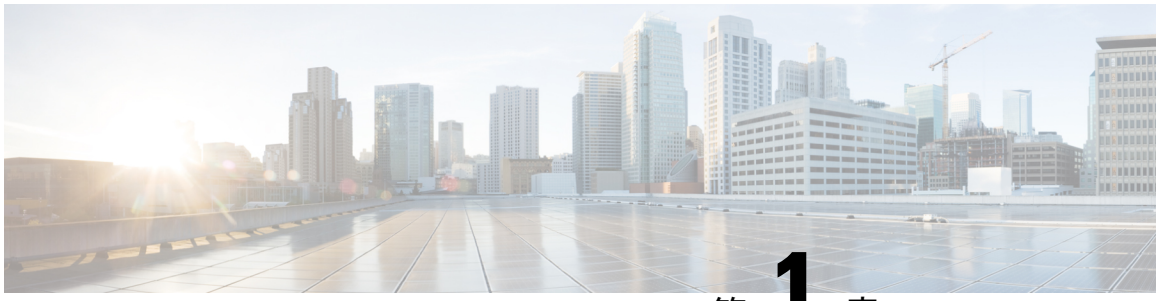
Cisco Cloud APIC Azure のインストール ガイド、リリース 5.2(x)

初版：2021 年 6 月 4 日

最終更新：2022 年 1 月 5 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/

目 次



第 1 章

新機能および変更された機能に関する情報

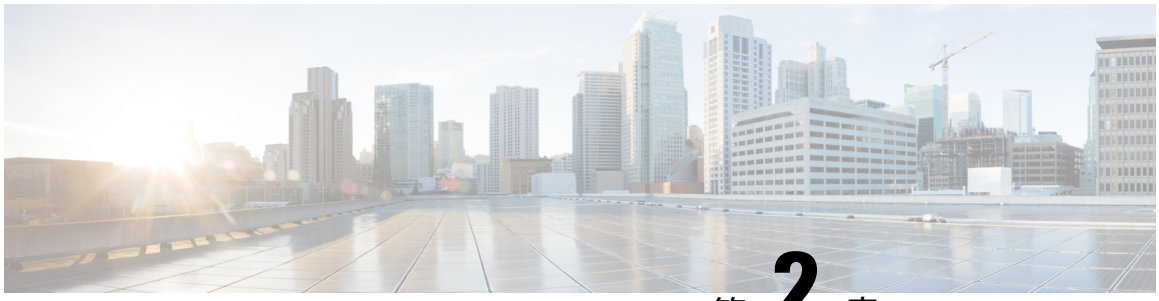
新機能および変更された機能に関する情報

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

表 *1 : Cisco APIC* リリース *5.2(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
アップグレードとは無関係のCSRアップグレードのトリガーのサポートCisco Cloud APIC	リリース5.2（1）より前は、のアップグレードをトリガーするたびにCSRが自動的にアップグレードされました。Cisco Cloud APICリリース5.2（1）以降では、アップグレードに関係なく、CSRのアップグレードをトリガーできます。Cisco Cloud APIC	クラウド サービス ルータのアップグレードのトリガー（115 ページ）

新機能および変更された機能に関する情報



第 2 章

概要

Cisco ACI ファブリックをパブリック クラウドに拡張する

Cisco Application Centric Infrastructure プライベートクラウドを所有している（ACI）顧客は、パブリッククラウドでワークロードの一部を実行することがあります。ただし、ワークロードをパブリッククラウドに移行するには、別のインターフェイスで作業し、接続を設定してセキュリティポリシーを定義するさまざまな方法を学習する必要があります。これらの課題に対処すると、運用コストが増加し、一貫性が失われる可能性があります。

（APIC）リリース4.1（1）以降では、を使用してマルチサイトファブリックをAmazon Web Services（AWS）パブリッククラウドに拡張できます。Cisco Application Policy Infrastructure ControllerCisco ACICisco Cloud APICCisco ACI

APICリリース4.2（1）以降では、を使用して、マルチサイトファブリックをMicrosoft Azureパブリッククラウドに拡張することもできます。Cisco ACICisco Cloud APICCisco ACI

Cisco Cloud APICとは

Cisco Cloud APICは、クラウドベースの仮想マシン（VM）に導入できるのソフトウェアコンポーネントです。Cisco APICCisco Cloud APICは次の機能を提供します。

- Amazon AWSまたはMicrosoft Azureパブリッククラウドと対話するための既存のインターフェイスと同様のインターフェイスを提供します。Cisco APIC
- クラウド接続の導入と設定を自動化します。

- クラウド ルーターのコントロール プレーンを設定します。
- オンプレミス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ポリシーに変換します。Cisco ACI
- エンドポイントを検出します。

Cisco ACI Extension to the Public Cloudのメリット

パブリッククラウドへの拡張の重要な部分です。Cisco Cloud APICCisco ACICisco Cloud APIC は、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に導入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。

Cisco ACI また、パブリッククラウドへの拡張により、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が提供され、プロビジョニングとモニタリングが容易になります。また、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、またはクラウドサイト間でポリシーを管理、モニタリング、およびトラブルシューティングするための単一のポイントを提供します。

Azureガバメントサポート

リリース4.2（3）以降では、オンプレミスからクラウドへの接続（ハイブリッドクラウドおよびハイブリッドマルチクラウド）、クラウドサイトからクラウドへの接続（マルチクラウド）、およびシングルクラウドの設定について、Azure Governmentをサポートしています。（クラウドファースト）。Cisco Cloud APIC

Cisco Cloud APIC 次のAzure政府リージョンをサポートします。

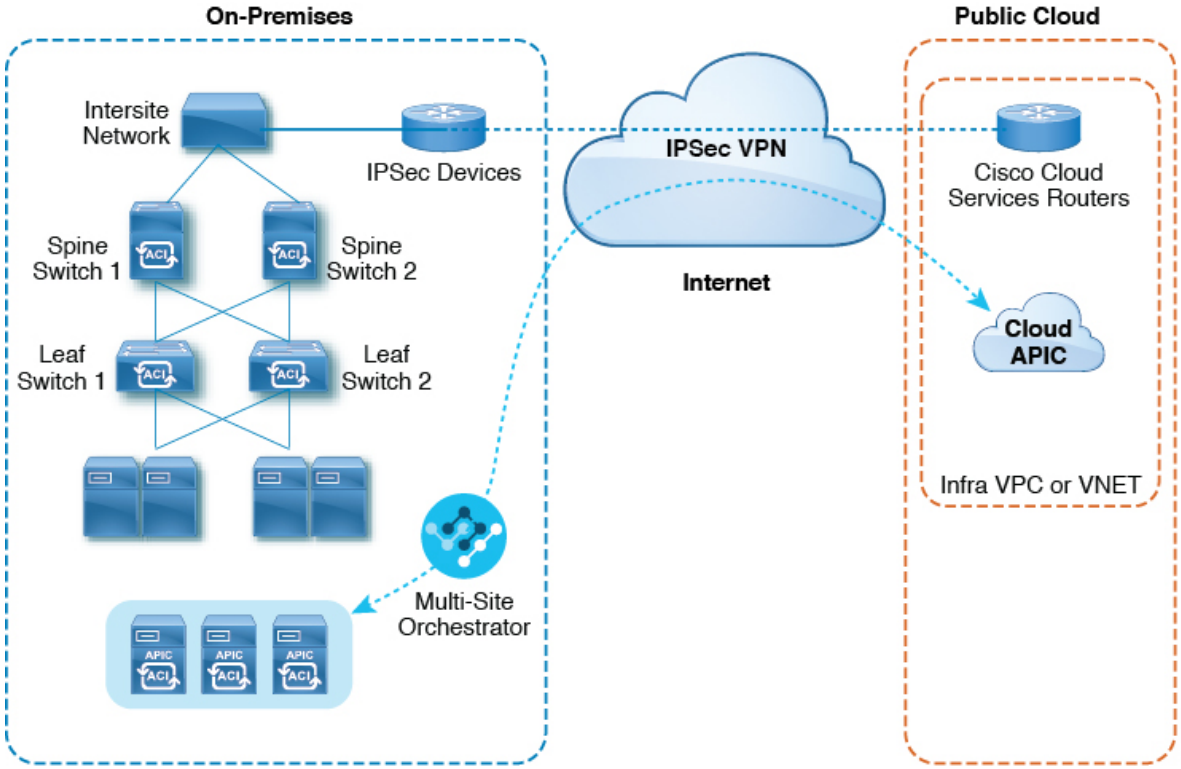
- US DoD セントラル
- US DoD 東部
- 米国政府、アリゾナ州
- 米国政府、テキサス州
- 米国政府、バージニア州

Cisco ACI ファブリックをパブリック クラウドに拡張するためのコンポーネント

（ACI）マルチサイトファブリックをMicrosoft Azureパブリッククラウドに拡張するには、それぞれに固有のロールを持つ複数のコンポーネントが必要です。Cisco Application Centric Infrastructure

次の図はアーキテクチャの内容を示していますCisco Cloud APIC。

図 *1 : Cisco Cloud APIC* のアーキテクチャ



オンプレミスデータセンターコンポーネント

Cisco ACI ファブリックおよび Cisco APIC

では、アプリケーション要件でネットワークを定義できます。Cisco ACIこのアーキテクチャにより、アプリケーションの展開ライフサイクル全体が簡素化、最適化、および促進されます。（APIC）の主要コンポーネントです。Cisco Application Policy Infrastructure ControllerCisco ACIこれによりアプリケーションはネットワーク、コンピューティング、およびストレージ機能を含む、安全な共有の高パフォーマンス リソース プールと直接接続することができます。

Cisco ACI マルチサイト および Cisco ACI マルチサイト オーケストレータ

Cisco ACI マルチサイトは、プログラムを利用してアプリケーションがネットワーク要件を定義することを可能にするアーキテクチャです。このアーキテクチャにより、アプリケーションの展開が簡素化・最適化され、そして促進されます。Cisco Cloud APICを使用してファブリックをパブリッククラウドに拡張するには、Multi-Siteをインストールする必要があります。Cisco ACI

詳細については、Cisco.comのCisco ACI Multi-Siteのマニュアルおよびこのガイドの Multi-Siteの設定情報を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html#ACI_Multi-SiteCisco ACI

Multi-Site Orchestrator（MSO）は、複数のファブリック（サイト）で複数の（APIC）のインスタンスを管理します。Cisco ACICisco Application Policy Infrastructure Controller

ファブリックをパブリッククラウドに拡張すると、Multi-Site Orchestratorは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接続を作成します。Cisco ACICisco ACIマルチサイトを使用して、オンプレミスのデータセンターとパブリッククラウド全体にテナントを作成します。Cisco ACI

（注） オンプレミスファブリックを設定する必要があります。ファブリック外部接続ポリシーを作成し、マルチサイトに必要なオーバーレイTEPおよびその他の情報を定義します。Cisco ACIまた、マルチサイトアーキテクチャにオンプレミスファブリックを追加する必要があります。Cisco ACIポリシーについては、『*Cisco ACI* マルチサイト構成ガイド』を参照してください。

詳細については、Cisco.com の Cisco ACI Multi-Site のマニュアルおよびこのガイドの Multi-Site の設定情報を参照してください。Cisco ACI

IP セキュリティ（IPSec）ルータ

Microsoft Azureのオンプレミスサイトとクラウドサイトの間でIPsec接続を確立するには、インターネットプロトコルセキュリティ（IPsec）対応のルータが必要です。

Azureパブリッククラウドコンポーネント

Cisco クラウド APIC

Cisco Cloud APICは次のアクションを実行します。

- パブリッククラウド上のサイトを定義し、クラウドインフラ仮想ネットワーク（VNET）をプロビジョニングし、すべてのリージョンでCisco Cloud Services Router（CSR）を管理します。
- パブリッククラウドでポリシーモデルをレンダリングし、クラウドの健全性を管理します。Cisco ACI

詳細については、『Cisco Cloud APIC Release Notes』を参照してください。

シスコ クラウド サービス ルータ

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

Microsoft Azure パブリック クラウド

Microsoft Azureは、コンピューティング、ストレージ、ネットワーク、データベースなどのオンデマンドサービスを提供するクラウドベースのプラットフォームです。Azureのサブスクライバは、ワークロードを実行できる仮想コンピュータにインターネット経由でアクセスできます。

詳細については、Microsoft Azure の Web サイトのマニュアルを参照してください。

オンプレミスデータセンターとパブリッククラウド間の接続

IPsec VPN

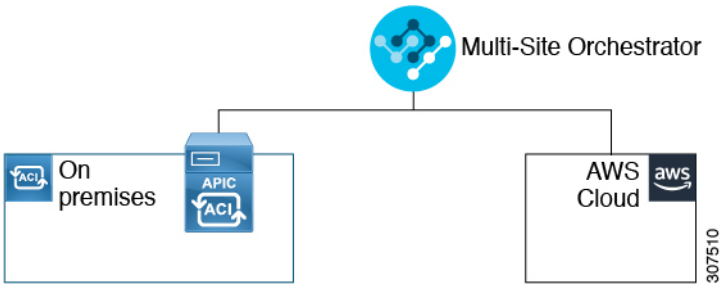
パブリックにルーティング可能なIPアドレスを含み、Microsoft Azure接続に十分な帯域幅を持つ、IPsecルータからのVPNとのインターネット接続が必要です。

管理接続

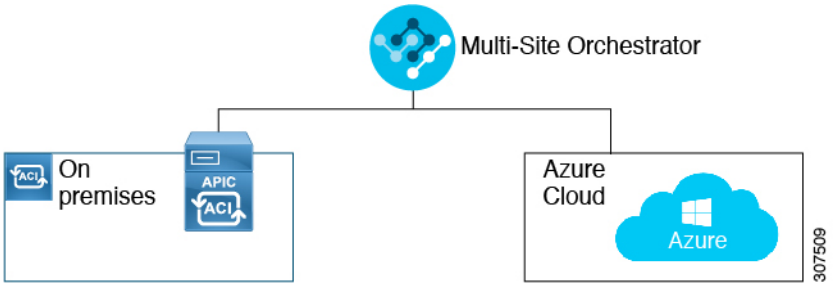
オンプレミスのデータセンターのMulti-Site OrchestratorとMicrosoft Azureパブリッククラウドの間に管理接続が必要です。Cisco Cloud APIC

APIC リリース 4.2(1) での変更点

APICリリース4.1(1)の最初のリリースの一部として、オンプレミスからクラウドへの接続、またはシスコを使用してオンプレミスを拡張できる初期リリースのサポートが提供されました。サイトを Amazon AWS パブリック クラウドに接続します。Cisco Cloud APICACI マルチサイト オーケストレータCisco ACI



APIC リリース4.2(1) 以降、シスコを使用してオンプレミス サイトを Microsoft Azure パブリック クラウドに拡張できるようになりました。ACI マルチサイト オーケストレータCisco ACI

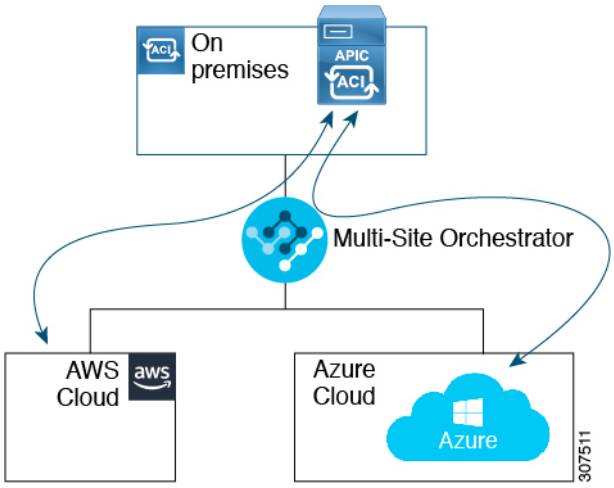


このリリースで利用可能な拡張機能により、シスコを使用して次のコンポーネント間の接続を確立することもできます。ACI マルチサイト オーケストレータ

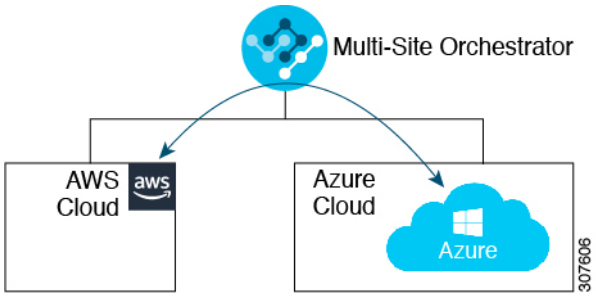
- オンプレミスからクラウドへの接続：
  - 次のパブリック クラウド サイトの接続：
    - オンプレミスおよび Amazon AWS パブリック クラウド サイト（以前は APIC リリース4.1 [1]で利用可能）Cisco ACI

- オンプレミスおよび Microsoft Azure パブリック クラウド サイトCisco ACI

- オンプレミスからシングル クラウド サイトへの接続（ハイブリッド クラウド）
- オンプレミスから複数のクラウド サイトへの接続（ハイブリッド マルチクラウド）



- クラウド サイト間接続（マルチクラウド）：
  - Amazon AWS パブリック クラウド サイトと Microsoft Azure パブリック クラウド サイト間
  - Amazon AWS パブリック クラウド サイト間（Amazon AWS パブリック クラウド サイトから Amazon AWS パブリック クラウド サイト）
  - Microsoft Azure パブリック クラウド サイト間（Microsoft Azure パブリック クラウド サイトから Microsoft Azure パブリック クラウド サイト）



さらに、シングル クラウド設定（Cloud First）もサポートされます。

ポリシーの用語

Cisco Cloud APIC の主要な機能は、パブリック クラウドのネイティブ構成要素への（ACI）ポリシーの変換です。Cisco Application Centric Infrastructure

Cisco ACI と Microsoft Azure 間のポリシー マッピング

次の表に、Microsoft Azure のポリシー用語と同等の用語を示します。Cisco ACI

Cisco ACI	Azure
テナント（リージョン、VRF）	リソース グループ
Virtual Routing and Forwarding（VRF）	仮想ネットワーク
BD サブネット	Subnet
契約、フィルタ	アウトバウンドルール、インバウンドルール
EP から EPG へのマッピング	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 セキュリティ グループ（NSG）
エンドポイント	VM インスタンスのネットワーク アダプタ

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 とコンポーネントのマッピングCloud APIC （10 ページ）
- Azureサブスクリプションについて （10 ページ）
- テナントとアイデンティティについて （10 ページ）

Azure とコンポーネントのマッピングCloud APIC

Cloud APIC では、各 Azure リソース グループは 1 つのテナントにマッピングされ、1 つのテナントが複数の Azure リソースグループを持つことができます。Cloud APICCloud APIC

特定のコンポーネント間の関係は次のとおりです。Cloud APIC

テナントVRFリージョン ＞ ＞

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。Cloud APIC

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IDを複数のACIファブリック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。ACI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およびで使用できるさまざまなタイプのテナントとIDを次に示します。Cloud APIC

（注） リリース5.2（1）より前のリリースでは、管理対象アイデンティティのみがインフラテナントのアクセスタイプとしてサポートされ、管理対象アイデンティティとサービスプリンシパルの両方がユーザテナントのアクセスタイプとしてサポートされていました。

リリース5.2（1）以降、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るようになりました。

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

管理対象アイデンティティを使用してでテナントを設定する場合は、Azureポータルとで次の設定を行います。Cloud APICCloud APIC

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。

仮想マシンのAzureにロール割り当てを追加する手順については、を参照してください。仮想マシンへのロール割り当ての追加 （37 ページ）

2. では、でテナントを設定するときに[Create Your Own Managed Identity]オプションを選択します。Cloud APICCloud APICこのオプションは、の手順を使用してGUIで設定します。Cloud APICテナントの設定 （71 ページ）

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を使用してでテナントを設定する場合は、Azureポータルとで次の設定を行います。Cloud APICCloud APIC

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。

   アプリにAzureのロール割り当てを追加する手順については、を参照してください。アプリへのロール割り当ての追加 （39 ページ）

2. では、テナントを設定するときに **[サービスプリンシパル（Service Principal）]** オプションを選択します。Cloud APICCloud APIC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。このオプションは、Cloud APIC の手順を使用して テナントの設定 （71 ページ） GUI で設定します。

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。

でテナントを共有テナントとして設定する場合は、Azureポータルとで次の設定を行います。Cloud APICCloud APIC

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. では、テナントを設定するときに[共有（Shared）]オプションを選択します。Cloud APICCloud APICこのオプションは、Cloud APIC の手順を使用して テナントの設定 （71 ページ） GUI で設定します。

Cisco Cloud APIC ライセンス

ここでは、使用するライセンス要件（APIC）を示します。Cisco Cloud Application Policy Infrastructure Controller

Cisco Cloud APIC およびシスコ クラウド サービス ルータ

シスコが管理する各仮想マシン（VM）インスタンスごとのシスコライセンス。Cisco Cloud APICバイナリイメージはMicrosoft Azureポータルで利用可能で、Bring Your Own License（BYOL）モデルをサポートしています。Cisco Cloud APIC

Essentials Cloud 階層には、パブリック クラウド上の単一のポリシー ドメイン用または単一の Cisco Cloud APIC インスタンス用のライセンスが含まれています。の複数のインスタンスを展開する場合は、管理するVMインスタンスごとにAdvantage Cloudライセンスを購入します。Cisco Cloud APICCisco Cloud APIC

ライセンスの詳細は、『*Cisco Application Centric Infrastructure Ordering Guide*』を参照してください。

1 つ以上の Cisco Cloud APIC ライセンスを取得することに加えて、シスコ スマート ソフトウェア ライセンシングに Cisco Cloud APIC とシスコ クラウド サービス ルータ（CSR）を登録する必要があります。

シスコのスマート ライセンスは、複数のシスコ製品間でソフトウェア ライセンスを管理する統合ライセンス管理システムです。スマートソフトウェアライセンシングの詳細については、https：//www.cisco.com/go/smartlicensingを参照してください。

Cisco Cloud APIC および CSR を登録するためのステップは以下のとおりです。

1. 製品がインターネットにアクセスできること、またはネットワーク上にインストールされた Smart Software Manager サテライトにアクセスできることを確認してください。
2. スマートアカウントにログインします。
    1. Smart Software Manager : https://software.cisco.com/

2. Smart Software Manager サテライト:
https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

3. この製品インスタンスで使用するライセンスが含まれている仮想アカウントに移動します。

4. 製品インスタンスの登録トークン（これによりスマートアカウントを識別）を生成し、そのトークンをコピーするか、または保存します。

（注） セットアップウィザードの[Throughput of the routers]フィールドで選択した設定に基づいて、適切なサイズのCSRを展開します。Cisco Cloud APICCisco Cloud APIC

（注） 将来のある時点で展開からCSRを削除すると（GUIまたはクラウドコンソールまたはポータルを使用してCSRを削除することにより）、CSRスマートライセンスサーバがそのCSRから切断されます。Cisco Cloud APIC削除されたCSRインスタンスは90日間は失効としてマークされ、その期間は他の新しいCSRによってライセンスを再利用できません。

この状況を回避するには、次の手順に従って、新しいライセンスを古いライセンスに再ホストします。

オンプレミスのCisco ACIライセンス

1つ以上のクラウドサイトを持つ単一のオンプレミスサイトがある場合は、Essential、Advantage、Premierのいずれかのライセンスレベルでオンプレミスファブリックを実行できます。Cisco ACICisco ACI

Microsoft Azure

Microsoft Azure Marketplaceから適切なCSRライセンスに登録する必要があります。

Microsoft Azure Marketplaceからサブスクライブするには、の手順に従ってください。Cisco Cloud Services Router への登録 （23 ページ）

Cisco Cloud APIC 関連のマニュアル

Cisco Cloud Application Policy Infrastructure Controller（APIC）、Cisco ACI マルチサイト、および Microsoft Azure に関する情報は、さまざまなリソースから入手できます。

シスコ マニュアル

Cisco.com でシスコ製品のマニュアルを参照してください。

- 『*Cisco Cloud Application Policy Infrastructure Controller* のリリース ノート、リリース *4.2*』

他の Cisco Cloud APIC ドキュメントのリストが含まれます。

- Cisco ACI および Cisco APIC のマニュアル

  ビデオ、リリース ノート、基礎、インストール、設定、およびユーザ ガイドが含まれています。

- Cisco ACI マルチサイトのマニュアル

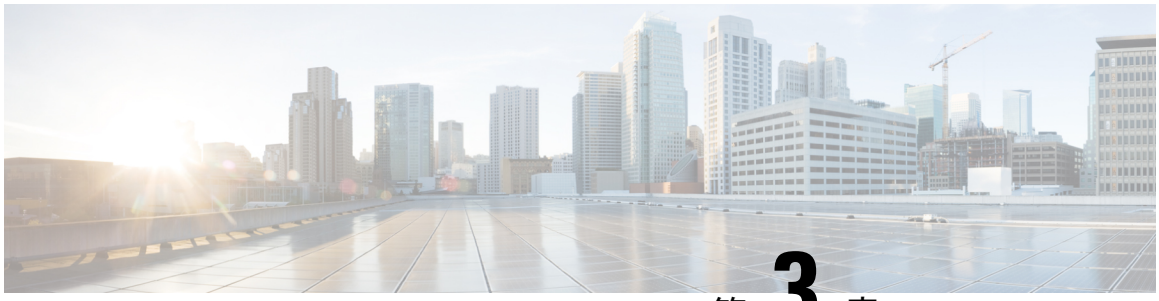
  ビデオ、リリース ノート、インストール、設定、およびユーザ ガイドが含まれています。

- Cisco Cloud Services Router のマニュアル

  リリース ノート、コマンド リファレンス、データ シート、インストール、アップグレード、および設定ガイドが含まれています。

Microsoft Azure のマニュアル

Microsoft Azure Web サイトで、ユーザ ガイド、FAQ、ケース スタディ、ホワイト ペーパーなどのドキュメントを検索できます。



第 3 章

Cisco Cloud APICのインストールの準備

Cisco ACI ファブリックをパブリック クラウドに拡張するための要件

Cisco Application Centric Infrastructure (ACI) をパブリック クラウドに拡張するには、その前に、Cisco ACI オンプレミスのデータセンターと Microsoft Azure の展開要件を満たす必要があります。

オンプレミス データ センターの要件

このセクションでは、（ACI）ファブリックをパブリッククラウドに拡張するためのオンプレミスデータセンター要件を示します。Cisco Application Centric Infrastructure

- ファブリックに次のコンポーネントが取り付けられていることを確認します。Cisco ACI
  - Cisco Nexus 9000シリーズACIモードスイッチソフトウェアリリース14.1以降を実行している、少なくとも2つのCisco Nexus EXまたはFXスパインスイッチ、またはNexus 9332Cおよび9364Cスパインスイッチ。
  - Cisco Nexus 9000シリーズACIモードスイッチソフトウェアリリース14.1以降を実行している少なくとも2台のCisco Nexus pre-EX、EX、またはFXリーフスイッチ。
  - リリース4.1以降およびCisco ACI Multi-Site Orchestrator（MSO）リリース2.2（x）以降を実行している少なくとも1つのオンプレミス（APIC）。Cisco Application Policy Infrastructure Controller
- 基本設定で展開されたCisco ACI Multi-Site Orchestrator 2.2（x）。
- インターネットプロトコルセキュリティ（IPsec）を終了できるネットワークデバイス。

- オンプレミスとクラウドサイト間のテナントトラフィックに十分な帯域幅があることを確認する必要があります。
- Cisco SMART LicensingアカウントとLeaf Advantageライセンス。Cisco ACI

  オンプレミスサイト上のすべてのリーフには、リーフライセンスが必要です。Cisco ACI
- ファブリックに接続されているワークロード。Cisco ACI
- ファブリック（スパイン）とIPセキュリティ（IPsec）終端デバイス間で設定されるサイト間ネットワーク（ISN）。Cisco ACI

  ISNの作成については、『Cisco APIC Layer 3 Networking Configuration Guide、Release 4.0（1）』の「Multipod」の章を参照してください。
- オンプレミス展開とAzure展開の間にファイアウォールを展開する場合は、特定のファイアウォールポートを許可する必要があります。これには、Cisco Cloud APICのHTTPSアクセス、各Azure CSRのIPsecポート、およびAzure CSRリモート管理のSSH接続が含まれます。

  これらのファイアウォールポートについては、このガイドで詳しく説明します。Cloud APIC 通信ポート （19 ページ）

Azure パブリック クラウドの要件

ここでは、（ACI）ファブリックをパブリッククラウドに拡張するためのMicrosoft Azure要件を示します。Cisco Application Centric Infrastructure

Azureアカウント

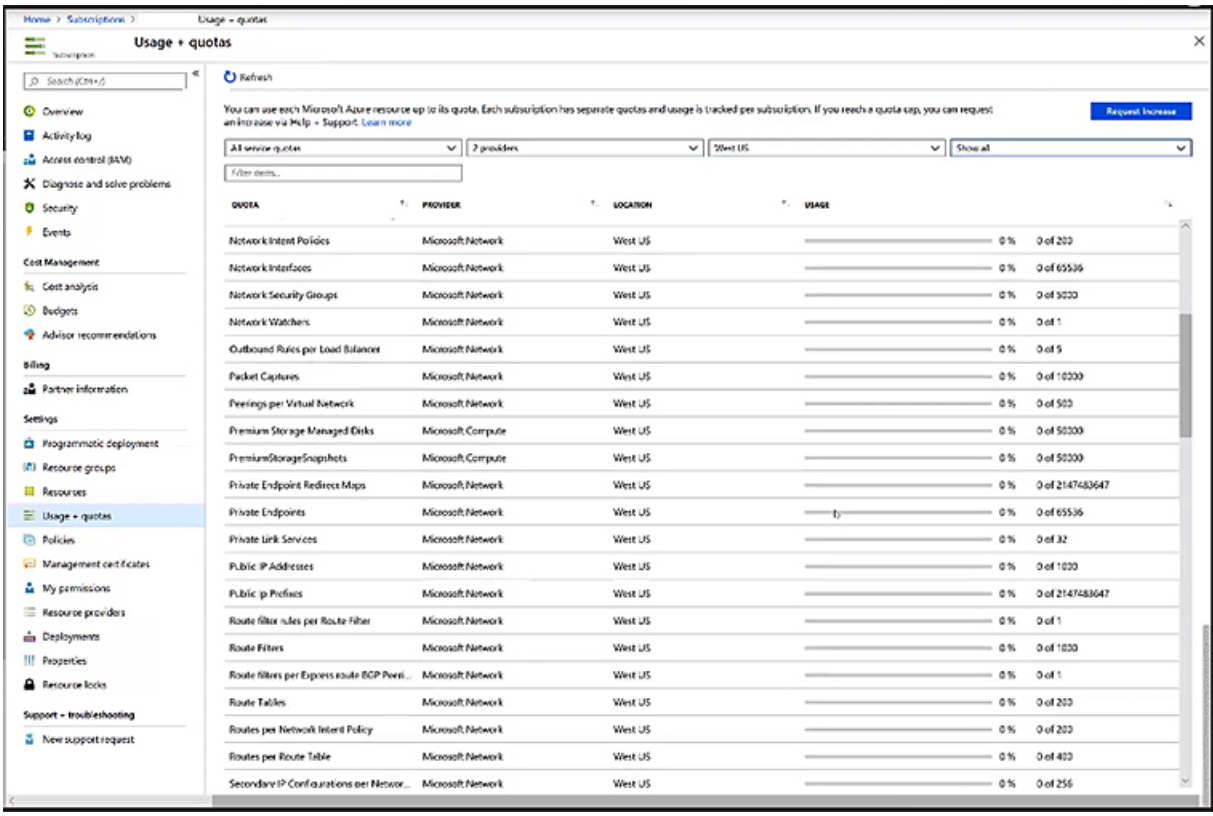
少なくとも1つのAzureアカウントが必要です。次に、Azureアカウントでサブスクリプションを作成します。このサブスクリプションでは、同じサブスクリプション内に複数のテナントを展開することも、テナントに複数のサブスクリプションを作成することもできます。

Azureクォータの制限

適切なAzureクォータ制限があることを確認します。

1. [サブスクリプション（Subscriptions）]：[設定（Settings）]：[使用量+クォータ（Usage + クォータ）]に移動します。
2. [Select a provider]フィールドで、次を選択します。
   - Microsoft.Compute
   - Microsoft.Network
3. **[ロケーションの選択（Select a location）]** フィールドで、地域（たとえば、**米国西部**）を選択します。
4. 最後のフィールドで、**[Show only items with usage]** を **[Show all]** に変更します。

次のような出力が表示されます。この出力を使用して、適切なAzureクォータ制限があることを確認します。



Azure のリソース

Azure 展開の一部として次のリソースが必要です。

- Azure Marketplaceオファーへのアクセス。Azure MarketplaceでCisco Cloud APICオファーを探し、そのページの手順に従います。

  https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-aci-cloud-apic

- 次のクラウドリソース要件（1つのテナント、1つのVRFを想定）。

リソース名	Resource Type	最小要件
仮想ネットワーク	ネットワーク	2
スタティック パブリック IP アドレス	ネットワーク	9
パブリック IP アドレスの合計（スタティック パブリック IP アドレスとダイナミック パブリック IP アドレス）	ネットワーク	12

リソース名	Resource Type	最小要件
ネットワーク セキュリティ グループ	ネットワーク	5
アプリケーションのセキュリティ グループ	ネットワーク	5
アプリケーションゲートウェイ	ネットワーク	1
仮想マシン	コンピューティング	8
標準 DSv2 ファミリ vCPU	コンピューティング	16
標準 DSv3 ファミリ vCPU	コンピューティング	8
Premium Storage Managed Disks	コンピューティング	4

Azureリソースプロバイダー

クラウドAPICで使用するすべてのサブスクリプションについて、後で追加する可能性のあるサブスクリプションがあるテナントを含めて、次のリソースプロバイダーを登録する必要があります。

- `microsoft.insights`
- `Microsoft.EventHub`
- `Microsoft.Logic`
- `Microsoft.ServiceBus`

詳細については、「必要なリソースプロバイダーの登録（25ページ）」を参照してください。

Cisco Cloud Services Router（CSR）

セットアップ時に定義した帯域幅要件に応じて、適切なサイズでCSRを展開します。Cisco Cloud APIC

ルータのスループットの値によって、展開するCSRインスタンスのサイズが決まります。スループットの値を大きくすると、より大きなVMが展開されます。CSRライセンスは、Cisco Cloud APICセットアッププロセスの一部として設定したスループット設定に基づきます。コンプライアンスのために、Smartアカウントに同等以上のライセンスとAXフィーチャセットが必要です。

次の表に、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。

CSR スループット	Azure VMサイズ	Premium Storage	Accelerated Networking
最大1 GB	DS3_v2	対応	点灯

CSR スループット	Azure VMサイズ	Premium Storage	Accelerated Networking
1 GB - 5 GB	DS4_v2	対応	点灯

リリース5.1（2）以降では、CSR 1000vのバージョン17.3 CSRで最大40Gのスループットがサポートされています。CSRがサポートする最大スループットは、インスタンスタイプによって異なります。40Gのスループットを実現するには、少なくとも8つのCSRが必要です。

次の表に、40Gスループットを達成するために必要なCSRの数とインスタンスタイプを示します（リージョンごと）。

CSRあたりのスループット	CSR インスタンス タイプ	CSR の数
5 Gbps	F16s_v2	8

Cisco Cloud APIC

Cisco Cloud APIC はStandard_D8s_v3を使用して展開されます。

Cloud APIC 通信ポート

Cloud APIC 環境を設定する際は、下記のポートがネットワーク通信に必要であることに注意してください。

- と間の通信用：HTTPS（TCPポート443インバウンド/アウトバウンド）ACI マルチサイトオーケストレータCloud APIC

  には、の開始時ににログインするために使用するものと同じ管理IPアドレスを使用します。Cloud APICCloud APICCloud APICセットアップ ウィザードを使用した Cisco Cloud APIC の設定 （52 ページ）

- オンプレミスのIPsecデバイスと、Azureでによって導入されたCSR間の通信の場合：標準IPsecポート（UDPポート500および4500が開いている必要があります）Cloud APIC

  2つのAzure CSRについては、の手順を使用してISNデバイスコンフィギュレーションファイルをダウンロードした場合のパブリックIPsecピアリングIP。サイト間インフラストラクチャの設定 （65 ページ）

- Azureでによって展開されたCSRを接続および管理する場合は、各CSRのパブリックIPアドレスへのTCPポート22のインバウンド/アウトバウンドを許可します。Cloud APIC

- ライセンス登録の場合（tools.cisco.comへ）：ポート443（アウトバウンド）が必要です。

- DNSの場合：UDPポート53アウトバウンド

- NTPの場合：UDPポート123アウトバウンド

- リモート認証（LDAP、Radius、TACACS+、SAML）を使用する場合は、適切なポートを開きます。

- 認証局を使用する場合は、適切なポートを開きます。

Cisco Cloud APIC のインストール ワークフロー

このセクションでは、Cisco Cloud APIC をインストールして展開するために必要なタスクの概要について説明します。インストールタスクは、Azure管理ポータル、Azure Resource Manager（ARM）テンプレート、Cloud APIC Setup Wizard、および（ACI）Multi-Siteを使用して実行します。Cisco Application Centric Infrastructure

1. オンプレミスデータセンターとパブリッククラウドのタスクを含む、すべての前提条件を満たします。

   セクション「Cisco ACI ファブリックをパブリック クラウドに拡張するための要件 （15 ページ）」を参照してください。

2. Azureに導入します。Cisco Cloud APIC

   このタスクには、Cisco Cloud Services Router 1000Vへの登録、必要なリソースプロバイダーの登録、およびAzureでのアプリケーションの作成が含まれます。

   また、Azure SSHキーペアを作成し、Azureにを展開して、VMのロール割り当てを追加する必要があります。Cisco Cloud APIC

   セクション「Azure でのクラウド APIC の導入 （23 ページ）」を参照してください。

3. セットアップ ウィザードを使用して Cisco Cloud APIC を設定します。

   このタスクには、パブリッククラウドに接続するためのCisco Cloud ACIファブリックへのログインと設定が含まれます。Cisco Cloud APICAzureリージョンの選択も追加します。サイト間ネットワーク（ISN）ピアリング用のボーダーゲートウェイプロトコル（BGP）自律システム番号（ASN）とOSPFエリアIDを指定し、外部サブネットを追加します。次に、IPsecピアアドレスを追加します。

   セクション「セットアップ ウィザードを使用したCisco Cloud APIC の設定 （43 ページ）」を参照してください。

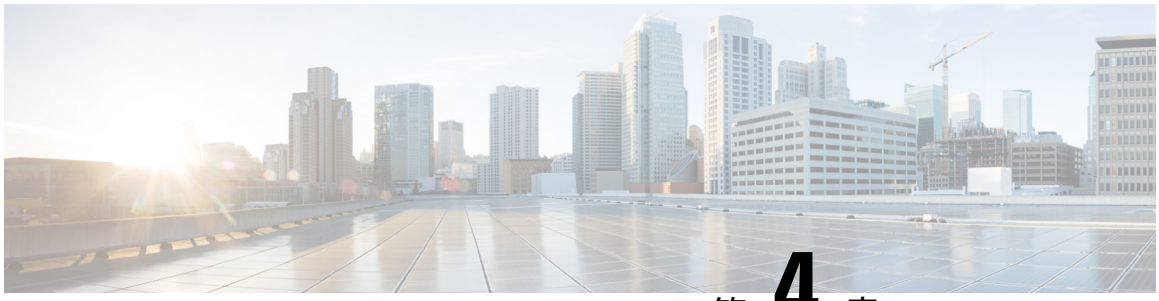
4. Cisco ACI マルチサイトを使用して Cisco Cloud APIC を設定します。

   - オンプレミスからクラウドへの接続の場合、このタスクには、Multi-Site Orchestrator GUIへのログイン、オンプレミスおよびクラウドサイトの追加、ファブリック接続インフラストラクチャの設定、およびオンプレミスサイトのプロパティの設定が含まれます。Cisco ACI次に、スパイン、BGPピアリングを設定し、オンプレミスサイトとAzureクラウドサイト間の接続を有効にします。Cisco ACI
   - クラウド間接続の場合、このタスクには、Multi-Site Orchestrator GUIへのログイン、クラウドサイトの追加、ACI Multi-Siteオプションの有効化、および設定を展開する際の[Deploy Only]オプションの選択が含まれます。Cisco ACI

   セクション「Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 （63 ページ）」を参照してください。

5. Azureパブリッククラウドにポリシーを拡張するために使用します。Cisco Cloud APICCisco ACI

   「」および「」の項を参照してください。Cisco Cloud APIC GUI の操作 （85 ページ）Cisco Cloud APIC コンポーネントの設定 （86 ページ）



第 4 章

Azure でのクラウド APIC の導入

Cisco Cloud Services Router への登録

Cisco Cloud Services Router（CSR）に登録する手順は、ソフトウェアのリリースによって異なります。Cisco Cloud APIC

- 5.2（3）までのリリースでは、クラウドサービスルータとしてCSR 1000vを使用するため、の手順を参照してください。Cisco Cloud APICCisco Cloud Services Router 1000V への登録 （23 ページ）
- リリース5.2（3）以降では、クラウドサービスルータとしてCSR 8000vを使用するため、の手順を参照してください。Cisco Cloud APICCisco Cloud Services Router 8000V への登録

Cisco Cloud Services Router 1000V への登録

最大パフォーマンスを得るには、Cisco Cloud Services Router（CSR）1000V-Bring Your Own License（BYOL）に登録する必要があります。Microsoft Azure Marketplace でサブスクライブするには、次の手順を実行します。

ステップ 1 Azure Marketplace の検索テキスト フィールドに、*Cisco Cloud Services Router（CSR）1000V*と入力し、表示されるオプションを選択します。

Cisco Cloud Services Router（CSR）1000V オプションが検索候補として表示されます。

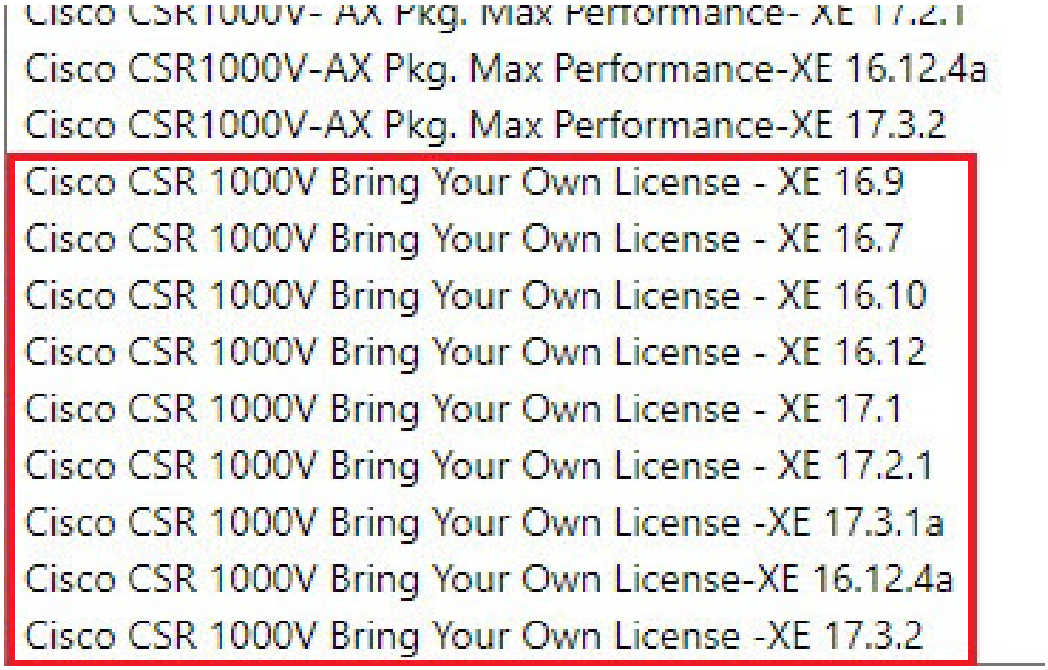
ステップ 2 **[Cisco Cloud Services Router（CSR）1000V]** オプションをクリックします。

Microsoft Azure Marketplace の **Cisco Cloud Services Router（CSR）1000V** ページにリダイレクトされます。

ステップ 3 **[ソフトウェア プランの選択（Select a software plan）]** ドロップダウン メニューを開きます。

メイン ページに **[ソフトウェア プランの選択（Select a software plan）]** ドロップダウン メニューが表示されない場合、**[プラン+価格設定（Plans + Pricing）]** タブをクリックしてください。このオプションが使用可能であれば、**[ソフトウェア プランの選択（Select a software plan）]** ドロップダウン メニューにアクセスします。

ステップ 4 [ソフトウェアプランの選択（Select a software plan）]ドロップダウンメニューで、[Cisco CSR 1000V Bring Your Own License]オプションがリストされている領域を見つけます。



ステップ 5 ソフトウェアリリースに応じて、適切なオプションを選択します。Cisco Cloud APIC

クラウド **APIC** リリースの場合	この特定のオプションを選択します
リリース 4.2x	Cisco CSR 1000V Bring Your Own License-XE 16.12
リリース 5.0(1)	Cisco CSR 1000V Bring Your Own License-XE **16.12**
Release 5.0(2)	Cisco CSR 1000V Bring Your Own License-XE 17.1
リリース 5.1(2)	Cisco CSR 1000V Bring Your Own License-XE 17.3.1（a）

ステップ 6 **プログラマビリティを導入しますか？** フィールドを特定し **[開始（Get Started）]** をクリックします。

ステップ 7 **[プログラマビリティ導入の設定（Configure Programmability Deployment）]** ページでサブスクリプションまでスクロールし、[ステータス（Status）] 列でサブスクリプションのステータスを **[無効（Disable）]** から **[有効（Enable）]** に変更します。

ステップ 8 **[Save]** をクリックします。

次のタスク

必要なリソースプロバイダーの登録 （25 ページ） に進みます。

必要なリソースプロバイダーの登録

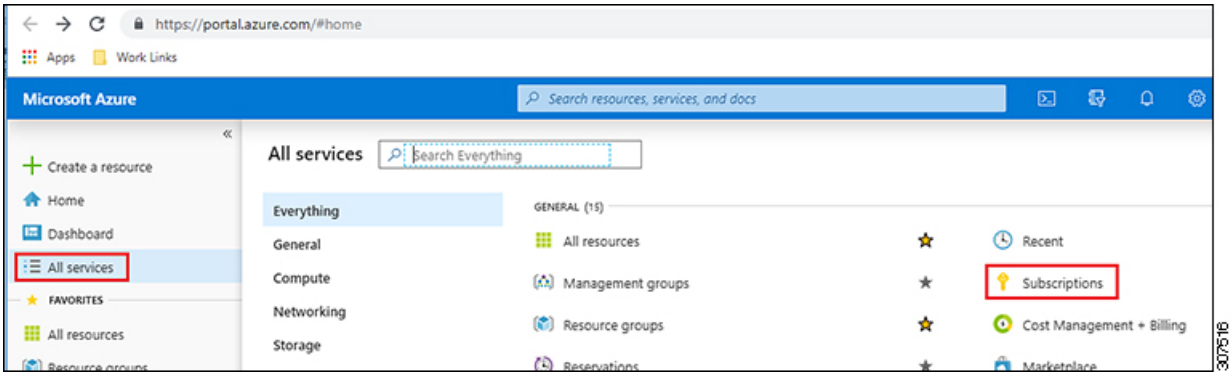
後で追加する可能性があるサブスクリプションがあるテナントを含め、で使用するすべてのサブスクリプションについて、次のリソースプロバイダーを登録する必要があります。Cloud APIC

- `microsoft.insights`
- `Microsoft.EventHub`
- `Microsoft.Logic`
- `Microsoft.ServiceBus`

これらの手順では、サブスクリプションに必要なこれらのリソースプロバイダーを登録する方法について説明します。

ステップ 1 リソースプロバイダーを表示できるAzureの領域にアクセスします。

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[すべてのサービス（All services）]リンクをクリックし、[サブスクリプション（Subscriptions）]リンクをクリックします。

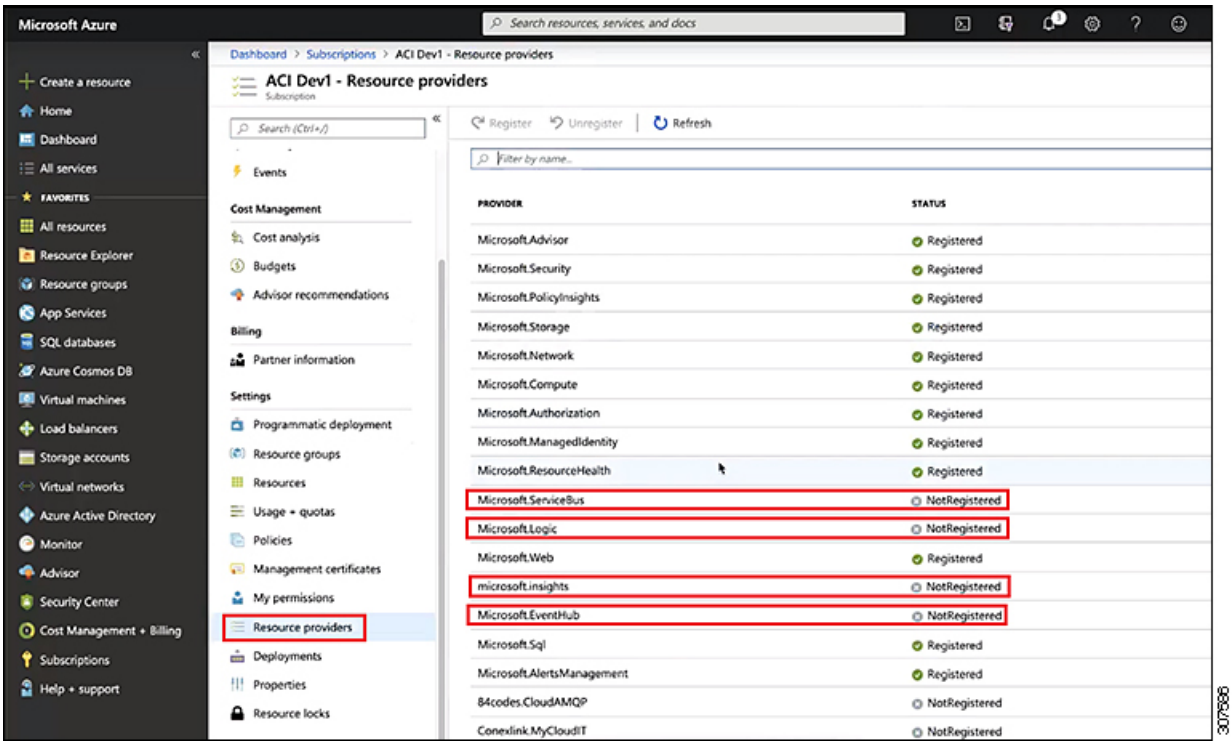


b) Azure管理ポータルの[サブスクリプション（Subscriptions）]ページで、Microsoftアカウントのサブスクリプションアカウントをクリックします。

そのサブスクリプションの概要情報が表示されます。

c) そのサブスクリプションの概要ページで、左側のナビゲーションバーにある[リソースプロバイダー]リソースリンクを見つけ、そのリンクをクリックします。

そのサブスクリプションの[リソースプロバイダー（Resource Providers）]ページが表示されます。

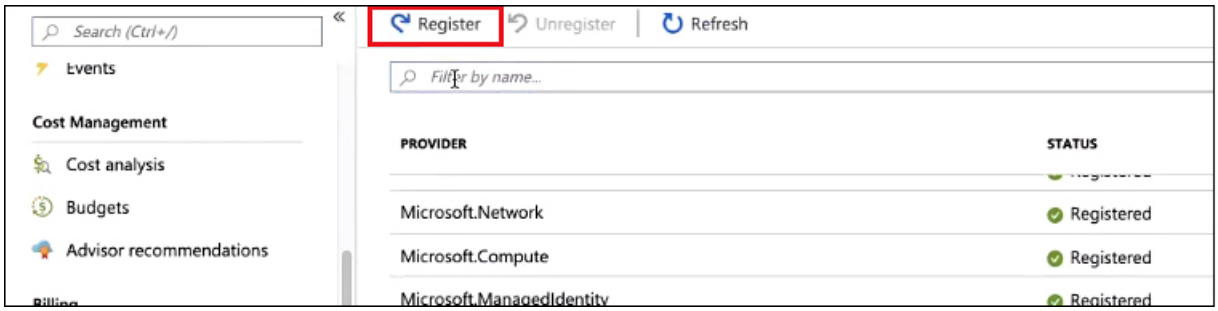


ステップ 2 前のスクリーンショットに示すように、プロバイダーのリストで次の4つのリソースプロバイダーを見つけます。

- `microsoft.insights`
- `Microsoft.EventHub`
- `Microsoft.Logic`
- `Microsoft.ServiceBus`

ステップ 3 4つすべてのリソースプロバイダーがRegisteredまたはNotRegistered状態であるかどうかを確認します。

- 4つすべてのリソースプロバイダーが[登録済み（Status）]列に[登録済み（Registered）]と表示されている場合、このサブスクリプションにこれらのリソースプロバイダーを登録するためにこれ以上何もする必要はありません。
- [ステータス（Status）]列に[未登録（NotRegistered）]と表示されているすべてのリソースプロバイダーについて、次の手順を実行します。
  1. NotRegisteredと表示されている特定のリソースプロバイダーをクリックします。
  2. 画面上部の[登録（Register）]をクリックして、そのリソースプロバイダーを登録します。



登録プロセスが完了すると、ステータスがNotRegisteredからRegisteringに変わり、Registeredに変わります。

3. NotRegisteredと表示されているすべてのリソースプロバイダーについて、4つのリソースプロバイダーがすべてRegisteredと表示されるまで、これらの手順を繰り返します。

Azure でのアプリケーションの作成

必要に応じて、次の手順に従ってAzureでアプリケーションを作成します。テナントの新しいサブスクリプションを作成し、特定のアプリケーションを介してクラウドリソースを管理するために[管理対象外ID（Unmanaged Identity）]を選択する場合は、次の手順が必要です。

（注） Azureのアプリケーションは、サービスプリンシパルとも呼ばれます。

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 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にある[Azure Active Directory]リンクをクリックし、[App registrations]リンクをクリックします。

ステップ 3 **[アプリケーションの登録（App registrations）]** ページで、**[+ New registration]** をクリックします。

ステップ 4 **[アプリケーションの登録（Register an application）]** ページに必要な情報を入力します。

- **Name**
- **[サポートされるアカウントのタイプ（Supported Account Types）]**: 最初のオプションを選択します（この組織ディレクトリ内のアカウントのみ）
- （オプション）**リダイレクト URI**

[登録（Register）] をクリックします

このアプリケーションの概要ページが表示されます。

ステップ 5 左側のナビゲーションバーで **[Certificates & secrets]** をクリックし、**[Add a client secret]** 領域に必要な情報を入力して **[追加（Add）]** をクリックします。

これにより、これらの手順の後半でアプリケーションシークレットフィールドに必要な情報が生成されます。

ステップ 6 テキストファイルを開き、必要な情報をテキストファイルにコピーアンドペーストします。

- [Client Secret]：[Clients & Secrets]ページの[Client Secrets]領域の[Value]フィールドのテキストをコピーします。
- アプリケーションID：ホームアプリケーション登録に移動します<application-name>、[概要（Overview）]ページで、[アプリケーション（クライアント）ID（Application（client）ID）]フィールドからテキストをコピーします。＞＞
- Azure Active Directory ID：[Home App registrations]に移動します。<application-name>、[概要（Overview）]ページで、[ディレクトリ（テナント）ID]フィールドからテキストをコピーします。＞＞

ステップ 7 テキストファイルを保存し、その場所をメモします。

このドキュメントの後半の手順を実行するときに、この情報を参照します。テナントの設定 （71 ページ）

AzureのSSHキーペアの生成

セットアッププロセスの一環として、管理者公開キー（SSH公開キー）をのAzureリソースマネージャ（ARM）テンプレートに入力するように求められます。Cloud APICCloud APIC次の項では、WindowsまたはLinuxシステムでSSH公開キーと秘密キーのペアを生成する手順について説明します。

Windows での SSH キー ペアの生成

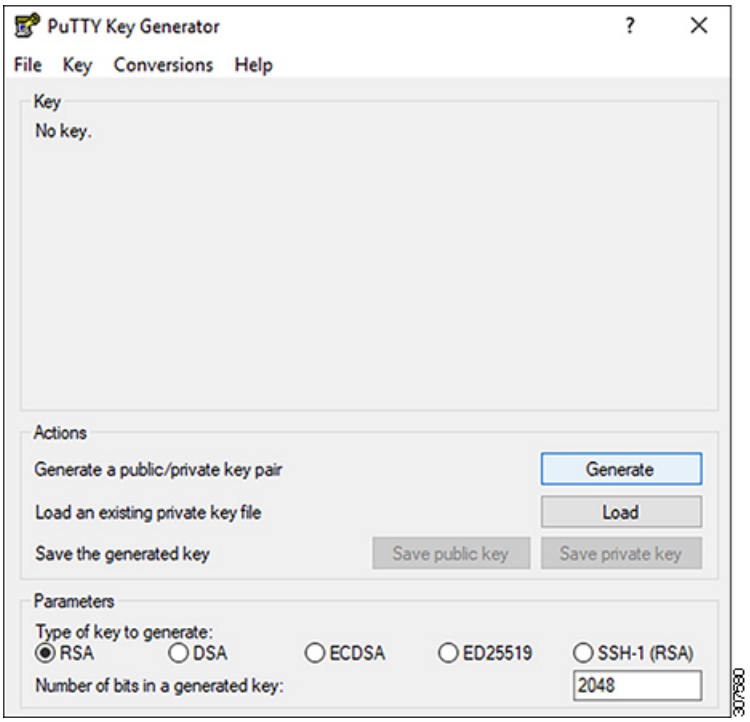
次の手順では、WindowsでSSH公開キーと秘密キーのペアを生成する方法について説明します。LinuxでSSH公開キーと秘密キーのペアを生成する手順については、を参照してください。Linux または MacOS での SSH キー ペアの生成 （31 ページ）

ステップ 1 PuTTYキージェネレータ（puttygen）をダウンロードしてインストールします。

https://www.puttygen.com/download-putty

ステップ 2 **Windows** > **[スタート]** > **[すべてのプログラム]** > **[PuTTY]** > **[PuTTYgen]**

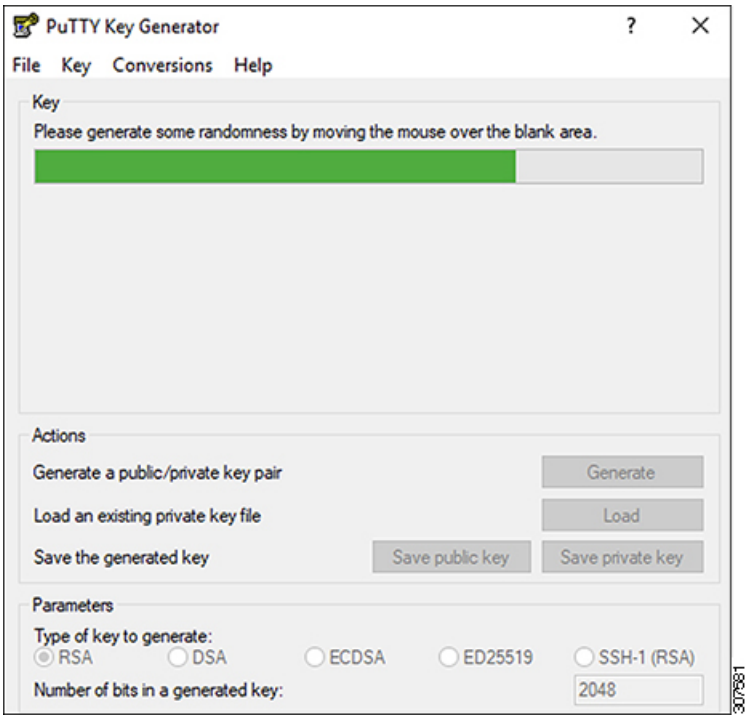
画面にPuTTYキージェネレータのウィンドウが表示されます。



ステップ 3 **[生成（Generate）]** をクリックします。

公開キーを生成するために空白領域にマウスを移動するように求める画面が表示されます。

ステップ 4 空白領域の周囲にカーソルを移動して、公開キーのランダムな文字を生成します。



ステップ 5 公開キーを保存します。

a) 公開キーファイルを保存するラップトップ上のフォルダに移動し、この公開キーのテキストファイルを作成します。

b) PuTTYキージェネレータの情報をコピーします。

次の内容を含めて、ウィンドウに公開キー情報をコピーします。

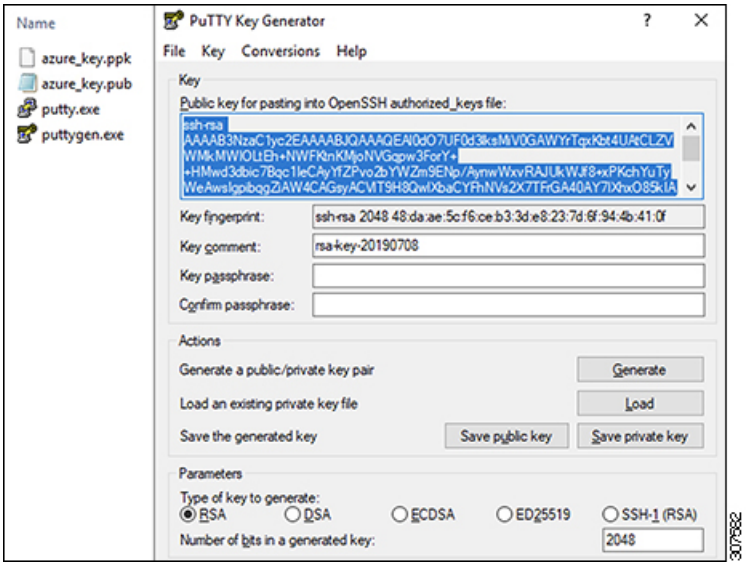
- 公開キーの先頭にssh-rsaテキストを含める。
- 末尾の次のテキスト文字列を除外します。

```
== rsa-key-<date-stamp>
```

== rsa-key-を含まないようにキーを切り捨てます。<date-stamp>末尾のテキスト文字列。

（注） 次の一連の手順では、公開キー情報をAzure ARMテンプレートに貼り付けます。フォームがこの形式のキーを受け入れない場合は、キーの末尾に==を追加します。一部の地域ではこの形式が必要になるためです。

キーが正しい形式でない場合、Cloud APICはインストールを完了しません。



c) で作成した公開キーテキストファイルに情報を貼り付け、ファイルを保存して、一意のファイル名を付けます。5.a （30 ページ）

この公開キーテキストファイルには、1行のテキストのキーが含まれています。次の一連の手順では、この公開キーテキストファイルの情報が必要になります。

（注） PuTTYキージェネレータの[公開キーの保存（Save public key）]オプションを使用して公開キーを保存しないでください。これにより、複数行のテキストを含む形式でキーが保存されます。これは、クラウドAPIC導入プロセスと互換性がありません。

ステップ 6 秘密キーを保存します。

a) **[プライベート キーの保存（Save private key）]** をクリックします。

パスフレーズなしでファイルを保存するかどうかを確認する画面が表示されます。この画面で **[はい（Yes）]** をクリックします。

b) ラップトップのフォルダに移動し、一意のファイル名を付けて秘密キーファイルを保存します。

（注） 秘密キーファイルは、インストールプロセスでは使用されません。ただし、SSH を介したクラウド APIC へのログイン （121 ページ）で説明されているように、SSH を介して Cloud APIC にログインするなど、他の理由で必要になる場合があります。

次のタスク

Azure でのクラウド APIC の導入 （32 ページ） の手順に従って Azure の設定プロセスを続行します。これには、Azure ARM テンプレートへの公開キー情報の貼り付けが含まれます。

Linux または MacOS での SSH キー ペアの生成

次の手順では、Linux または MacOS で SSH 公開キーと秘密キーのペアを生成する方法について説明します。Windows で SSH 公開キーと秘密キーのペアを生成する手順については、を参照してください。Windows での SSH キー ペアの生成 （28 ページ）

ステップ 1 Linux 仮想マシンまたは Mac で、ssh-keygen を使用して公開キーと秘密キーのペアを作成し、出力をファイルに送信します。

```
# ssh-keygen -f filename
```

次に例を示します。

```
# ssh-keygen -f azure_key
```

次のような出力が表示されます。パスフレーズを入力するように求められたら、テキストを入力せずに Enter キーを押します（パスフレーズがないようにフィールドを空のままにします）。

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in azure_key.
Your public key has been saved in azure_key.pub.
The key fingerprint is:
SHA256:gTsQIIAadjgNsgcguifIloh4XGpVWMdcXVV6U0dyBNs
...
```

ステップ 2 保存した公開キーファイルと秘密キーファイルを見つけます。

```
# ls
```

2 つのファイルが表示されます。

- 拡張子が .pub のファイルには、公開キー情報が含まれています。
- 同じ名前でサフィックスのないファイルに秘密キー情報が含まれている

たとえば、出力を `azure_key` という名前のファイルに送信すると、次の出力が表示されます。

```
# ls
azure_key
azure_key.pub
```

その場合、次のようになります。

- azure_key.pub ファイルには、公開キー情報が含まれています。
- azure_key ファイルには秘密キー情報が含まれています。

ステップ 3 公開キーファイルを開き、そのファイルから公開キー情報をコピーします。末尾にusername @ hostname情報は含めません。

（注） 秘密キーファイルは、インストールプロセスでは使用されません。ただし、で説明されているように、SSH を介して Cloud APIC にログインするなど、他の理由で必要になる場合があります。SSH を介したクラウド APIC へのログイン （121 ページ）

次のタスク

の手順に従って Azure の設定プロセスを続行します。これには、公開キー情報を公開キーファイルから Azure ARM テンプレートに貼り付けることが含まれます。Azure でのクラウド APIC の導入 （32 ページ）

Azure でのクラウド APIC の導入

始める前に

- このセクションのタスクに進む前に、Cisco ACI ファブリックをパブリック クラウドに拡張するための要件 （15 ページ） に示されている要件を満たしていることを確認します。たとえば、エラスティック IP アドレスの数が正しいこと、およびインスタンス展開の許可の制限をチェックしたことを確認します。

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 Azure管理ポータルのメインページで、検索テキストフィールドに「Cisco Cloud APIC」と入力します。

ステップ 3 [Cisco Cloud APIC]ページの[Select a plan]フィールドで、[Release 5.1（2）]を選択し、[Create]をクリックします。

[Cisco Cloud APIC]画面の[Basics]ページが表示されます。

ステップ 4 [基本（Basics）]ページの必要なフィールドに入力します。

- **[サブスクリプション（Subscription）]**: ドロップダウン リストから、Cloud APIC インフラ サブスクリプション アカウントを選択します。
- **[リソース グループ（Resource group）]**：ドロップダウン リストから既存のリソース グループを選択するか、**[新規作成（Create new）]**をクリックして新しいリソース グループの名前を入力します。

  Azure リソース グループは、Azure ソリューションの関連リソースを保持するコンテナーです。

  リリース5.0（2）以降では、クラウドAPIC自体のリソースグループを除き、クラウドAPICによって作成されたほとんど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。ここで選択したリソースグループ名が正しいことを確認します。
- [Region]：ドロップダウンリストから、仮想マシンを展開する場所を選択します。Cloud APIC
- 仮想マシン名：仮想マシン名を入力します。このエントリは、この仮想マシンの名前になります。Cloud APIC仮想マシン名は英数字のみである必要がありますが、ダッシュで区切ることができます（CloudAPICなど）。
- [パスワード（Password）]：管理者パスワードを入力します。このエントリは、 SSH アクセスを有効にした後に Cloud APICにログインするために使用するパスワードです。

  パスワードの特徴は次のとおりです。
  - 長さは 12 ー 72 文字にする必要があります
  - 次の 3 つが必要です。
    - 小文字を 1 つ
    - 大文字
    - 数字を 1 つ
    - 許容される次の特殊文字のいずれか：

      @$!%*#?&
- **[パスワードの確認（Confirm Password）]**：管理者パスワードを再度入力します。
- SSH公開キー：次のいずれかの手順の最後にコピーした公開キー情報を貼り付けます。
  - Windows での SSH キー ペアの生成 （28 ページ）
  - Linux または MacOS での SSH キー ペアの生成 （31 ページ）

  Cloud APIC には、この SSH キーペアを使用してログインします。ssh-rsa文字列は、このフィールドに貼り付ける公開キー文字列の先頭にある必要があります。

  （注） WindowsでSSHキーペアを生成した場合、PuTTYキージェネレータのキーは==rsa-key-で終わります。<date-stamp> 。== rsa-key-が含まれないようにキーを切り捨てます。<date-stamp> 。フォームがこの形式のキーを受け入れない場合は、キーの末尾に == を追加します。一部の地域ではこの形式が必要になるためです。

  キーが正しい形式でない場合、Cloud APIC はインストールを完了しません。

ステップ 5 このページのフィールドへの入力が完了したら、[Next：ACI Settings]をクリックします。

[Cisco Cloud APIC]画面の[ACI Settings]ページが表示されます。

ステップ 6 [ACI設定（ACI Settings）]ページの必要なフィールドに入力します。

- **[ACI ファブリック名 (ACI Fabric name):]**デフォルト値のままにしておくか、ファブリック名を入力します。このエントリは、この Cloud APIC の名前になります。ファブリック名は英数字のみにする必要がありますが、ダッシュで区切ることができます（ACI-Cloud-Fabricなど）。
- 仮想マシンのサイズ：仮想マシンのサイズは、Standard_D8s_v3のデフォルトの展開サイズに自動的に設定されます。デフォルトの仮想マシンサイズ設定は変更できません。
- [Image Version]：このフィールドで[5.1（2）]を選択します。
- インフラサブネット：のインフラプール。Cloud APICこのフィールドには、デフォルト値の 10.10.0.0/24 が、自動的に入力されます。デフォルト値がオンプレミスファブリックからのインフラプールと重複している場合は、このフィールドの値を変更します。このエントリは /24 サブネットである必要があります。
- Public IP Address：パブリックIPアドレスを静的に設定します。
  1. [Public IP Address]フィールドで、[Create New]をクリックします。

     （注） クラウドAPICにプライベートIPアドレスを割り当てるには、ドロップダウンリストから[none]を選択します。

     [Create public IP address]フィールドがページの右側に表示されます。
  2. [SKU]領域で、[Basic]または[Standard] SKUを選択します。

     Basic SKUとStandard SKUの違いの詳細については、Microsoftのドキュメントサイトの 『Public IP Addresses in Azure』ドキュメントを参照してください。
  3. [Assignment]領域で、[Static]を選択します。

     [Assignment]領域の設定を[Dynamic]のままにしないでください。
  4. [Create public IP address]領域で[OK]をクリックします。
- パブリックIPアドレスのDNSプレフィックス：DNS名のプレフィックス。Cloud APICが展開されると、DNS名を使用してにアクセスできます。Cloud APICCloud APIC

  （注） Azureの制限により、このフィールドに入力するDNS名のプレフィックスにはピリオド（。）を使用できません。Cloud APIC
- **[外部サブネット (Access Control):]** Cloud APIC への接続を許可する外部ネットワークの IP アドレスとサブネットを入力します (たとえば、192.0.2.0/24)。このサブネットからの IP アドレスだけが、Cloud APIC への接続を許可されます。値 `0.0.0.0/0` を入力すると、誰でも Cloud APIC への接続が許可されます。
- **[仮想ネットワーク名（Virtual Network Name）]**：必要に応じて、仮想ネットワーク名のデフォルトエントリをそのままにするか、このフィールドのエントリを変更します。

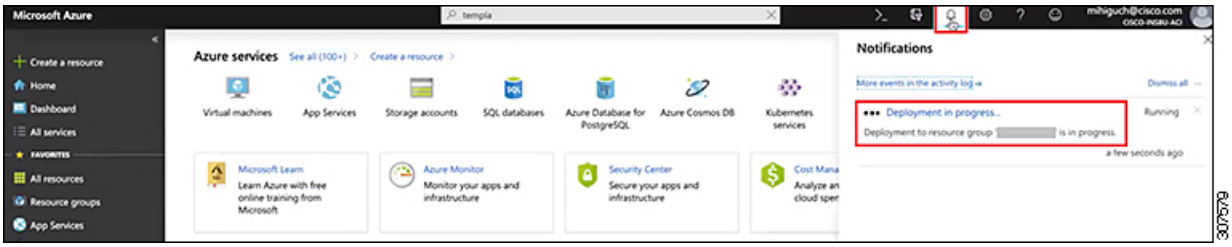
- **[Management NSG Name]**：管理ネットワークセキュリティグループ名のデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。
- **[Management ASG Name]**：管理アプリケーションセキュリティグループ名のデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。
- **サブネットプレフィックス**：サブネットプレフィックスのデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。

ステップ 7 このページのフィールドへの入力が完了したら、**[Next**：**Review + create]** をクリックします。

[Cisco Cloud APIC] 画面の**[Review + create]** ページが表示されます。

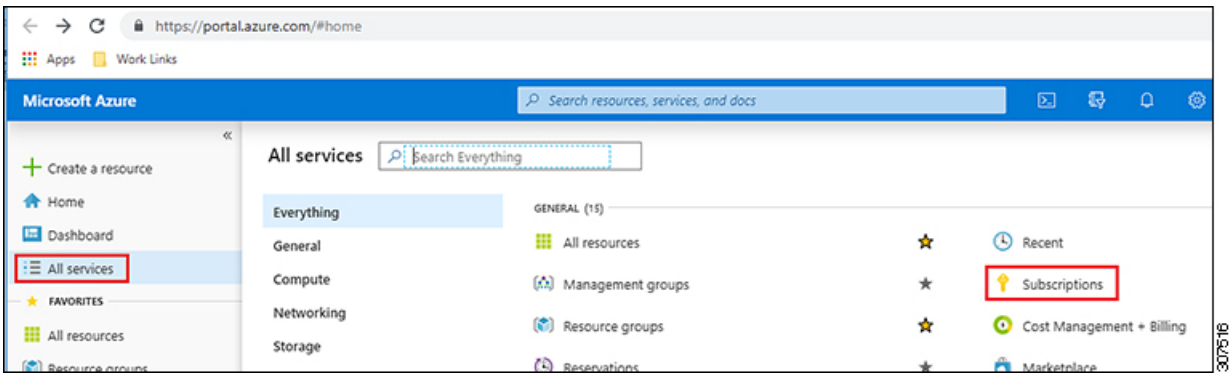
ステップ 8 **[Review + create]**ページで情報を確認し、**[Create]**をクリックします。

システムは、テンプレートに指定された情報を使用して Cloud APIC VM インスタンスを作成するようになりました。プロセスが完了するのに 5 ～ 10 分かかります。通知アイコン（ベル型のアイコン）をクリックして、の展開のステータスを確認します。Cloud APIC



ステップ 9 展開が完了したら、ユーザアクセス管理者ロールの割り当てを追加します。

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**[すべてのサービス（All services）]** リンクをクリックし、**[サブスクリプション（Subscriptions）]** リンクをクリックします。



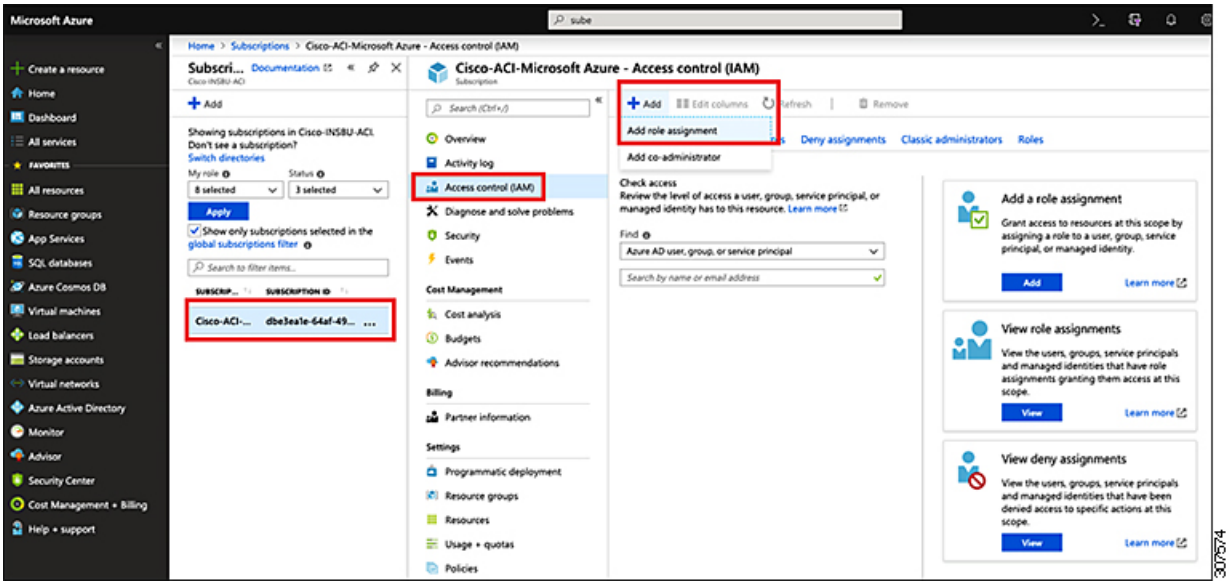
b) Azure 管理ポータルの**[サブスクリプション（Subscriptions）]**ページで、展開されたサブスクリプションアカウントをクリックします。Cloud APIC

そのサブスクリプションの概要情報が表示されます。

c) そのサブスクリプションの概要ページで、左側のナビゲーションバーにある **[Access control（IAM）]** リンクを見つけ、そのリンクをクリックします。

そのサブスクリプションの[アクセス制御（Access Control）]ページが表示されます。

d) **[+ 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。



e) **[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 **[管理者（Administrator）]** を選択します。
- [Assign access to]フィールドで、[Virtual Machine]を選択します。
- [サブスクリプション（Subscription）]フィールドで、が展開されているサブスクリプションを選択します。Cloud APIC
- Cloud APIC 仮想マシンを選択します。

f) 画面の下部にある**[保存（Save）]** をクリックします。

次のタスク

アクセスタイプに管理対象IDまたは管理対象外IDのロール割り当てを追加する必要があるかどうかを判断するには、に移動します。ロール割り当ての追加 （36 ページ）

ロール割り当ての追加

追加するロール割り当てのタイプは、アクセスタイプに管理対象IDがあるかどうかによって異なります。

- アクセスタイプの管理対象IDがある場合は、ユーザテナントのロール割り当てを追加する必要があります。仮想マシンへのロール割り当ての追加 （37 ページ） に進みます。

このアクセスタイプは、このマニュアルで後述する手順で[アカウントの関連付け（Associate Account）]ページに情報を入力するときに、次のいずれかを選択した場合に適用されます。テナントの設定 （71 ページ）

- [Mode：Create Own]を選択し、[Associate Account]ページで[Managed Identity]を選択したか、または
- [モード（Mode）]を選択し、[共有（Shared）]を選択すると、インフラテナントと共有します。

- アクセスタイプの管理対象外ID（サービスプリンシパル）がある場合、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。アプリへのロール割り当ての追加 （39 ページ） に進みます。

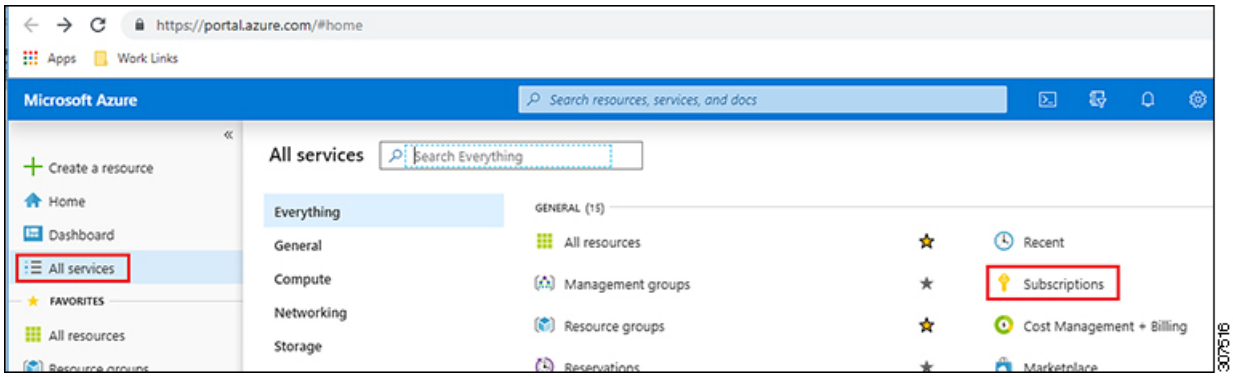
  このアクセスタイプは、このマニュアルで後述する手順で[アカウントの関連付け（Associate Account）]ページで[管理対象外アイデンティティ（Unmanaged Identity）]（サービスプリンシパル）を選択した場合に適用されます。テナントの設定 （71 ページ）

仮想マシンへのロール割り当ての追加

アクセスタイプの**管理**対象IDがある場合は、このセクションの手順に従います。ここで、ユーザテナントのロール割り当てを追加する必要があります。Azure サブスクリプション タイプとクラウド APIC テナントの関係の詳細については、テナント、ID、およびサブスクリプションについて （9 ページ） を参照してください。

（注） クラウドリソースが特定のアプリケーションを介して管理されるアクセスタイプの**管理対象外** ID がある場合は、の手順に従います。アプリへのロール割り当ての追加 （39 ページ）

ステップ 1 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 **[すべてのサービス（All services）]** リンクをクリックし、**[サブスクリプション（Subscriptions）]** リンクをクリックします。



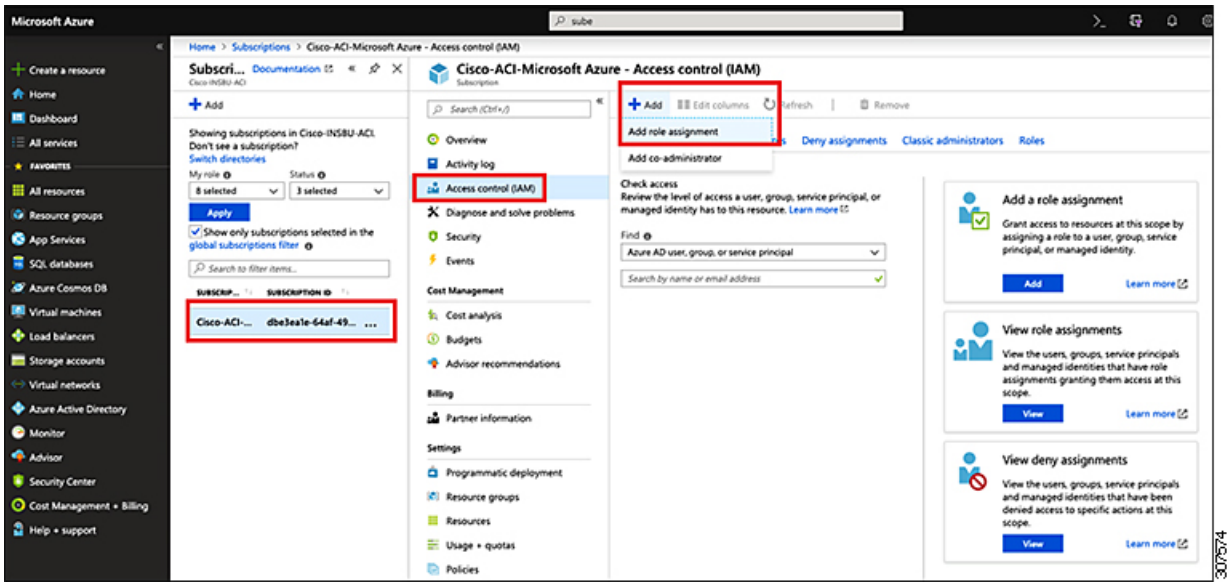
ステップ 2 Azure 管理ポータルの **[サブスクリプション（Subscriptions）]** ページで、展開されたサブスクリプション アカウントをクリックします。Cloud APIC

そのサブスクリプションの概要情報が表示されます。

ステップ 3 そのサブスクリプションの概要ページで、左側のナビゲーションバーにある [**Access control（IAM）**] リンクを見つけ、そのリンクをクリックします。

そのサブスクリプションの[アクセス制御（Access Control）]ページが表示されます。

ステップ 4 **[+ 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。



ステップ 5 **貢献者** ロールの割り当てを追加します。

a) **[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 **[貢献者（Contributor）]** を選択します。
- **[Assign access to]** フィールドで、**[仮想マシン（Virtual Machine）]** を選択します。
- **[サブスクリプション（Subscription）]** フィールドで、Cloud APIC が展開されているサブスクリプションを選択します。
- Cloud APIC 仮想マシンを選択します。

b) 画面の下部にある**[保存（Save）]** をクリックします。

ステップ 6 **[ユーザ アクセス管理者]** ロールの割り当てを追加します。

a) **[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 **[管理者（Administrator）]** を選択します。
- **[Assign access to]** フィールドで、**[仮想マシン（Virtual Machine）]** を選択します。
- **[サブスクリプション（Subscription）]**フィールドで、Cloud APIC が展開されているサブスクリプションを選択します。
- Cloud APIC 仮想マシンを選択します。

b) 画面の下部にある**[保存（Save）]** をクリックします。

（注） ユーザテナントのサブスクリプションを共有している場合、新しいIAMロールの割り当てがAzureで有効になるまでに最大30分かかります。30分以上待ってから、次のセクションに進みます。

次のタスク

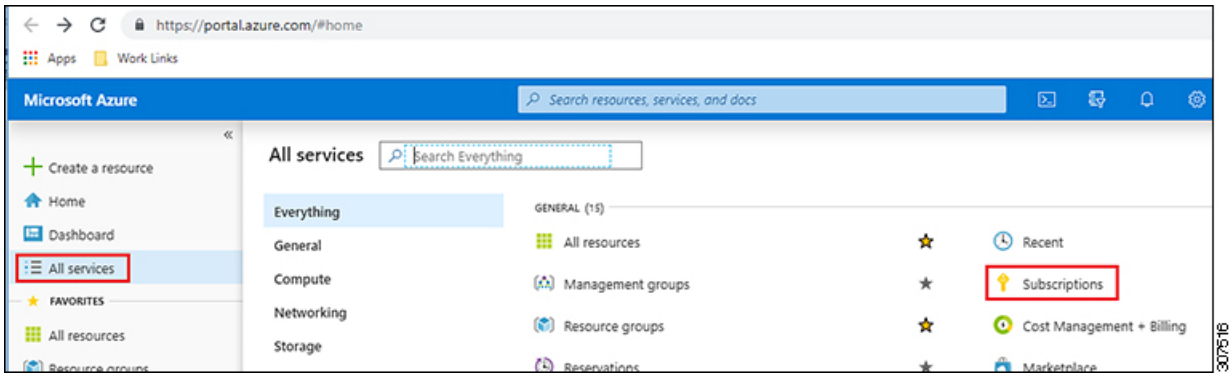
セットアップ ウィザードを使用した Cisco Cloud APIC の設定 （43 ページ） の設定を続行するには、Cloud APIC に移動します。

アプリへのロール割り当ての追加

クラウドリソースが特定のアプリケーションを介して管理されるアクセスタイプの管理対象外IDがある場合は、このセクションの手順に従います。AzureサブスクリプションタイプとクラウドAPICテナントの関係の詳細については、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 （9 ページ）

（注） ユーザテナントのロール割り当てを追加する必要があるアクセスタイプの管理対象アイデンティティがある場合は、の手順に従います。仮想マシンへのロール割り当ての追加 （37 ページ）

ステップ 1 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 **[すべてのサービス（All services）]** リンクをクリックし、**[サブスクリプション（Subscriptions）]** リンクをクリックします。



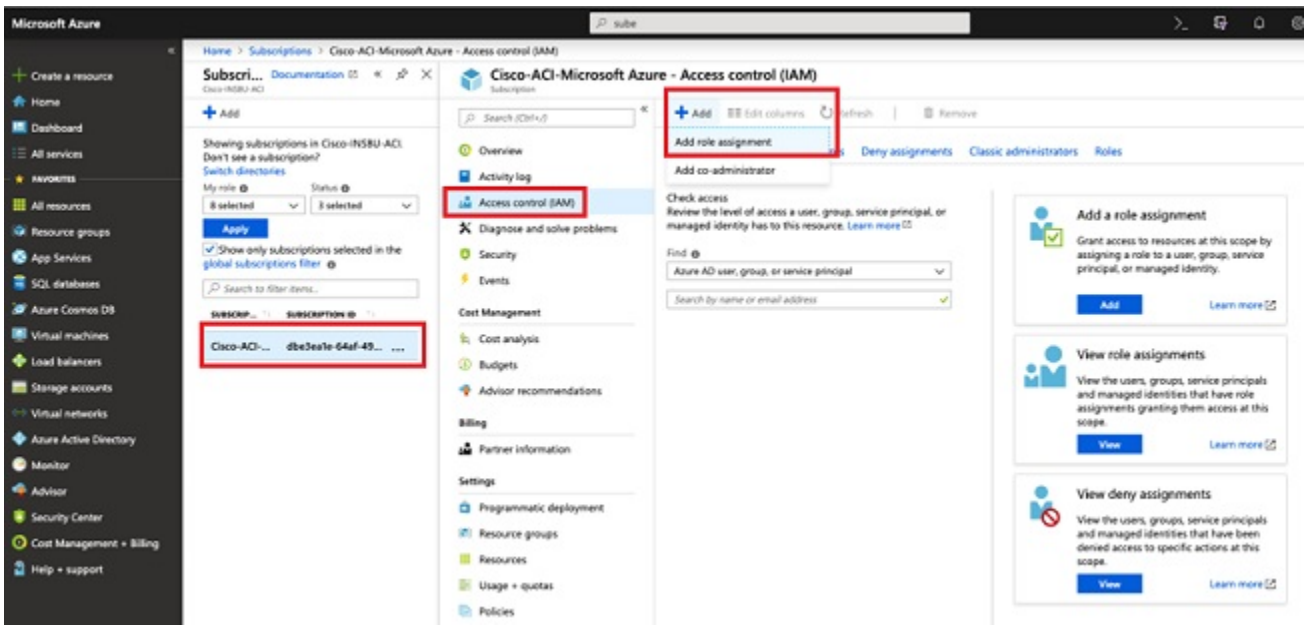
ステップ 2 Azure管理ポータルの[サブスクリプション（Subscriptions）]ページで、展開されたサブスクリプションアカウントをクリックします。Cloud APIC

そのサブスクリプションの概要情報が表示されます。

ステップ 3 そのサブスクリプションの概要ページで、左側のナビゲーションバーにある[Access control（IAM）]リンクを見つけ、そのリンクをクリックします。

そのサブスクリプションの[アクセス制御（Access Control）]ページが表示されます。

ステップ 4 [+ 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。

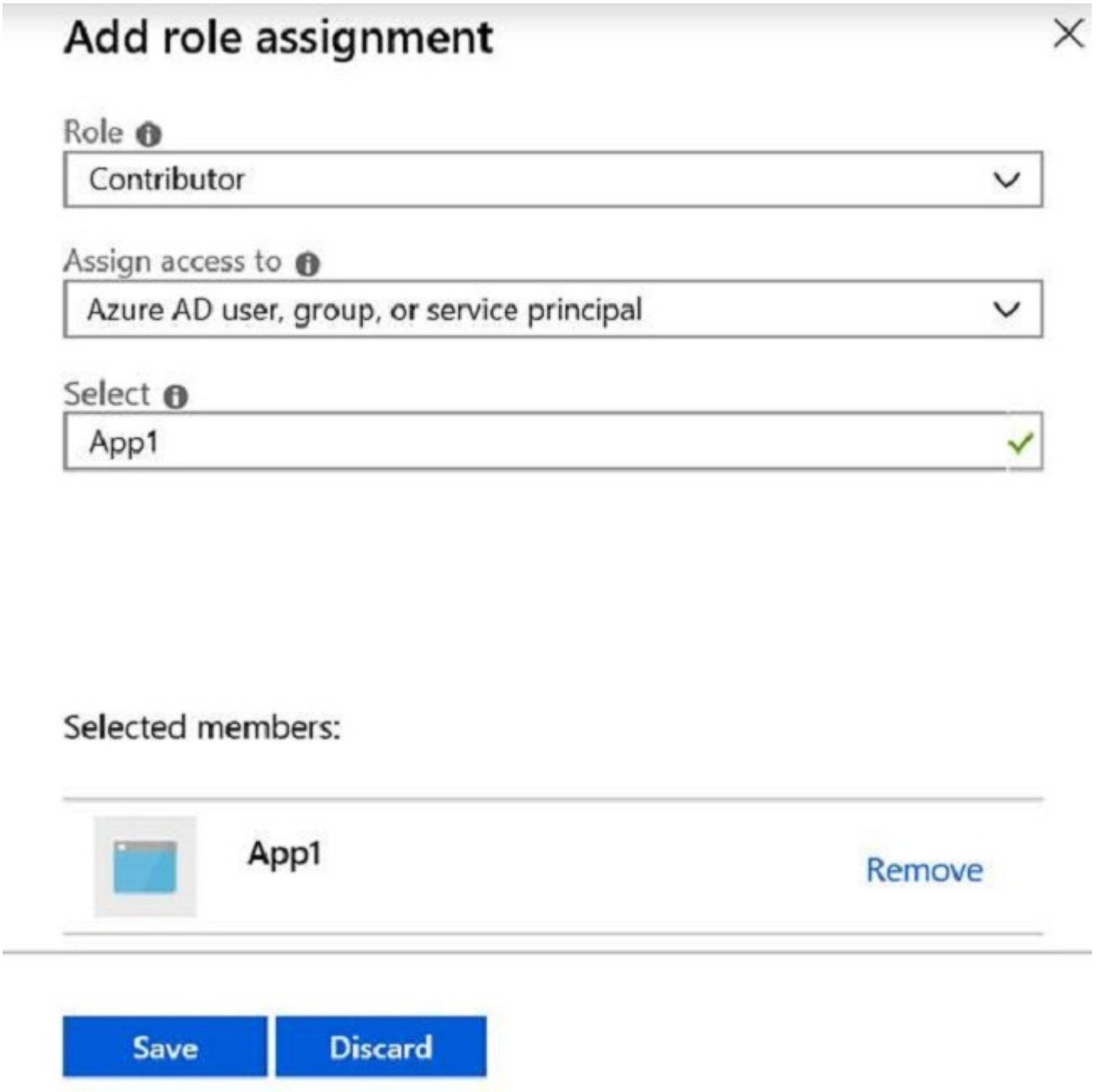


ステップ 5 貢献者ロールの割り当てを追加します。

a) [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 **[貢献者（Contributor）]** を選択します。

- **[Assign access to]** フィールドで **Azure AD ユーザー、グループ、またはサービス プリンシパル** を選択します。
- **[選択（Select）]** フィールドで、Azure アプリケーションに関連付けられているクレデンシャルを選択します。



b) 画面の下部にある **[保存（Save）]** をクリックします。

ステップ 6 **[ユーザ アクセス管理者]** ロールの割り当てを追加します。

a) **[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。

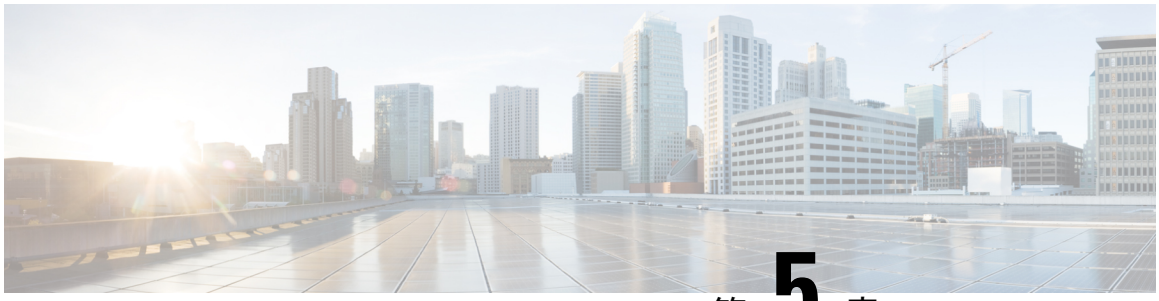
- **[ロール（Role）]** フィールドで、ドロップダウン メニューから **[管理者（Administrator）]** を選択します。
- **[Assign access to]** フィールドで **Azure AD ユーザー、グループ、またはサービス プリンシパル** を選択します。
- **[選択（Select）]** フィールドで、Azure アプリケーションに関連付けられているクレデンシャルを選択します。

b) 画面の下部にある**[保存（Save）]** をクリックします。

（注） 新しい IAM ロールの割り当てが Azure で有効になるまでに最大 30 分かかります。30 分以上待ってから次の章に進みます。Azure で IAM ロールの割り当てが有効になる前にセットアップウィザードを使用してクラウド APIC を設定しようとすると、CSR の展開は失敗します。

次のタスク

セットアップ ウィザードを使用した Cisco Cloud APIC の設定 （43 ページ） の設定を続行するには、Cloud APIC に移動します。



第 5 章

セットアップウィザードを使用したCisco Cloud APICの設定

サイト間接続の設定と展開

の設定と展開を開始する前に、オンプレミスサイトをクラウドサイトに接続する場合は、とをオンプレミスで設定して展開する必要があります。Cloud APICCisco ACI マルチサイトCisco ACIそれぞれの実際の設定は、要件と設定によって異なります。オンプレミスサイトをクラウドサイトに接続する場合は、Microsoft Azureでによって展開されたCisco Cloud Services Router 1000Vに接続するために、オンプレミスのIPsec終端デバイスを設定して展開する必要もあります。Cloud APIC詳細については、「Cisco ACI ファブリックをパブリック クラウドに拡張するためのコンポーネント （4 ページ）」を参照してください。

次に、これらのコンポーネントの設定と展開のプロセスを支援するドキュメントを示します。

- ドキュメンテーション：『Cisco Application Policy Infrastructure Controller（APIC）』のドキュメント（『Operating Cisco Application Centric Infrastructure』および『Cisco APIC Basic Configuration Guide、Release 4.0（1）』など）で入手できます。Cisco ACIhttps://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.htmlhttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/Operating_ACI/guide/b_Cisco_Operating_ACI.htmlhttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/basic-configuration/Cisco-APIC-Basic-Configuration-Guide-401.html

- ：『Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide、Release 2.0（1）』などのCisco ACI Multi-Siteのマニュアルを参照してください。Cisco ACI マルチサイト https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html#ACI_Multi-Sitehttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/aci_multi-site/sw/2x/installation/Cisco-ACI-Multi-Site-Installation-Upgrade-Guide-201.html
- Cisco Cloud Services Router（CSR）：
  - Cisco Cloud Services Router 1000v: Cisco CSR 1000v のマニュアルで入手できます。

オンプレミス設定情報の収集

（注） クラウドサイト間接続のみを設定している場合は、このセクションの情報を収集する必要はありません。Cisco Cloud APIC

次のリストを使用して、を設定するためにこれらの手順全体で必要なオンプレミスの設定情報を収集し、記録します。Cisco Cloud APIC

必要なオンプレミス情報	入力する値
オンプレミスの IPsec デバイスのパブリック IP アドレス	
IPsec 終端デバイスから CSR への OSPF エリア	
オンプレミス APIC IP アドレス	
Cisco Cloud APIC の IP アドレス	

サイト、リージョン、および CSR の数の制限について

このドキュメントでは、サイト、リージョン、およびCSRのさまざまな設定を決定するよう求められます。次に、それぞれの設定を決定する際に留意すべき制限事項のリストを示します。

サイト（Sites）

使用できるサイトの合計数は、設定する設定のタイプによって異なります。Cloud APIC

- オンプレミスのACIサイト間設定（AWSまたはAzure）：ACI Multi-Siteマルチクラウド導入は、1つまたは2つのクラウドサイト（AWSまたはAzure）と最大1つまたは2つのオンプレミスサイトの任意の組み合わせをサポートします。合計4つのサイトがあります。接続オプションは次のとおりです。

- Hybrid-Cloud：オンプレミスから単一のクラウドサイトへの接続
- Hybrid Multi-Cloud：オンプレミスから複数のクラウドサイトへの接続

- マルチクラウド：クラウドサイト間接続（AWSまたはAzure）：ACIマルチサイトマルチクラウド展開では、合計2つのサイトの任意の2つのクラウドサイト（AWS、Azure、またはその両方）の組み合わせをサポートします。
- Cloud First：シングルクラウド構成：ACIマルチサイトマルチクラウド導入は、単一のクラウドサイト（AWSまたはAzure）をサポートします。

[Regions]

各サイト内では、サイトごとに最大4つのリージョンを設定できます。は複数のリージョンを1つのサイトとして管理できます。Cloud APIC

CSR

一部のリージョン内には一定数のCSRを含めることができますが、次の制限があります。

- VNET間（Azure）、VPC間（AWS）、またはVRF間通信を行うには、少なくとも1つのリージョンにCSRを展開する必要があります。
- すべての地域にCSRを配置する必要はありません。
- 接続を有効にするためにCSRが展開されているリージョンの場合：
  - CSRは、4つの管理対象リージョンすべてに導入できます。
  - 管理対象リージョンごとにサポートされるCSRの数は、リリースによって異なります。
    - 5.1（2）よりも前のリリースでは、管理対象リージョンごとに最大4つのCSRがサポートされ、クラウドサイトごとに合計16のCSRがサポートされます。
    - リリース5.1（2）以降では、管理対象リージョンごとに最大8つのCSRがサポートされ、クラウドサイトごとに合計32のCSRがサポートされます。CSRの数の増加の詳細については、『Cloud APIC for Azure User Guide』を参照してください。

注 管理対象リージョンあたりのCSRの数は、AWSとAzureでは異なります。AWSではリージョンごとに4つのCSRがサポートされ、リリース5.1（2）以降では、リージョンごとに8つのCSRがサポートされます。

クラウドリソースの命名

クラウドAPICリリース5.0（2）より前では、AzureのクラウドAPICによって作成されたクラウドリソースには、ACIオブジェクトの名前から派生した名前が割り当てられていました。

- リソースグループは、テナント、VRF、およびリージョンに基づいて作成されました。たとえば、`CAPIC_<tenant>_<vrf>_<region>`。
- VNET名は、クラウドAPIC VRFの名前と一致しました。
- サブネット名はCIDRアドレス空間から取得されました。たとえば、10.10.10.0 / 24クラウドサブネットの場合はsubnet-10.10.10.0_24です。
- クラウドアプリケーション名は、EPG名とアプリケーションプロファイル名から取得されました。たとえば、`<epg-name>_cloudapp_<app-profile-name>`

このアプローチは、クラウドリソースの命名規則が厳格な導入には適していません。また、クラウドリソースの命名とタグ付けに関するAzureのベストプラクティスに従っていません。

クラウド APIC リリース 5.0（2）以降、クラウド APIC 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、クラウド APIC 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。クラウド APIC ARM テンプレートの導入に使用される**リソース グループ**名を除き、クラウド APIC 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 を使用して各クラウド APIC 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。

クラウド APIC リリース 5.1（2）以降、レイヤ 4ーレイヤ 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、削除して再作成する必要があります。

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、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。Cisco Cloud APIC

- $ {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ーレイヤ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ーレイヤ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、によって障害が発生します。Cisco Cloud APIC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、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。Cisco Cloud APIC

Azureには名前の最大長の制限があります。名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、設定が拒否され、リソースの作成に失敗したというエラーが発生します。Cisco Cloud APICその後、障害の詳細を確認し、命名規則を修正できます。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。Cisco Cloud APIC

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 *2:* クラウドリソースでサポートされる変数

Azure のリソース	`${tenant}`	`${ctx}`	`${ctxprofile}`	`${subnet}`	`${app}`	`${epg}`	`${contract}`	`${region}`	`${priority}`
リソースグループ 最長：90	対応*	対応*						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	対応	対応	対応	○*				○	
アプリケーション セキュリティ グループ（ASG） 最長：80	対応				○*	対応*		○	
ネットワーク セキュリティ グループ（NSG） 最長：80	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	対応						対応		Yes *（自動）

表 *3:* 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}	${deviceInterfaceDN}
インターネットネットワークロードバランサ 最長：80	対応	対応	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	対応	対応	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	対応	対応	対応	○*		
インターネット向けApplication Load Balancer 最長：80	対応	対応	対応	○*		
デバイスASG 最長：80	対応	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。

- クラウドAPIC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。
  - ハブリソース名前付けルールは、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、オーバーレイ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。クラウドAPICをリリース5.0（2）にアップグレードし、一部のリソースがすでにAzureに導入されている場合は、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。

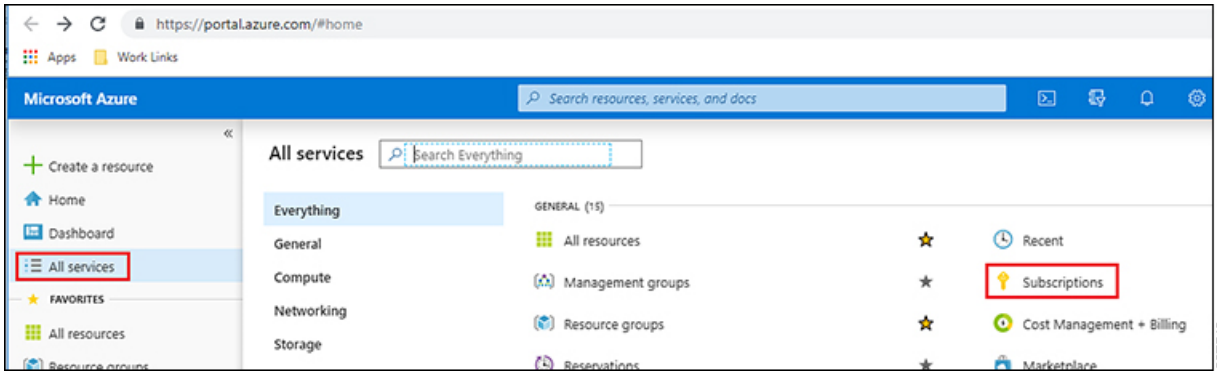
  最初に命名規則を定義することをお勧めします。それからテナント設定も行ってください。

  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APICのIPアドレスの特定

次の手順では、AzureサイトでのIPアドレスを検索する方法について説明します。Cloud APIC

ステップ 1 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 **[すべてのサービス（All services）]** リンクをクリックし、**[サブスクリプション（Subscriptions）]** リンクをクリックします。



ステップ 2 Azure管理ポータルの[サブスクリプション（Subscriptions）]ページで、作成したサブスクリプションアカウントをクリックします。

そのサブスクリプションの概要情報が表示されます。

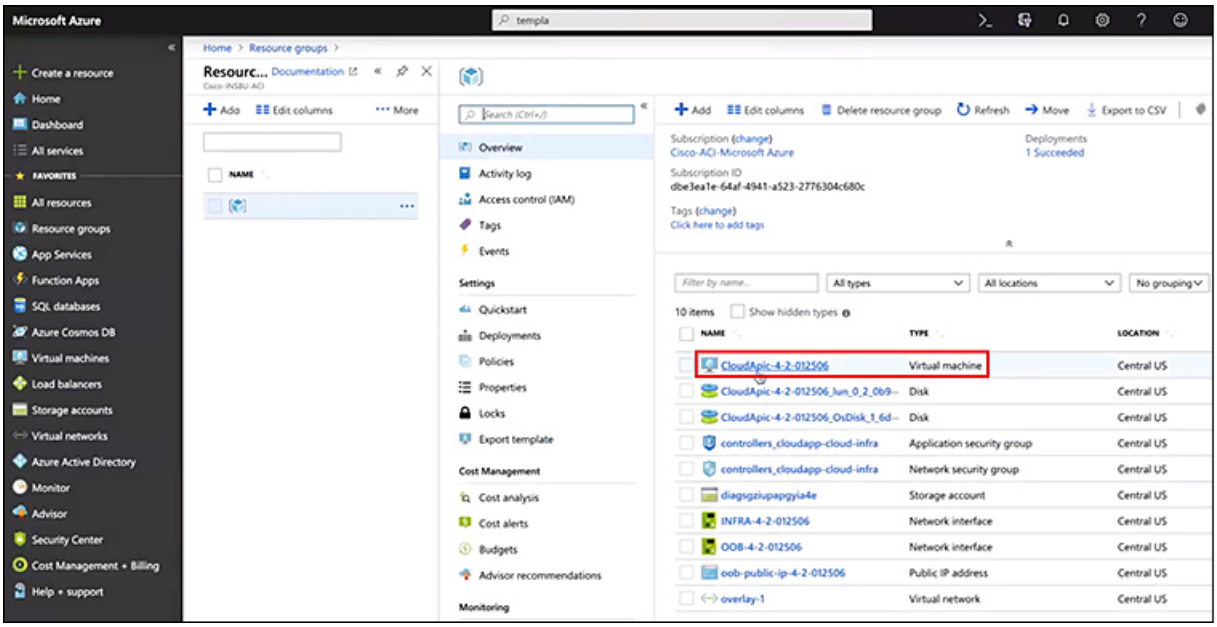
ステップ 3 そのサブスクリプションの概要ページで、左側のナビゲーションバーにある[リソースグループ（Resource groups）]リンクを見つけ、そのリンクをクリックします。

そのサブスクリプションのリソースグループが表示されます。

ステップ 4 選択または作成したリソースグループを選択します。Azure でのクラウド APIC の導入 （32 ページ）

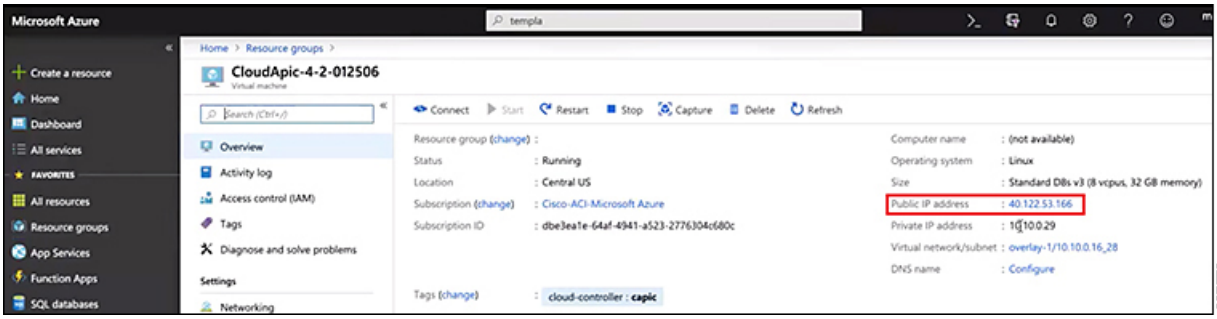
そのリソースグループの概要情報が表示されます。

ステップ 5 リソースグループの概要ページで、VMインスタンス（[TYPE]列の下に[Virtual machine]と表示）を見つけ、そのVMインスタンスのリンクをクリックします。Cloud APIC



VMインスタンスの概要情報が表示されます。Cloud APIC

ステップ 6 このページの[パブリックIPアドレス（Public IP address）]フィールドでエントリを見つけ、そのIPアドレスエントリをコピーします。



これは、にログインするために使用するIPアドレスです。Cloud APICCloud APIC

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

のクラウドインフラストラクチャ設定をセットアップするには、このトピックの手順に従います。は、必要なAzureコンストラクトと必要なCSRを自動的に展開します。Cloud APICCloud APIC

始める前に

このタスクの前提条件は次のとおりです。

- このセクションのタスクに進む前に、Cisco ACI ファブリックをパブリック クラウドに拡張するための要件 （15 ページ） に示されている要件を満たしています。
- Azure でのクラウド APIC の導入 （23 ページ） に記載されている手順を正常に完了しました。

ステップ 1 Cloud APIC の IP アドレスを検索します。

手順については、クラウドAPICのIPアドレスの特定 （50 ページ）を参照してください。

ステップ 2 ブラウザウィンドウを開き、セキュアバージョンのHTTP（https：//）を使用して、URLフィールドにIPアドレスを貼り付け、Returnを押してアクセスします。Cloud APIC

たとえば、https：//192.168.0.0と入力します。

[リスクを無視して証明書を受け入れる（Ignore Risk and Accept Certificate）]というメッセージが表示された場合は、証明書を受け入れて続行します。

ステップ 3 Cloud APIC のログイン ページに次の情報を入力します。

- ユーザ名：このフィールドにadminと入力します。
- **[パスワード（Password）]**：クラウドAPICにログインするために指定したパスワードを入力します。
- [ドメイン（Domain）]：[ドメイン（Domain）]フィールドが表示された場合は、デフォルトの[ドメイン（Domain）]エントリをそのままにします。

ステップ 4 ページの下部にある **[ログイン]** をクリックします。

（注） ログインしようとしたときに、RESTエンドポイントのユーザ認証データストアが初期化されていないなどのエラーメッセージが表示された場合は、このファブリックノードのファブリックメンバーシップステータスを確認し、数分待ってから数分後に再試行してください。ログインするためにページを更新する必要がある場合もあります。

[Cloud APIC へようこそ（Welcome to Cloud APIC）] セットアップ ウィザードのページが表示されます。

ステップ 5 **[セットアップの開始（Begin Setup）]** をクリックします。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

[基本設定（Let's Configure the Basics）]ページが表示され、次の領域が設定されます。

- **DNS サーバと NTP サーバ**
- **リージョン管理**
- **スマート ライセンス**

ステップ 6 [DNS and NTP Servers]行で、[Edit Configuration]をクリックします。

[DNS および NTP] ページが表示されます。

ステップ 7 [DNS and NTP]ページで、必要に応じてDNSおよびNTPサーバを追加します。

- DNSサーバはデフォルトですでに設定されています。特定のDNSサーバを使用する場合は、DNSサーバを追加します。
- ただし、NTPサーバはデフォルトでは設定されないため、NTPサーバを設定することを推奨します。NTPサーバを設定し、DNSサーバを設定しない場合は、に進みます。7.d （53 ページ）

a) 特定のDNSサーバを使用する場合は、[DNS Servers]領域で[+ Add DNS Provider]をクリックします。
b) DNSサーバのIPアドレスを入力し、必要に応じて[優先DNSプロバイダー（Preferred DNS Provider）]の横にあるボックスをオンにします。
c) DNSサーバの横にあるチェックマークをクリックし、追加する追加のDNSサーバについて繰り返します。
d) [NTP Servers]領域で、[+ Add Providers]をクリックします。
e) NTPサーバのIPアドレスを入力し、必要に応じて、[Preferred NTP Provider]の横にあるボックスをオンにします。
f) NTPサーバの横にあるチェックマークをクリックし、追加するNTPサーバを繰り返します。

ステップ 8 DNSサーバとNTPサーバの追加が完了したら、[保存して続行（Save and Continue）]をクリックします。

[Let's Configure the Basics]ページが再度表示されます。

ステップ 9 [Region Management]行で、[Begin]をクリックします。

[地域管理（Region Management）] ページが表示されます。

ステップ 10 必要に応じて、[内部ネットワークの接続（Connectivity for Internal Network）]領域で、内部ネットワークに必要な接続のタイプを設定します。

グローバルレベルのVNetピアリングは、[内部ネットワークの接続（Connectivity for Internal Network）]エリアで設定されます。これにより、クラウドAPICレベルでVNetピアリングが有効になり、CSRを使用してすべてのリージョンにNLBが展開されます。VNetピアリング機能の詳細については、Cisco Cloud APICドキュメンテーションページの「Configuring VNet Peering for Cloud APIC for Azure」を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/series.html#Configuration

- リリース5.1（2）以降では、グローバルレベルのVNetピアリングはデフォルトで有効になっており、無効にすることはできません。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

- リリース5.1（2）よりも前のリリースでは、[内部ネットワークの接続性（Connectivity for Internal Network）]領域で内部ネットワークに必要な接続のタイプを設定できます。
  - Azure VNetピアリングをグローバルレベルで有効にするには、[Virtual Network Peering]をクリックします。
  - VNetピアリングではなくCSRによる従来のVPN接続を有効にするには、[VPN Connectivity via CSR]をクリックします。

ステップ 11 リージョン内の接続に加えて、オンプレミスサイトまたは別のクラウドサイトに接続する場合は、[サイト間接続（Inter-Site Connectivity）]チェックボックスをオンにします。

ステップ 12 ホームリージョンが選択されていることを確認します。Cloud APIC

クラウドサイトの設定時に選択したリージョンがホームリージョンであり、このページですでに選択されている必要があります。これは、が展開されるリージョン（によって管理されるリージョン）で、[リージョン（Region）]列に[クラウドAPIC展開（Cloud APIC Deployed）]というテキストが表示されます。Cloud APICCloud APIC

（注） Azure VNetピアリングを有効にした場合は、[Home]リージョンの[Cloud Routers]列のチェックボックスもオンにする必要があります。ステップ 10 （53 ページ）Cloud APIC

ステップ 13 で追加のリージョンを管理し、場合によっては他のリージョンでVNET間通信とHybrid-Cloud、Hybrid Multi-Cloud、またはMulti-Cloud接続を持つようにCSRを展開する場合は、追加のリージョンを選択します。Cloud APIC

CSRは、展開されているホームリージョンを含む最大4つのリージョンを管理できます。Cloud APIC

は、複数のクラウドリージョンを単一のサイトとして管理できます。Cloud APIC一般的な設定では、サイトはAPICクラスタで管理できるすべてのものを表します。Cisco ACIが2つのリージョンを管理する場合、それらの2つのリージョンは単一のサイトと見なされます。Cloud APICCisco ACI

選択した地域の行では、次のオプションを使用できます。

- クラウドルータ：この領域にCSRを展開する場合は、このオプションを選択します。VNET間またはVPC間通信を行うには、少なくとも1つのリージョンにCSRが展開されている必要があります。ただし、このページで複数のリージョンを選択した場合は、選択したすべてのリージョンにCSRを設定する必要はありません。詳細については、「サイト、リージョン、およびCSR の数の制限について（44 ページ）」を参照してください。
- [サイト間接続（Inter-Site Connectivity）]：このリージョンを他のサイトに接続する場合は、このオプションを選択します（たとえば、このリージョンをオンプレミスサイトに接続する場合、またはCisco ACIを介してクラウドサイト間接続する場合）マルチサイト）。インフラVNETまたはVPCは、サイト間接続用に選択されたすべてのリージョンに展開されます。リージョンのサイト間接続を選択すると、サイト間接続ハブ用に2つのクラウドルータが展開されている必要があるため、このリージョンのクラウドルータオプションも自動的に選択されることに注意してください。

ステップ 14 適切なリージョンをすべて選択したら、ページの下部にある[Next]をクリックします。

[General Connectivity]ページが表示されます。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

ステップ 15 [General Connectivity]ページで次の情報を入力します。

a) [General]領域の[Subnet Pools for Cloud Routers]フィールドで、CSRのサブネットを追加する場合は、[Add Subnet Pool for Cloud Routers]をクリックします。

最初のサブネットプールが自動的に入力されます（System Internalとして表示）。このサブネットプールのアドレスは、クラウドAPIC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。このフィールドに追加するサブネットプールは、マスク/ 24の有効なIPv4サブネットである必要があります。

次の状況では、この手順でCSRのサブネットを追加します。

- ホームリージョンにCSRを展開している場合は、自動的に生成されるシステム内部サブネットプールに加えて、1つのサブネットプールを追加します。Cloud APIC
- 前のページで管理対象となる追加のリージョンを選択した場合：Cloud APIC
  - 管理対象リージョンごとに2ー4のCSRを持つすべての管理対象リージョンに1つのサブネットプールを追加します（の[Number of Routers Per Region]フィールドに2、3、または4を入力した場合）。15.d （57 ページ）
  - 管理対象リージョンごとに5つ以上のCSRがあるすべての管理対象リージョンに2つのサブネットプールを追加します（の[Number of Routers Per Region]フィールドに5ー8を入力した場合）。15.d （57 ページ）

次に例を示します。

- 前のページで選択したホームリージョンのみがあり、ホームリージョンにCSRが展開されているとします。Cloud APICCloud APIC2つのサブネットプール（自動的に入力されるシステム内部サブネットプールと、自分で作成した1つの追加サブネットプール）が必要です。
- 次に、前のページで管理対象として2つの追加のリージョンを選択し、両方の追加のリージョンにCSRが展開されているとします。Cloud APICさらに、[Number of Routers Per Region]フィールド（）で、各管理対象リージョンに展開する2ー4のCSRを選択するとします。15.d （57 ページ）この場合、合計4つのサブネットプール（1つはシステム内部として自動的に入力され、もう1つはシステム作成されます）。
- 最後に、各管理対象リージョンのCSRの数を後日8に増やし、このページに戻り、[リージョンあたりのルータ数（Number of Routers Per Region）]フィールド（）の値を8に変更するとします。15.d （57 ページ）前の画面で3つのリージョン（ホームリージョンと管理対象として選択した2つの追加リージョン）があり、管理対象リージョンあたりのCSRの数が4を超えているため、3つのサブネットプールを追加する必要があります。ここでも、4つ以上のCSRがある管理対象リージョンごとに1つ、合計7つのサブネットプールがあります。Cloud APICCloud APIC
  - 1つはシステム内部として自動的に入力されます。
  - ホームリージョンのCSR用に2つ（以前に作成したサブネットプールと、管理対象リージョンごとにCSRの数を8に増やしたときにもう1つ作成）
  - 管理対象として選択した2つの追加リージョンのCSRに4つ（以前に作成した2つのサブネットプールと、管理対象リージョンごとにCSRの数を8に増やしたときに作成した他の2つ）Cloud APIC

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

b) [CSR]領域の[BGP Autonomous System Number for CSRs]フィールドに、このサイトに固有のBGP自律システム番号（ASN）を入力します。

BGP自律システム番号は1ー65534の範囲で指定できます。

次のMicrosoft Azure ASNの制限に注意してください。

- このフィールドでは、自律システム番号として64518を使用しないでください。
- 32ビットASNは使用しないでください。Azure VPNゲートウェイは、現時点で16ビットASNをサポートしています。
- 次のASNは、内部ピアリングと外部ピアリングの両方のためにAzureによって予約されています。
  - Public ASNs：8074、8075、12076
  - Private ASNs：65515、65517、65518、65519、65520

  Azure VPNゲートウェイに接続するときに、オンプレミスVPNデバイスにこれらのASNを指定することはできません。
- 次のASNはIANAによって予約されており、Azure VPNゲートウェイで設定できません。23456、64496-64511、65535-65551、429496729http://www.iana.org/assignments/iana-as-numbers-special-registry/iana-as-numbers-special-registry.xhtml

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

CSR インターフェイス IP アドレスは次の目的で使用されます。

- GUIの管理インターフェイスを使用してCSRを設定できます。Cloud APIC
- マルチクラウドおよびハイブリッドクラウド接続のために、サイト全体のインターフェイスをクロスプログラムできます。 ACI マルチサイト オーケストレータ
- コントロールプレーントラフィックとデータプレーントラフィックの両方のCSR

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。つまり、パブリックIPアドレスをCSRに割り当てることができます。

- パブリックIPアドレスをCSR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アドレスをCSRに割り当てるには、[有効（Enabled）]の横にあるチェックボックスをオフにします。

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

（注） リリース5.1（2）以降では、CSR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、[Cloud Resources]領域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。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

d) [Number of Routers Per Region]フィールドで、各リージョンで使用するCiscoクラウドサービスルータ（CSR）の数を選択します。

リージョンごとのCSR数の制限の詳細については、を参照してください。サイト、リージョン、および CSR の数の制限について （44 ページ）

e) [Username]に、Cisco Cloud Services Routerのユーザ名を入力します。

（注） Azureクラウドサイトに接続する場合は、Ciscoクラウドサービスルータのユーザ名としてadminを使用しないでください。

f) **[Password]** に、Cisco Cloud Services Router のパスワードを入力します。

[Confirm Password] フィールドに、もう一度パスワードを入力します。

g) [Throughput of the routers]フィールドで、Cisco Cloud Services Routerのスループットを選択します。

このフィールドの値を変更すると、展開されるCSRインスタンスのサイズが変更されます。スループットの値を高くすると、導入されるVMのサイズが大きくなります。

次の点に注意してください。

- CSRのライセンスは、この設定に基づきます。準拠するには、Smartアカウントに同等以上のライセンスが必要です。詳細については、「Azure パブリック クラウドの要件 （16 ページ）」を参照してください。
- 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クレデンシャルを変更する前に、すべてのリージョンから展開解除する必要があります。

  将来のある時点でこの値を変更する場合は、CSRを削除してから、この章のプロセスを再度繰り返し、同じ[ルータのスループット（Throughput of the routers）]フィールドで新しい値を選択する必要があります。

h) 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。

リリース5.0（2i）以降では、TCP MSSオプションを使用してTCP最大セグメントサイズ（MSS）を設定できます。この値は、データギガビットイーサネットインターフェイス、クラウドルータのIPSecトンネルインターフェイス、およびクラウド、オンプレミス、またはその他のクラウドサイトに対するVPNトンネルインターフェイスを含む、すべてのクラウドルータ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。

i) [License Token]フィールドに、Cisco Cloud Services Routerのライセンストークンを入力します。

これは、シスコスマートソフトウェアライセンシングアカウントからの製品インスタンス登録トークンです。このライセンストークンを取得するには、に移動し、[Smart Software Licensing Inventory Virtual Account]に移動して、製品インスタンス登録トークンを見つけます。http://software.cisco.com>>詳細については、「Cisco Cloud APIC ライセンス （12 ページ）」を参照してください。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

（注） プライベートIPアドレスをにCSRに割り当てた場合、プライベートIPアドレスを使用してCSR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。15.c （56 ページ） 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 16 サイト間接続を設定するかどうかに応じて、適切なボタンをクリックします。

- サイト間接続を設定しない場合（[リージョン管理（Region Management）]ページで管理するリージョンを選択したときに[サイト間接続（Inter-Site Connectivity）]を選択しなかった場合）、[保存して続行（Save and Continue）]をクリックします。[Let's Configure the Basics] ページが再度表示されます。ステップ 22 （59 ページ） にスキップします。
- サイト間接続を設定する場合（[リージョン管理（Region Management）]ページで管理するリージョンを選択したときに[サイト間接続（Inter-Site Connectivity）]を選択した場合）、ページの下部にある[次へ（Next）]をクリックします。[サイト間接続（Inter-Site Connectivity）] ページが表示されます。

ステップ 17 [サイト間接続（Inter-Site Connectivity）]ページに次の情報を入力します。

- IPSec Tunnels to Inter-Site Routers：このフィールドは、クラウドサイトへのオンプレミス接続にのみ必要です。オンプレミスサイトがない場合は、このフィールドに情報を入力する必要はありません。

  この領域で、[Add Public IP of IPsec Tunnel Peer]フィールドの横にある[+]ボタンをクリックします。

  - オンプレミスデバイスへのIPsecトンネル終端のピアIPアドレスを入力します。
  - このピアIPアドレスを追加するには、チェックマークをクリックします。

- OSPF Area for Inter-Site Connectivity：オンプレミスISNピアリングで使用されるアンダーレイOSPFエリアIDを入力します（0.0.0.1など）。
- [External Subnets for Inter-Site Connectivity]見出しの下で、[+ Add External Subnet]フィールドの横にある[+]ボタンをクリックします。
  - Azureで使用されるサブネットトンネルエンドポイントプール（クラウドTEP）を入力します。これは、/ 16ー/ 22のマスクを持つ有効なIPv4サブネットである必要があります（30.29.0.0/16など）。このサブネットは、オンプレミス接続に使用されるクラウドルータのIPsecトンネルインターフェイスおよびループバックに対処するために使用され、他のオンプレミスTEPプールと重複することはできません。
  - 適切なサブネットプールに入力したら、チェックマークをクリックします。

ステップ 18 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 19 [Cloud Resource Naming mode]を選択します。

リリース5.0（2）以降、クラウドAPIC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、クラウドAPIC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

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

則を定義できます。命名規則、使用可能なオブジェクト名変数、ガイドライン、および制限事項の詳細については、この章の前の項を参照してください。クラウドリソースの命名 （46 ページ）

次のいずれかを選択できます。

- デフォルト。Azureのクラウドapicによって作成されたクラウドリソースには、ACIオブジェクトの名前から派生した名前が割り当てられます。たとえば、リソースグループの名前はテナント、VRF、およびリージョンに基づいて作成されます。CAPIC_<tenant> _<vrf> _<region> 。
- [カスタム（Custom）]：各クラウドリソースの命名方法について独自のルールを定義できます。

  カスタム命名を選択すると、各クラウドリソースの横に[編集（Edit）]アイコンが表示されます。編集アイコンをクリックして、表示される1つ以上のリソースの命名規則を定義できます。

  このタイプのリソースで使用可能な変数は、命名規則テキストボックスの下に表示されます。変数は必須キーワードとオプションキーワードに分かれています。更新するルールの必須キーワードをすべて含める必要があります。たとえば、Azureのリソースグループの命名ルールを定義する場合は、テナント名、VRF名、および地域キーワードを含める必要があります。

ステップ 20 グローバルリソース命名ポリシーを確認し、受け入れたことを確認します。

クラウドリソースが作成されると、その名前は変更できません。したがって、クラウドリソースを展開する前に、前の手順で定義したグローバル名前付けポリシーを確認して受け入れる必要があります。準備ができたら、[これらの命名規則に基づいてクラウドリソースを展開する（Deploy cloud resources based on these rules）]チェックボックスをオンにします。

チェックボックスをオフのままにして続行することもできます。この場合、変更は保存されますが、設定は展開されません。展開する命名ポリシーを受け入れるには、この画面に戻る必要があります。

ステップ 21 このページに必要な情報をすべて入力したら、ページの下部にある[保存して続行（Save and Continue）]をクリックします。

[Let's Configure the Basics] ページが再度表示されます。

ステップ 22 [Smart Licensing]行で、[Register]をクリックします。

[Smart Licensing] ページが表示されます。

ステップ 23 [Smart Licensing]ページに必要な情報を入力します。

シスコのスマートライセンスは、複数のシスコ製品間でソフトウェアライセンスを管理する統合ライセンス管理システムです。お使いのCloud APICをシスコのスマートライセンスに登録するには、以下のようにします。

- 製品がインターネットにアクセスできること、またはネットワーク上にインストールされた Smart Software Manager サテライトにアクセスできることを確認してください。
- スマート アカウントにログインします。
  - Smart Software Manager: https://software.cisco.com/
  - Smart Software Manager サテライト: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

- この製品インスタンスで使用するライセンスが含まれている仮想アカウントに移動します。
- 製品インスタンスの登録トークン（これによりスマートアカウントを識別）を生成し、そのトークンをコピーするか、または保存します。

スマート ソフトウェア ライセンシングの詳細については、https://www.cisco.com/go/smartlicensing を参照してください。

ステップ 24 このページで必要なライセンス情報を入力した場合はページの下部にある[登録（Register）]をクリックします。代わりに評価モードで続行する場合は[評価モードで続行（Continue in Evaluation Mode）]をクリックします。

[概要（Summary）] ページが表示されます。

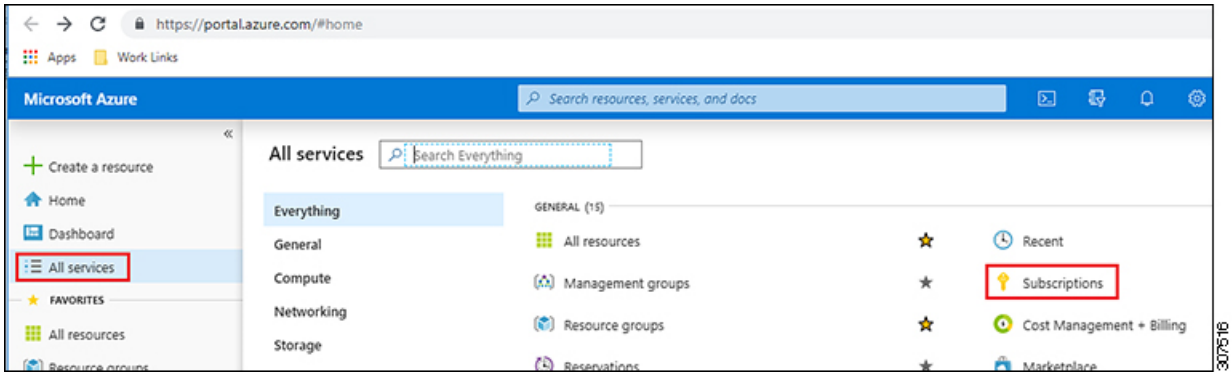
ステップ 25 [Summary]ページで情報を確認し、[Finish]をクリックします。

この時点で、の内部ネットワーク接続の設定は完了です。Cloud APIC

を初めて展開する場合は、このプロセスが正常に完了するまでにかなりの時間（30分程度）がかかることがあります。Cloud APIC

ステップ 26 CSRが正常に展開されたことを確認します。

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 **[すべてのサービス（All services）]** リンクをクリックし、**[サブスクリプション（Subscriptions）]** リンクをクリックします。



b) Azure管理ポータルの **[サブスクリプション（Subscriptions）]** ページで、作成したサブスクリプションアカウントをクリックします。

そのサブスクリプションの概要情報が表示されます。

c) そのサブスクリプションの概要ページで、左側のナビゲーションバーにある **[リソースグループ（Resource groups）]** リンクを見つけ、そのリンクをクリックします。

そのサブスクリプションのリソースグループが表示されます。

d) [カスタム導入（Custom deployment）]ページで選択または作成したリソースグループを選択します。Azure でのクラウド APIC の導入 （32 ページ）

そのリソースグループの概要情報が表示されます。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

e) リソースグループの概要ページで、CSR VMインスタンス（[TYPE]列の下に[Virtual machine]と表示）を見つけ、そのVMインスタンスのリンクをクリックします。

CSR VMインスタンスには、ct_routerp_ region_x _0形式の名前が付けられます。ここで、

- regionは管理対象リージョンです（たとえば、westus、westus2、centralus、またはeastus）。
- xは、ゼロから始まるCSRカウントです。

例：ct_routerp_centralus_0_0またはct_routerp_centralus_1_0

CSR VMインスタンスの概要情報が表示されます。

f) ページの左上にある[ステータス（Status）]フィールドを見つけます。

- [ステータス（Status）]フィールドに[作成中（Creating）]というテキストが表示される場合は、CSRがまだ完全に展開されていません。
- [ステータス（Status）]フィールドに[実行中（Running）]というテキストが表示された場合は、CSRが完全に展開されています。

次のタスク

Cisco Cloud APICサイトとともに追加のサイトを管理するかどうかを決定します。

- Cisco Cloud APICサイトとともに追加のサイト（オンプレミスサイトまたはクラウドサイト）を管理する場合（[リージョン管理（Region Management）]ページで[サイト間接続（Inter-Site Connectivity）]オプションを選択した場合）。Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 （63 ページ）
- クラウドファースト設定をセットアップする場合は、Cisco Cloud APICサイトとともに他のサイトも管理しません（[リージョン管理（Region Management）]ページで[クラウドルータ（Cloud Routers）]オプションのみを選択した場合）。追加設定用のマルチサイト。ただし、この場合、Cisco Cloud APIC GUIで追加の設定を実行する必要があります。

  また、の手順に従って、Cisco Cloud APIC GUIを使用してテナントを作成する必要もあります。Cisco Cloud APIC GUIを使用したテナントの作成 （86 ページ）

  Cisco Cloud APIC GUIの[Global Create]オプションを使用して、次のコンポーネントを設定します。

  - テナント
  - アプリケーション プロファイル
  - EPG

  詳細については、「Cisco Cloud APIC GUI の操作 （85 ページ）」と「Cisco Cloud APIC コンポーネントの設定 （86 ページ）」を参照してください。

Cisco Cloud APIC セットアップ ウィザードの設定の確認

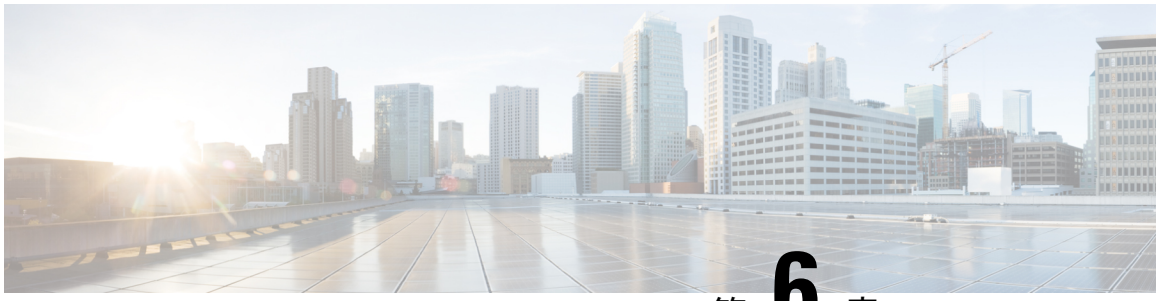
このトピックの手順を使用して、 Cloud APIC セットアップ ウィザードに入力した設定情報が正しく適用されていることを確認します。

Cisco Cloud APICで、次の設定を確認します。

- [Cloud Resources]で、[Regions]をクリックし、選択したリージョンが[Admin State]列に管理対象として表示されていることを確認します。
- [Infrastructure]で[Inter-Region Connectivity]をクリックし、この画面の情報が正しいことを確認します。
- [Infrastructure]で、[Inter-Site Connectivity]をクリックし、この画面の情報が正しいことを確認します。
- [ダッシュボード (Dashboard)] をクリックし、オンプレミス接続ステータスおよびリージョン間接続ステータス ボックスの情報を使用してセットアップ ウィザードとトンネル設定が適切であることを確認します。

次のタスク

に示す手順を使用して、マルチサイト設定を完了します。Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 （63 ページ）



第 6 章

Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理

Cisco Cloud APIC と Cisco ACI マルチサイトについて

セットアップウィザードを使用して Cisco Cloud APIC を設定するときに **[サイト間接続 (Inter-Site Connectivity)]** オプションを **[リージョン管理 (Region Management)]** ページで選択した場合は、Cisco ACI マルチサイトを使用して、オンプレミス サイトやクラウド サイトなどの別のサイトを、Cisco Cloud APIC サイトとともに管理します。Cisco Cloud APIC のセットアップウィザードで、**[クラウド ルータ (Cloud Routesr)]** オプションだけを **[リージョン管理 (Region Management)]** ページで選択した場合は、Cisco ACI マルチサイトは必要ありません。

Cisco Cloud APIC の管理専用に使用される、いくつかの新しいページが ACI マルチサイト オーケストレータに導入されています。この章のトピックでは、これらの新しい Cisco Cloud APIC 管理ページについて説明します。これらの Cisco Cloud APIC 管理ページに必要な情報を入力すると、Cisco Cloud APIC は、実質的に、Cisco ACI マルチサイトを介して管理する別のサイトになります。

Cisco Cloud APIC サイトとともにオンプレミス サイトを管理している場合は、まだ設定していなければ、これらの手順を開始する前にオンプレミス サイトを設定しておくことを推奨します。これらの手順については、次の URL にある *CISCO ACI Multi Site Orchestrator Installation And Upgrade Guide* を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Cisco ACI マルチサイトへの Cisco Cloud APIC サイトの追加

ステップ 1 まだログインしていない場合は、ACI マルチサイト オーケストレータ にログインします。

ステップ 2 メイン メニューで **[サイト]** をクリックします。

ステップ 3 **[サイト リスト]** ページで、**[サイトの追加 (ADD SITE)]** をクリックします。

ステップ 4 **[接続設定]** ページで、次の操作を実行します。

a) **[名前 (NAME)]** フィールドに、サイト名を入力します。

たとえば、`cloudsite1`です。

b) （任意） **[ラベル (LABELS)]** フィールドで、ラベルを選択するか作成します。

c) **[APIC CONTROLLER URL]** フィールドに、Cloud APIC の URL を入力します。これは、Azure によって割り当てられるパブリック IP アドレスです。これは、セットアップ ウィザードを使用してCloud APIC設定Cisco Cloud APICする手順の開始時ににログインするために使用したのと同じパブリック IP アドレスです。

たとえば、`https://192.0.2.1`です。

d) **[ユーザ名 (USERNAME)]**フィールドにユーザ名を入力します。

たとえば、`admin`とします。`admin`と同じ権限を持つ任意のアカウントに登録することもできます。

e) **[パスワード (PASSWORD)]** フィールドに、パスワードを入力します。

f) このフィールドが自動的に入力されていない場合は、**[APIC SITE ID]** フィールドに、一意のサイト ID を入力します。

サイト ID は、Cloud APIC サイトの固有識別子である必要があります。範囲は 1 ～ 127 です。

g) **[保存 (SAVE)]** をクリックします。

ステップ 5 Cloud APIC サイトが正しく追加されたことを確認します。

複数のサイトを管理している場合は、ACI マルチサイト オーケストレータ の [サイト (Sites)] 画面にすべてのサイトを表示する必要があります。ACI マルチサイト オーケストレータ は、サイトがオンプレミスであるか、Cloud APIC サイトであるかを自動的に検出します。

次のタスク

[サイト間インフラストラクチャの設定（Configuring the Intersite Infrastructure）] セクションに移動します。

サイト間インフラストラクチャの設定

ステップ 1 **[サイト (Sites)]** ビューで、**[インフラの構築 (CONFIGURE INFRA)]** をクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

ステップ 2 左側のペインの **[サイト (SITES)]** の下で、クラウド サイトをクリックします。

クラウドサイト領域のほとんどすべての情報は自動的に入力され、次のステップで説明する [BGP パスワード (BGP Password)] フィールドを除き、変更できません。

ステップ 3 オンプレミス サイトとクラウド サイト間でパスワードを設定するかどうかを決定します。

- オンプレミス サイトとクラウド サイトの間でパスワードを設定しない場合は、ステップ 4 （65 ページ）に進みます。
- オンプレミス サイトとクラウド サイト間でパスワードを設定するには、次のようにします。

a) 右側のペインで、**[BGP パスワード (BGP password)]** フィールドをクリックして、パスワードを入力します。

b) [CloudSite] ウィンドウの右上隅にある [更新 (Refresh)] アイコンをクリックします。

すべてのクラウド プロパティは、 Cloud APICから自動的に取得されます。サイトが正常に更新されたことを示すメッセージが表示され、すべてのクラウドプロパティが Cloud APIC から正常に取得されたことを確認します。

ステップ 4 クラウド サイトでマルチサイト接続を有効にするには、 **[ACI マルチサイト (ACI Multi-Site)]**ボタンをクリックします。

ステップ 5 サイト間インフラストラクチャを設定するために使用する展開のタイプを選択します。

画面の右上にある **[展開 (Deploy)]** ボタンをクリックすると、次のスクロールダウンメニューオプションが表示されます。

- **[展開のみ (Deploy Only):]** マルチクラウド (クラウドサイトからクラウドサイト) への接続を設定する場合は、このオプションを選択します。

  このオプションは、クラウドサイトとCloud APICサイトに設定をプッシュし、クラウド サイト間のエンドツーエンド インターコネクト接続を有効にします。

- **[展開 & IPN デバイス設定ファイルをダウンロード (Deploy & Download IPN Device config files:):]** オンプレミスの APIC サイトと Cloud APIC サイトの両方に設定をプッシュし、オンプレミスとクラウド サイト間のエンドツーエンド インターコネクト接続を有効にします。さらに、このオプションでは、Azure に導入された Cisco クラウド サービス ルータ（CSR）とオンプレミスの IPsec 終端 デバイスとの間の接続を有効にするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一

部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[IPN デバイス設定ファイルのみをダウンロード (Download IPN Device config files only):]** Azure に展開された CSR とオンプレミスの IPsec 終端デバイス間の接続を有効にするために使用する、設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

Cisco Cloud APIC と ISN デバイス間の接続の有効化

（注） このセクションの手順は、オンプレミス サイトとクラウド サイト間の接続を有効にしている場合にのみ実行してください。オンプレミスサイトがない場合は、これらの手順をスキップして、 Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成 （70 ページ） に進みます。

Azure に展開された Cisco Cloud Services Router（CSR）とオンプレミスの IPsec ターミネーション デバイス間の接続を手動で有効にするには、次の手順に従います。

デフォルトでは、Cisco Cloud APIC は冗長 CSR のペアを展開します。このセクションの手順では、2 つのトンネルを作成します。1 つはオンプレミスの IPsec デバイスからこれらの各 CSR に対する IPsec トンネルです。

次の情報は、オンプレミスの IPsec ターミネーション デバイスとして CSR のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

ステップ 1 Azure に導入された Csr とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な必要な情報を収集します。

- サイト間インフラストラクチャの設定 （65 ページ）で示されている手順の一部として ACI マルチサイト オーケストレータで、**IPN デバイス設定ファイルを展開してダウンロードする**か、**IPN デバイス設定ファイルのみをダウンロードする**ように選択した場合、ISN デバイスの設定ファイルが含まれている zip ファイルを見つけます。
- Azure に展開された CSR とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な情報を手動で検索する場合は、『*Cisco Cloud APIC* インストール ガイド』の付録で説明されているように、CSR とテナントの情報を収集します。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CSR のトンネルを設定します。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、最初の CSR の設定情報を見つけて、その設定情報を入力します。

次に、最初の CSR の設定情報がどのように表示されるかの例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<first-CSR-tunnel-ID>
    pre-shared-key address <first-CSR-elastic-IP-address> key <first-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<first-CSR-tunnel-ID>
    local-address <interface>
    match identity address <first-CSR-elastic-IP-address>
    keyring infra:overlay-1-<first-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<first-CSR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <first-CSR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <first-CSR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
exit
```

それぞれの説明は次のとおりです。

- <first-CSR-tunnel-ID> は、このトンネルに割り当てる一意のトンネル ID です。
- <first-CSR-tunnel-ID> は、最初の CSR の3番目のネットワーク インターフェイスの柔軟な IP アドレスです。
- <first-CSR-preshared-key> は、最初の CSR の事前共有キーです。
- <interface>は、Azureに導入されたCSRへの接続に使用されるインターフェイスです。
- <peer-tunnel-for-onprem-IPsec-to-first-CSR> は、最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。

- <process-id> は OSPF プロセス ID です。
- <area-id> は、OSPF エリア ID です。

次に例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1000
    pre-shared-key address 192.0.2.20 key 12345678900987654321234567890
exit

crypto isakmp profile infra:overlay-1-1000
    local-address GigabitEthernet1
    match identity address 192.0.2.20
    keyring infra:overlay-1-1000
exit

crypto ipsec transform-set infra:overlay-1-1000 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1000
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel 1000
    ip address 30.29.1.2 255.255.255.252
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.20
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-1000
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit
```

ステップ 4 *2* 番目の CSR のトンネルを設定します。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、2 番目の CSR の設定情報を見つけて、その設定情報を入力します。

次に、2 番目の CSR の設定情報がどのように見えるかの例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
```

```
    hash sha
exit

crypto keyring infra:overlay-1-<second-CSR-tunnel-ID>
    pre-shared-key address <second-CSR-elastic-IP-address> key <second-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<second-CSR-tunnel-ID>
    local-address <interface>
    match identity address <second-CSR-elastic-IP-address>
    keyring infra:overlay-1-<second-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<second-CSR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <second-CSR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-second-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <second-CSR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
exit
```

次に例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1001
    pre-shared-key address 192.0.2.21 key 12345678900987654321234567891
exit

crypto isakmp profile infra:overlay-1-1001
    local-address GigabitEthernet1
    match identity address 192.0.2.21
    keyring infra:overlay-1-1001
exit

crypto ipsec transform-set infra:overlay-1-1001 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1001
    set pfs group2
```

```
    set security-association lifetime seconds 86400
exit

interface tunnel 1001
    ip address 30.29.1.6 255.255.255.252
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.21
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-1001
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit
```

ステップ 5 設定する必要があるその他の CSR について、これらの手順を繰り返します。

ステップ 6 オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

次に例を示します。

```
ISN_CSR# show ip interface brief | include Tunnel
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1000             30.29.1.2       YES manual up                    up
Tunnel1001             30.29.1.4       YES manual up                    up
```

両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

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

セキュリティドメインは、追加するセキュリティドメインにテナントを制限します。セキュリティドメインを追加しない場合、すべてのセキュリティドメインがこのテナントにアクセスできます。の手順を使用して共有テナントを設定する場合は、これらのセキュリティドメインを選択できます。テナントの設定 （71 ページ）

このセクションでは、クラウドAPIC 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 クラウドAPICシステムにログインします。

ステップ 2 **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 3 [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 4 [Intent]メニューの[Administrative]リストで、[Create Security Domain]をクリックします。**[セキュリティ ドメインの作成（Create Security Domain）]** ダイアログ ボックスが表示されます。

ステップ 5 **[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 6 **[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 7 設定が終わったら **[保存（Save）]** をクリックします。

テナントの設定

オンプレミスサイトと Cloud APIC イト間で共有されるテナントを設定するには、この項の手順に従います。AzureサブスクリプションタイプとクラウドAPICテナントの関係の詳細については、テナント、ID、およびサブスクリプションについて （9 ページ） を参照してください。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左側のナビゲーションメニューで、[Tenants]をクリックします。

ステップ 3 メイン ペインで、**[テナントの追加(Add Tenants）]** をクリックします。

ステップ 4 **[テナントの追加（Add Tenant）]** ウィンドウで、テナントの名前を入力します。

テナントの説明を入力することもできます。

ステップ 5 テナントをオンプレミスサイトに展開する必要がある場合は、[関連付けられたサイト（Associated Sites）]領域の横にあるチェックボックスをオンにしてオンプレミスサイトを選択します。

（オプション）サイトのドロップダウンリストからセキュリティドメインを選択することもできます。

ステップ 6 Azureクラウドサイトをテナントに追加するには、[関連付けられたサイト（Associated Sites）]領域の横にあるチェックボックスをオンにして、Azureクラウドサイトを選択します。

Azureクラウドサイトをテナントに関連付ける場合は、Azureサブスクリプション情報も提供する必要があります。

ステップ 7 Azureサイトを確認したら、ドロップダウンリストからセキュリティドメインを選択し（該当する場合）、その横にある[アカウントの関連付け（Associate Account）]をクリックします。

ステップ 8 Azureアカウントのモードを選択します。

- テナントを新しいAzureサブスクリプションに関連付ける場合は、[Mode：Create Own]を選択し、次のフィールドに情報を入力します。

  1. [Azure Subscription ID]フィールドに、AzureサブスクリプションのIDを入力します。

     Azureアカウントにログインし、ホームサブスクリプションに移動することで、サブスクリプションIDを取得できます。＞Azureポータルにリストされているサブスクリプション名ではなく、サブスクリプションIDを使用する必要があります。

2. （オプション）このセキュリティアカウントを他のセキュリティドメインと共有する場合は、[セキュリティドメイン（Security Domain）]フィールドでクラウドアカウントの下のセキュリティドメインを選択します。

   詳細については、「Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成 （70 ページ）」を参照してください。

3. [Access Type]フィールドで、VMとテナント間のアクセスタイプを選択します。Cloud APIC

   （注） リリース5.2（1）より前のリリースでは、管理対象アイデンティティのみがインフラテナントのアクセスタイプとしてサポートされ、管理対象アイデンティティと管理対象外アイデンティティ/サービスプリンシパルの両方がユーザテナントのアクセスタイプとしてサポートされていました。アンマネージドアイデンティティ/サービスプリンシパルは、リリース5.2（1）より前のリリースのインフラテナントのアクセスタイプとしてサポートされていませんでした。

   リリース5.2（1）以降、マネージドアイデンティティとアンマネージドアイデンティティ/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るようになりました。

   - 特定のアプリケーションを介してクラウドリソースを管理するには、[Unmanaged Identity]を選択します。

     これは、異なるサブスクリプションでテナントを設定する場合に使用できます。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。

     この場合、アプリケーションのクレデンシャルもに提供する必要があります。Cloud APICの手順の最後に保存した情報を参照してください。Azure でのアプリケーションの作成 （27 ページ）

     - アプリケーションID：Azureアプリケーションのアプリケーション IDを入力します。このIDは、ホームアプリケーション登録にリストされます。<application-name> [アプリケーション（クライアント）ID（Application（client）ID）]フィールドに入力します。＞＞

     - [Client Secret]：アプリケーションシークレットを入力します。ホームアプリケーションの登録でシークレットを作成できます。<application-name> Certificates & secrets新しいクライアントシークレット。＞＞＞＞

     - Azure Active Directory ID：Azureアプリケーションのアプリケーションディレクトリ ID を入力します。このIDは、ホームアプリケーション登録にリストされます。<application-name>、[Directory（tenant）ID]フィールドに入力します。＞＞

     （注） この場合、アプリケーションのロール割り当ても追加する必要があります。これらの手順については、アプリへのロール割り当ての追加 （39 ページ） を参照してください。

   - [Managed Identity]を選択して、VMがクラウドリソースを管理できるようにします。Cloud APIC

これは、Azureサブスクリプションが（同じ組織の）同じディレクトリにある場合に使用できます。

（注） この場合、VMのロール割り当ても追加する必要があります。これらの手順については、仮想マシンへのロール割り当ての追加 （37 ページ） を参照してください。

- [モードの選択（Choose Mode）]：既存のテナントと共有されている既存のサブスクリプションを使用する場合は、[共有（Shared）]を選択します。

  Azureでは、同じサブスクリプションを使用して複数のテナントを作成できます。

  [共有の選択（Select Shared）]を選択した場合は、ドロップダウンリストからクラウドアカウントを選択できます。ドロップダウンリストで使用可能なクラウドアカウントは、選択したセキュリティドメインに基づいています。ステップ 7 （71 ページ） 新しいテナントは、選択したアカウントと同じAzureサブスクリプションに関連付けられます。

  （注） セキュリティドメインを設定した場合は、選択したクラウドアカウントが、テナント用に選択したものと同じセキュリティドメインと共有されている必要があります。同じAzureサブスクリプションを共有するすべてのテナントは、同じセキュリティドメインに存在する必要があります。

ステップ 9 必要に応じて、[Associated Users]領域で、テナントにアクセスできるユーザを選択します。

ステップ 10 (オプション) 整合性チェッカを有効にします。

このテナントのスケジュール済み整合性チェッカを有効にすることもできます。整合性チェックの詳細については、『設定ガイド』を参照してください。*Cisco ACI* マルチサイト

ステップ 11 **[保存（Save）]** をクリックしてテナントを追加します。

次のタスク

スキーマの作成 （73 ページ） に移動してスキーマを作成します。

スキーマの作成

Cisco Cloud APIC に固有ではない一般的な Cisco ACI Multi-Site 手順がいくつかありますが、Cisco ACI Multi-Site を介してオンプレミスサイトと Cisco Cloud APIC サイトを管理している場合は Cisco Cloud APIC の全体的なセットアップの一部として実行する必要があります。ここでは、APIC の Cisco Cloud 全体的なセットアップの一部である Cisco ACI Multi-Site の一般的な手順について説明します。

Cisco Cloud APIC サイトの新しいスキーマを作成する場合は、この項の手順に従ってください。

Cisco Cloud APIC サイトに使用するスキーマがすでにある場合は、これらの手順をスキップして、サイトをスキーマに追加する （77 ページ） に移動することができます。

ステップ 1 メイン メニューで **[スキーマ]** をクリックします。

ステップ 2 [スキーマ] ページで、**[スキーマの追加]** をクリックします。

ステップ 3 [無題スキーマ] ページで、ページの上部にあるテキスト 無題スキーマを、作成するスキーマの名前 (たとえば、 `Cloudbursting スキーマ` に置き換えます。

ステップ 4 左側のペインで **[ロール (Roles)]** をクリックします。

ステップ 5 中央のペインで、**スキーマを作成するエリアをクリックしてテナントを選択してください**をクリックしてください。

ステップ 6 **[テナントの選択]** ダイアログ ボックスにアクセスし、ドロップダウン メニューから テナントの設定 （71 ページ） で作成したテナントを選択します。

アプリケーション プロファイルと EPG の設定

この手順では、アプリケーション プロファイルを設定し、2 つの EPG を追加する方法について説明します。1 つはクラウド サイト用、もう 1 つは、プロバイダ コントラクトが 1 つの EPG に関連付けられており、コンシューマ コントラクトが他の EPG に関連付けられている場合です。

ステップ 1 中央のペインで、[アプリケーション プロファイル (Application Profile)] エリアを見つけて、**[+ アプリケーション プロファイル (+ Application profile)]** をクリックします。

ステップ 2 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドにアプリケーション プロファイルの名前を入力します。

ステップ 3 中央のペインで、**[+ EPG の追加 (+ ADD EPG)]** をクリックして、クラウド サイトの EPG を作成します。

ステップ 4 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドに EPG の名前を入力します (たとえば `epg1`)。

ステップ 5 オンプレミス サイトの EPG を作成する場合には、中央のペインで、**[+ EPG の追加 (+ ADD EPG)]** をクリックします。

ステップ 6 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドに EPG の名前を入力します (たとえば `epg2`)。

ステップ 7 VRF を作成します。

a) 中央のペインで、[VRF] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

b) 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドに EPG の名前を入力します (たとえば `vrf1`)。

ステップ 8 **[保存 (SAVE)]** をクリックします。

ブリッジ ドメインの作成と VRF への関連付け

この項の手順に従って、オンプレミス サイトのブリッジ ドメインを作成し、それを VRF に関連付けます。これらの手順は、クラウドのみのスキーマには必要ではないことに注意してください。

ステップ 1 中央のペインで、**[EPG]** まで上にスクロールして戻り、以前にオンプレミス サイト用に作成した EPG をクリックします。

ステップ 2 右側のペインの**[オンプレミス プロパティ (ON-PREM PROPERTIES)]** エリアの **[ブリッジ ドメイン (BRIDGE DOMAIN)]**)] の下で、フィールドに名前を入力し (たとえば、 `bd1`)、**[作成 (create)]** エリアをクリックして新しいブリッジ ドメインを作成します。

ステップ 3 中央のペインで、今作成したブリッジ ドメインをクリックします。

ステップ 4 **[仮想ルーティング/フォワーディング (Virtual Routing & Forwarding)]** フィールドで、アプリケーション プロファイルと EPG の設定 （74 ページ） で作成した VRF を選択します。

ステップ 5 **[サブネット (SUBNETS)]** エリアまで下にスクロールし、 **[GATEEAY (ゲートウェイ)]** 見出しの下の **[サブネット (SUBNET)]** の横にある + をクリックします。

ステップ 6 **[サブネットの追加 (Add Subnet)]** ダイアログで、**[ゲートウェイ IP (Gateway IP)]**アドレスと、追加する予定のサブネットの説明を入力します。このゲートウェイ IP アドレスは、オンプレミスのサブネットのものです。

ステップ 7 **[範囲 (Scope)]** フィールドで、**[外部にアドバタイズ (Advertised Externally)]** を選択します。

ステップ 8 **[保存 (SAVE)]** をクリックします。

コントラクトのフィルタの作成

ステップ 1 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

ステップ 2 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドにフィルタの名前を入力します。

ステップ 3 **[+ 入力(+ Entry)]** をクリックして、**[エントリの追加 (Add Entry)]** ディスプレイ上のスキーマ フィルタについての情報を入力します。

a) **Name** フィールド (**Add Entry** ダイアログ) のスキーマ フィルタ エントリの名前を入力します。

b) オプション。**Description** フィールドにフィルタの説明を入力します。

c) EPG の通信のフィルタ処理を行うために、必要に応じて詳細を入力します。

たとえば、フィルタを通過する HTTPS トラフィックを許可するエントリを追加するには、次のように選択します。

TYPE: IP、IP PROTOCOL: TCP、および DESTINATION PORT RANGE FROM および DESTINATION PORT range TO: https。

d) **[保存 (SAVE)]** をクリックします。

コントラクトの作成

ステップ 1 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

ステップ 2 右側のペインで、**[表示名 (DISPLAY name)]** フィールドにコントラクトの名前を入力します。

ステップ 3 **[範囲 (SCOPE)]** エリアで、VRF の選択をそのままにします。

ステップ 4 **[フィルタ チェーン (FILTER CHAIN)]** エリアで、**[+ フィルタ (+ FILTER)]** をクリックします。

[フィルタ チェーンの追加 (Add Filter Chain)] 画面が表示されます。

ステップ 5 **[名前 (NAME)]** フィールドで、コントラクトのフィルタの作成 （75 ページ） で作成したフィルタを選択します。

ステップ 6 中央のペインで、**[EPG]** までスクロールして戻り、クラウド サイト用に作成した EPG をクリックします。

ステップ 7 右側のペインで、 **[+コントラクト (+ CONTRACT)]** をクリックします。

[コントラクトの追加] 画面が表示されます。

ステップ 8 **[コントラクト (contract)]** フィールドで、この手順で以前に作成したコントラクトを選択します。

ステップ 9 **[タイプ (TYPE)]** フィールドで、**コンシューマ**または**プロバイダ**のいずれかを選択します。

ステップ 10 **[クラウドのプロパティ (CLOUD PROPERTIES)]** エリアまでスクロールし、**[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)]**] エリアで、アプリケーション プロファイルと EPG の設定 （74 ページ） で作成した VRF を選択します。

ステップ 11 **[保存 (SAVE)]** をクリックします。

ステップ 12 中央のペインで、**[EPG]** までスクロールして戻り、オンプレミス サイト用に作成した EPG をクリックします。

ステップ 13 右側のペインで、 **[+コントラクト (+ CONTRACT)]** をクリックします。

[コントラクトの追加] 画面が表示されます。

ステップ 14 **[コントラクト (contract)]** フィールドで、この手順で以前に作成したコントラクトを選択します。

ステップ 15 **[タイプ (TYPE)]** フィールドで、**[コンシューマ (CONSUMER)]** または **[プロバイダ (PROVIDER)]** を選択します。これは、前の EPG に選択しなかったものです

たとえば、最初の EPG に **[プロバイダ (PROVIDER)]** を選択した場合は、2番目の EPG の **[コンシューマ (CONSUMER)]** を選択します。

ステップ 16 **[クラウドのプロパティ (CLOUD PROPERTIES)]** エリアまでスクロールし、**[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)]** エリアで、アプリケーション プロファイルと EPG の設定（74 ページ） で作成したものと同じ VRF を選択します。

サイトをスキーマに追加する

ステップ 1 左側のペインで、**[サイト (Sites)]** の横にある + をクリックします。

ステップ 2 **[サイトの追加 (Add Sites)]** ページで、それぞれの横にあるボックスをオンにして、オンプレミスおよびクラウド サイトをスキーマに追加し、**[保存 (Save)]** をクリックします。

ステップ 3 左側のペインのクラウド サイトの下にあるテンプレートをクリックして、テンプレートのサイト ローカル プロパティを設定します。

ステップ 4 中央のペインで、VRF をクリックします。

ステップ 5 右側のペインの **[サイト ローカル プロパティ (SITE LOCAL PROPERITES)]** 領域で、次の情報を入力します。

a) **[リージョン (region)]** フィールドで、この VRF を導入する Azure リージョンを選択します。

b) **CIDR**フィールドで、**+CIDR** をクリックします。

[クラウド CIDR の追加（ADD CLOUD CIDR）]ダイアログボックスが表示されます。次の情報を入力します。

- **CIDR**: VNET CIDR 情報を入力します。たとえば、`11.11.0.0/16`とします。

  CIDR には、Azure VNET で使用可能になるすべてのサブネットの範囲が含まれています。

  （注） このフィールドに入力した VPC CIDR 情報は、インフラ プール と重複させることはできません。このフィールドに入力した CIDR 情報が、Azure でのクラウド APIC の導入 （32 ページ） の ステップ 6 （34 ページ） の **[インフラ サブネット（Infra Subnet）]** フィールドに入力した インフラ プール情報と重複していないことを確認します。

- **[CIDR タイプ (CIDR TYPE)]**: [プライマリ (Primary)] または [セカンダリ (Secondary)] を選択します。これが最初の CIDR の場合は、CIDR タイプとして [プライマリ (Primary)] を選択します。

- **[サブネット追加 (ADD SUBNETS)]**: サブネット情報を入力し、チェック マークをクリックします。たとえば、`11.11.1.0/24`とします。

  Cisco Cloud APIC の場合、サブネットはサブネット マスク付きの有効なサブネットであり、サブネット マスク付きの IP アドレスではありません。たとえば、11.11.0.0 / 24は有効なサブネットおよびサブネットマスクですが、11.11.0.1はIPアドレスおよびサブネットマスクですが、で使用する有効なサブネットではありません。Cisco Cloud APIC

  （注） VGW専用のサブネットを1つ追加する必要があります。この特定のサブネットに対して[Used by VGW]を選択します。

c) ウィンドウで **[保存 (Save)]** をクリックします。

エンド ポイント セレクタの追加

Cisco Cloud APICでは、クラウドEPGは、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウドEPGは、1つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウドEPGに割り当てるために使用される、エンドポイント セレクタと呼ばれる機能があります。エンドポイント セレクタは、基本的に言って、Cisco ACI によって管理される 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 セレクタ ルールは、そのエンドポイントをクラウドEPGに割り当てます。エンドポイント セレクタは、Cisco ACI で使用可能な属性ベースのマイクロセグメンテーションに似ています。

エンドポイント セレクタは、 Cisco Cloud APIC GUI またはACI マルチサイト オーケストレータ GUI のいずれかを使用して設定できます。2 つの GUI 間で使用可能なオプションにはわずかな違いがありますが、エンドポイントセレクタを追加するための一般的な概念と全体的な手順は、基本的にこの 2 つの間で同じです。

このセクションの手順では、 ACI マルチサイト オーケストレータ GUI を使用してエンドポイント セレクタを設定する方法について説明します。Cisco Cloud APIC GUI を使用したエンドポイント セレクタの設定の詳細については、『*Cisco Cloud APIC User Guide, Release 4.2 (x)*』を参照してください。

ステップ 1 Cisco Cloud APIC のエンドポイント セレクタに使用できる Azure サイトから、必要な情報を収集します。

（注） これらの手順は、最初に Azure でインスタンスを設定してから、その後に Cisco Cloud APIC のエンドポイントセレクタを追加することを前提としています。ただし、最初にCisco Cloud APIC のエンドポイント セレクタを追加してから、これらのエンドポイント セレクタの手順の最後に、この Azure インスタンスの設定手順を実行することもできます。

ステップ 2 ログインしていない場合は、ACI マルチサイト オーケストレータ にログインします。

ステップ 3 左側のペインで、**[スキーマ (schema)]** をクリックし、以前に作成したスキーマを選択します。

ステップ 4 エンドポイント セレクタを作成する方法を決定します。

- 今後追加される、任意のクラウドサイトに適用できるエンドポイントセレクタを作成するには、次の手順を実行します。

  1. 左側のペインで、テンプレートを選択したままにします。

     これらの手順で特定のサイトを選択しないでください。

  2. 中央のペインで、クラウド サイト用に作成した EPG を選択します。

3. 右側のペインの **[クラウドのプロパティ (CLOUD PROPERITES)]** 領域で、**+ ([セレクタ (SELECTORS)]** の横にあるもの) をクリックして、エンドポイント セレクタを設定します。
4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。
5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタのタイプを選択します。

   このように作成されたエンドポイント セレクタの場合、[キー (Key)] フィールドで使用できるオプションは `[EPG]` のみです。
6. ステップ 5 （80 ページ） に進みます。

- このクラウド サイト専用のエンドポイント セレクタを作成するには、次の手順を実行します。

1. 左ペインで、クラウド サイトを選択します。
2. 中央のペインで、クラウド サイト用に作成した EPG を選択します。
3. 右側のペインの **[サイトのローカルのプロパティ (SITE LOCAL PROPERITES)]** 領域の **[セレクタ (SELECTOR)]**領域で、**+ ([セレクタ （SELECTOR)]** の横にあるもの) をクリックして、エンドポイント セレクタを設定します。
4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。

   たとえば、IP サブネット分類のエンドポイント セレクタの場合は、`[IP-Subnet-EPSelector]` などの名前を使用できます。
5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタで使用するキーを選択します。

   - **[IP アドレス (IP Address)]**: IP アドレスまたはサブネットによって選択するために使用されます。エンドポイントセレクタとしてのIPアドレスの値は、CIDRで作成されたユーザサブネットに属します。サイトをスキーマに追加する （77 ページ）

     さらに、特にAzureスケールセットVMの場合、エンドポイントセレクタとしてのIPアドレスの値は、そのスケールセットが存在する場所で設定された完全なサブネットである必要があります。サイトをスキーマに追加する （77 ページ）サブネット内のIPアドレスは使用できません。

     たとえば、AzureスケールセットVMのこれらのフィールドで次の値を使用した場合。

     - CIDR：10.1.0.0/16
     - Subnet：10.1.0.0/24

     エンドポイントセレクタとしてのIPアドレスの有効な値は10.1.0.0/24です。10.1.0.1/32または10.1.0.0/16のエントリは、AzureスケールセットVMのエンドポイントとしてのIPアドレスの有効な値ではありません。

（注） IPv6はAzureではサポートされていません。Cisco Cloud APIC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。

- **[リージョン (Region)]**: エンドポイントの Azure リージョンで選択するために使用されます。
- エンドポイントセレクタのカスタム タグを作成する場合は、**[検索または作成のために入力 (Type to search or create)] フィールド**で入力を開始してカスタム タグまたはラベルを入力し、新しいフィールドで **[作成 (Create)]** をクリックして、新しいカスタム タグまたはラベルを作成します。

  Azure にタグを追加するときに、これらの手順の前の例を使用すると、以前に Azure で追加したロケーション タグと一致するように、このフィールドにカスタム タグのロケーションを作成できます。

ステップ 5 **[演算子 (Operator)]** フィールドで、エンドポイント セレクタに使用する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 (value)] 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 6 **[値 (value)]** フィールドで、2 つ前のフィールドに対して行った選択に基づいて、エンドポイント セレクタに使用する値を選択します。**[値 (Value)]** フィールドには、複数のカンマ区切りのエントリを含めることができます。このフィールドのエントリの間には論理 OR があるものとみなされます。

（注） **[キーを持つ (Has Key)]** または **[キーの不在 (Key Not Exist)]** を選択していない場合には、[演算子 (Operator)] フィールドは表示されません。

たとえば、エンドポイント セレクタに、`westus` など特定の Azure リージョンがある場合には、この画面で次の項目を選択します。

- **[キー (Key):]** Region
- **[演算子 (Operator):]** Equals
- 値：westus

別の例として、これらのフィールドで次の値を使用したとします。

- **[キー (Key):]** IP
- **[演算子 (Operator):]** Has Key

- **[値 (Valuse):]**は、演算子 (Operator)] フィールドで [Has Key] が使用されているため、使用できません。

EPG ルールは、この状況で IP アドレスを持つすべてのエンドポイントに適用されます。

最後の例として、これらのフィールドで次の値を使用したとします。

- **[キー (Key):]** custom tag: Location
- **[演算子 (Operator):]** Has Key
- **[値 (Valuse):]**は、演算子 (Operator)] フィールドで [Has Key] が使用されているため、使用できません。

この場合、EPGルールは、Azureタグキーとして Locationを持つすべてのエンドポイントに、ロケーションの値に関係なく適用されます。

ステップ 7 このエンドポイント セレクタ式の作成が完了したら、チェックマークをクリックします。

ステップ 8 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):]** Region
  - **[演算子 (Operator):]** Equals
  - 値：eastus
- エンドポイント セレクタ1、式 2:
  - **[キー (Key):]** IP
  - **[演算子 (Operator):]** Equals
  - **[値 (Value):]** 192.0.2.1/24

この場合、これらの式の両方が真になる場合 (regionが eastus 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。

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ます。

ステップ 9 このエンドポイント セレクタの式の作成が完了したら、**[保存 (SAVE)]** をクリックします。これは **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** の右下隅にあります。

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

- エンドポイント セレクタ 2、式 1:
  - **[キー (Key):]** Region

- **[演算子 (Operator):]** In
- 値：centralus、eastus2

その場合、次のようになります。

- リージョンが eastus で、IP アドレスが 192.0.2.1/24 サブネットに属している (エンドポイント セレクタ 1 の式)

  または

- リージョンが centralus または eastus2 (エンドポイント セレクタ 2 の式) のいずれかである

その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 10 エンドポイント セレクタの作成が完了したら、右上隅の **[保存 (SAVE)]** をクリックします。

ステップ 11 画面の右上隅にある **[サイトに展開 (DEPLOY TO SITES)]** ボタンをクリックして、スキーマをサイトに展開します。

`[正常に展開 (Successfully Deployed)]` されたというメッセージが表示されます。

次のタスク

Cisco ACI Multi-Site 設定の検証 （82 ページ） の手順を使用して、Cisco ACI マルチサイト エリアが正しく設定されていることを確認します。

Cisco ACI Multi-Site 設定の検証

このトピックの手順を使用して、ACI マルチサイト オーケストレータ に入力した設定が正しく適用されていることを確認します。

ステップ 1 Cloud APIC にログインし、次のことを確認します。

a) [ダッシュボード (Dashboard)] をクリックしサイト間接続ステータスおよびリージョン間接続ステータスボックスの情報を使用して、次のことを確認します。

- トンネルは、Azure 上の Cisco Cloud Services Router 1000V から、オンプレミスの ISN (IPsec ターミネーション ポイント)、およびユーザ VNet の VGW に対して動作しています。
- OSPF ネイバーが Cisco Cloud サービス ルータと ISN オンプレミス デバイスの間で起動していることを示します。
- VRF の BGP EVPN ルートにはクラウドとオンプレミスのルートが表示され、クラウドルートは ACI スパイン スイッチの BGP EVPN を介して入力されます。

b) [アプリケーション管理 (Application Management)] → [テナント] をクリックし、テナントが正しく設定されていることを確認します。

c) [アプリケーション管理(Application Management)]→[アプリケーションプロファイル]をクリックし、アプリケーションプロファイルが正しく設定されていることを確認します。
d) [アプリケーション管理 (Application Management)] → [EPG] をクリックし、EPG が正しく設定されていることを確認します。
e) [アプリケーション管理 (Application Management)] → [コントラクト] をクリックし、契約が正しく設定されていることを確認します。
f) [アプリケーション管理 (Application Management)] → [VRF] をクリックし、VRF が正しく設定されていることを確認します。
g) [アプリケーション管理 (Application Management)] → [クラウド コンテキスト Cloudプロファイル] をクリックし、クラウド コンテキスト プロファイルが正しく設定されていることを確認します。
h) [クラウド リソース (Cloud Resources)] → [リージョン] をクリックし、リージョンが正しく設定されていることを確認します。
i) [クラウド リソース (Cloud Resources)] → [VNETs] をクリックし、VNETs が正しく設定されていることを確認します。
j) [クラウド リソース (Cloud Resources)] → [クラウド エンドポイント] をクリックし、クラウド エンドポイントが正しく設定されていることを確認します。
k) [クラウド リソース (Cloud Resources)] → [ルータ] をクリックし、CSR が正しく設定されていることを確認します。

ステップ 2 オンプレミスの APIC サイトにログインし、APIC のスキーマを確認します。

ACI マルチサイト オーケストレータ で設定した共有テナントが APIC のテナントエリアに表示され、 ACI マルチサイト オーケストレータ スキーマから展開された VRF と EPG がオンプレミス APIC で設定されていることが確認できます。

ステップ 3 コマンドラインから、Azure の Cisco Cloud サービス ルータ 1000V で VRF が 正しく作成されていることを確認します。

show vrf

テナント`t1`と VRF `v1`が ACI マルチサイト オーケストレータ から展開されている場合、CSR の出力は次のようになります。

```
Name                             Default RD            Protocols   Interfaces
t1:v1                            64514:3080192         ipv4        BD1
                                                                   Tu4
                                                                   Tu5
```

ステップ 4 コマンドラインから、Azure サービス ルータ 1000V と ISN オンプレミス デバイスの間 Cisco Cloud でトンネルがアップしていることを確認します。

Azure または ISN オンプレミスのデバイスで、Cisco Cloud サービス ルータ 1000V で次のコマンドを実行できます。

show ip interface brief | inc Tunnel

以下のような出力が表示されます。

```
Interface        IP-Address        OK?        Method        Status        Protocol
Tunnel1          1.2.3.22          YES        manual        up            up
Tunnel2          1.2.3.30          YES        manual        up            up
```

```
Tunnel3          1.2.3.6          YES        manual        up            up
Tunnel4          1.2.3.14         YES        manual        up            up
```

ステップ 5 コマンド ラインから、OSPF ネイバーが Azure 上の Cisco Cloud サービス ルータ 1000V と ISN オンプレミス デバイスの間でアップしていることを確認します。

show ip ospf neighbor

以下のような出力が表示されます。

```
Neighbor ID      Pri              State      Dead Time     Address       Interface
10.200.10.201    0                FULL/ -    00:00:36      1.2.3.13      Tunnel4
20.30.40.50      0                FULL/ -    00:00:36      1.2.3.29      Tunnel2
10.202.101.202   0                FULL/ -    00:00:38      1.2.3.5       Tunnel3
```

ステップ 6 コマンド ラインから、オンプレミスの BGP EVPN ネイバーが Cisco Cloud サービス ルータ 1000V に存在することを確認します。

show bgp l2vpn evpn summary

以下のような出力が表示されます。

```
Neighbor     V     AS    MsgRcvd   MsgSent   TblVer   InQ    OutQ   Up/Down   State/PfxRcd
10.1.1.2     4     100   139       137       99       0      0      01:30:36  6
```

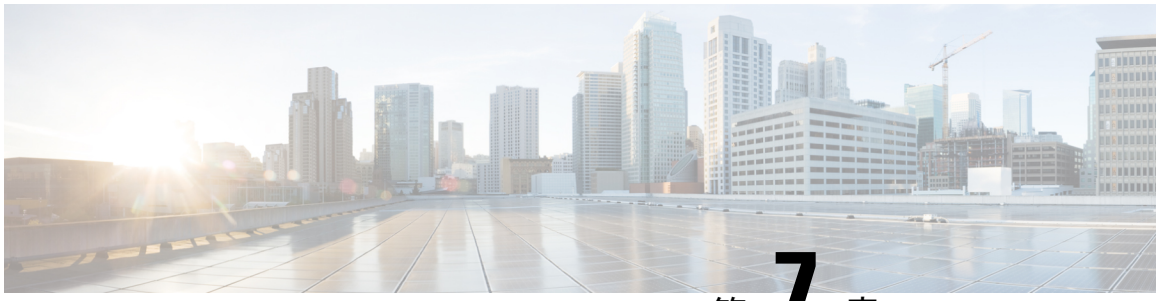
ステップ 7 コマンド ラインから、VRF の BGP ルートにクラウドとオンプレミスの両方のルートが表示されていることを確認します。

（注） 現在 Cloud APIC のワークフローでは、VRF は、対応する VNET が Azure で作成されるまで、Cisco Cloud サービスルータ 1000V で設定されません。

show ip route vrf t1:v1

以下のような出力が表示されます。

```
B     129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1
B     130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```



第 7 章

Cisco Cloud APIC GUI について

Cisco Cloud APIC GUI の操作

インストール後、これを使用してAmazon Web Services（AWS）またはMicrosoft Azureパブリッククラウドに拡張（ACI）ポリシーを適用できます。Cisco Cloud APICCisco Application Centric InfrastructureこれはGUIを使用して行います。Cisco Cloud APIC

GUIでは、テナントを作成し、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（EPG）、コントラクト、フィルタ、およびVRFを設定できます。Cisco Cloud APICトポロジ、設定、およびリソースを表示することもできます。Cisco Cloud APIC

を使用して設定手順を実行します。インテント機能。インテント機能の使用方法については、を参照してください。Cisco Cloud APIC コンポーネントの設定 （86 ページ）また、『Cisco Cloud APIC User Guide』の「Understanding the Cisco Cloud APIC GUIアイコン」の項も参照してください。

の基本的なタスクを実行する手順は、通常の手順とは異なります。Cisco Cloud APICCisco APICただし、テナントの機能、アプリケーションプロファイル、およびその他の要素は同じです。Cisco APIC詳細については、Cisco.com の『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

左側のナビゲーションペインで設定やその他の情報を表示します。[Dashboard]（デフォルトビュー）、[Topology]、[Application Management]、[Cloud Resources]、[Operations]、[Infrastructure]、および[Administrative]を選択できます。

アイコンの詳細については、Cisco.comの『Cisco User Guide』の「Understanding the GUIアイコン」の項を参照してください。Cisco Cloud APIC*Cisco Cloud APIC*

Cisco Cloud APIC GUIを使用したテナントの作成

次の項では、Cisco Cloud APIC GUIを使用してテナントを作成する方法について説明します。

Cisco Cloud APIC コンポーネントの設定

このセクションでは、テナント、アプリケーションプロファイル、およびエンドポイントグループ（EPG）の作成など、主要なタスクの実行の概要について説明します。Cisco Cloud APIC

始める前に

がインストールされている必要があります。Cisco Cloud APICこのガイドの前のインストールの項を参照してください。

ステップ 1 Cisco Cloud APIC にログインします。

ステップ 2 [ダッシュボード（Dashboard）]ペインの右上で、ブルズアイを指す矢印の付いたアイコンをクリックします。

このアイコンは、インテントアイコンまたは機能と呼ばれることがあります。

ステップ 3 [何をしますか。ウィンドウで、検索ウィンドウに用語を入力して、オプションのリストを表示します。

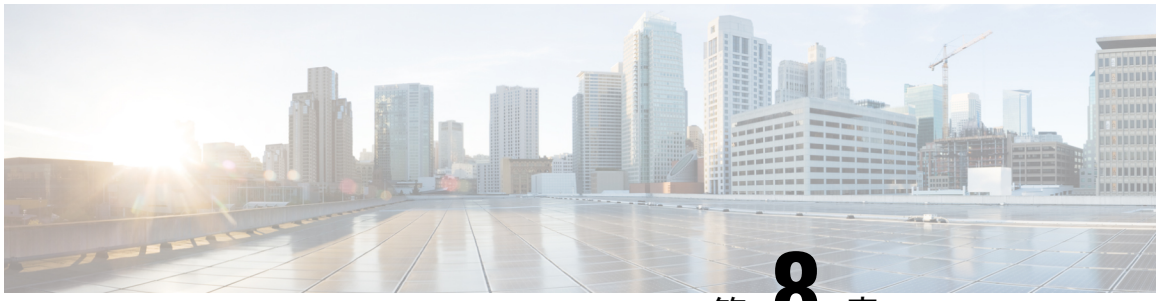
たとえば、テナントを設定する場合は、検索ウィンドウにtenantと入力します。検索は、テナントの作成と設定に関連するタスクのリストを返します。

ステップ 4 タスクをクリックし、開いたウィンドウで設定手順を実行します。

次のタスク

左側のナビゲーションペインで設定を確認できます。[ダッシュボード（Dashboard）]ペインの左上にあるハンバーガーアイコンをクリックして、ペインを展開します。該当する見出しを展開して設定を表示します。

たとえば、テナントを設定した場合は、[アプリケーション管理（Application Management）]を展開し、[テナント（Tenants）]をクリックします。テナントに関する情報が中央の作業ウィンドウに表示されます。



第 8 章

システムのアップグレード、ダウングレード、またはリカバリの実行

ソフトウェアのアップグレード

Cisco Cloud APICソフトウェアをアップグレードする前に、の情報を確認してください。ソフトウェアのアップグレードの前提条件 （88 ページ）

Cisco Cloud APICソフトウェアのアップグレードに使用する方法は、状況によって異なります。

- 5.0（1）より前のリリースからリリース5.1（2）にアップグレードする場合は、移行ベースのプロセスを使用してソフトウェアをアップグレードします。これらの指示については、移行ベースのアップグレード （89 ページ） にアクセスしてください。

  注 で説明したように、アップグレードに使用したのと同じ移行ベースの手順をシステムリカバリにも使用できます。システム リカバリの実行 （115 ページ）

- リリース5.0（1）または5.0（2）からリリース5.1（2）にアップグレードする場合は、ポリシーベースのプロセスを使用してソフトウェアをアップグレードします。これらの指示については、ポリシーベースのアップグレード （105 ページ） にアクセスしてください。

注 リリース5.0（1）または5.0（2）からリリース5.1（2）へのポリシーベースのアップグレードが何らかの理由で機能しない場合は、リリース5.0（1）または5.0（2）からリリース5.1（2）にアップグレードできます。で説明されている移行ベースのプロセスを使用します。移行ベースのアップグレード （89 ページ）

CSRのアップグレード

Cisco Cloud APICソフトウェアのアップグレードに使用する方法に関係なく、クラウドAPICソフトウェアをアップグレードするたびに、クラウドサービスルータ（CSR）もアップグレードする必要があります。

- リリース5.2（1）より前のリリースでは、Cisco Cloud APICのアップグレードをトリガーするたびにCSRが自動的にアップグレードされます。
- リリース5.2（1）以降では、Cisco Cloud APICのアップグレードとは関係なく、CSRのアップグレードをトリガーし、それらのCSRのアップグレードをモニタできます。これは、管理プレーン（Cisco Cloud APIC）とデータプレーン（CSR）のアップグレードを分割できるため、トラフィック損失を削減するのに役立ちます。

詳細については、「クラウドサービスルータのアップグレードのトリガー（115ページ）」を参照してください。

ソフトウェアのアップグレードの前提条件

次に、Cisco Cloud APIC ソフトウェアをアップグレードする前に行う必要がある前提条件を示します。

- Cisco Cloud APIC が Cisco マルチサイト ACI ファブリックの一部であり、シスコ マルチサイト と連携している場合は、Cisco Cloud APIC ソフトウェアをアップグレードする前に、Cisco ACI マルチサイト オーケストレータ ソフトウェアを同等またはそれ以降のリリースにアップグレードする必要があります。つまり、シスコACIマルチサイト オーケストレータ ソフトウェアのリリースは、常にCisco Cloud APIC ソフトウェアのリリース以降である必要があります。
  - シスコ ACI マルチサイト オーケストレータ ソフトウェアのリリース日を確認するには、ソフトウェア ダウンロード サイトの ACI Multi-Site Software に移動し、左側のナビゲーション バーで該当するリリースを選択して、そのリリース日を確認します。
  - Cisco Cloud APIC ソフトウェアのリリース日を確認するには、ソフトウェア ダウンロード サイトの Cloud Application Policy Infrastructure Controller に移動し、左側のナビゲーション バーで該当するリリースを選択して、そのリリース日を確認します。

  たとえば、リリース 5.1(2e) にアップグレードする場合：Cisco Cloud APIC

1. ソフトウェア ダウンロード サイト（この場合は 28-Nov-2020）の Cloud Application Policy Infrastructure Controller の情報を使用して、リリース 5.1(2e) の Cisco Cloud APIC リリース日を確認し、ソフトウェア ダウンロード サイトの ACI Multi-Site Software に移動して、シスコ ACI マルチサイト オーケストレータ ソフトウェアの同等またはそれ以降のリリース（この場合は、マルチサイトリリース3.1(1g)、リリースは2020 年 11 月 28 日）を検索します。
2. 最初に、Cisco ACI マルチサイト オーケストレータ ソフトウェアをマルチサイトリリース 3.1(1g) にアップグレードします。これらの手順については、『Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide、Release 3.1(x)』を参照してください。
3. Cisco ACI マルチサイト オーケストレータ ソフトウェアをアップグレードしたら、このドキュメントの手順に従ってCisco Cloud APICリリース 5.1(2e) Cloud APICにアップグレードします。

- マルチサイトリリース 3.0(2) 以降、Cisco ACI マルチサイト オーケストレータの AV ペア形式は、シングル サインオン（SSO）機能をサポートするために、Cisco APIC で使用される形式と一致するように更新されました。Cisco ACI マルチサイト オーケストレータ ソフトウェアをマルチサイトリリース 3.1(1) 以降にアップグレードする場合は、AV ペア文字列を新しい形式に更新するまで、リモート認証を使用してログインできないことがあります。

  考えられる問題を回避するために、次のように AV ペア文字列の新しい形式を使用して、ACI マルチサイト オーケストレータ の AV ペアおよび APIC ロールを 1 行にまとめることを推奨します。

```
Cisco-AVPair = "shell：domains = all / custom-privilege /、msoall / powerUser /"
```

  詳細については、『Cisco ACI Multi-Site Configuration Guide、Release 3.1(x)』の「Authentication」の章の「Configuring Remote Authentication Server for Orchestrator Users」の項を参照してください。

移行ベースのアップグレード

リリース4.2（4）以前からリリース5.1（2）にアップグレードする場合は、次の手順に従います。この場合、移行ベースのプロセスを使用してソフトウェアをアップグレードします。

このセクションの手順を実行する前に、に記載されている情報を確認してください。ソフトウェアのアップグレードの前提条件 （88 ページ）

（注） アップグレードに使用されるこれらの移行ベースの手順は、で説明されているように、システムリカバリにも使用できます。システム リカバリの実行 （115 ページ）

既存のクラウドAPIC設定情報の収集

ソフトウェアをアップグレードする前に、このトピックの手順に従って特定のフィールドの既存の設定情報を検索し、これらの各フィールドのエントリを書き留めます。Cisco Cloud APIC リリース5.1（2）リカバリテンプレートを使用してをアップグレードする場合は、次の手順の後の手順で、これらのフィールドに同じエントリを使用します。Cisco Cloud APIC

次の各フィールドについて、で実行した元の導入の一部として入力したエントリをメモします。Azure でのクラウド APIC の導入 （32 ページ）

- サブスクリプション （90 ページ）
- リソース グループ （90 ページ）
- ロケーション （91 ページ）
- ファブリック名 （91 ページ）
- 外部サブネット （92 ページ）
- Virtual Machine Name （92 ページ）
- インフラVNETプール （92 ページ）
- ストレージ アカウント名 （93 ページ）

サブスクリプション

1. **[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]** の順に移動します。
2. [Name]列の名前の下にinfraがあるテナントの行を見つけます。
3. [Azure Subscription]列の値をメモします。

   これはのサブスクリプションエントリです。Cisco Cloud APIC

リソース グループ

1. [Cloud Resources Virtual Machines]に移動します。 >

   [仮想マシン（Virtual Machines）] ウィンドウが表示されます。
2. [VM]リストでVMを見つけてメモします。Cisco Cloud APIC

   VMの値は通常、次の形式で表示されます。

   - 「vm_name」は、で説明されているように、仮想マシン名です。Virtual Machine Name （92 ページ）
   - （<resource_group>）は、のリソースグループエントリです。Cisco Cloud APIC

ロケーション

1. **[クラウド リソース仮想マシン（Cloud Resources Virtual Machines]** >

   [仮想マシン] ウィンドウが表示されます。

2. VMリストでVMを見つけます。Cisco Cloud APIC

3. [VM]リストでVMの値をクリックします。Cisco Cloud APIC

   VMの詳細が記載されたナビゲーションパネルが画面の右側から表示されます。Cisco Cloud APIC

4. [General]領域で、[Region]フィールドの値を見つけてメモします。

   これはのロケーションエントリです。Cisco Cloud APIC

ファブリック名

1. CLIからにSSHで接続します。Cisco Cloud APIC

   ```
   # ssh admin@<cloud_apic_ip_address>
   ```

   プロンプトが表示されたら、パスワードを入力します。

2. 次の CLI を入力します。

   ```
   ACI-Cloud-Fabric-1# acidiag avread
   ```

3. 出力でFABRIC_DOMAIN領域を見つけます。

```
Local appliance ID=1 ADDRESS=10.100.0.13 TEP ADDRESS=10.100.0.12/30 ROUTABLE IP
ADDRESS=0.0.0.0
CHASSIS_ID=afe36d66-042a-11eb-ab21-7b2dc494b182

Cluster of 1 lm(t):1(zeroTime) appliances (out of targeted 1
lm(t):1(2020-10-01T21:15:48.743+00:00))
with FABRIC_DOMAIN name=ACI-Cloud-Fabric set to version=5.0(2i)
lm(t):1(2020-10-01T21:15:48.746+00:00);
discoveryMode=PERMISSIVE lm(t):0(zeroTime); drrMode=OFF lm(t):0(zeroTime);
kafkaMode=OFF lm(t):0(zeroTime)

appliance id=1 address=10.100.0.13 lm(t):1(2020-10-01T21:14:23.001+00:00) tep
address=10.100.0.12/30
lm(t):1(2020-10-01T21:14:23.001+00:00) routable address=0.0.0.0 lm(t):1(zeroTime)
oob address=10.100.0.29/28 lm(t):1(2020-10-01T21:14:26.723+00:00) version=5.0(2i)
lm(t):1(2020-10-01T21:14:26.841+00:00) chassisId=afe36d66-042a-11eb-ab21-7b2dc494b182

lm(t):1(2020-10-01T21:14:26.841+00:00) capabilities=0X7EEFFFFFFFFF--0X2020--0X1
lm(t):1(2020-10-01T21:20:27.483+00:00) rK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) aK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobrK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobaK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) cntrlSbst=(APPROVED, E8E6DDB1D800)
lm(t):1(2020-10-01T21:14:26.841+00:00) (targetMbSn= lm(t):0(zeroTime),
failoverStatus=0 lm(t):0(zeroTime)) podId=1 lm(t):1(2020-10-01T21:14:23.001+00:00)
commissioned=YES lm(t):1(zeroTime) registered=YES
lm(t):1(2020-10-01T21:14:23.001+00:00)
standby=NO lm(t):1(2020-10-01T21:14:23.001+00:00) DRR=NO lm(t):0(zeroTime) apicX=NO

lm(t):1(2020-10-01T21:14:23.001+00:00) virtual=YES
```

```
lm(t):1(2020-10-01T21:14:23.001+00:00)
active=YES(2020-10-01T21:14:23.001+00:00) health=(applnc:255
lm(t):1(2020-10-01T21:16:16.514+00:00) svc's)
--------------------------------------------
clusterTime=<diff=-1 common=2020-10-02T07:46:19.717+00:00
local=2020-10-02T07:46:19.718+00:00
pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):1(2020-10-01T21:15:50.026+00:00)>>
--------------------------------------------
```

これはのファブリック名エントリです。Cisco Cloud APIC

外部サブネット

1. **[アプリケーション管理]** > **[EPG s]** の順に移動します。
2. ext-networksという名前のEPGを見つけ、そのEPGをクリックします。

   画面の右側からナビゲーションパネルがスライドします。
3. ナビゲーションパネルで、[詳細（Details）]アイコン（）をクリックします。

   この EPG の**概要**ページが表示されます。
4. [Endpoints]領域で、[ext-Network1]の行を見つけ、[Subnet]列の値を確認します。

   これはの外部サブネットエントリです。Cisco Cloud APIC値 `0.0.0.0/0` は、誰でも Cisco Cloud APIC への接続が許可されることを意味します。

Virtual Machine Name

1. **[クラウド リソース仮想マシン]** >

   [仮想マシン] ウィンドウが表示されます。
2. リスト内のVMの値を見つけてメモします。Cisco Cloud APIC

   VM の値は通常、次の形式で表示されます。*<vm_name>*(*<resource_group>*)

   - は、の仮想マシン名エントリです。Cisco Cloud APIC
   - （<resource_group>）は、で説明されているリソースグループです。リソース グループ （90 ページ）

インフラVNETプール

インフラVNETプールの場合、複数のインフラサブネットプールがある可能性があるため、手順の一部として、ARMテンプレートを使用して元のを起動したときに使用したインフラサブネットの情報を確認してください。Cisco Cloud APICAzure でのクラウド APIC の導入 （32 ページ）

1. Cisco Cloud APIC GUI で、[インターネット（Intent）]アイコン（）をクリックし、**[cAPIC 設定（cAPIC Setup）]** を選択します。

2. [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。

3. [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。

4. [一般（General）]の下の[クラウドルータのサブネットプール（Subnet Pools for Cloud Routers）]領域で、[作成者（Created By）]列に[システム内部（System Internal）]値がある行を見つけ、[サブネット（Subnet）]列の値をメモします。

   これはのInfra VNETプールエントリです。Cisco Cloud APIC

ストレージ アカウント名

が以前に展開されたリソースグループの下にあるAzureの[ストレージアカウント（Storage accounts）]ページに移動します。Cisco Cloud APIC

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

2. **[サービス（Services）]**の**[ストレージ アカウント（Storage accounts）]**を選択します。

   [ストレージ アカウント（Storage accounts）]ページが表示されます。

3. リソースグループのストレージアカウント名を見つけてメモします。Cisco Cloud APIC

   これはのストレージアカウント名エントリです。Cisco Cloud APIC

次の作業

アップグレード前の手順の実行 （93 ページ）の手順を実行します。

アップグレード前の手順の実行

始める前に

これらの手順に進む前に、既存のクラウドAPIC設定情報の収集 （90 ページ） の手順を完了してください。

ステップ 1 暗号化パスフレーズ制御が有効になっていない場合は、有効にします。

a) GUIで、[インフラストラクチャシステム設定（Infrastructure System Configuration）]に移動します。Cisco Cloud APIC >

   デフォルトでは、[General]タブの下にあります。そうでない場合は、[General]タブをクリックします。

b) 暗号化されたパスフレーズ制御がすでに有効になっているかどうかを確認します。

- [Global AES Encryption]領域で、[Encryption]フィールドと[Key Configured]フィールドの下に[Yes]と表示されている場合は、暗号化されたパスフレーズ制御がすでに有効になっています。ステップ 2（94 ページ） に進みます。
- [Encryption]フィールドと[Key Configured]フィールドの下に[Yes]が表示されない場合は、次の手順を実行します。

  1. [Global AES Encryption]領域の右上にある鉛筆アイコンをクリックします。

     [Global AES 暗号 Settings] ウィンドウが表示されます。

  2. [Encryption：Enabled]領域の横にあるボックスをクリックし、[Passphrase / Confirm Passphrase]フィールドにパスフレーズを入力して、ウィンドウの下部にある[Save]をクリックします。

     この手順で入力したパスフレーズは、後の手順のステップで必要になるため、メモしておきます。

ステップ 2 既存の Cisco Cloud APIC 設定をバックアップします。

設定をバックアップするには、さまざまな方法があります。Cisco Cloud APIC詳細については、Cloud APIC for Azure Users Guideを参照してください。リモート バックアップを使用する場合は、最初にリモート ロケーションを追加する必要があることに注意してください。

ステップ 3 展開に非ホームリージョン CSR がある場合は、ホームリージョンを除くすべてのリージョンから CSR を削除します。

（注） 展開に非ホームリージョンCSRがない場合は、この手順の手順を実行する必要はありません。その場合はステップ 4 （95 ページ）にスキップします。

a) Cisco Cloud APIC GUI で、[インターネット（Intent）] アイコン（）をクリックし、**[cAPIC 設定（cAPIC 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) **[クラウド ルータ（Cloud Routers）]** 列でボックスが選択されているリージョンをメモします。

次の手順で、**[クラウドルータ（Cloud Routers）]**列のボックスを選択解除します。これらの手順の後半でバックアップされた設定を復元すると、これらの同じクラウドルータの選択が自動的に選択されます。ただし、同じクラウドルータが正しく選択されたことを確認する場合は、この手順でメモしたリストを使用できます。

d) ホーム リージョン（テキスト **Cloud APIC Deployed** を含むリージョン）を除くすべてのリージョンの **[クラウド ルータ（Cloud Routers）]** 列で、チェックボックスをオフにします。

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。

[Save and Continue]をクリックした後、次の変更が行われるまで待ちます。

- Azureポータルからすべての非ホームリージョンCSR仮想マシンが削除されます。

- CSRインターフェイスのパブリックIPアドレスがすべてAzureポータルから削除されます。
- これらの仮想マシンに割り当てられたすべてのネットワークインターフェイスがAzureポータルから削除されます。

CSR の削除プロセスには約 30 分かかる場合があります。Azureポータルでインフラリソースグループの仮想マシンを調べることで、CSRの削除プロセスを監視できます。

ステップ 4 Cisco Cloud APIC VM を削除します。

a) Microsoft Azureポータルで、[**Services Virtual Machines**]に移動します。

b) **[仮想マシン（Virtual Machines）]**ウィンドウで Cisco Cloud APIC VM を見つけ、[Cloud APIC VM]をクリックします。

このCisco Cloud APIC VM の**概要**ページが表示されます。

c) **[削除（Delete）]** をクリックし、このアクションの確認を求められたら **[はい（Yes）]** をクリックします。

[通知（Notifications）]領域で削除プロセスを確認できます。

次のタスク

リカバリ テンプレートのダウンロードと展開 （95 ページ）の手順を実行します。

リカバリ テンプレートのダウンロードと展開

始める前に

これらの手順に進む前に、アップグレード前の手順の実行 （93 ページ） の手順を完了してください。

ステップ 1 リリース 5.1(2) リカバリ テンプレートをダウンロードします。Cisco Cloud APIC

a) Cisco Cloud APIC の Cisco Software Download サイトに移動し、最新リリースを選択します（まだ選択されていない場合）。

https://software.cisco.com/download/home/286323635/type/286325191/release/

b) **リカバリ テンプレート エントリのクラウド ACI イメージ**を見つけ、ダウンロード アイコンをクリックして json ファイルをダウンロードします。

ダウンロードを開始するように求められたら、ライセンス契約に同意します。

ステップ 2 Azureポータルにリリース5.1（2）リカバリテンプレートを展開します。

a) Azureポータルで、[All Services]ページに移動します。

https://portal.azure.com/#allservices

b) [General]領域で、[Templates]をクリックします。

c) [テンプレート（Templates）]ページで、[追加（Add）]をクリックします。

[テンプレートの追加] ページが表示されます。

d) [テンプレートの追加（Add Template）]ページに必要な情報を入力します。

- [名前（Name）]：このテンプレートをリリース5.1（2）リカバリテンプレートとして識別する一意の名前を入力します（template-512-recoveryなど）。
- [説明（Description）]：必要に応じて、このテンプレートの説明テキストを入力します。

e) **OK** をクリックします。

[ARM テンプレート（ARM template）] ページが表示されます。

f) **[ARM テンプレート（ARM Template）]** ページで、テンプレートに自動的に追加されるデフォルトのテキストを削除します。

g) リリース 5.1(2) リカバリ テンプレートをダウンロードした領域に移動します。ステップ 1 （95 ページ）

h) テキストエディタを使用して、リリース5.1（2）リカバリテンプレートを開き、テンプレートの内容をコピーします。

i) Azureポータルウィンドウで、[ARMテンプレート（ARM Template）]ページに内容を貼り付けます。

j) **OK** をクリックします。

[テンプレートの追加] ページが再度表示されます。

k) **[追加（Add）]** をクリックします。

新しいリリース 5.1(2) リカバリ テンプレートが **[テンプレート（Templates）]** ページに追加されます。**[テンプレート（Templates）]** ページに新しいリリース 5.1(2) リカバリ テンプレートが表示されない場合は、**[更新（Refresh）]** をクリックしてページを更新します。

ステップ 3 リカバリ テンプレートを使用して、同じリソース グループに VM を展開します。Cisco Cloud APIC

a) [テンプレート（Templates）]ページで、追加した新しいリリース 5.1(2) リカバリ テンプレートをクリックします。

b) **[展開（Deploy）]** をクリックします。

[カスタムの展開（Custom Deployment）] ページが表示されます。

c) リカバリ テンプレートに必要な情報を入力します。

- **基本**：
  - **[サブスクリプション（Subscription）]**：を最初に展開したときに使用したものと同じサブスクリプションを選択します。Cisco Cloud APICサブスクリプション （90 ページ）
  - **リソースグループ**：Cisco Cloud APIC で説明したように、リソース グループ （90 ページ）を最初に展開したときに使用したものと同じリソース グループを選択する必要があります。
  - **[場所（Location）]**：Cisco Cloud APIC の説明に従って、ロケーション （91 ページ） を最初に展開したときに使用したのと同じリージョンを選択します。

（注） 同じリソース グループを使用している場合、**[ロケーション（Location）]** オプションは使用できない場合があります。

- **[設定]**：
  - [Vm Name]：前に使用したのと同じVM名を入力します。Virtual Machine Name （92 ページ）
  - Vm Size：VMのサイズを選択します。
  - イメージSKU：5_0_2_byolイメージSKUを選択します。
  - [Admin Username]：このフィールドのデフォルトエントリはそのままにします。が起動すると、管理者ユーザ名のログインが機能します。Cisco Cloud APIC
  - [Admin Password or Key]：管理者パスワードを入力します。
  - [管理者公開キー（Admin Public Key）]：管理者公開キー（sshキー）を入力します。
  - Fabric Name：前に使用したものと同じファブリック名を入力します。ファブリック名 （91 ページ）
  - [インフラVNETプール（Infra VNET Pool）]：前に使用したものと同じインフラサブネットプールを入力します。インフラVNETプール （92 ページ）
  - 外部サブネット：にアクセスするために以前に使用された外部ネットワークのIPアドレスとサブネットを入力します。Cisco Cloud APIC外部サブネット （92 ページ）これは、実行した元の導入の一部として入力したのと同じ外部サブネットプールです。Cisco Cloud APICAzure でのクラウド APIC の導入 （32 ページ）
  - [ストレージアカウント名（Storage Account Name）]：前に使用したものと同じストレージアカウント名を入力します（の説明を参照）。ストレージ アカウント名 （93 ページ）
  - **[仮想ネットワーク名（Virtual Network Name）]**: 仮想ネットワークの名前。
    - リリース5.1（2）より前のリリースから5.1（2）にアップグレードする場合は、これらのパラメータの値を変更しないでください。このフィールドの仮想ネットワーク名はデフォルト値のままにします。
    - 5.1（2）からのリカバリを実行する場合は、このフィールドの仮想ネットワーク名が、の導入に最初に使用された仮想ネットワーク名と一致することを確認します。Cisco Cloud APIC
  - Mgmt Nsg Name：管理ネットワークセキュリティグループの名前。
    - リリース5.1（2）より前のリリースからリリース5.1（2）へのリカバリまたはアップグレードを実行する場合は、これらのパラメータの値を変更しないでください。このフィールドでは、管理ネットワークセキュリティグループ名のデフォルト値をそのままにします。
    - 5.1（2）からのリカバリを実行する場合は、このフィールドの管理ネットワークセキュリティグループ名が、の展開に最初に使用された管理ネットワークセキュリティグループ名と一致することを確認します。Cisco Cloud APIC

- Mgmt Asg Name：管理アプリケーションセキュリティグループの名前。
  - リリース5.1（2）より前のリリースからリリース5.1（2）へのリカバリまたはアップグレードを実行する場合は、これらのパラメータの値を変更しないでください。このフィールドでは、管理アプリケーションセキュリティグループ名のデフォルト値をそのままにします。
  - 5.1（2）からのリカバリを実行している場合は、このフィールドの管理アプリケーションセキュリティグループ名が、を展開するために最初に使用された管理アプリケーションセキュリティグループ名と一致することを確認します。Cisco Cloud APIC
- サブネットプレフィックス：このフィールドのエントリは、自動的に設定されるインフラサブネットに使用する必要があるサブネットプレフィックスになります。
  - リリース 5.1(2) より前のリリースから 5.1 (2) にアップグレードする場合は、これらのパラメータの値を変更しないでください。このフィールドはデフォルト値のままにします。
  - 5.1（2）からのリカバリを実行する場合は、このフィールドのサブネットプレフィックスが、の展開に最初に使用されたサブネットプレフィックスと一致することを確認します。Cisco Cloud APIC仮想ネットワーク上のサブネット名の形式を調べることで、そのプレフィックスを確認できます。Cisco Cloud APICたとえば、サブネット名がsubnet-10.10.0.0_28の場合、このフィールドのサブネットプレフィックスはsubnet-である必要があります。

d) 契約書の横にあるボックスをクリックし、[購入（Purchase）]をクリックします。

[Azure services]ウィンドウが開き、[Deployment in progress]という小さなポップアップウィンドウが表示されます。[通知（Notifications）]アイコンをクリックして、展開の進行状況の監視を続行します。通常、展開には約5分かかります。

しばらくすると、[Deployment successful]ウィンドウが表示されます。

次のタスク

アップグレード後の手順の実行 （98 ページ）の手順を実行します。

アップグレード後の手順の実行

始める前に

これらの手順に進む前に、リカバリ テンプレートのダウンロードと展開 （95 ページ） の手順を完了してください。

ステップ 1 インフラサブスクリプションのVMに貢献者ロールを付与します。Cisco Cloud APIC

a) Microsoft Azureポータルの[Services]で、[Subscription]を選択します。
b) 導入されたサブスクリプションを選択します。Cisco Cloud APIC

c) **[アクセス制御（IAM）（Access control (IAM)]** を選択します。
d) 上部のメニューで、[追加（Add）] [追加（Add role role）]をクリックします。 >
e) [Role]フィールドで、[Contributor]を選択します。
f) **[Assign access to]** フィールドで、**[仮想マシン（Virtual Machine）]** を選択します。
g) [サブスクリプション（Subscription）]フィールドで、が展開されたサブスクリプションを選択します。Cisco Cloud APIC
h) [選択（Select）]で、仮想マシンをクリックします。Cisco Cloud APIC
i) **[Save]** をクリックします。

（注） また、ユーザテナントを管理している場合は、VMに貢献者ロールを付与します。Cisco Cloud APICこれは、ユーザテナントの展開に使用されるユーザサブスクリプションで行う必要があります。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 （9 ページ）と 仮想マシンへのロール割り当ての追加 （37 ページ）を参照してください。

ステップ 2 同じ暗号化パスフレーズが使用可能です。

a) Microsoft Azureポータルの[Services]で、[Virtual Machines]を選択します。
b) **[仮想マシン（Virtual machine）]** ウィンドウで、Cisco Cloud APIC をクリックします。

Cisco Cloud APIC の **概要** ページが表示されます。

c) [パブリックIPアドレス（Public IP address）]フィールドを見つけて、IPアドレスをコピーします。
d) 別のブラウザウィンドウで、IPアドレスを入力し、Return：

```
https://<IP_address>
```

初めてログインすると、[クラウドAPICへようこそ（Welcome to Cloud APIC）]画面が表示されます。

e) **[初回セットアップの開始（Begin First Time Setup）]** をクリックします。

[Let's Configure the Basics]ウィンドウが表示されます。右上隅の[X]をクリックしてこのウィンドウを終了し、同じ暗号化パスフレーズを有効にする手順に進みます。

f) Cisco Cloud APIC GUIで、**[インフラストラクチャシステム設定（Infrastructure System Configuration）]** に移動します。

デフォルトでは、**[General]** タブの下にあります。そうでない場合は、**[General]** タブをクリックします。

最初のログイン後、ウェルカム画面が表示されます。[初回セットアップの開始（Begin first time setup）]をクリックします。初回セットアップページが開き、初回セットアップページを閉じてから、パスフレーズの設定に進みます。

g) [Global AES Encryption]領域で、[Global AES Encryption]領域の右上にある鉛筆アイコンをクリックします。

[Global AES 暗号 Settings] ウィンドウが表示されます。

h) [Encryption：Enabled]領域の横にあるボックスをクリックし、[Passphrase / Confirm Passphrase]フィールドに同じパスフレーズを入力してから、ウィンドウの下部にある[Save]をクリックします。ステップ 1 （93 ページ）アップグレード前の手順の実行 （93 ページ）

ステップ 3 リリース5.2（1）への移行ベースのアップグレードを実行している場合は、以前にバックアップした設定をインポートする前に、Pythonスクリプトを実行して必要な設定をクリーンアップします。

Cisco TACに連絡し、CSCvy42684で発生した問題に対処するPythonスクリプトを入手して、必要な設定をクリーンアップします。https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy42684

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

ステップ 4 でバックアップした設定をインポートします。ステップ 2 （94 ページ）アップグレード前の手順の実行 （93 ページ）

設定のバックアップ時にリモートロケーションを設定した場合は、バックアップにアクセスするためにリモートロケーションを再度作成する必要があります。

a) GUIで、[Operations Backup & Restore]に移動します。Cisco Cloud APIC >
b) [Backup & Restore]ウィンドウで、[Backups]タブをクリックします。
c) [Actions]スクロールダウンメニューをクリックし、[Restore Configuration]を選択します。

[復元の設定（Restore Configuration）] ウィンドウが表示されます。

d) でバックアップした設定を復元するために必要な情報を入力します。ステップ 2 （94 ページ）アップグレード前の手順の実行 （93 ページ）

4.2（x）リリースからリリース5.0（x）以降にアップグレードする場合は、この特定のバックアップの復元に、次の設定を使用します。

- **[復元タイプ（Restore Type）]** フィールドで、**[結合（Merge）]** を選択します。
- [Restore Mode]フィールドで、[Best Effort]を選択します。

このウィンドウに必要な情報を入力したら、[Restore Configuration]をクリックします。

e) 復元プロセスが完了してから、次のステップに進みます。

[Backup & Restore] ウィンドウの **[Job Status]** タブをクリックして、復元プロセスのステータスを取得し、復元プロセスが成功したことを確認します。

ステップ 5 命名ポリシーを確認します。

a) Cisco Cloud APIC GUI で、[インターネット（Intent）] アイコン（）をクリックし、**[cAPIC 設定（cAPIC 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) 移行前の選択内容がバックアップインポートで正常に転送されたことを確認し、[次へ（Next）]をクリックします。

（注） この時点では、管理対象リージョンまたはCSRの設定を変更しないでください。

d) セットアップの最後のページに移動し、[Cloud Resource Naming Rules]領域の情報を確認します。

- リリース5.1（2）より前のリリースからリリース5.1（2）へのリカバリまたはアップグレードを実行する場合は、デフォルトのクラウドリソースの命名規則を変更しないでください。この場合、デフォルトのクラウドリソース命名ルールはそのままにします。
- 5.1（2）からのリカバリを実行している場合は、クラウドリソースの命名規則が、を展開するために最初に使用されたクラウドリソースの命名規則と一致することを確認します。Cisco Cloud APIC

[これらの命名規則に基づいてクラウドリソースを展開する（Deploy cloud resources based on these rules）]の横にあるボックスをクリックし、この画面の情報を確認してから[保存して続行（Save and Continue）]をクリックします。命名ルールが確認され、承認されるまで、リソースはクラウドに展開されません。

プロセスのこの時点で、非ホームリージョンのCSRが新しいCSRイメージで自動的に展開されます。

（注） 次のステップに進む前に、がすべての障害をクリアするまでしばらく待ちます。Cisco Cloud APIC詳細については、『Cisco Cloud APIC for Azure User Guide』の「Viewing Health Details Using the GUI」を参照してください。Cisco Cloud APIC

ステップ 6 非ホームリージョンのCSRがクラウドで起動するのを待ち、すべてのVGWトンネルが新しく作成されたCSRで起動し、設定の調整が完了することを確認します。

さらに、CSRのアップグレードが必要な場合は、プロセスのこの時点でホームリージョンのCSRが削除され、再作成されることがあります。これらのアクションと、結果として表示される可能性のある障害は無視してください。これらのアクションは、この手順の次の手順を完了すると解消されます。

この場合、ホームリージョンのCSRが最新のCSRバージョンにアップグレードされるまで待ちます。たとえば、リリース5.0（2i）の場合、最新のCSRバージョンは17_1になります。

ステップ 7 （任意） サイト間接続があり、サイト間トラフィックの完全なドロップを回避する場合は、次のステップでホームリージョンのCSRを停止する前に、非ホームリージョンのサイト間トンネルを再設定し、を介してトンネルを起動します。ACI マルチサイト オーケストレータ

この手順は、サイト間接続がない場合、またはサイト間接続があるが、トラフィックの損失を気にしない場合は必要ありません。

a) ACI マルチサイト オーケストレータ **[サイト (Sites)]** ビューで、**[インフラの構築 (CONFIGURE INFRA)]** をクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

b) 左側のペインの **[サイト (SITES)]** の下で、クラウド サイトをクリックします。
c) [サイトデータのリロード（Reload Site Data）]をクリックします。
d) 新しいCSRがUIに追加されたことを確認します。
e) 画面の右上にある[Deploy]ボタンをクリックし、[Deploy & Download IPN Device config files]オプションを選択します。

このアクションは、オンプレミスの APIC サイトと Cloud APIC サイトの両方に設定をプッシュし、オンプレミスとクラウド サイト間のエンドツーエンド インターコネクト接続を有効にします。さらに、このオプションでは、Azure に導入された Cisco クラウド サービス ルータ（CSR）とオンプレミスの IPsec 終端 デバイスとの間の接続を有効にするための設定情報を含む zip ファイルをダウンロー

ドします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

（注） この手順でからクラウドCSRでサイト間トンネルを削除して再作成し、オンプレミスのIPsec終端デバイスで新しいキーをプログラムする必要がある場合は、同じパブリックIPアドレスのキーを変更します。クラウドCSRの場合は、最初にオンプレミスのIPsec終端デバイス上の既存のキーを手動で削除し、新しいキーを追加する必要があります。Cisco Cloud APICオンプレミスのIPsec終端デバイスの特定のクラウドCSR宛先IPアドレスに一致するIPsec事前共有キーは1つだけです。

ステップ 8 ホームリージョンのCSRを展開解除します。

（注） 4.2（3）から5.1（2）にアップグレードする場合、ホームリージョンのCSRを展開解除して再展開すると、CSRパブリックIP SKUも基本SKUから標準SKUに移行されます。

a) Cisco Cloud APIC GUI で、[インターネット（Intent）] アイコン（）をクリックし、**[cAPIC 設定（cAPIC 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) ホームリージョン（[Cloud APIC Deployed]というテキストがあるリージョン）を見つけ、そのホームリージョンの[Cloud Routers]カラムのボックスを選択解除します。

d) **[Save]** をクリックします。

これにより、ホームリージョンの古いCSRが削除されます。

e) ホームリージョンのCSR VM、CSR NIC、およびCSRパブリックIPアドレスがクラウドで削除されるのを待ちます。

ホームリージョンのCSR VM、CSR NIC、およびCSRパブリックIPアドレスがクラウドで削除されると、ホームリージョンにCSRを再展開できます。

ステップ 9 ホームリージョンのCSRを再展開します。

この手順では、以前に設定したホームリージョンのCSRが削除され、新しいホームリージョンのCSRが再作成されます。

a) [Previous]をクリックして[Regions to to Manage]画面に戻り、ホームリージョンの[Cloud Routers]列のボックスをクリックして、ホームリージョンのCSRを再度有効にします。

b) **[Save]** をクリックします。

4.2（3）から5.1（2）にアップグレードする場合、このアクションはCSRパブリックIP SKUをホームリージョンの標準SKUに移行します。

ステップ 10 （任意） サイト間接続が必要な場合は、この手順の手順を実行します。

- サイト間接続が不要な場合は、この手順の手順を実行する必要はありません。その場合はVNetピアリングへの移行（オプション） （103 ページ） にスキップします。
- サイト間接続が必要な場合は、次の手順を実行します。

a) 新しいホームリージョンのCSRが表示されたら、[サイト（Sites）]画面で[インフラストラクチャの設定（CONFIGURE INFRA）]をクリックします。ACI マルチサイト オーケストレータ

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

b) 左側のペインの **[サイト (SITES)]** の下で、クラウド サイトをクリックします。
c) **[サイトデータのリロード（Reload Site Data）]** をクリックします。
d) 新しいCSRがUIに追加されたことを確認します。
e) 画面の右上にある **[展開（Deploy）]** ボタンをクリックし、**[IPN デバイスの展開およびダウンロード config ファイル（Deploy & Download IPN Device config files）]** オプションを選択します。
f) ダウンロードした IPN 設定を使用して、オンプレミス CSR の IPN IPsec トンネルを再設定します。

Cisco Cloud APIC と ISN デバイス間の接続の有効化 （66 ページ）を参照してください。

（注） 何らかの理由でからクラウドCSRのサイト間トンネルを削除して再作成し、オンプレミスのIPsec終端デバイスで新しいキーをプログラムする必要がある場合は、同じパブリックIPアドレスのキーを変更するクラウドCSRの場合は、最初にオンプレミスのIPsec終端デバイス上の既存のキーを手動で削除し、新しいキーを追加する必要があります。Cisco Cloud APIC オンプレミスの IPsec 終端デバイスの特定のクラウド CSR 宛先 IP アドレスに一致する IPsec 事前共有キーは 1 つだけです。

次のタスク

VNet間接続のためにAzure VNetピアリングに移行する場合は、の手順に従います。VNet ピアリングへの移行（オプション） （103 ページ）

VNet ピアリングへの移行（オプション）

CSR を介した従来のトンネルベースの VPN 接続を使用するのではなく、VNet 間接続のために Azure VNet ピアリングに移行する場合は、このタスクの手順に従います。VNet ピアリング機能の詳細については、『Configuring VNet Peering for Cloud APIC for Azure』ドキュメントを参照してください。

（注） VNet ピアリング モードへの移行は中断を伴う操作です。プロセス中にトラフィック損失が発生することに注意してください。

始める前に

これらの手順に進む前に、の手順を完了してください。アップグレード後の手順の実行 （98 ページ）

ステップ 1 Cisco Cloud APIC GUI で、[インターネット（Intent）]アイコン（）をクリックし、**[cAPIC 設定（cAPIC Setup）]** を選択します。

ステップ 2 **[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。

ステップ 3 **[内部ネットワークの接続性（Connectivity for Internal Network）]** 領域を見つけ、**仮想ネットワーク ピアリング**が使用可能であることを確認します。

ステップ 4 **[仮想ネットワークピアリング（Virtual Network Peering）]** をクリックして、Azure VNet ピアリング機能を有効にします。

これにより、レベルで VNet ピアリングが可能になり、インフラ VNet 内の CSR を持つすべてのリージョンに NLB が展開されます。Cisco Cloud APIC

VNet ピアリングをレベルで有効にした後、各ユーザ クラウド コンテキスト プロファイルで、**VNet ピアリング** オプションを有効にし、**VNet ゲートウェイ ルータ** オプションを無効にする必要があります。Cisco Cloud APIC

（注） 次の手順では、GUI を使用して各クラウド コンテキスト プロファイルで VNet ピアリングを有効にする方法について説明します。Cisco Cloud APIC必要に応じて、次の手順を実行することもできます。ACI マルチサイト オーケストレータ

ステップ 5 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）]**

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 6 [アクション（Actions）]をクリックし、**[クラウド コンテキスト プロファイル）Create Cloud Context Profile]** を選択します。

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

ステップ 7 **[VNet ゲートウェイ ルータ（VNet Gateway Router]** フィールドを見つけて、**[VNet Gateway Router]** チェックボックスのチェックを外し（無効）ます。

ステップ 8 **[VNet ペアリング（VNet Peering）]** フィールドを見つけて、**[VNet ペアリング]** チェックボックスにチェック（有効)します）。

ステップ 9 設定が終わったら **[保存（Save）]** をクリックします。

ステップ 10 インフラ サブスクリプションとユーザ テナント サブスクリプションの両方にネットワーク貢献者ロールを設定します。

たとえば、次のようなケースがあるとします。

- インフラ テナントはアクセス クレデンシャル/サービス プリンシパル **C1** でサブスクリプション **S1** を使用しています
- ユーザ テナントは、アクセス クレデンシャル/サービス プリンシパル **C2** でサブスクリプション **S2** を使用しています

この状況では、ユーザ テナントと infra VNet の間でピアリングが機能するように、次を設定する必要があります。

- ハブ ツー スポーク ピアリングリンクの S2 に C1 ネットワーク投稿者ロール権限を付与する必要があります。
- ハブ ピアリングリンクへのスポークのアクセス許可を S1 に付与する必要があります。

a) 表示される黄色のウィンドウで、指定された **az** コマンドをコピーします。
   - ユーザテナントのネットワーク投稿者ロールを設定している場合は、**[ユーザサブスクリプション用に実行するコマンド**（Command to run）]のテキストをコピーします。
   - インフラテナントのネットワーク投稿者ロールを設定している場合は、**[インフラサブスクリプション用に実行するコマンド**（Command to run）]領域のテキストをコピーします。

b) Azure 管理ポータルに戻り、左側のナビゲーションバーで **[登録（Registrations）]** をクリックします。
c) クラウド シェルをオープンします。
d) **[Bash]** を選択します。
e) コピーした **az** コマンドを貼り付けます。10.a （105 ページ）

ポリシーベースのアップグレード

リリース5.0（1）または5.0（2）からリリース5.1（2）にアップグレードする場合は、次の項の手順を使用して、Cisco Cloud APICソフトウェアのポリシーベースのアップグレードを実行します。

このセクションの手順を実行する前に、ソフトウェアのアップグレードの前提条件 （88 ページ） に記載されている情報を確認してください。

イメージのダウンロード中

ステップ 1 ログインしていない場合は、Cisco Cloud APIC にログインします。

ステップ 2 [Navigation]メニューから、[Operations] [Firmware Management]を選択します。 >

[ファームウェア管理] ウィンドウが表示されます。

ステップ 3 **[ファームウェア管理]** ウィンドウの **[イメージ（Images）]** タブをクリックします。

ステップ 4 [Actions]をクリックし、スクロールダウンメニューから[Add Firmware Image]を選択します。

[ファームウェア イメージを追加] ポップアップが表示されます。

ステップ 5 ファームウェア イメージをローカルまたはリモート ロケーションから追加するかを決めます。

- ローカル ロケーションからファームウェア イメージを追加する場合は、**[イメージの場所（Image Location）]** フィールドの **[ローカル]** ラジオボタンをクリックします。**[ファイルの選択（Choose File）]** ボタンをクリックし、インポートするファームウェア イメージがあるローカル システムのフォルダに移動します。ステップ 6 （106 ページ） に進みます。

- リモートロケーションからファームウェアイメージをインポートする場合は、**[イメージの場所（Image Location）]** フィールドの **[リモート（Remote）]** オプション ボタンをクリックし、次の操作を実行します。

a) **[プロトコル（Protocol）]** フィールドで、**[HTTP]** または **[SCP]** のどちらかのオプション ボタンをクリックします。

b) [URL] フィールドに、イメージのダウンロード元の URL を入力します。

- 前の手順で [HTTP] オプション ボタンを選択した場合は、ソフトウェア イメージのダウンロードに使用する http ソースを入力します。URL が例 **`10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`** .</username>ステップ 6 （106 ページ） に進みます。

- 前の手順で **[SCP]** オプション ボタンを選択した場合は、**<SCP サーバ>:/<パス>** の形式を使用して、ソフトウェア イメージのダウンロードに使用する Secure Copy Protocol（SCP）ソースを入力します。URL が例 **`10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`** .</username>

c) [Username] フィールドに、セキュア コピーのユーザ名を入力します。

d) [認証タイプ（Authentication Type）] フィールドで、ダウンロードの認証タイプを選択します。次のタイプを選択できます。

- **Password**
- **SSH Key**

デフォルトは、「**Password**」です。

e) **[パスワード（Password）]** を選択した場合は、**[パスワード（Password）]** フィールドにセキュア コピーのパスワードを入力します。ステップ 6 （106 ページ） に進みます。

f) **[SSH 公開/秘密キー ファイルを使用（Use SSH Public/Private Key Files）]** を選択した場合は、次の情報を入力します。

- **[SSH キー コンテンツ（SSH Key Contents）]**：SSH キー コンテンツを使用して SSH キー ファイルを作成します。SSH キー ファイルは、ダウンロード用のリモート ロケーションの作成時に必要です。

（注） 公開キーは、転送時に生成されます。転送後、バックグラウンドで生成されたキー ファイルは削除されます。一時的なキー ファイルは、Cisco Cloud APIC の dataexport ディレクトリに保存されます。

- [SSH キー パスフレーズ（SSH Key Passphrase）]：SSH キー パスフレーズを使用して SSH キー ファイルを作成します。SSH キー ファイルは、ダウンロード用のリモート ロケーションの作成時に必要です。

（注） [パスフレーズ（Passphrase）] フィールドは空白にしておくことができます。

ステップ 6 [Select] をクリックします。

Cisco Cloud APIC のファームウェア イメージがダウンロードされるのを待ちます。

ポリシーベースのアップグレードプロセスを使用したソフトウェアのアップグレード

リリース5.0（1）または5.0（2）からリリース5.1（2）以降にアップグレードする場合は、次の項の手順を使用して、Cisco Cloud APICソフトウェアのポリシーベースのアップグレードを実行します。

始める前に

- の手順を使用してイメージをダウンロードしました。イメージのダウンロード中（105ページ）

ステップ 1 Cisco Cloud Services Router（CSR）の正しいイメージに登録します。

- Cisco Cloud Services Router（CSR）1000V-Bring Your Own License（BYOL）のイメージをサブスクライブするには、次の手順を実行します。

a) Azure Marketplaceの検索テキストフィールドに、Cisco Cloud Services Router（CSR）1000Vと入力し、表示されるオプションを選択します。http://azuremarketplace.microsoft.com

Cisco Cloud Services Router（CSR）1000Vオプションが検索候補として表示されます。

b) **[Cisco Cloud Services Router（CSR）1000V]** オプションをクリックします。

Microsoft Azure MarketplaceのCisco Cloud Services Router（CSR）1000Vページにリダイレクトされます。

c) [ソフトウェアプランの選択（Select a software plan）]ドロップダウンメニューを見つけます。

メインページに[ソフトウェアプランの選択（Select a software plan）]ドロップダウンメニューが表示されない場合、[ソフトウェアプランの選択（Select a software plan）]ドロップダウンメニューにアクセスするには、[プラン+価格設定（Plans + Pricing）]タブをクリックする必要があります。

d) [ソフトウェアプランの選択（Select a software plan）]ドロップダウンメニューで、適切なオプションを選択します。

- リリース5.1（2）では、[Cisco CSR 1000V Bring Your Own License-XE 17.3.1a]オプションを選択します。
- リリース 5.2(1) 向け、???

e) プログラマビリティを導入しますか？ [Get Started]をクリックします。

f) [Configure Programmability Deployment]ページでサブスクリプションまでスクロールし、[Status]列でサブスクリプションのステータスを[Disable]から[Enable]に変更します。

g) **[Save]** をクリックします。

ステップ 2 リリース5.0（1）からリリース5.1（2）にアップグレードする場合は、ホームリージョンを除くすべてのリージョンからCSRを削除します。

（注） リリース5.0（2）以降からリリース5.1（2）にアップグレードする場合は、CSRを削除しないでください。その場合は ステップ 3 （108 ページ） に移動します。

この時点では、ホームリージョンからCSRを削除しないでください。この時点でホームリージョンのCSRを削除すると、停止が発生します。

a) クラウド APIC GUI で、[インターネット（Intent）]アイコン（）をクリックし、**[cAPIC セットアップ（cAPIC 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) **[クラウド ルータ（Cloud Routers）]** 列でボックスが選択されているリージョンをメモします。

次の手順で **[クラウド ルータ（Cloud Routers）]** 列のボックスの選択を解除します。そのため、この手順の最後に、どの領域を再度選択する必要があるかを確認してください。

d) ホームリージョン（テキストCloud APIC Deployedを含むリージョン）を除くすべてのリージョンの[Cloud Routers]カラムで、チェックボックスをオフにします。

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。

CSR の削除プロセスには約 30 分かかる場合があります。Azure ポータルでリソース グループの仮想マシンを確認することで、CSR の削除プロセスを監視できます。

必要な CSR が完全に削除されるまで、次の手順に進まないでください。

ステップ 3 **[移動（Navigation）]** メニューから、**[オペレーションズ（Operations）]**>**[ファームウェア管理（Firmware Management）]**を選択します。

[ファームウェア管理] ウィンドウが表示されます。

ステップ 4 **[アップグレードをスケジュール（Schedule Upgrade）]** をクリックします。

[アップグレードをスケジュール] ポップアップが表示されます。

ファブリックに障害があることを示すメッセージが表示された場合は、アップグレードを実行する前にこれらの障害を解決することを推奨します。詳細については、『*Cisco Cloud APIC for Azure User Guide*』の「Viewing Health Details Using the Cisco Cloud APIC GUI」を参照してください。

ステップ 5 **[ターゲット ファームウェア（Target Firmware）]** フィールドで、スクロールダウン メニューからファームウェア イメージを選択します。

ステップ 6 [Upgrade Start Time]フィールドで、アップグレードを今すぐ開始するか、後で開始するかを決定します。

- 今すぐアップグレードをスケジュールする場合は、[Now]をクリックします。ステップ 7 （109 ページ） に進みます。
- 後で日付または時刻にアップグレードをスケジュールする場合は、[後で（Later）]をクリックし、スケジュールされたアップグレードの日時をポップアップカレンダーから選択します。

ステップ 7 互換性チェック機能を無効にするように特に指示されている場合を除き、**[互換性チェックを無視(Ignore Compatibility check)]** フィールドでは設定をデフォルトの [オフ (off)] のままにします。

クラウド APIC 内では、システムの現在稼働中のバージョンから特定の新しいバージョンへのアップグレードパスがサポートされているか否かを確認する互換性チェック機能が存在します。**[互換性チェックを無視]**設定はデフォルトでは[オフ]に設定されているため、システムは可能なアップグレードの互換性をデフォルトで自動的にチェックします。

（注） 次に、ボックスにチェック マークを入力して、互換性チェック機能を無効にする] を選択すると、 **互換性の確認を無視** に移動して、システム内で発生する可能性がありますシステムには、サポートされていないアップグレードを加えるのリスクを実行する]フィールドで、使用不可の状態。

ステップ 8 **[アップグレードをスケジュール（Schedule Upgrade）]** をクリックします。

[Upgrade Status]領域のメインの[Firmware Management]ウィンドウで、アップグレードの進行状況をモニタできます。

ステップ 9 リリース5.0（1）からリリース5.1（2）にアップグレードする場合は、アップグレードが完了したら、必要なCSRを再度追加します。

（注） この手順は、リリース5.0（1）からリリース5.1（2）にアップグレードする場合にのみ必要です。リリース5.0（2）以降からリリース5.1（2）にアップグレードする場合は、このセクションでこれ以上の手順を実行する必要はありません。

他のリージョンにCSRを再度追加する前に、ホームリージョンのCSRが安定していることを確認します。

a) クラウド APIC GUI で、[インターネット（Intent）]アイコン（）をクリックし、**[cAPIC セットアップ（cAPIC 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) CSRが含まれていたすべてのリージョンを特定し、それらの各リージョンの[クラウドルータ（Cloud Routers）]列のボックスをオンにして、CSRを再度追加します。
d) [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。

ステップ 10 すべてのCSR（ホームリージョンのCSRと非ホームリージョンのCSR）がリリース17.3.1aになっていることを確認します。

すべてのCSRがリリース17.3.1aになるまで、Cisco Cloud APIC VMの電源をオフにしないでください。

ステップ 11 リリース5.0（1）からリリース5.1（2）にアップグレードする場合は、CSRを介した従来のトンネルベースのVPN接続を使用するのではなく、VNet間接続のためにAzure VNetピアリングに移行するかどうかを決定します。

VNet ピアリング機能の詳細については、 *『Configuring VNet Peering for Cloud APIC for Azure』* ドキュメントを参照してください。

（注） VNetピアリングモードへの移行は中断を伴う操作です。プロセス中にトラフィック損失が発生することに注意してください。

VNetピアリング機能を有効にするには、次の手順を実行します。

a) クラウドAPIC GUIで、[インターネット（Intent）]アイコン（）をクリックし、**[cAPICセットアップ（cAPIC 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) **[内部ネットワークの接続性（Connectivity for Internal Network）]**領域を見つけ、**仮想ネットワーク ピアリング**が使用可能であることを確認します。

- 仮想ネットワークピアリングが使用可能な場合、ホームリージョンCSRは基本SKUから標準SKUにすでに正常に移行されています。その場合は11.i （110 ページ） に移動します。
- 仮想ネットワークピアリングが使用できない場合、ホームリージョンのCSRは、更新された標準SKUではなく基本SKUに設定されたままになります。ホームリージョンのCSRを標準SKUに移行します。11.d （110 ページ）

d) ホームリージョン（「Cloud APIC Deployed」というテキストがあるリージョン）を検索し、ホームリージョンの[Cloud Routers]カラムのボックスを選択解除します。

e) **[Save]**をクリックします。

このアクションにより、ホームリージョンの基本SKUを持つCSRが削除されます。

f) [Previous]をクリックして[Regions to to Manage]画面に戻り、ホームリージョンの[Cloud Routers]列のボックスをクリックして、ホームリージョンのCSRを再度有効にします。

g) **[Save]**をクリックします。

この操作により、CSRがホームリージョンの標準SKUに追加されます。

h) [Previous]をクリックして[Regions to to Manage]画面に戻り、[Connector for Internal Network]領域を見つけて、仮想ネットワークピアリングが使用可能であることを確認します。

i) **[仮想ネットワークピアリング（Virtual Network Peering）]**をクリックして、Azure VNet ピアリング機能を有効にします。

これにより、クラウドAPICレベルでVNetピアリングが可能になり、インフラVNet内のCSRを持つすべてのリージョンにNLBが導入されます。

（注） CSR経由のVPN接続オプションは、VNetピアリングを使用する代わりに、CSRとAzure VPNゲートウェイルータ間のオーバーレイIPsecトンネルを介した従来のVPN接続を有効にするために使用されます。

クラウドAPICレベルでVNetピアリングを有効にした後、各ユーザクラウドコンテキストプロファイルで、VNetピアリングオプションを有効にし、VNetゲートウェイルータオプションを無効にする必要があります。

j) 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）]**

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。

k) [アクション（Actions）]をクリックし、**[クラウドコンテキスト プロファイル）Create Cloud Context Profile]** を選択します。

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

l) **[VNet ゲートウェイ ルータ（VNet Gateway Router]** フィールドを見つけて、**[VNet Gateway Router]** チェックボックスのチェックを外し（無効）ます。

m) **[VNet ペアリング（VNet Peering）]** フィールドを見つけて、**[VNet ペアリング]** チェックボックスにチェック（有効)します）。

n) 設定が終わったら [Save] をクリックします。

ソフトウェアのダウングレード

次の項では、Cisco Cloud APIC ソフトウェアを正常にダウングレードするために必要な情報を提供します。

ソフトウェアのダウングレードの前提条件

次に、Cisco Cloud APIC ソフトウェアをダウングレードする前に従う必要がある前提条件を示します。

- がCisco ACIファブリックの一部であり、シスコと連携している場合は、Cisco ソフトウェアをダウングレードする前に、まず同等またはそれ以前のリリースにソフトウェアをダウングレードする必要があります。Cisco Cloud APICマルチサイトマルチサイトCisco Cloud APICACI マルチサイト オーケストレータつまり、シスコ ソフトウェアのリリースは、常にソフトウェアのリリース以降である必要があります。ACIマルチサイト オーケストレータCisco Cloud APIC
  - シスコ ソフトウェアのリリース日を確認するには、ソフトウェア ダウンロード サイトの ACI Multi-Site Software に移動し、左側のナビゲーション バーで該当するリリースを選択して、そのリリースのリリース日を確認します。ACIマルチサイト オーケストレータ
  - ソフトウェアのリリース日を確認するには、ソフトウェア ダウンロード サイトの Cloud Application Policy Infrastructure Controller に移動し、左側のナビゲーションバーで該当するリリースを選択して、そのリリースのリリース日を確認します。Cisco Cloud APIC

たとえば、リリース 5.0（2i）にダウングレードする場合は、次のようになります。Cisco Cloud APIC

1. ソフトウェア ダウンロードサイト（この場合は、25-Sep-2020）のクラウドアプリケーション ポリシー インフラストラクチャ コントローラの情報を使用して、リリース 5.0

（2i）のリリース日を確認し、ソフトウェア ダウンロード サイトの ACI Multi-Site Software に移動します。シスコ ソフトウェアの同等またはそれ以降のリリース（この場合、Release 3.0（2k）は、2020 年 10 月 2 日にリリースされました）を検索します。Cisco Cloud APICACI マルチサイト オーケストレータマルチサイト

2. 最初に、このドキュメントの手順に従って、ソフトウェアをリリース 5.0（2i）にダウングレードします。Cisco Cloud APICCloud APIC
3. ソフトウェアをダウングレードしたら、Cisco ソフトウェアをリリース 3.0（2k）にダウングレードします。Cisco Cloud APICACI マルチサイト オーケストレータマルチサイトこれらの手順については、『Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide、Release 3.1（x）』を参照してください。

ソフトウェアのダウングレード

始める前に

5.1（2）から5.1（2）より前のリリースにダウングレードする場合は、次の前提条件が適用されます。

- Cisco Cloud APIC が常にリリース 5.1（2）で実行されている場合（5.1（2）より前のリリースからリリース 5.1（2）にアップグレードしたことがない場合）、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ことはできません。）。Cisco Cloud APIC が以前のリリースで実行されなかった 5.1（2）より前のリリースへのダウングレードはサポートされていません。
- Cisco Cloud APIC をリリース 5.1（2）にアップグレードし、特定のリリース 5.1（2）固有の設定を後で完了し、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、CSR を削除する必要があります。ホーム リージョンを除くすべてのリージョンから。これらの指示については、ステップ 1 （112 ページ） にアクセスしてください。
- Cisco Cloud APIC をリリース 5.1（2）にアップグレードしたが、その後リリース 5.1（2）固有の設定を完了しておらず、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、任意の地域からの CSR を削除する必要はありません。その場合はに移動します。ステップ 3 （113 ページ）

ステップ 1 ダウングレードする前に、5.1（2）固有の設定を削除します。

ステップ 2 リリースに応じて、必要なリージョンから CSR を削除します。

- リリース 5.1（2）から**リリース 5.0（1）**にダウングレードする場合は、ホームリージョンを含むすべてのリージョンから CSR を削除します。
- リリース 5.0（2j）より前のリリース 5.1（2）から 5.0（2）リリースにダウングレードする場合は、ホームリージョンからのみ CSR を削除します。

- リリース 5.1（2）からリリース **5.0（2j）以降**にダウングレードする場合は、CSR を削除する必要はありません。その場合はにスキップします。ステップ 3 （113 ページ）

a) クラウド APIC GUI で、[Intent] アイコン（複数の円を指す矢印の付いたアイコン）をクリックし、[cAPIC 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) **[クラウド ルータ（Cloud Routers）]** 列でボックスが選択されているリージョンをメモします。

次の手順で[クラウドルータ（Cloud Routers）]列のボックスの選択を解除します。そのため、この手順の最後に、どの領域を再度選択する必要があるかを確認してください。

d) リリースに応じて、必要なリージョンから CSR を除去します。

- リリース 5.1（2）から**リリース 5.0（1）**にダウングレードする場合は、ウィンドウのすべてのリージョンで **[クラウド ルータ（Clour Routers）]** 列の選択を解除（ボックスからチェックを外す）します。ホーム リージョン（テキスト **Cloud APIC Deployed** のあるリージョン）を含みます。
- **リリース 5.0（2j）よりも前のリリース 5.1（2） から 5.0（2）** リリースにダウングレードする場合は、**[クラウドルータ（Cloud Routers）]** 列のホーム リージョン（テキスト **Cloud APIC Deployed** のあるリージョン） で選択解除します（ボックスをオフにする）。

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。

CSR の削除プロセスには約 30 分かかる場合があります。Azure ポータルでリソース グループの仮想マシンを確認することで、CSR の削除プロセスを監視できます。

（注） 必要な CSR が完全に削除されるまで、次の手順に進まないでください。

ステップ 3 イメージのダウンロード中 （105 ページ） で説明している手順を使用して、ダウングレードのイメージをダウンロードします。

ステップ 4 イメージが完全にダウンロードされたら、**[ナビゲーション]** メニューから **[オペレーション]** > **[ファームウェア管理]**を選択します。

[ファームウェア管理] ウィンドウが表示されます。

ステップ 5 **[アップグレードのスケジュール設定]** をクリックします。

[アップグレードのスケジュール設定] ポップアップが表示されます。

ファブリックに障害があることを示すメッセージが表示された場合は、ダウングレードを実行する前にこれらの障害を解決することを推奨します。詳細については、『*Cisco Cloud APIC for Azure User Guide*』の「Viewing Health Details Using the Cisco Cloud APIC GUI」を参照してください。

ステップ 6 **[ターゲット ファームウェア（Target Firmware）]**フィールドで、スクロールダウン メニューからファームウェア イメージを選択します。

ステップ 7 **[開始時間のアップグレード（Upgrade Start Time）]** フィールドで、ダウングレードを今すぐ開始するか、後で開始するかを決定します。

- ダウングレードを今すぐスケジュールする場合は、**[今すぐ（Now）]** をクリックします。ステップ 8（114 ページ） に進みます。
- ダウングレードを後の日付または時刻にスケジュールする場合は、**[後で（Later）]** をクリックし、スケジュールされたダウングレードの日時をポップアップカレンダーから選択します。

ステップ 8 互換性チェック機能を無効にするように特に指示されている場合を除き、**[互換性チェックを無視(Ignore Compatibility Check)]** フィールドでは設定をデフォルトの [オフ (off)] のままにします。

クラウド APIC 内では、システムの現在稼働中のバージョンから特定の新しいバージョンへのダウングレードパスがサポートされているか否かを確認する互換性チェック機能が存在します。**[互換性チェックを無視]** 設定はデフォルトでは[オフ]に設定されているため、システムは可能なダウングレードの互換性をデフォルトで自動的にチェックします。

（注） **[互換性チェックを無視]** フィールドの隣のボックスにチェック マークを入力して互換性チェック機能を無効に設定することを選択する場合、システム内でサポートされていないダウングレードを発生させるリスクを生じ、これにより使用不能な状態を引き起こす可能性があります。

ステップ 9 **[アップグレードをスケジュール（Schedule Upgrade）]** をクリックします。

[ステータスのアップグレード（Upgrade Status）] 領域のメインの **[ファームウェア管理（Firmware Management）]** ウィンドウで、ダウングレードの進行状況をモニタできます。

ステップ 10 ダウングレードが完了したら、必要なCSRを再度追加します。

a) クラウド APIC GUI で、[インターネット（Intent）]アイコン（  ）をクリックし、**[cAPIC セットアップ（cAPIC 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) CSR が含まれていた適切なリージョンを見つけ、それらのリージョンの **[クラウド ルータ（Cloud Routers）]** 列のチェックボックスをオンにして、リリースに応じて CSR を再度追加します。

- リリース 5.1（2）からリリース **5.0（1）** にダウングレードする場合は、ホーム リージョン（**Cloud APIC Deployed** というテキストがあるリージョン）を含む、ウィンドウ内のすべてのリージョンの **[クラウド ルータ（Cloud Routers）]** 列のチェック ボックスをオンにします。
- リリース 5.0（2j）よりも前のリリース 5.1（2）から 5.0（2）リリースにダウングレードする場合は、**[クラウド ルータ（Cloud Routers）]**列のボックスを、ホームリージョン（[**Cloud APIC** Deployed]というテキストが含まれるリージョン）のみをオンにします。

リリース 5.1（2）からリリース **5.0（2j）以降**にダウングレードする場合、CSR を削除しなかったため、CSR を再度追加する必要はありません。ステップ 2 （112 ページ）

d) **[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。

- リリース 5.1（2）からリリース **5.0**（**1**）にダウングレードする場合、CSR バージョンはリリース16.12に戻る必要があります。
- リリース 5.1（2）からリリース **5.0**（**2**）にダウングレードする場合、CSR バージョンはリリース 17.1に戻ります。

システム リカバリの実行

システム リカバリを実行する手順は、移行ベースのアップグレードを実行する手順と同じです。これらの手順については、セクション 移行ベースのアップグレード（89 ページ） を参照してください。

クラウド サービス ルータのアップグレードのトリガー

次のトピックでは、クラウドサービスルータ（CSR）のアップグレードをトリガーするための情報と手順について説明します。

クラウド サービス ルータのアップグレードのトリガー

リリース5.2（1）より前は、のアップグレードをトリガーするたびに、クラウドサービスルータ（CSR）が自動的にアップグレードされます。Cisco Cloud APICリリース5.2（1）以降では、CSRのアップグレードをトリガーし、アップグレードとは無関係にCSRのアップグレードをモニタできます。Cisco Cloud APICこれは、管理プレーン（）とデータプレーン（CSR）のアップグレードを分割できるため、トラフィック損失を減らすのに役立ちます。Cisco Cloud APIC

リリース5.2（1）以降、この機能はデフォルトで有効になっています。デフォルトの前提は、へのアップグレードをトリガーした後にCSRへのアップグレードをトリガーすることです。Cisco Cloud APICこの機能を有効にすると、無効にすることはできません。

この機能を有効にすると、とCSRの適切なアップグレードシーケンスは次のようになります。Cisco Cloud APIC

（注） 次に、CSRへのアップグレードをトリガーするための全体的なプロセスを説明する上位レベルの手順を示します。具体的な手順については、を参照してください。Cisco Cloud APIC GUIを使用したクラウドサービスルータのアップグレードのトリガー （117 ページ）

1. この章の手順に従ってアップグレードします。Cisco Cloud APIC
2. Cisco Cloud APIC のアップグレードが完了するまで待ちます。そのアップグレードが完了すると、システムはCSRがと互換性がなくなったことを認識します。Cisco Cloud APICその後、CSRとに互換性がなく、に設定された新しいポリシーはCSRをアップグレードするま

でCSRに適用されないことを示すメッセージが表示されます。Cisco Cloud APICCisco Cloud APIC

3. AzureポータルでCSRの契約条件を確認し、同意します。
4. CSRアップグレードをトリガーして、の互換バージョンになるようにします。Cisco Cloud APIC

   次の 2 つの方法のいずれかを使用して、CSR アップグレードのトリガープロセスを開始できます。

   - 画面上部のバナーで、**[CSR のアップグレード（Upgrade CSRs）]** リンクをクリックします。
   - **[ファームウェアの管理（Firmware Management）]** ページの **[CSRs]** 領域を使用します。次のとおりに移動します。

     [オペレーション（Operations）] > **[ファームウェア管理]**

     [CSR] タブをクリックし、**[CSRのアップグレード（Upgrade CSRs）]** を選択します。

また、REST APIを使用してCSRのアップグレードをトリガーすることもできます。手順については、REST APIを使用したクラウドサービスルータのアップグレードのトリガー （118 ページ）を参照してください。

注意事項と制約事項

- をアップグレードした後、CSRとに互換性がないことを示すメッセージが表示されない場合は、そのメッセージを表示するためにブラウザを更新する必要があります。Cisco Cloud APICCisco Cloud APIC
- をアップグレードした後、CSRへのアップグレードをトリガーします。Cisco Cloud APIC をアップグレードする前に、CSRへのアップグレードをトリガーしないでください。Cisco Cloud APIC
- CSRへのアップグレードをトリガーすると、停止することはできません。
- CSRへのアップグレードをトリガーした後にエラーが表示された場合は、それらのエラーを確認して解決します。これらのCSRアップグレードエラーが解決されると、CSRアップグレードが自動的に続行されます。

CiscoCloudAPICGUIを使用したクラウドサービスルータのアップグレードのトリガー

ここでは、GUIを使用してクラウドサービスルータ（CSR）へのアップグレードをトリガーする方法について説明します。Cisco Cloud APIC詳細については、「クラウド サービス ルータのアップグレードのトリガー （115 ページ）」を参照してください。

ステップ 1 CSRソフトウェアバージョンがソフトウェアバージョンと互換性がない場合は、まずAzureポータルでCSRの契約条件を確認し、同意します。Cisco Cloud APIC

- Cisco Cloud Services Router（CSR）1000V-Bring Your Own License（BYOL）：

a) Azure Marketplace の検索テキスト フィールドに、*Cisco Cloud Services Router（CSR）1000V*と入力し、表示されるオプションを選択します。

Cisco Cloud Services Router（CSR）1000V オプションが検索候補として表示されます。

b) **[Cisco Cloud Services Router（CSR）1000V]** オプションをクリックします。

Microsoft Azure Marketplace の **Cisco Cloud Services Router（CSR）1000V** ページにリダイレクトされます。

c) **[ソフトウェア プランの選択（Select a software plan）]** ドロップダウン メニューを開きます。

メイン ページに **[ソフトウェア プランの選択（Select a software plan）]**ドロップダウン メニューが表示されない場合、**[プラン+価格設定（Plans + Pricing）]** タブをクリックしてください。このオプションが使用可能であれば、**[ソフトウェア プランの選択（Select a software plan）]** ドロップダウン メニューにアクセスします。

d) **[ソフトウェアプランの選択（Select a software plan）]** ドロップダウンメニューで、適切なオプションを選択します。

- リリース 5.1(2) では、**[Cisco CSR 1000V Bring Your Own License-XE 17.3.1a]** オプションを選択します。
- リリース 5.2(1) 向け、???

e) **プログラマビリティを導入しますか？** フィールドを特定し **[開始（Get Started）]** をクリックします。

f) **[プログラマビリティ導入の設定（Configure Programmability Deployment）]**ページでサブスクリプションまでスクロールし、[ステータス（Status）]列でサブスクリプションのステータスを **[無効（Disable）]** から **[有効（Enable）]** に変更します。

g) **[Save]** をクリックします。

ステップ 2 互換性のあるCSRバージョンへのCSRアップグレードをトリガーするプロセスを開始します。

次の2つの方法のいずれかを使用して、CSRアップグレードのトリガープロセスを開始できます。

- 画面上部のバナーで、[CSRのアップグレード（Upgrade CSRs）]リンクをクリックします。
- [Firmware Management]ページの[CSRs]領域を使用します。次のとおりに移動します。

[オペレーション（Operations）] > [ファームウェア管理]

[CSR]タブをクリックし、[CSRのアップグレード（Upgrade CSRs）]を選択します。

[CSRのアップグレード（Upgrade CSRs）]をクリックすると、CSRをアップグレードするとCSRがリブートし、トラフィックが一時的に中断する可能性があることを示す警告が表示されます。

ステップ 3 この時点でCSRをアップグレードし、トラフィックが一時的に中断された場合は、警告メッセージで[Confirm Upgrade]をクリックします。
CSR ソフトウェアのアップグレードが開始されます。CSRのアップグレードが進行中であることを示すバナーが画面の上部に表示されます。メッセージ内の[View CSR upgrade status]をクリックして、CSRアップグレードのステータスを表示します。

ステップ 4 CSRのアップグレード中に発生する可能性のある障害を修正します。

アップグレード中に障害が発生した場合は、次の場所に移動して障害の詳細情報を取得できます。

Operations Event Analytics Faults > >

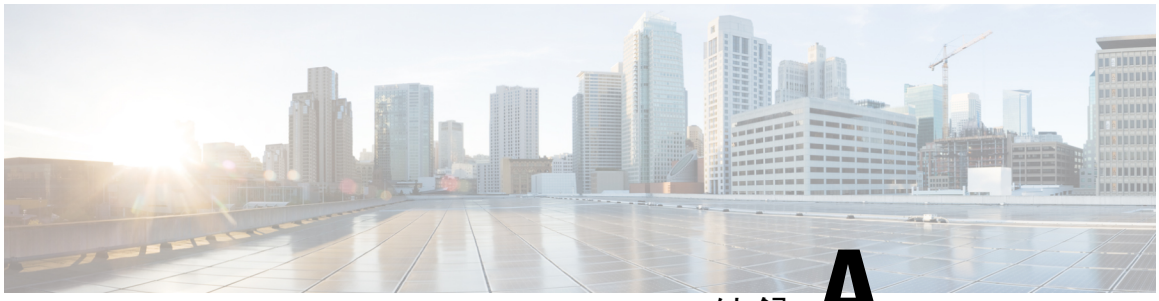
REST APIを使用したクラウドサービスルータのアップグレードのトリガー

ここでは、REST APIを使用してクラウドサービスルータ（CSR）へのアップグレードをトリガーする方法について説明します。詳細については、「クラウド サービス ルータのアップグレードのトリガー （115 ページ）」を参照してください。

クラウドテンプレートでrouterUpgradeフィールドの値を「true」に設定し、REST APIを介してCSRへのアップグレードをトリガーします（routerUpgrade = "true"）。

```
<polUni>
<fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
        <cloudtemplateProfile name="defaultxyz" routerUsername="SomeFirstName"
routerPassword="SomePass" routerUpgrade="true">
        </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="aws" region="us-west-2"/>
            <cloudtemplateVpnNetwork name="default">
                <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />
                <cloudtemplateOspf area="0.0.0.1"/>
            </cloudtemplateVpnNetwork>
          <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
 />
        </cloudtemplateExtNetwork>
```

```
    </cloudtemplateInfraNetwork>
</fvTenant>
</polUni>
```



付録 A

SSH を介したクラウド APIC へのログイン

通常は、で説明されているように、ブラウザからにログインします。Cloud APICセットアップウィザードを使用した Cisco Cloud APIC の設定 （52 ページ）ただし、何らかの理由で SSH 経由で Cloud APIC にログインする必要がある場合は、前のセクションで生成した SSH キーまたは SSH パスワード認証を使用して Cloud APIC にログインする方法について説明します。

SSH キーを使用したクラウド APIC へのログイン

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 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 **[すべてのサービス（All services）]** リンクをクリックし、**[仮想マシン（Virtual Machines）]** リンクをクリックします。

ステップ 3 [仮想マシン（Virtual Machines）]ページでクラウドAPICシステムを見つけ、[パブリックIPアドレス（Public IP address）]列に表示されているIPアドレスを見つけます。

ステップ 4 SSHキーを使用してクラウドAPICにログインします。

- Linuxシステムの場合は、次を入力してCloud APICにログインします。

  ```
  # ssh -i private-key-file admin@public-IP-address
  ```

  ここで、private-key-fileは作成した秘密キーファイルです。Linux または MacOS での SSH キー ペアの生成 （31 ページ）

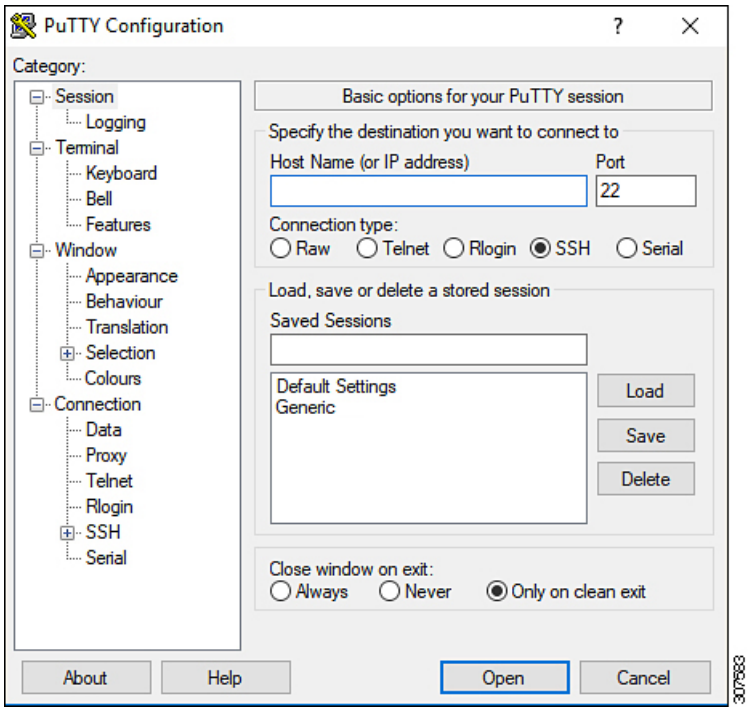
  次に例を示します。

  ```
  # ssh -i azure_key admin@192.0.2.1
  ```

- Windowsシステムの場合、PuTTYを使用してCloud APICにログインします。

  1. Windowsの[スタート]メニューの[すべてのプログラム] [PuTTY PuTTY]に移動して、PuTTY設定プログラムを実行します。 > > > >

2. 左側のナビゲーションバーで[セッション（Session）]をクリックし、クラウドAPICのパブリックIPアドレスを入力します。



3. 左側のナビゲーションバーで、[Connection SSH Auth]をクリックします。＞＞
4. [Authentication parameters]領域で、[Private key file for authentication]フィールドを見つけ、[Browse ...]ボタンをクリックします。
5. で作成した秘密キーファイルに移動し、[Open]をクリックします。Windows での SSH キー ペアの生成 （28 ページ）
6. PuTTYのメインウィンドウで[開く（Open）]をクリックして、クラウドAPICにログインします。ログイン プロンプトが表示されます。
7. クラウド APIC に `admin` としてログインします。

SSHパスワード認証を使用したクラウドAPICへのログイン

公開キーを使用するSSHとは異なり、SSHパスワード認証はデフォルトで無効になっています。ユーザ名とパスワードを使用してクラウドAPICにSSH接続できるように、次の手順を使用してSSHパスワード認証を有効にします。

SSH を介したクラウド APIC へのログイン

ステップ 1 ブラウザウィンドウを開き、セキュアバージョンのHTTP（https：//）を使用して、URLフィールドにIPアドレスを貼り付け、Returnを押してこのCloud APICにアクセスします。

たとえば、 `https://192.0.2.1`です。

ステップ 2 Cloud APICのログインページに次の情報を入力します。

- [Username]：このフィールドにadminと入力します。
- [パスワード（Password）]：クラウドAPICにログインするために指定したパスワードを入力します。
- [ドメイン（Domain）]：[ドメイン（Domain）]フィールドが表示される場合は、デフォルトの[ドメイン（Domain）]エントリをそのままにします。

ステップ 3 ページの下部にある **[ログイン]** をクリックします。

ステップ 4 [Infrastructure System Configuration]に移動し、[System Configuration]ページの[Management Access]タブをクリックします。 >

ステップ 5 SSH設定を編集するには、画面の右上隅にある鉛筆アイコンをクリックします。

SSH 用の設定ページが表示されます。

ステップ 6 [パスワード 認証ステータス（Password Authentication State] フィールドで、[有効（Enabled）] を選択します。

ステップ 7 **[Save]** をクリックします。

これで、公開キーファイルと秘密キーファイルにアクセスしなくても、クラウドAPICにSSH接続できます。

```
# ssh admin@192.0.2.1
```

SSH を介したクラウド APIC へのログイン

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。