



Azure でのクラウド APIC の導入

- [CCR のサブスクリプション \(1 ページ\)](#)
- [必要なリソースプロバイダーの登録 \(4 ページ\)](#)
- [Azure でのアプリケーションの作成 \(6 ページ\)](#)
- [Azure の SSH キーペアの生成 \(7 ページ\)](#)
- [Azure でのクラウド APIC の導入 \(11 ページ\)](#)
- [ロール割り当ての追加 \(18 ページ\)](#)

CCR のサブスクリプション

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

- 25.0(3) までのリリースでは、Cisco Cloud APIC はクラウドサービスルータとして **CSR 1000v** を使用するため、[Cisco Cloud Services Router 1000V への登録 \(1 ページ\)](#) の手順を参照してください。
- 25.0(3) より後のリリースでは、Cisco Cloud APIC はクラウドサービスルータとして **CSR 8000v** を使用するため、[Cisco Cloud Router 8000V への登録 \(3 ページ\)](#) の手順を参照してください。

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 でサブスクリプションするには、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。

CISCO CSR1000V- AX Pkg. Max Performance- XE 17.2.1
 Cisco CSR1000V-AX Pkg. Max Performance-XE 16.12.4a
 Cisco CSR1000V-AX Pkg. Max Performance-XE 17.3.2
 Cisco CSR 1000V Bring Your Own License - XE 16.9
 Cisco CSR 1000V Bring Your Own License - XE 16.7
 Cisco CSR 1000V Bring Your Own License - XE 16.10
 Cisco CSR 1000V Bring Your Own License - XE 16.12
 Cisco CSR 1000V Bring Your Own License - XE 17.1
 Cisco CSR 1000V Bring Your Own License - XE 17.2.1
 Cisco CSR 1000V Bring Your Own License -XE 17.3.1a
 Cisco CSR 1000V Bring Your Own License-XE 16.12.4a
 Cisco CSR 1000V Bring Your Own License -XE 17.3.2

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
<ul style="list-style-type: none"> • リリース 5.1(2) • リリース 5.2(1) • リリース 25.0(1) • リリース 25.0(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 [保存 (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 \(4 ページ\)](#)」に進みます。

Cisco Cloud Router 8000V への登録

最大パフォーマンスを得るには、Cisco Cloud Router (CCR) 8000V-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 Catalyst 8000V Edge Software* と入力し、表示されるオプションを選択します。

[Cisco Catalyst 8000V Edge Software] 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 Catalyst 8000V Edge Software] オプションをクリックします。

Microsoft Azure Marketplace の [Cisco Catalyst 8000V Edge Software] 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 Cloud APIC 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。

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
25.0(3)	Cisco Catalyst 8000V Edge ソフトウェア -BYOL- 17.7.1

- ステップ5 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6 [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7 [保存 (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 (4 ページ)」に進みます。

必要なリソースプロバイダーの登録

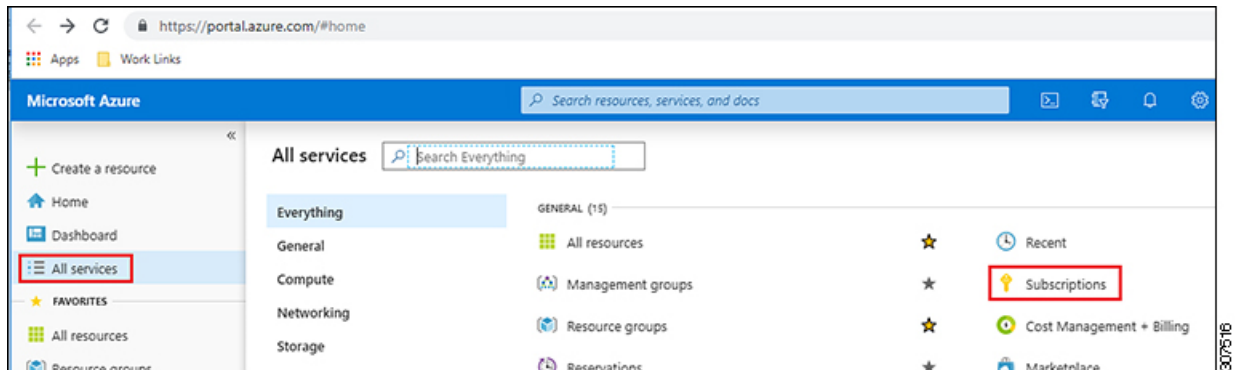
後で追加する可能性があるサブスクリプションがあるテナントを含め、で使用するすべてのサブスクリプションについて、次のリソースプロバイダーを登録する必要があります。Cloud APIC

- 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。

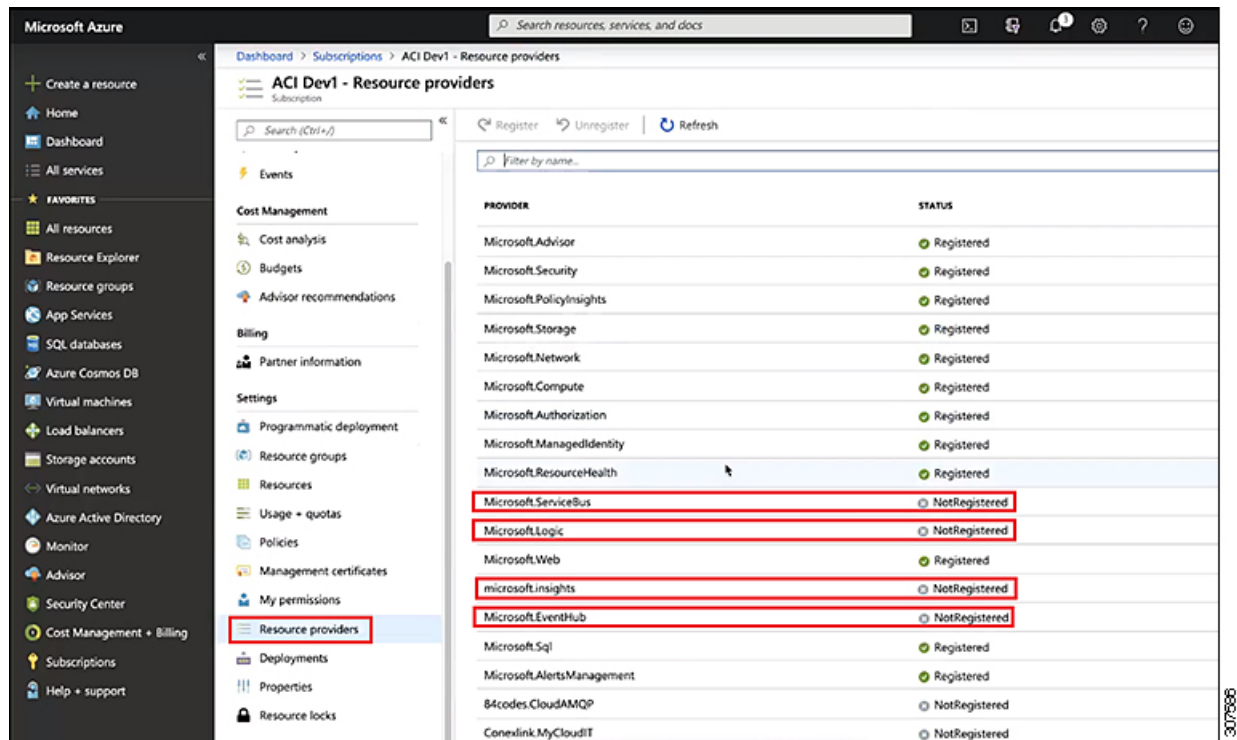


- b) Azure 管理ポータル の [サブスクリプション (Subscriptions)] ページで、Microsoft アカウントのサブスクリプションアカウントをクリックします。

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。

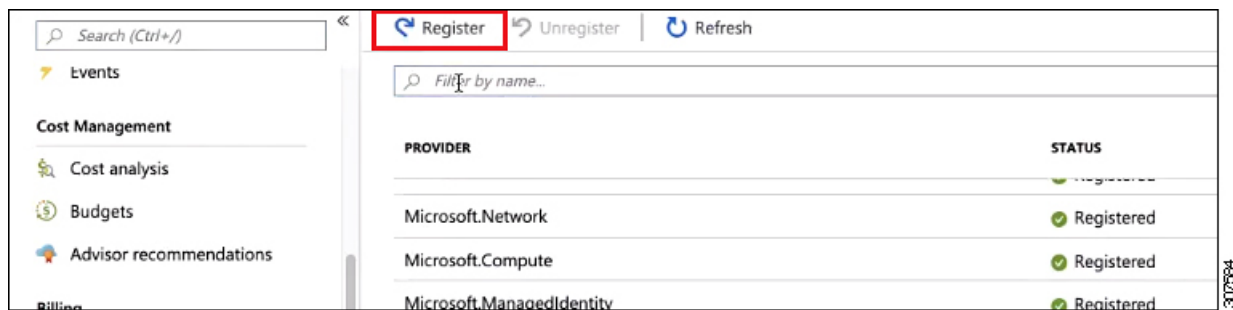


ステップ 2 前のスクリーンショットに示すように、プロバイダーのリストで次の4つのリソースプロバイダーを見つけます。

- 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。

- 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](#)

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

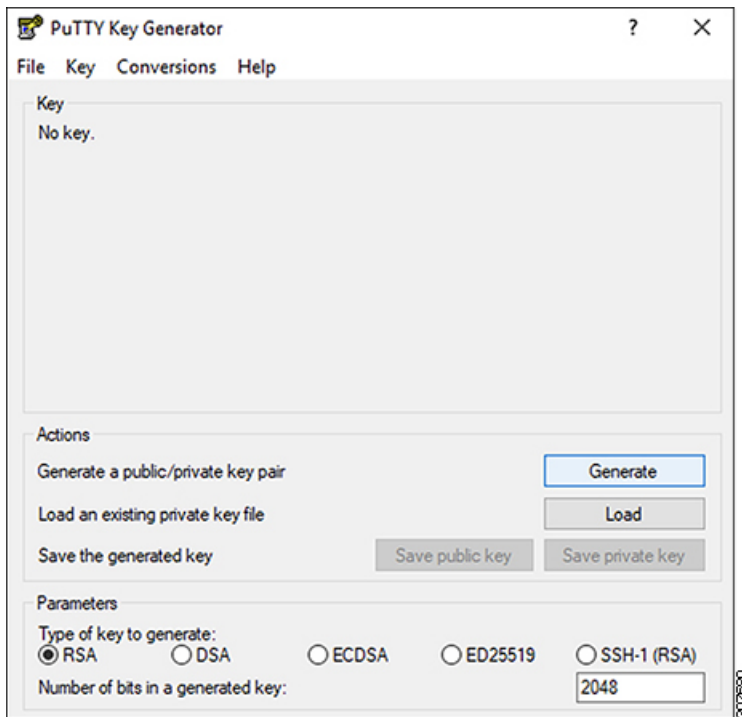
次の手順では、WindowsでSSH公開キーと秘密キーのペアを生成する方法について説明します。LinuxでSSH公開キーと秘密キーのペアを生成する手順については、[を参照してください。Linux または MacOS での SSH キー ペアの生成 \(10 ページ\)](#)

ステップ 1 PuTTYキージェネレーター (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の > **[スタート] メニュー** > **[すべてのプログラム]** > **[PuTTY]** > **[PuTTYgen]** に移動して、PuTTYキージェネレーターを実行します。

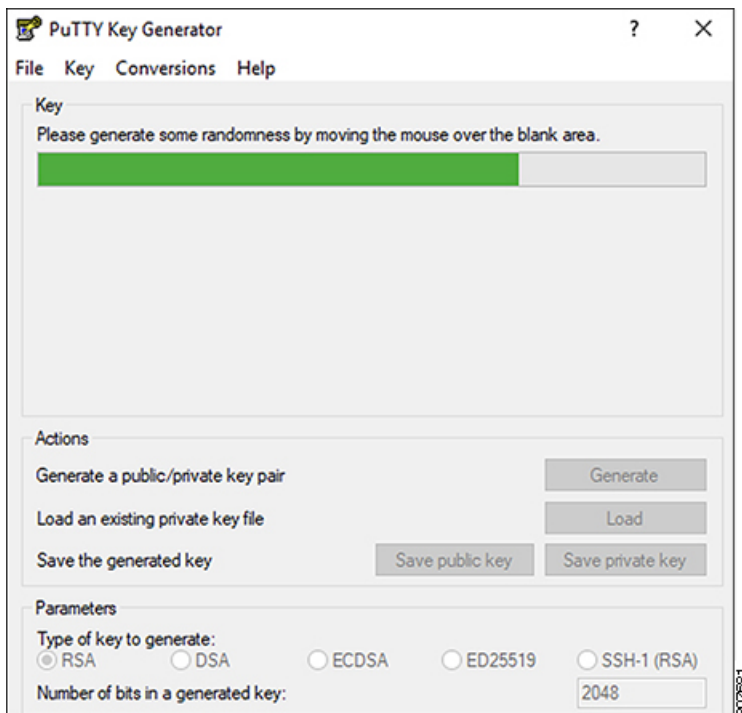
画面にPuTTYキージェネレーターのウィンドウが表示されます。



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。

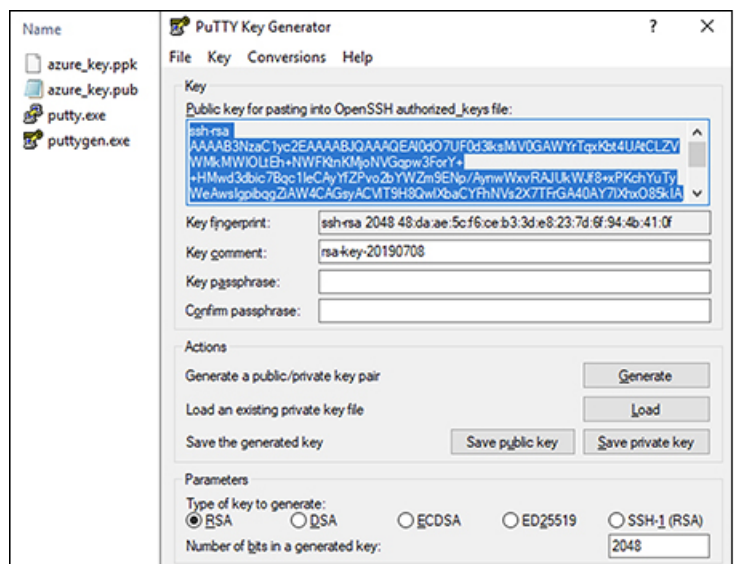
- 公開キーの先頭にssh-rsaテキストを含める。
- 末尾の次のテキスト文字列を除外します。

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

== rsa-key-を含め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 (9 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、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](#)

次のタスク

[Azure でのクラウド APIC の導入 \(11 ページ\)](#) 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 \(7 ページ\)](#)

- 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:gTsQIIAadjgNsgcguifI1oh4XGpVWMdcXVV6U0dyBNs
...
```

- 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](#)

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が含まれます。[Azure でのクラウド APIC の導入 \(11 ページ\)](#)

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](#)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 [プランの選択 (Select a plan)] フィールドで、適切なリリースを選択し、[作成 (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です。

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 ~ 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 \(7 ページ\)](#)
 - [Linux または MacOS での SSH キー ペアの生成 \(10 ページ\)](#)

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。
- **[イメージバージョン (Image Version)]:** このフィールドで適切なリリースを選択します。
- **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。

(注) 172.17.0.0/16からのサブネット (たとえば、172.17.10.0/24) をインフラサブネットとして使用しないことをお勧めします。これは、[インフラサブネットとのサブネット競合問題の解決 \(16 ページ\)](#) で説明されているように、DockerブリッジIPサブネットとの競合を引き起こす可能性があるためです。

- **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。

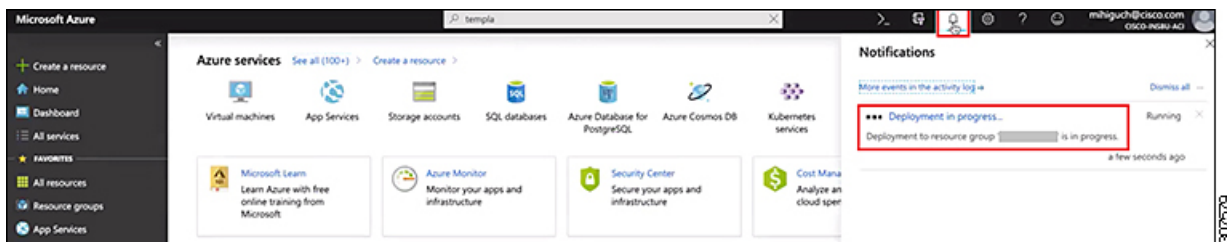
- **[仮想ネットワーク名 (VirtualNetworkName)]** : 必要に応じて、仮想ネットワーク名のデフォルトエントリをそのままにするか、このフィールドのエントリを変更します。
- **[Management NSG Name]** : 管理ネットワークセキュリティグループ名のデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。
- **[Management ASG Name]** : 管理アプリケーションセキュリティグループ名のデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。
- **サブネットプレ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

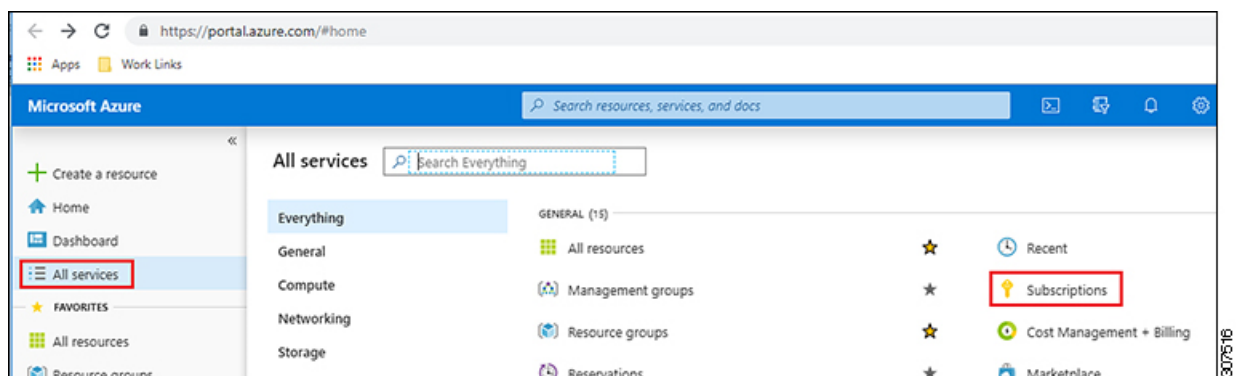
ステップ 8 **[Review + create]** ページで情報を確認し、**[Create]** をクリックします。

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。



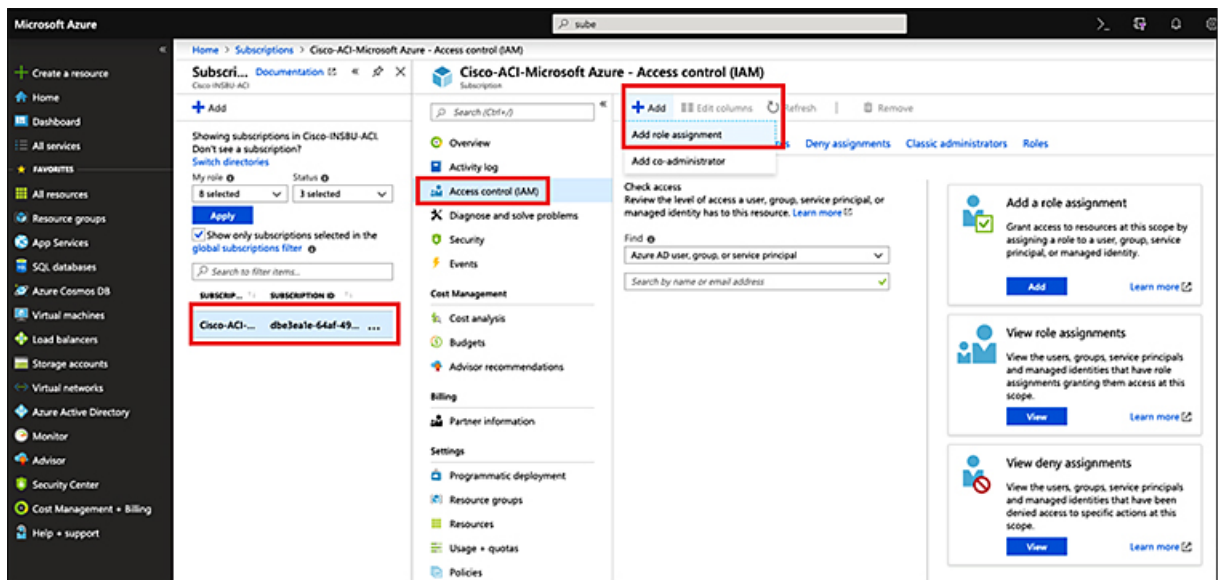
- b) Azure 管理ポータル**[サブスクリプション (Subscriptions)]** ページで、展開されたサブスクリプションアカウントをクリックします。Cloud APIC

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、**[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。

- 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 \(18 ページ\)](#)

インフラサブネットとのサブネット競合問題の解決

状況によっては、Cloud APIC とのサブネットの競合に関する問題が発生することがあります。この問題は、次の条件が満たされた場合に発生する可能性があります。

- Cloud APIC はリリース 25.0(2) で実行されています
- Cloud APIC のインフラ サブネットは、172.17.0.0/16 CIDR 内に設定されています (たとえば、[Azure でのクラウド APIC の導入 \(11 ページ\)](#) の手順の一部として [インフラサブネット] フィールドに 172.17.10.0/24 と入力した場合)。
- Cloud APIC のインフラ サブネットに使用している 172.17.0.0/16 CIDR と重複する何かが構成されています (たとえば、Docker ブリッジ IP サブネットが 172.17.0.0/16 で構成されている場合、Cloud APIC のデフォルト サブネット)。

この状況では、このサブネットの競合が原因で Cloud APIC が CCR プライベート IP アドレスに到達できない可能性があります、Cloud APIC は影響を受ける CCR に対して SSH 接続障害を発生させます。

root として Cloud APIC にログインし、`route -n` コマンドを入力することで、競合の可能性があるかどうかを判断できます。

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
```

以下のような出力が表示されることが想定されます。

```
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          172.17.0.17   0.0.0.0         UG    16     0      0 oobmgmt
169.254.169.0   0.0.0.0       255.255.255.0   U     0      0      0 bond0
169.254.254.0   0.0.0.0       255.255.255.0   U     0      0      0 lxcbr0
172.17.0.0     0.0.0.0       255.255.0.0     U     0      0      0 docker0
172.17.0.12     0.0.0.0       255.255.255.252 U     0      0      0 bond0
172.17.0.16     0.0.0.0       255.255.255.240 U     0      0      0 oobmgmt
```

この出力例では、強調表示されたテキストは、Docker ブリッジが 172.17.0.0/16 で構成されていることを示しています。

これは、Cloud APIC のインフラ サブネットに使用した 172.17.0.0/16 CIDR と重複するため、CCR への接続が失われ、CCR に SSH で接続できないという問題が発生する可能性があります。CCR に ping を実行しようとする、ホストに到達できないというメッセージが表示されます (次の例では、172.17.0.84 が CCR のプライベート IP アドレスです)。

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
From 172.17.0.1 icmp_seq=1 Destination Host Unreachable
From 172.17.0.1 icmp_seq=2 Destination Host Unreachable
From 172.17.0.1 icmp_seq=3 Destination Host Unreachable
From 172.17.0.1 icmp_seq=5 Destination Host Unreachable
From 172.17.0.1 icmp_seq=6 Destination Host Unreachable
^C
--- 172.17.0.84 ping statistics ---
 9 packets transmitted, 0 received, +5 errors, 100% packet loss, time 8225ms
```



```
pipe 4
[root@ACI-Cloud-Fabric-1 ~]#
```

この状況で競合を解決するには、次のような REST API 投稿を入力して、競合の原因となっている他の領域の IP アドレスを変更します。

```
https://{apic}/api/plgnhandler/mo/.xml
<apPluginPolContr>
  <apContainerPol containerBip="<new-IP-address>" />
</apPluginPolContr>
```

たとえば、上記のシナリオ例で示した 172.17.0.0/16 CIDR の下から Docker ブリッジの IP アドレスを移動するには、次のような REST API 投稿を入力します。

```
https://{apic}/api/plgnhandler/mo/.xml
<apPluginPolContr>
  <apContainerPol containerBip="172.19.0.1/16" />
</apPluginPolContr>
```

ここで、172.19.0.1/16 は Docker ブリッジの新しいサブネットです。これにより、Docker ブリッジの IP アドレスが 172.19.0.0/16 CIDR の下に移動し、172.17.0.0/16 CIDR 内で構成されている Cloud APIC のインフラサブネットとの競合がなくなります。

以前と同じコマンドを使用して、競合がなくなったことを確認できます。

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          172.17.0.17    0.0.0.0        UG    16     0      0 oobmgmt
169.254.169.0    0.0.0.0        255.255.255.0  U     0     0      0 bond0
169.254.254.0    0.0.0.0        255.255.255.0  U     0     0      0 lxcbr0
172.17.0.12      0.0.0.0        255.255.255.252 U     0     0      0 bond0
172.17.0.16      0.0.0.0        255.255.255.240 U     0     0      0 oobmgmt
172.19.0.0      0.0.0.0        255.255.0.0    U     0     0      0 docker0
```

この出力例では、強調表示されたテキストは、Docker ブリッジが IP アドレス 172.19.0.0 で構成されていることを示しています。Cloud APIC のインフラサブネットに使用している 172.17.0.0/16 CIDR との重複がないため、CCR との接続に問題はありません。

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
64 bytes from 172.17.0.84: icmp_seq=1 ttl=255 time=1.15 ms
64 bytes from 172.17.0.84: icmp_seq=2 ttl=255 time=1.01 ms
64 bytes from 172.17.0.84: icmp_seq=3 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=4 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=5 ttl=255 time=1.09 ms
64 bytes from 172.17.0.84: icmp_seq=6 ttl=255 time=1.06 ms
64 bytes from 172.17.0.84: icmp_seq=7 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=8 ttl=255 time=1.05 ms
^C
--- 172.17.0.84 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7005ms
rtt min/avg/max/mdev = 1.014/1.061/1.153/0.046 ms
[root@ACI-Cloud-Fabric-1 ~]#
```

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 \(18 ページ\)](#) 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](#)

- [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 \(21 ページ\)](#) 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](#)

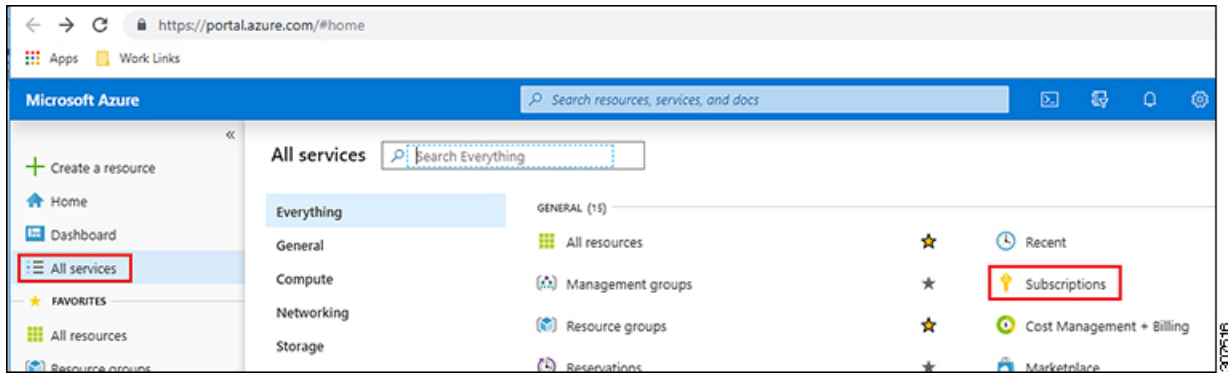
仮想マシンへのロール割り当ての追加

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](#) 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、 [この手順に従います。](#) [アプリへのロール割り当ての追加 \(21 ページ\)](#)
-

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。



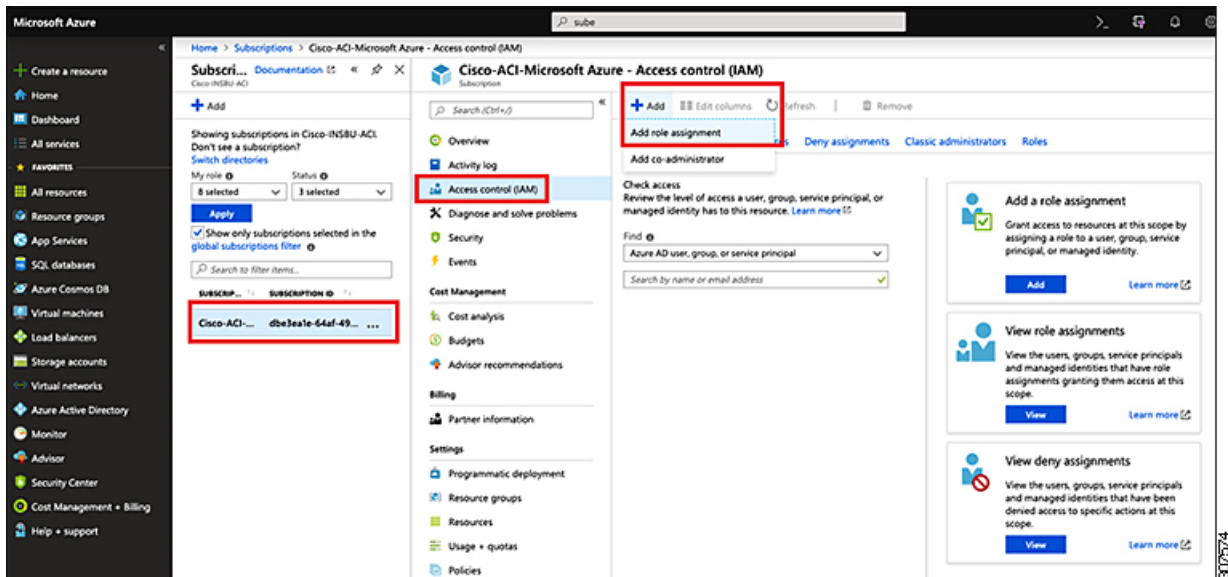
ステップ 2 Azure 管理ポータル内の [サブスクリプション (Subscriptions)] ページで、展開されたサブスクリプションアカウントをクリックします。Cloud APIC

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分以上待つてから、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](#) 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

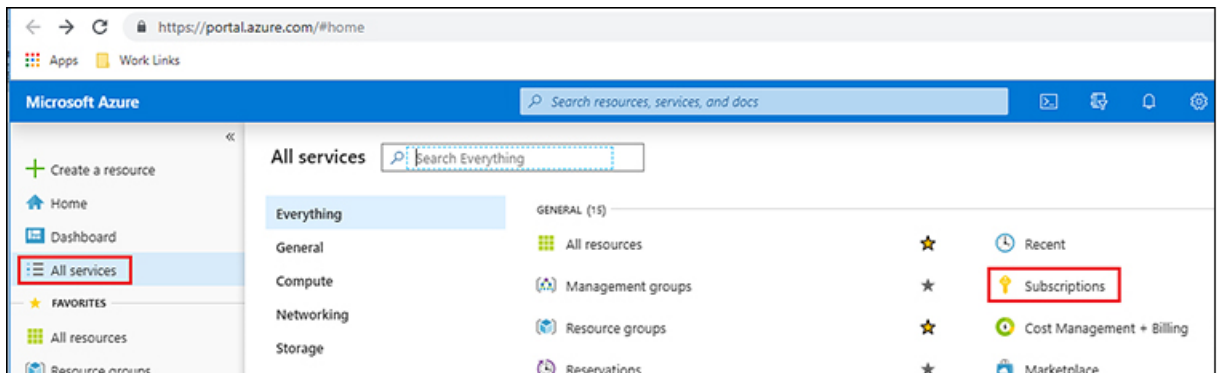
クラウドリソースが特定のアプリケーションを介して管理されるアクセスタイプの管理対象外IDがある場合は、このセクションの手順に従います。AzureサブスクリプションタイプとクラウドAPICテナントの関係の詳細については、[テナント、ID、およびサブスクリプションについて](#)



(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 \(18 ページ\)](#)

ステップ 1 Azure 管理ポータル¹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。

アプリへのロール割り当ての追加



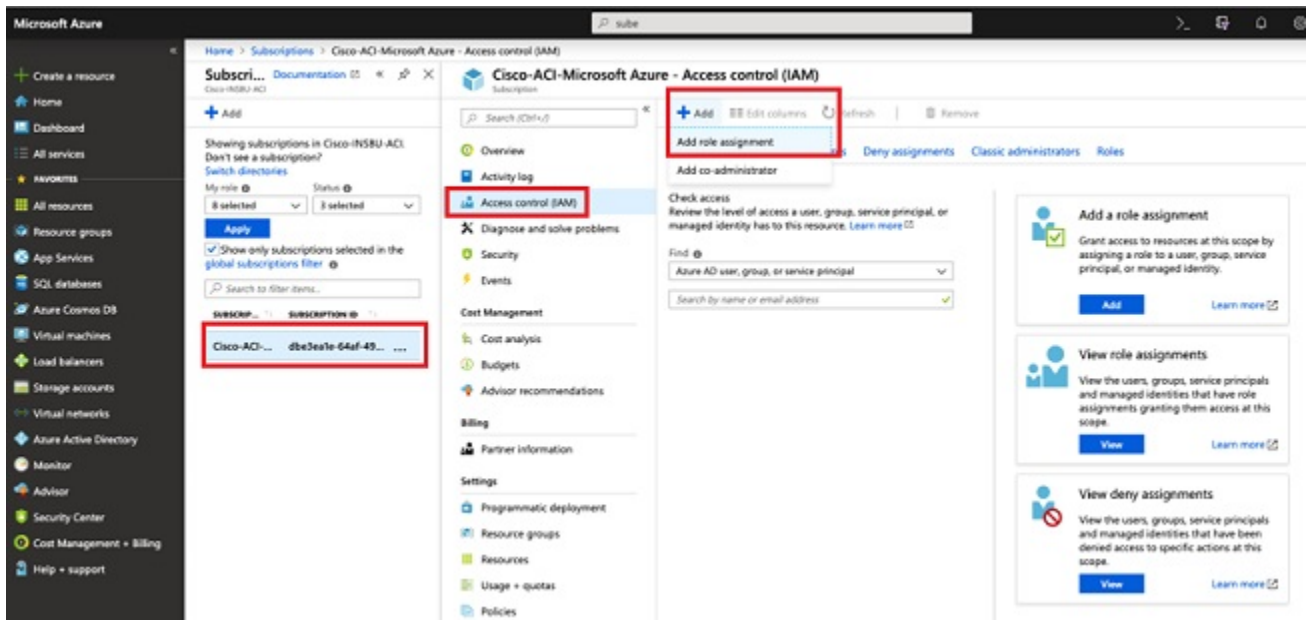
ステップ 2 Azure 管理ポータル内の [サブスクリプション (Subscriptions)] ページで、展開されたサブスクリプションアカウントをクリックします。Cloud APIC

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。


Add role assignment ✕

Role ⓘ
Contributor ▼

Assign access to ⓘ
Azure AD user, group, or service principal ▼

Select ⓘ
App1 ✓

Selected members:

	App1	Remove
---	------	--------

Save Discard

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ヤルを選択します。
- 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 分以上待つ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、CCR 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](#) の設定を続行するには、Cloud APIC に移動します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。