtxProfile name="cProfilewestus151" status="" azVirtualNetwork="vnet1" status="">
    <cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only" status="" />
    <cloudRsCtxProfileToRegion status="" tDn="uni/cloudomp/provp-azure/region-westus" status="" />

    <cloudRsToCtx tnFvCtxName="ctx151" />
    <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status="" />
    <cloudBrownfield status="">
    <cloudIDMapping
cloudProviderId="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx/resourceGroups/BrownfieldResGrp/providers/Microsoft.Network/virtualNetworks/VNET1"
status="" />
</cloudBrownfield>
    <cloudCidr name="cidr1" addr="xx.10.0.0/16" primary="yes" status="" />
    <cloudCidr name="cidr2" addr="xx.50.0.0/16" primary="no" status="" />
  </cloudCtxProfile>
</fvTenant>
```

## Azure での管理対象外 VNet からインフラ VNet へのピアリングの追加

このタスクでは、[管理対象外（ブラウフィールド）VNets の VNet ピアリングの概要（4 ページ）](#) で説明されているとおり、アンマネージド（ブラウフィールド）VNet から Azure のインフラ VNet への VNet ピアリングをプログラミングします。

[Cisco Cloud APIC がブラウフィールド VNet で行うことと行わないこと（5 ページ）](#) および [管理対象外（ブラウフィールド）VNets の VNet ピアリングの概要（4 ページ）](#) で説明されているように、Cisco Cloud APIC ではブラウフィールド VNet からインフラ VNet への VNet ピアリングはプログラムされません。ブラウフィールド VNet からインフラ VNet への VNet ピアリングをプログラムする必要があります。

### 始める前に

これらの手順を開始する前に、[管理対象外（ブラウフィールド）クラウドコンテキストプロファイルの作成（11 ページ）](#) の手順を実行してください。これらの手順の最後で、Cisco Cloud APIC は VNet ピアリングの最初のレッグ（インフラ VNet からアンマネージド VNet へ）を設定します。

## 手順

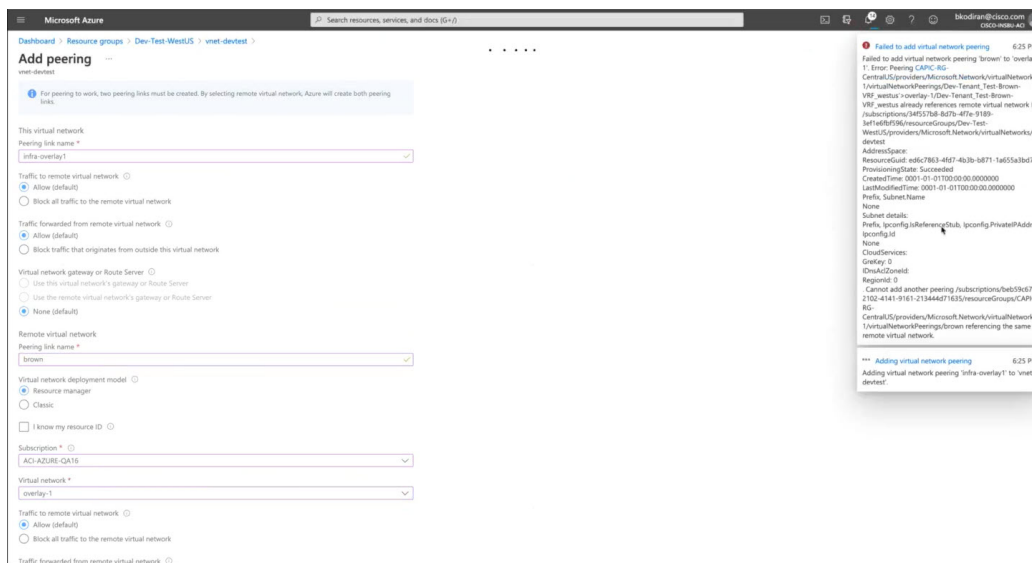
**ステップ 1** Azure ポータルで、[仮想ネットワーク (Virtual networks)] ページに移動し、非管理型 (ブラウнフィールド) VNet を選択します。

**ステップ 2** 管理対象外 (ブラウнフィールド) VNet のページで [ピアリング (Peerings)] オプションを選択します。

**ステップ 3** [+Add] をクリックして、このアンマネージド (ブラウнフィールド) VNet からピアリングを追加します。

**ステップ 4** 管理対象外 (ブラウнフィールド) VNet からインフラ VNet への VNet ピアリングを設定するには、[ピアリングの追加 (Add peering)] ページで設定を完了します。

Azure サイトで VNet ピアリングを設定する場合、VNet ピアリングを両方向に設定することを前提としていることに注意してください。Cisco Cloud APIC は、インフラ (ハブ) VNet からブラウнフィールド VNet への VNet ピアリング接続をすでに開始しているため、このピアリングは失敗します。Azure サイトの [ピアリングの追加 (Add peering)] ページで [追加 (Add)] をクリックすると、次のようなエラーが表示されます。これは予想どおりの結果です。Azure は、関係なく VNet ピアリング設定を完了し、ブラウнフィールド VNet からインフラ (ハブ) VNet への VNet ピアリングを設定します。



**ステップ 5** 管理対象外 (ブラウнフィールド) VNet からインフラ (ハブ) VNet への VNet ピアリングが設定されていることを確認します。

管理対象外 (ブラウнフィールド) VNet の [ピアリング (Peerings)] ページでは、この VNet ピアリングのピアリングステータスが [接続済み (Connected)] として表示され、[ピア (Peer)] 列にインフラ (ハブ) VNet が表示されます。

## 次のタスク

[GUI を使用したブラウнフィールド クラウド コンテキスト プロファイルと関連付けられた EPG の作成 \(21 ページ\)](#) に示す手順を使用して、ブラウнフィールド クラウド コンテキスト プロファイルに関連付ける EPG を作成します。

# ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成

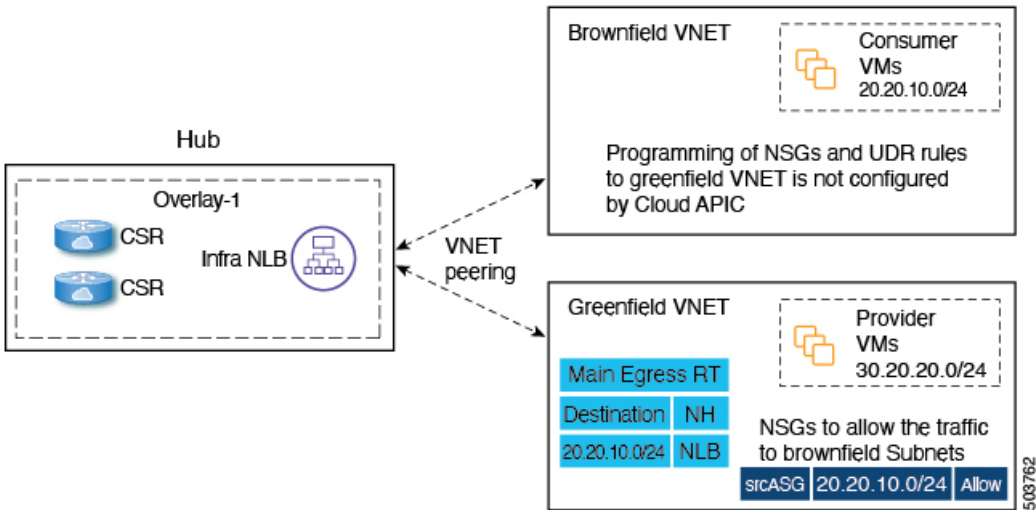
次のトピックでは、ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成について説明します。

## EPG が VRF を通じたブラウフィールドクラウドコンテキストプロファイルと関連付けられている方法

EPG が VRF を介してブラウフィールド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ことをよりよく理解するために、EPG が正常にマッピングされる方法と比較すると役立ちます。

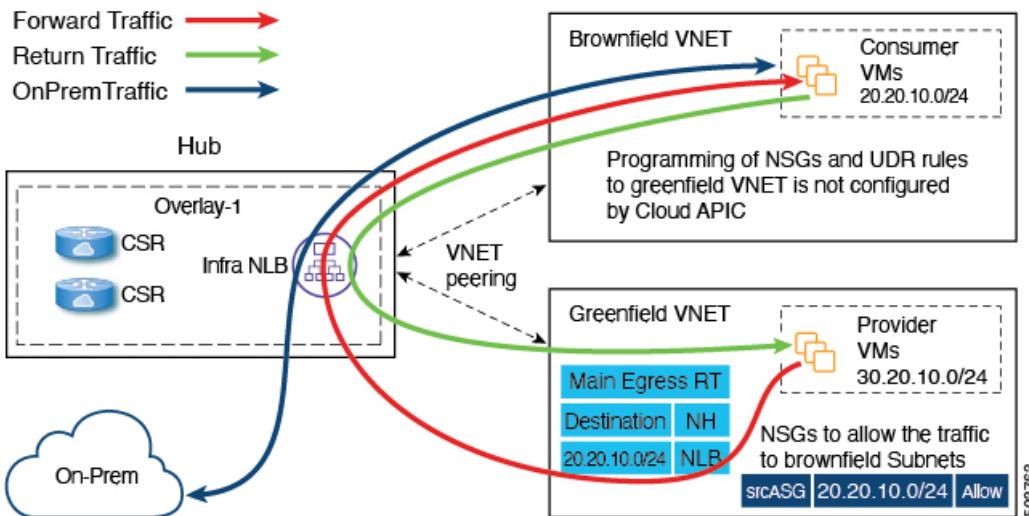
- **通常の EPG マッピング** : 通常、通常のクラウド EPG を定義する場合は、クラウド EPG を VRF に関連付けます。クラウドコンテキストプロファイルも、このプロセスの一部として VRF に関連付けられます。したがって、EPG が定義されると、EPG はすべてのクラウドコンテキストプロファイル (リソースグループ/VNet) の下の適切なセキュリティグループに変換され、Azure クラウドで ASG に変換されます。
- **ブラウフィールドクラウドコンテキストプロファイルに関連付けられている EPG** : アンマネージド (ブラウフィールド) クラウドコンテキストプロファイルが定義され、VRF に関連付けられている場合、およびこの同じ VRF に関連付けられている EPG を定義すると、この EPG は **ブラウフィールドクラウドコンテキストプロファイルと関連付けられた EPG** と呼ばれます。ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成する理由は、グリーンフィールド VNet 上のセキュリティやルーティングなど、Cisco Cloud APIC のすべてのネットワーキングおよびセキュリティ構造をオーケストレーションして、ブラウフィールド VNet への通信を可能にするためです。

たとえば、次の図の設定を考えます。



この設定では、ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成し、契約を作成する理由は、グリーンフィールド VNet 側のルーティングとセキュリティをプロビジョニングして、トラフィックがこの管理対象外 VNet に到達できるようにするためです。

この例の目標は、グリーンフィールド VNet のパケットフローが 20.20.10.0/24（ルール）にパケットを送受信できるようにし、このサブネット宛てのトラフィックをインフラ NLB に送信して、CSR をブラウンフィールド VNet にパケットを送信します。これらはすべてコントラクトを使用して実現されます。



Cisco Cloud APIC は、ブラウンフィールド VNet 側のルート エントリまたはセキュリティ グループルールをプログラムしません。代わりに、Cisco Cloud APIC はコントラクトに基づいてブラウンフィールド VNet サブネットとの間でパケットを送受信するようにグリーンフィールド VNet 側のみをプログラムします。Cisco Cloud APIC は、グリーンフィールド VNet とブラウンフィールド VNet の間でルーティングが発生するように CSR を適宜プログラムします。

そのため、ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられた EPG を作成し、他のグリーンフィールド VNet がブラウンフィールド VNet との間でトラフィックを送受信できるようにします。

ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられている EPG には、サブネットベースまたは正確な IP ベースのエンドポイントセレクタのみがあり、タグベースのエンドポイントセレクタはないことに注意してください。Cisco Cloud APIC はアンマネージド VNet に属するエンドポイントを認識しません。このため、Cisco Cloud APIC はアンマネージド（ブラウンフィールド）の VNet に属するタグベースのエンドポイントを認識しません。Cisco Cloud APIC がエンドポイントを検出できない場合、IP アドレスが見つからないため、グリーンフィールド VNet 側のセキュリティルールをプログラムして、ブラウンフィールド VNet 側との間でパケットを送受信することはできません。

ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられた EPG を作成し、その EPG でサブネットベースまたは特定の IP ベースのエンドポイント セレクタを定義する理由は次のとおりです。

- この EPG（ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられている）から別の EPG（グリーンフィールドクラウド コンテキスト プロファイルに関連付けられている）へのコントラクトを作成すると、グリーンフィールド VNet 側のルート テーブルにあるアンマネージド VNet CIDR へのルート エントリのプログラミングが実行されます。
- これにより、グリーンフィールド VNet 側のすべてのセキュリティ グループルールがプログラミングされ、EPG のエンドポイントセレクタで定義されたこれらのサブネットとの間でパケットを送受信できるようになります。
- EPG がタグベースのエンドポイントセレクタで設定され、ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられている場合は、この EPG を使用できないというエラーが発生します。

Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VRF]-addr-[redacted]/16/sgroup-[unit/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudScaleSetGroup	Tag-Based EpSelector custom:tag==devmgr is not applicable on the EPG unit/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile unit/n-Dev-Tenant/ctxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VRF]-addr-[redacted]/16/sgroup-[unit/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudEndPoint	Tag-Based EpSelector custom:tag==devmgr is not applicable on the EPG unit/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile unit/n-Dev-Tenant/ctxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00

## GUIを使用したブラウフィールドクラウドコンテキストプロファイルと関連付けられた EPG の作成

このトピックでは、ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成します。これを行う必要がある理由については、[EPG が VRF を通じたブラウフィールドクラウドコンテキストプロファイルと関連付けられている方法 \(19 ページ\)](#) を参照してください。

### 始める前に

次の手順を実行する前に、次の手順を実行する前に、必要なすべての設定が完了していることを確認します。

- [GUIを使用したアンマネージド \(ブラウフィールド\) クラウドコンテキストプロファイルの作成 \(12 ページ\)](#)
- [Azure での管理対象外 VNet からインフラ VNet へのピアリングの追加 \(17 ページ\)](#)

### 手順

**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** EPGに必要な一般設定を入力します。

表 2: [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"> <li>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> <li>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。  リリース 5.0(2) 以降では、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。</li> <li>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。</li> </ol>
アプリケーションプロファイル(Application Profile)	<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"> <li>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。</li> <li>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。</li> <li>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。</li> </ol>
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"> <li>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。</li> <li>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。</li> <li>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。</li> </ol>

**ステップ5** [エンドポイントセレクタ (Endpoint Selectors) ]フィールドで、Azure ブラウンフィールドサイトに対応するサブネットベースまたは特定の IP ベースのエンドポイントセレクタを定義します。

詳細については、[EPG が VRF を通じたブラウンフィールドクラウドコンテキストプロファイルと関連付けられている方法 \(19 ページ\)](#) を参照してください。

- a) [エンドポイントセレクタの追加 (Add Endpoint Selector) ]をクリックして、エンドポイントセレクタを追加します。
- b) [名前 (Name) ]フィールドに名前を入力します。
- c) [一致表現 (Match Expressions) ]領域に次の情報を入力します。
  - キー：IP を選択します。  
演算子: equals (==) を選択します。
  - 値：適切なサブネットベースまたは特定の IP ベースの IP エンドポイントを入力します。  
たとえば、これは、Cloud APICにインポートするブラウンフィールド VNet のリソースグループ内の仮想マシンのプライベート IP アドレスです。
- d) この一致表現でこれらの値を受け入れるには、チェックマークをクリックします。
- e) [追加 (Add) ]をクリックして、このエンドポイントセレクタを追加します。

**ステップ6** この EPG を保存するには、[保存 (Save) ]をクリックします。

---

## 次のタスク

[GUI を使用した EPG 間のコントラクトの作成 \(23 ページ\)](#) に示す手順を使用して、EPG 間のコントラクトを設定します。

## GUI を使用した EPG 間のコントラクトの作成

このトピックでは、ブラウンフィールドクラウドコンテキストプロファイルに関連付けられた EPG からグリーンフィールドクラウドコンテキストプロファイルに関連付けられた EPG に使用されるコントラクトを作成します。これは、グリーンフィールド VNet 側のルートテーブル内の管理対象外 VNet CIDR へのルートエントリのプログラミングを実行するために行われます。これはまた、グリーンフィールド VNet 側のすべてのセキュリティグループルールのプログラミングを処理して、EPG のエンドポイントセレクタで定義されているこれらのサブネットからパケットを送受信できるようにします。

### 始める前に

[GUI を使用したブラウンフィールドクラウドコンテキストプロファイルと関連付けられた EPG の作成 \(21 ページ\)](#) の手順に従って、ブラウンフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成します。

### 手順

---

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

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

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

**ステップ 3** [Intent (Intent)] メニューの [Application Management (Application Management)] リストで、[Create Contract (Create Contract)] をクリックします。[Create Contract (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 [Create Contract Dialog Box Fields (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 3: [Create Contract (Create Contract)] ダイアログボックスのフィールド

[Properties (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"> <li>[Select Tenant (Select Tenant)] をクリックします。[Select Tenant (Select Tenant)] ダイアログボックスが表示されます。</li> <li>[Select Tenant (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。</li> </ol> <p>(注) リリース 5.0(2) 以降、インフラテナントで契約を作成できません。共有サービスの使用例では、インフラテナントから契約をエクスポートしたり、インフラテナントに契約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"> <li>[Select (Select)] をクリックします。[Create Contract (Create Contract)] ダイアログボックスに戻ります。</li> </ol>
説明	契約の説明を入力してください。
[Settings (Settings)]	
スコープ	ドロップダウンメニューから [Global (Global)] を選択します。これにより、あるテナントの EPG が別のテナントの EPG と通信できるようになります。



[プロパティ (Properties) ]	説明
フィルタの追加	<p>フィルタを選択します。</p> <ol style="list-style-type: none"> <li>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> <li>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> <li>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。</li> </ol> <p>[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。</p>

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 メインの [コントラクトの作成 (Create Contract) ] ウィンドウで、[EPG 通信の設定 (Configure EPG Communication) ] をクリックします。

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

ステップ 7 [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。

ステップ 8 作成したコントラクトをコントラクトのリストから選択し、[選択 (Select) ] をクリックします。  
[EPG 通信設定 (EPG Communication Configuration) ] ウィンドウに戻ります。

ステップ 9 右側の [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。

ステップ 10 グリーンフィールドクラウド コンテキスト プロファイルに関連付けられている EPG を選択し、[選択 (Select) ] をクリックします。  
[EPG 通信設定 (EPG Communication Configuration) ] ウィンドウに戻ります。

ステップ 11 右側の [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。

ステップ 12 ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられている EPG を選択し、[選択 (Select) ] をクリックします。  
[EPG 通信設定 (EPG Communication Configuration) ] ウィンドウに戻ります。

ステップ 13 [保存 (Save) ] をクリックします。

## 次のタスク

Azure でのブラウフィールド VNet の残りの構成の完了 (26 ページ) の手順に従って、Azure の残りの設定タスクを完了します。

## REST API を使用してブラウフィールドクラウドコンテキスト プロファイルと関連付けられた EPG の作成

### 手順

ブラウフィールド VNet のクラウド EPG を作成します。

クラウド EPG を作成して、オンプレミス サイトまたは別のクラウド サイトがこのアンマネージドブラウフィールド VNet とトラフィックを送受信できるようにします。

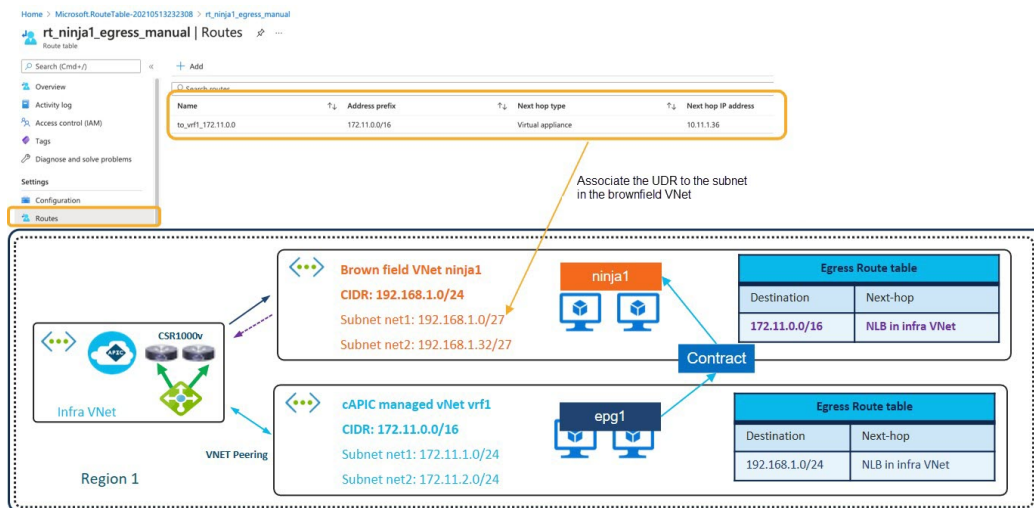
(注) これらのブラウフィールドクラウド EPG のエンドポイントセレクタは、タグベースではなく、サブネット ベースまたは IP ベースである必要があります。

```
<fvTenant name="UnManagedTenant1">
  <fvCtx name="VRF" />
  <cloudApp name="UnManagedapp" status="">
    <cloudEPg name="Epg" status="">
      <cloudRsCloudEPgCtx tnFvCtxName="VRF" />
      <cloudEPSelector name="1" subnet="20.0.0.0/24"/>
      <cloudEPSelector name="1" matchExpression="IP=='20.47.0.16/32'"/>
      <fvRsCons status="" tnVzBrCPName="http" />
      <fvRsCons tnVzBrCPName="contract_http_https_ssh" />
    </cloudEPg>
  </cloudApp>
</fvTenant>
```

## Azure でのブラウフィールド VNet の残りの構成の完了

次の手順では、Azure の残りの設定を完了します。

- 外部テーブルサブネットからパケットを送受信するように、ルートテーブルの UDR ルールをプログラムします。これらの外部サブネットは、ハブ VNet のいずれかのインフラ NLB のプライベート IP を指すネクストホップでプログラムする必要があります。



- セキュリティルールが外部サイトのエンドポイントまたはサブネットからパケットを送受信できるように、NSG または ASG ルールをプログラムします。

次のセクションでは、Azure でこれらの残りの設定を完了するための一般的な手順と設定例を示しますが、設定が異なる場合があることに注意してください。

## 始める前に

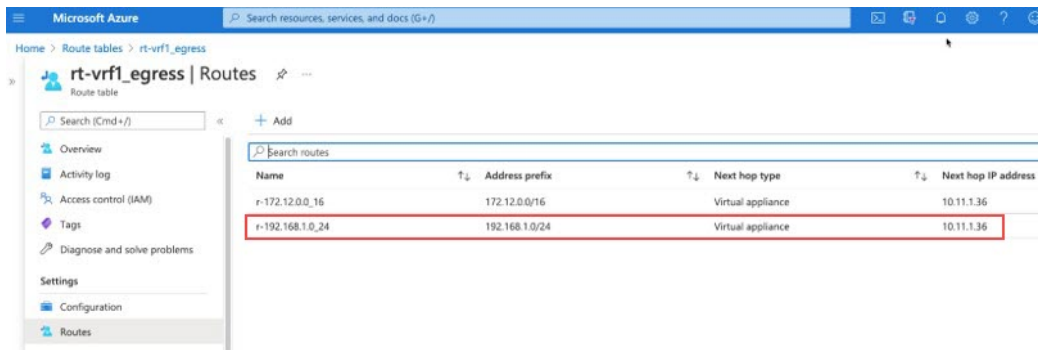
次の手順を実行する前に、次の手順を実行する前に、必要なすべての設定が完了していることを確認します。

- GUI を使用したアンマネージド (ブラウフィールド) クラウドコンテキストプロファイルの作成 (12 ページ)
- Azure での管理対象外 VNet からインフラ VNet へのピアリングの追加 (17 ページ)
- GUI を使用したブラウフィールドクラウドコンテキストプロファイルと関連付けられた EPG の作成 (21 ページ)
- GUI を使用した EPG 間のコントラクトの作成 (23 ページ)

## 手順

**ステップ 1** Azure ポータルで、Cisco Cloud APICによって管理される VRF からブラウフィールド VRF への UDR が Cisco Cloud APIC によって自動的に設定されたことを確認します。

- a) Azure 検索バーでルート テーブルを検索し、ルート テーブルの検索結果をクリックします。  
設定されたルート テーブルのリストが表示されます。
- b) Cisco Cloud APIC マネージド VRF に対してブラウフィールド VRF に対して設定されたルート テーブルをクリックし、そのルート テーブルで UDR が正しく設定されていることを確認します。



## ステップ2 ブラウンフィールド VRF から Cisco Cloud APIC マネージド VRF への UDR を作成します。

これは、ブラウンフィールド VNet の新しいルートテーブルになります。これは、前の手順で示した、Cisco Cloud APIC マネージド VRF からブラウンフィールド VRF に設定されたルートテーブルとは異なります。

- a) ルートテーブルのリストにレベルを戻し、**[+ New]** をクリックして新しいルートテーブルを作成します。

**[ロールの作成 (Create a Role)]** ウィンドウが表示されます。

- b) **[ルートテーブルの作成 (Create route table)]** ウィンドウに必要な情報を入力し、**[レビュー + 作成 (Review + create)]** をクリックします。

**[ルートテーブルの作成 (Create route table)]** ウィンドウに入力した情報が有効な場合は、**[検証合格 (Validation Passed)]** 画面が表示されます。

- c) **[作成 (Create)]** をクリックします。

展開が送信されると、展開が完了したことを示す画面が表示されます。

- d) **[リソースに移動 (Go to resource)]** をクリックします。

作成したルートテーブルのページが表示されます。

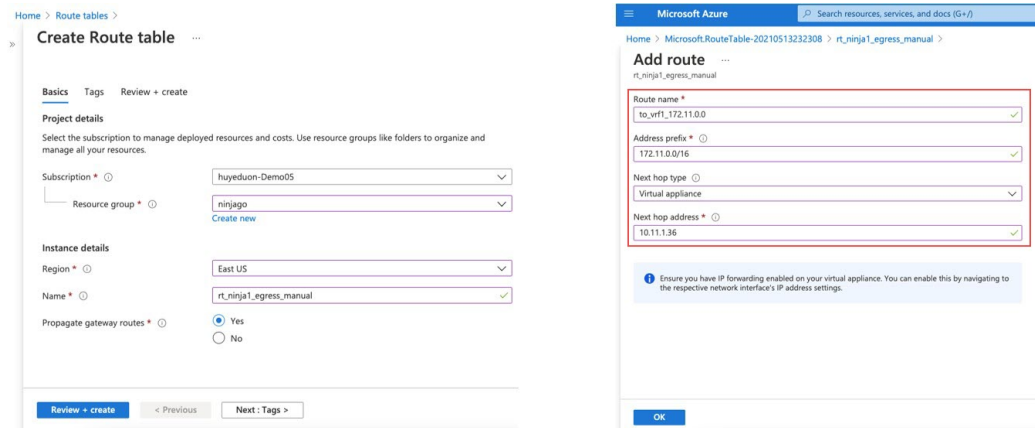
- e) 左側のペインで、**[ルート (Routes)]** をクリックし、**[+ 追加 (+ Add)]** をクリックします。

**[ルートの追加 (Add Router)]** ウィンドウが表示されます。

- f) **[ルートの追加 (Add route)]** ウィンドウに必要な情報を入力して、ブラウンフィールド VRF から Cisco Cloud APIC-マネージド VRF への UDR を作成し、**[OK]** をクリックします。

**[ルートの追加 (Add route)]** ページで、次の手順を実行します。

- **[アドレス プレフィックス (Address prefix)]** フィールドのエントリは、Cisco Cloud APIC-マネージド VNet CIDR です。
- **[次のホップアドレス (Next hop address)]** フィールドのエントリは、インフラ VNet で適切にプロビジョニングされた NLB の IP アドレスです。

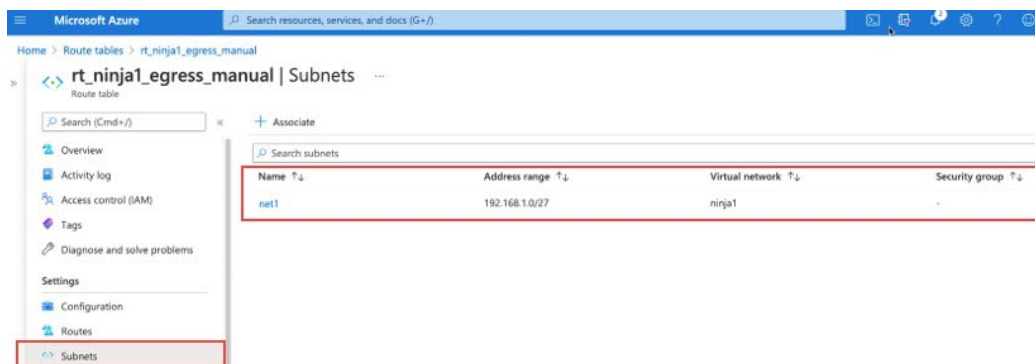


**ステップ 3** UDR をブラウフィールド VNet のサブネットに関連付けます。

- a) 左側のナビゲーションバーで [サブネット (Subnets)] をクリックし、 [+ 関連付け (+ Associate)] をクリックします。

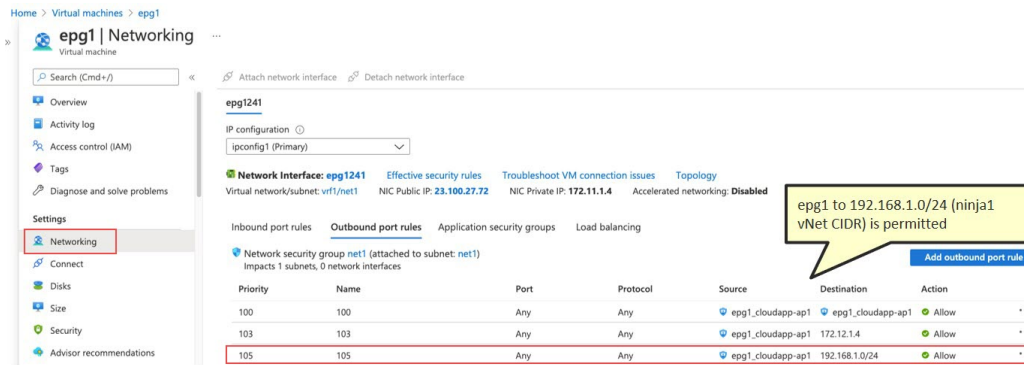
[サブネットの関連付け (Associate subnet)] ペインが右側に表示されます。

- b) ブラウフィールド VNet を見つけて選択します。  
その VNet のサブネットのリストが表示されます。
- c) UDR との関連付けに使用する適切なサブネットをブラウフィールド VNet で見つけ、そのサブネットを選択します。



**ステップ 4** Cisco Cloud APIC マネージド VNet に関連付けられたエンドポイントの NSG ルールを確認します。

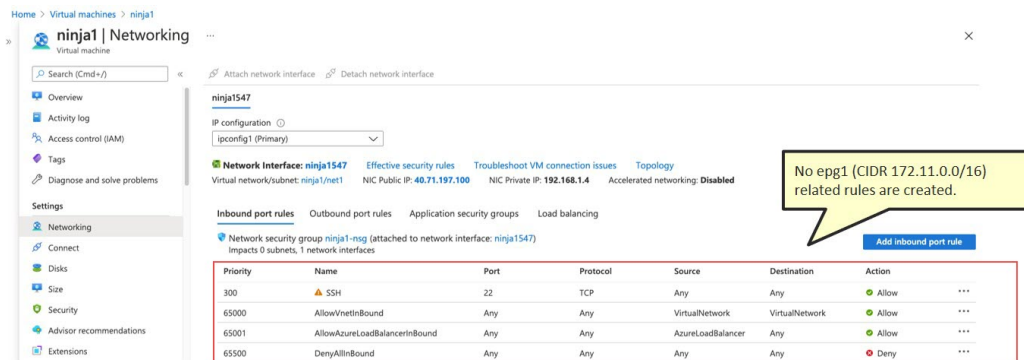
このルールは、Cisco Cloud APIC マネージド VNet の EPG とブラウフィールド VNet の EPG 間のコントラクトを適用した後に、Cisco Cloud APIC によって Cisco Cloud APIC マネージド VNet のエンドポイントに対して自動的に作成されます。



**ステップ 5** ブラウンフィールド エンドポイントの NSG ルールを手動で設定します。

ブラウンフィールド VNet の手動設定を実行する必要があります。使用方法は、設定する NSG ルールによって異なります。次に、ブラウンフィールド EPG の NSG ルールを手動で設定する方法の例を示します。この例では、グリーンフィールド (Cisco Cloud APIC マネージド) EPG epg1 (172.11.1.4) からブラウンフィールド EPG ninja1 (192.168.1.4) へのトラフィックが開始されます。

次の例では、グリーンフィールド (Cisco Cloud APIC マネージド) EPG epg1 に対してルールがまだ設定されていないことがわかります。



グリーンフィールド (Cisco Cloud APIC マネージド) EPG からのトラフィックを許可するインバウンドルールを設定します。

この例では、グリーンフィールド (Cisco Cloud APIC マネージド) EPG epg1 (172.11.1.4) からのトラフィックを許可するインバウンドルールを設定します。

- テーブルの上の領域で [インバウンド ポート ルール (Inbound port rules)] を選択した状態で、[インバウンド ポート ルールの追加 (Add inbound port rule)] をクリックします。
- [インバウンド セキュリティ ルールの追加 (Add inbound security rule)] ウィンドウに必要な情報を入力し、グリーンフィールド (Cisco Cloud APIC マネージド) EPG (この例では Cisco Cloud APIC マネージド) EPG epg1 からのトラフィックを許可します。

## Add inbound security rule

ninja1-nsg

Source ⓘ

IP Addresses

Source IP addresses/CIDR ranges \* ⓘ

172.11.0.0/16

Source port ranges \* ⓘ

\*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges \* ⓘ

\*

Protocol

Any

TCP

UDP

This example is to permit traffic from 172.11.0.0/16.

- c) グリーンフィールド（Cisco Cloud APICマネージド）EPGからのトラフィックを許可するインバウンドルールが正しく設定されていることを確認します。

次に、グリーンフィールドサブネットを許可した後のブラウンフィールドNSGルールの例を示します。

Manually add an inbound port rule.

Priority	Name	Port	Protocol	Source	Destination	Action	
300	SSH	22	TCP	Any	Any	Allow	...
310	allow_epg1	Any	Any	172.11.0.0/16	Any	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

### 次のタスク

設定の確認 (32 ページ) の手順を使用して設定を確認します。

## 設定の確認

### 手順

---

**ステップ 1** まだログインしていない場合は、Cloud APIC インフラ テナントの Azure アカウントにログインし、Azure 管理コンソールに移動します。

<https://portal.azure.com/#home>

**ステップ 2** グリーンフィールド VNet のリソース グループに移動します。

a) Azure 管理ポータルのメイン ページで、左側のナビゲーションバーの [リソース グループ] をクリックします。

リソース グループのリストが表示されます。

b) グリーンフィールド VNet のリソース グループを見つけ、そのリソース グループをクリックします。

そのリソース グループの概要情報が表示されます。

**ステップ 3** リストから適切なネットワーク セキュリティ グループを見つけ、そのネットワーク セキュリティ グループをクリックします。

そのネットワーク セキュリティ グループの概要ページが表示されます。

**ステップ 4** ブラウンフィールド サイトに到達するためのルールが **Inbound Security Rules** および **Outbound Security Rules** テーブルに表示されていることを確認します。

**ステップ 5** グリーンフィールド VNet のリソース グループのページに戻ります。

そのリソース グループの概要情報が表示されます。

**ステップ 6** リストからルート テーブルのエントリを見つけ、そのルート テーブル フィールドをクリックします。

そのルート テーブルの概要ページが表示されます。

**ステップ 7** ブラウンフィールド VNet の CIDR へのトラフィックを許可するようにルート エントリがルート テーブルにプログラムされていることを確認します。

---





**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



#### 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/>

## 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。