



## 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](#)
- [Cisco Cloud APIC GUI を使用したサービス EPG の作成](#)
- [REST API を使用したサービス EPG の作成](#)

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 \(1 ページ\)](#)

## 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 APIC 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>

- **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 APIC を介して作成)。たとえば、Azure Kubernetes Services (AKS) サービスは、Cisco Cloud APIC 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 APIC GUI を使用して設定を行います。

### 始める前に

- 1つのブラウザウィンドウで、Cisco Cloud APIC GUI にログインします。
- 別のブラウザウィンドウで、Cisco Cloud APIC インフラテナントの Azure アカウントにログインし、Azure 管理ポータルに移動します。

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

**ステップ 1** Cisco Cloud APIC 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: [Select Tenant >]
  - Description: [Text Input]
- Settings:**
  - Region: [Select Region >]
  - VRF: [Select VRF >]
  - CIDRs: [Text Input]
  - VNet Gateway Router:  Enabled
  - VNet Peering:  Enabled

Buttons: Cancel, Save

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 \(3 ページ\)](#)」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 APIC GUI を使用して設定を行います。

## 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（2 ページ）](#) の手順を完了してください。

- ステップ 1** Cisco Cloud APIC GUI で、**[Intent (Intent)]** アイコンをクリックします。  
**[Intent (Intent)]** メニューが表示されます。
- ステップ 2** **[Intent (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、**[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 APIC 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。

この時点で、**IP** はこのアクセスタイプのキーとして唯一のオプションです。

**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、**[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 \(5 ページ\)」](#) 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 APIC 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 \(3 ページ\)](#) 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)] 領域を見つけ、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 \(6 ページ\)](#)」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 portal を使用して構成を行います。



- (注) 次の手順では、Azure portal 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 APIC での Azure Kubernetes サービスの使用](#)」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 \(5 ページ\)](#) の手順を完了してください。

---

- ステップ 1** Azure portal で、Microsoft による Kubernetes サービス という用語を検索し、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、次の領域を構成します。

- 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。

Home > Kubernetes services > Create Kubernetes cluster

Basics Node pools **Authentication** Networking Integrations Tags Review + create

**Cluster infrastructure**  
The cluster infrastructure authentication specified is used by Azure Kubernetes Service to manage cloud resources attached to the cluster. This can be either a [service principal](#) or a [system-assigned managed identity](#).

Authentication method  
 Service principal  System-assigned managed identity

Service principal \*  [Configure service principal](#)

**Kubernetes authentication and authorization**  
Authentication and authorization are used by the Kubernetes cluster to control user access to the cluster as well as what the user may do once authenticated. [Learn more about Kubernetes authentication](#)

Role-based access control (RBAC)   Enabled  Disabled

AKS-managed Azure Active Directory   Enabled  Disabled

**Node pool OS disk encryption**  
By default, all disks in AKS are encrypted at rest with Microsoft-managed keys. For additional control over encryption, you can supply your own keys using a disk encryption set backed by an Azure Key Vault. The disk encryption set will be used to encrypt the OS disks for all node pools in the cluster. [Learn more](#)

Encryption type

[Review + create](#) < Previous Next: Networking > [Ok](#)

ステップ5 [認証 (Authentication)] タブで、次の領域を構成します。

- 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、次の領域を構成します。
  - 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。

- ロールベース 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：ネットワーク (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 \* ⓘ

Cluster subnet \* ⓘ

Kubernetes service address range \* ⓘ

Kubernetes DNS service IP address \* ⓘ

Docker Bridge address \* ⓘ

DNS name prefix \* ⓘ

---

Traffic routing

ステップ 7 [ ネットワーキング (Networking) ] タブで、次の領域を構成します。

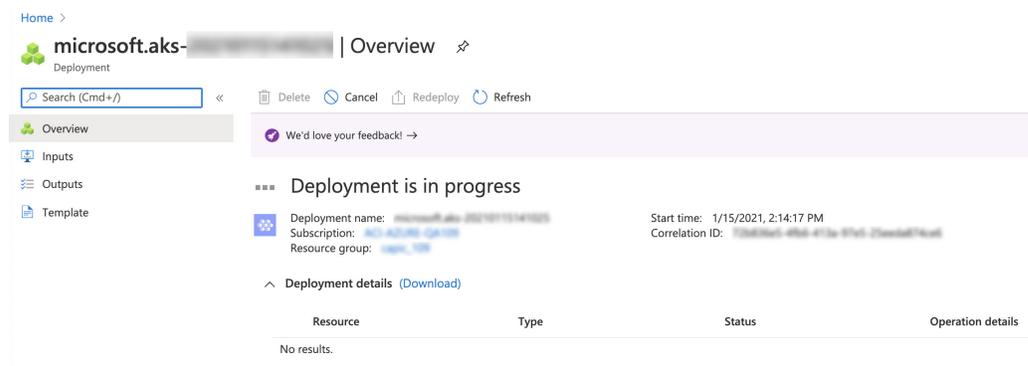
- ネットワーク構成 : [ **Azure CNI** ] を選択します。
- 仮想ネットワーク : 対応する仮想ネットワークを選択します。
- クラスタ サブネット : Cisco Cloud APIC で管理されるサブネットを選択します。
- **Kubernetes** サービスのアドレス範囲 : デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **Kubernetes DNS** サービスの IP アドレス : デフォルトの選択をそのままにするか、必要に応じてエントリを変更します。
- **Docker Bridge** アドレス : デフォルトの選択をそのままにするか、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 : Standard

- **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。

「展開が進行中」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 \(10 ページ\)](#)」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 \(6 ページ\)](#) の手順を完了してください。

- ステップ 1** Azure portal 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。

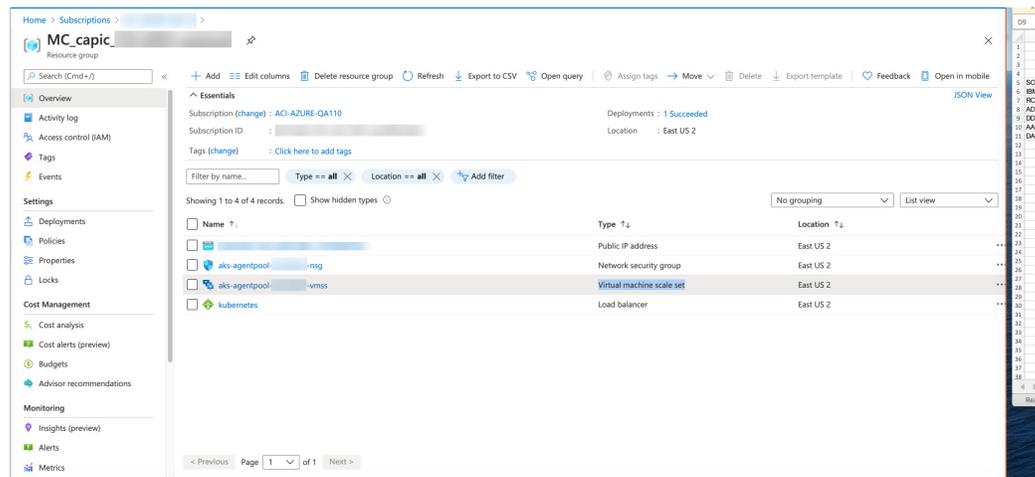
- `resourcegroupname` は、Kubernetes サービス専用で作成されたリソース グループの名前です (MC\_aks は、Azure によってデフォルトで使用されるリソース グループ名です)。
- `clustername` は、**ステップ 3 (7 ページ) の Kubernetes サービスの作成 (6 ページ)** で指定した Kubernetes クラスタ名です。
- `region` は、**ステップ 3 (7 ページ) の Kubernetes サービスの作成 (6 ページ)** で選択した地域です。

次に例を示します。

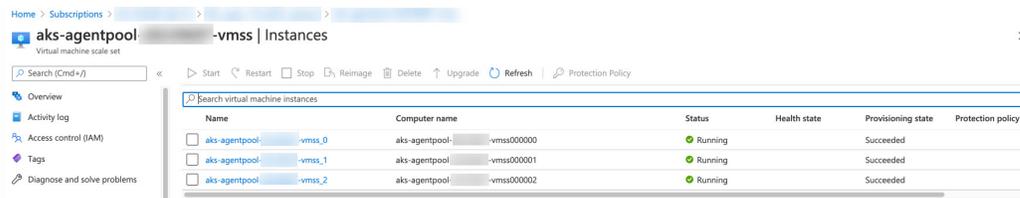
`MC_aks_acme-aks-cluster_centralus`

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。

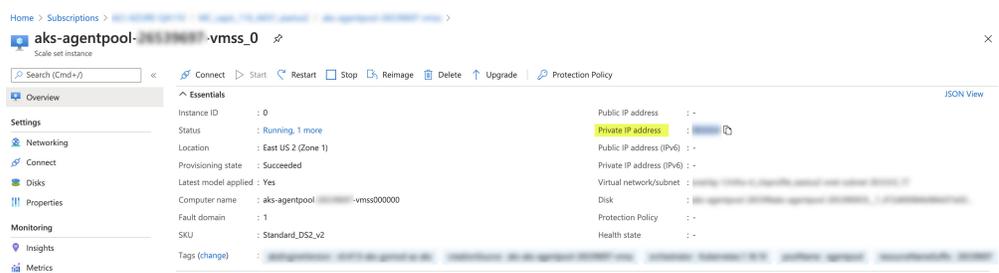


- ステップ 4** 左側のナビゲーションバーで [インスタンス (Instances)] をクリックして、この Kubernetes サービス リソース グループの仮想マシン インスタンスを表示します。



**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。

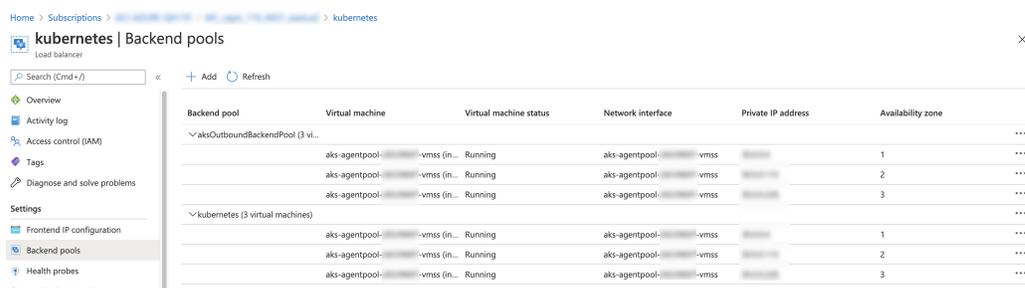
このウィンドウに表示される3つのインスタンスはすべて、**ステップ 7 (9 ページ)** の **Kubernetes サービスの作成 (6 ページ)** で選択したサブネットからの IP アドレスを持っている必要があります。



**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、タイプとしてロード バランサが表示されている 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** 契約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 portal 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] 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)] 領域が表示されるまで下にスクロールし、契約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 (outbound port rules)] 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 ポートの規則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)] 領域のエントリは、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 \(13 ページ\)](#)」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 \(10 ページ\)](#) 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 \(8 ページ\)](#) の [Kubernetes サービスの作成 \(6 ページ\)](#) 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 \(8 ページ\)](#) の [Kubernetes サービスの作成 \(6 ページ\)](#) 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 \(8 ページ\)](#) の [Kubernetes サービスの作成 \(6 ページ\)](#) 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 portal 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>

次に例を示します。

```
# 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 \(10 ページ\)](#) 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。

次に例を示します。

```
# 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/capic# 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 \(7 ページ\)](#) の [Kubernetes サービスの作成 \(6 ページ\)](#) に入力された Kubernetes クラスタの名前です。

次に例を示します。

```
root@hub-vm:/home/capic# az aks get-credentials --resource-group capic_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/capic# 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	KERNEL-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 (4 ページ) の AKS のクラウドサービス EPG の作成 (3 ページ)** で [プライベート (Private)] に設定されていたためです。[アクセスタイプ (Access Type)] が [パブリックおよびプライベート (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、新しいユーザーに管理者ロールを割り当てます。

- Azure portal で、インフラ リソース グループに戻ります。
- ページのレコード領域で、**Kubernetes サービス** 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、[ユーザー、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。