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

Cloud APIC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、Multi-Site と Cisco ACI をオンプレミスで設定して展開する必要があります。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 Cloud APIC によって展開された Cisco Cloud Services Router に接続するために、オンプレミスの IPsec 終端デバイスを構成して展開する必要もあります。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」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。

- Cisco ACIマニュアル： 『Cisco Application Policy Infrastructure Controller（APIC）』のマニュアル（『Operating Cisco Application Centric Infrastructure』および『Cisco APIC Basic Configuration Guide』など）で入手できます。
- Nexus ダッシュボードのマニュアル：Nexus Dashboard のマニュアル（Multi-Site Orchestrator 設置およびアップグレード ガイドなど）で入手できます。
- Cisco Cloud Router（CCR）：
  - クラウド サービス ルータ 1000v：Cisco CSR 1000v のマニュアルで入手できます。

- Cisco Catalyst 8000v Edgeソフトウェア：Cisco Catalyst 8000v Edgeソフトウェアのマニュアルで入手できます。https://www.cisco.com/c/en/us/support/routers/catalyst-8000v-edge-software/series.html

オンプレミス設定情報の収集

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

次のリストを使用して、Cisco Cloud APIC をセットアップ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。

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 CCR 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 CCR 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

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 サイト間構成（AWS または Azure）**：Multi-Site マルチクラウド展開は、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。合計のサイト数は 4 つになります。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）**：マルチサイト マルチクラウド展開は次の組み合わせをサポートします。
  - EVPN 展開モードの 2 つのクラウド サイト（AWS と Azure のみ）
  - リリース 25.0(2) 以降、BGP IPv4 展開モードの 3 つのクラウド（AWS、Azure、および GCP）

  GCP から GCP へは、BGP IPv4 または BGP EVPN のいずれでもまだサポートされていません。
- **クラウドファースト**：**単一クラウド設定**：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。

地域

Cisco Cloud APIC リリース 25.0(1) でサポートされるリージョン制限は次のとおりです。

- AWS および Azure クラウドで 4 つのリージョンを管理できます。4 つのリージョンはすべて、ワークロードの展開と外部接続に使用できます。
- すべてのリージョンを GCP クラウドで管理できます。4 つのリージョンをワークロードの展開と外部接続に使用できます。

Cisco Cloud APIC リリース 25.0(2) 以降では、サポートされるリージョン制限は次のとおりです。

- AWS および Azure クラウドで 16 のリージョンを管理できます。16 のリージョンのうち、4 つのリージョンのみが外部接続可能です。16 のリージョンすべてをワークロードのデプロイに使用できます。
- すべてのリージョンを GCP クラウドで管理できます。ワークロードの展開には 16 のリージョンを使用できますが、外部接続に使用できるのは 4 つのリージョンのみです。

CCR

一部のリージョン内には一定数の CCR 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 CCR を展開する必要があります。
- すべてのリージョンに CCR がある必要はありません。
- 接続を有効にするために CCR が展開されているリージョンの場合：
  - CCRは、4 つの管理対象リージョンすべてに展開できます。
  - 管理対象リージョンごとにサポートされる CCR 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 CCR がサポートされ、クラウド サイトごとに合計 16 の CCR 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 CCR がサポートされ、クラウドサイトごとに合計 32 の CCR がサポートされます。CCR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 CCR 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 CCR 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 CCR がサポートされます。

- Cloud APIC による GCP での CCR 展開はまだサポートされていません。

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、構成したすべてのクラウド リソースを削除して再作成する必要があります。削除されるクラウド リソースには、overlay-2 CIDR とサブネット、Cloud APIC によって展開された Cisco Cloud Router が含まれ、したがって、CCR からすべてのリモート サイトへの IPSec トンネルが含まれます。

命名ルールに使用できる変数

クラウドリソースの命名ポリシーを作成する場合、次の変数を使用して、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 *1*: 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	はい	はい	はい	対応*				○	
アプリケーション セキュリティ グループ（ASG） 最長：80	はい				対応*	対応*		○	

Azure のリソース	${tenant}	${ctx}	${ctxprofile}	${subnet}	${app}	${epg}	${contract}	${region}	${priority}
ネットワーク セキュリティ グループ（NSG） 最長：80	はい				対応*	対応*		○	
ネットワーク セキュリティ グループ ルール 最長：80	はい						はい		Yes *（自動）

表 *2:* 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	はい	はい	はい	対応*		
インターネット側のネットワークロードバランサ 最長：80	はい	はい	はい	対応*		
インターネット アプリケーション ロード バランサ 最長：80	はい	はい	はい	対応*		

Azure のリソース	${tenant}	${region}	${ctxprofile}	${device}	${interface}	${deviceInterfaceDN}
インターネット向けApplication Load Balancer 最長：80	はい	はい	はい	対応*		
デバイスASG 最長：80	はい	はい		対応*	対応*	対応*

命名ルールのガイドラインと制限事項

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

- 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。

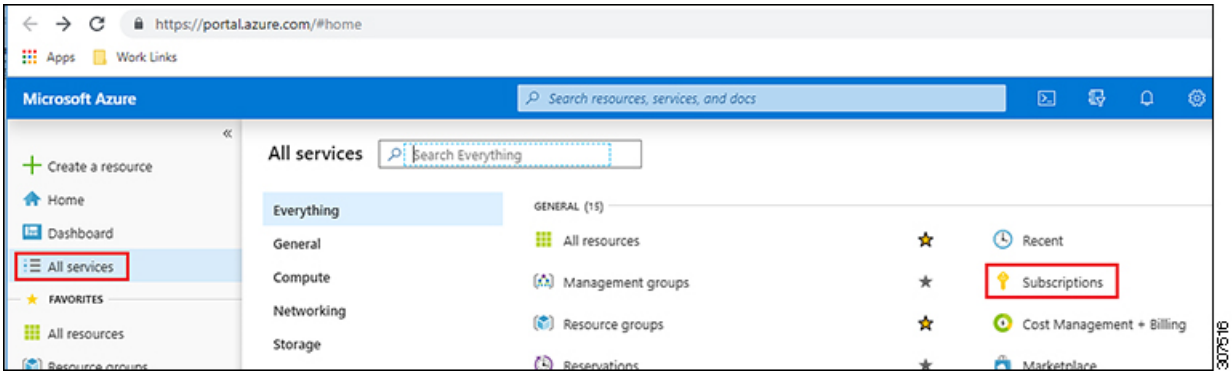
最初に命名規則を定義することをお勧めします。それからテナント設定も行ってください。

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 IP アドレスの特定

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

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。

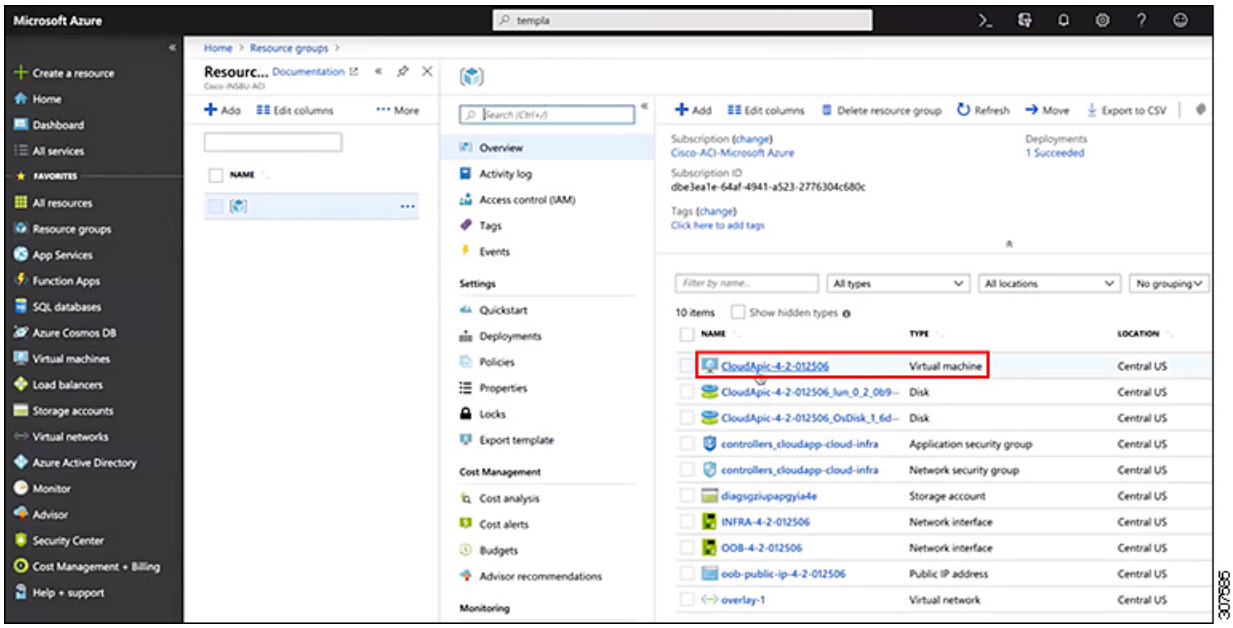
そのサブスクリプションのリソース グループが表示されます。

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

そのリソース グループの概要情報が表示されます。

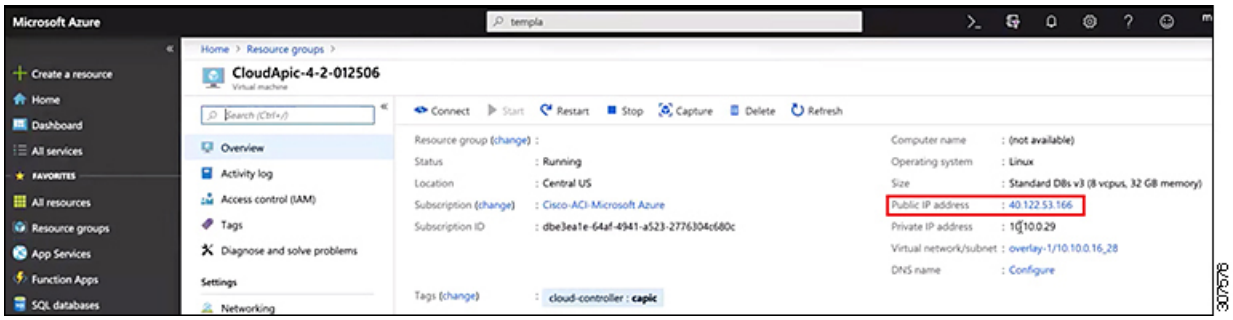
ステップ 5 リソース グループの概要ページで、Cloud APIC VMインスタンス（[TYPE]列の下に **[Virtual machine]** と表示）を見つけ、その VM インスタンスのリンクをクリックします。

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



Cloud APICVM インスタンスの概要情報が表示されます。

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

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

Cloud APIC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。Cloud APICは、必要なAzureコンストラクトと必要なCCRを自動的に展開します。

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

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 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 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 IP アドレスの特定 （9 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 を押してこの Cloud APIC にアクセスします。

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**：**[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。また、ログインするためにページを更新する必要があります。

[Cloud APIC へようこそ] 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 Set Up）]** をクリックします。

[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 と NTP サーバ（DNS and NTP Servers）]** 行で、**[構成の編集（Edit Configuration）]** をクリックします。

[DNS と NTP サーバ（DNS and NTP Servers）] 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 7 **[DNS と NTP サーバ（DNS and NTP Servers）]** ページで、必要に応じて DNS サーバと 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。
- 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、7.d （12 ページ） に進みます。

a) 特定の DNS サーバを使用する場合は、**[DNS サーバ（DNS Servers）]** 領域で **[+ DNS プロバイダの追加（+ 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 サーバ（NTP Servers）]** 領域で、**[+ プロバイダの追加（+ Add Provider）]** 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[優先NTPプロバイダー（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] ページが再び表示されます。

ステップ 9 **[リージョン管理（Region Management）]** 行で、**[開始（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、CCR 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。
- 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 CCR による従来の VPN 接続を有効にするには、**[CCR を介した VPN 接続（VPN Connectivity via CCR）]** 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

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 （12 ページ）Cloud APIC

ステップ 13 Cloud APIC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。

CCRは、Cloud APICが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。

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**：このリージョンに CCR 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 CCR 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 CCR 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 CCR の数の制限について （2 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、またはマルチ サイトを介してクラウド サイト間接続する場合）。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。

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

a) **[全般（General）]** 領域の **[クラウド ルータのサブネット プール（Subnet Pools for Cloud Routers）]** フィールドで、CCR のサブネットを追加する場合は、**[クラウド ルータのサブネット プールの追加（Add Subnet Pool for Cloud Routers）]** をクリックします。

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。

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

次の状況では、この手順で CCR のサブネットを追加します。

- Cloud APICホームリージョンにCCR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。
- 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CCR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（15.f （16 ページ） の **[リージョンごとのルータの数（Number of Routers Per Region）]** フィールドに**2**、**3**、または **4** を入力した場合）。
  - 管理対象リージョンごとに 5 つ以上の CCR 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（15.f （16ページ） の **[リージョンごとのルータの数（Number of Routers Per Region）]** フィールドに **5ー8** を入力した場合）。

次に例を示します。

- 前のページで選択したCloud APICホームリージョンのみがあり、Cloud APICホームリージョンにCSRが展開されているとします。2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Cloud APICのために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CCRが展開されているとします。さらに、**[リージョンごとのルータの数（Number of Routers Per Region）]** フィールド（15.f （16 ページ））で、各管理対象リージョンに展開する 2ー4 のCCRを選択するとします。この場合、2 つの追加サブネット プール（前のページで選択された CCR をもつ各リージョンに対して 1 つのサブネット プール）を追加して、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 つは自動的に作成されます）にする必要が生じます。
- 最後に、各管理対象リージョンの CCR の数を後日 8 個に増やし、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（15.f （16 ページ））の値を **8** に変更するとします。前の画面で3つのリージョン（Cloud APICホームリージョンとCloud APICの管理のために選択した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CCR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CCR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。
  - 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 CCR 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 CCR の数を 8 に増やしたときにもう 1 つ作成）
  - Cloud APICの管理対象として選択した2つの追加リージョンのCCR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CCRの数を8に増やしたときに作成した他の2つ）

b) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pool）]** 領域で、**[IPSec トンネル サブネット ツールの追加（Add IPSec Tunnel Subnet Pools）]** をクリックします。

[IPSec トンネル サブネット ツールの追加（Add IPSec Tunnel Subnet Pools）] ウィンドウが表示されます。

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

c) 必要に応じて、IPSec トンネルに使用するサブネットプールを入力します。

このサブネット プールは、クラウド ルータとブランチ オフィスまたは外部ネットワーク上のルーターとの間にIPSecトンネルを作成するために使用されます。このサブネットは、外部接続のため、IPsecトンネルインターフェイスとクラウドルータのループバックに対処するように使用されます。

このエリアのIPSecトンネルに使用するサブネットをさらに追加できます。サブネットがどのトンネルでも使用されていない場合は、このエリアのエントリを削除できます。

適切なサブネット プールを入力したら、チェックマークをクリックします。

d) **[CSR]** 領域の **[CSR の BGP 自律システム番号（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

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

CCR 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。

- Cloud APIC GUIの管理インターフェイスを使用してCCRを設定できます。
- 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。 Cisco Nexus Dashboard Orchestrator
- 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 CCR の場合

デフォルトでは、この **[有効]** チェック ボックスはオンになっています。これは、CCR にパブリック IP アドレスを割り当てられることを意味します。

- パブリック IP アドレスを CCR 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。

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

- プライベート IPアドレスをCCR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。

CCR 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、CCRに割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、[クラウド リソース（Cloud Resources）] 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。

f) **[リージョンあたりのルータ数（Number of Routers Per Region）]** フィールドで、各リージョンで使用する Cisco Cloud Router（CCR）の数を選択します。

リージョンごとの CCR の数の制限の詳細については、サイト、リージョン、および CCR の数の制限について （2 ページ） を参照してください。

g) **[ユーザー名（Username）]** に、Cisco Cloud Router のユーザー名を入力します。

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

h) **[パスワード（Password）]** に、Cisco Cloud 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。

i) **[価格タイプ]** フィールドで、2 種類のライセンス モデルのいずれかを選択します。

（注） Azuru マーケットプレイスでライセンスを使用するには、**Catalyst 8000V Cisco DNA Essentials** と **Catalyst 8000V Cisco DNA Advantage** の 2 つの PAYG オプションがあります。Cisco Cloud APIC は、**Catalyst 8000V Cisco DNA Advantage** を利用します。

1. **BYOL**
2. **PAYG**

[BYOL 価格タイプ（BYOL Pricing Type）] の場合、手順は次のとおりです。

1. **[ルータのスループット（Throughput of the routers）]** フィールドで、Cisco Cloud 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、展開されているCCR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。

   - CCR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」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。

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

将来のある時点でこの値を変更する場合は、CCR 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。

2. 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ー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。

3. **[ライセンス トークン（License Token）]** フィールドに、Cisco Cloud 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 ライセンシング」を参照してください。

   （注） プライベート IP アドレスを 15.e （15 ページ） の CCR に割り当てた場合、プライベート IP アドレスを使用して CCR のスマート ライセンスを登録するときに、**Cisco Smart Software Manager（CSSM）** に直接接続できます。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。

PAYG 料金設定タイプの場合、手順は次のとおりです。

1. **[VM タイプ]** フィールドで、要件に応じていずれかの VM サイズを選択します。

   Cisco Cloud APIC は、さまざまな VM タイプをサポートしています。以下の表は、使用可能な VM タイプのさまざまなインスタンスとその容量を示しています。

Azure 上の VmName	メモリ	vCPU の数	ネットワーク帯域
DS3V2	14GiB	4	最大 3 ギガビット
DS4V2	28GiB	8	最大 6 ギガビット
F16SV2	32GiB	16	最大 12.5 ギガビット
F32SV2	64GiB	32	最大 16 ギガビット

   （注） 将来のある時点でこの値を変更する場合は、CCR を削除してから、この章のプロセスを再度繰り返し、同じ [VM] フィールドで新しい値を選択する必要があります。

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

このフィールドの値を変更すると、上の表にリストされているCCRの他の要素が変更されます。VM サイズの値を大きくすると、スループットが高くなります。

2. 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(2l) 以降では、TCP 最大セグメントサイズ（MSS）を設定するために **TCP MSS** オプションを使用できます。この値は、クラウドへの VPN トンネルとオンプレミス サイトまたは他のクラウド サイトへの外部トンネルを含む、すべてのクラウド ルータ 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。

（注） ユーザーは、PAYG を選択する際にライセンス トークンを提供する必要はありません。

（注） BYOL でサポートされているすべての機能は、PAYG でサポートされます。

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 （19 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 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

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

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 （4 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 **[スマート ライセンシング]** 行で、**[登録]**をクリックします。

[スマート ライセンシング] ページが表示されます。

ステップ 23 **[スマート ライセンシング]** ページに必要な情報を入力します。

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

Cisco Smart Licensing 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 Cisco Smart Licensing 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
- 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 このページに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。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。

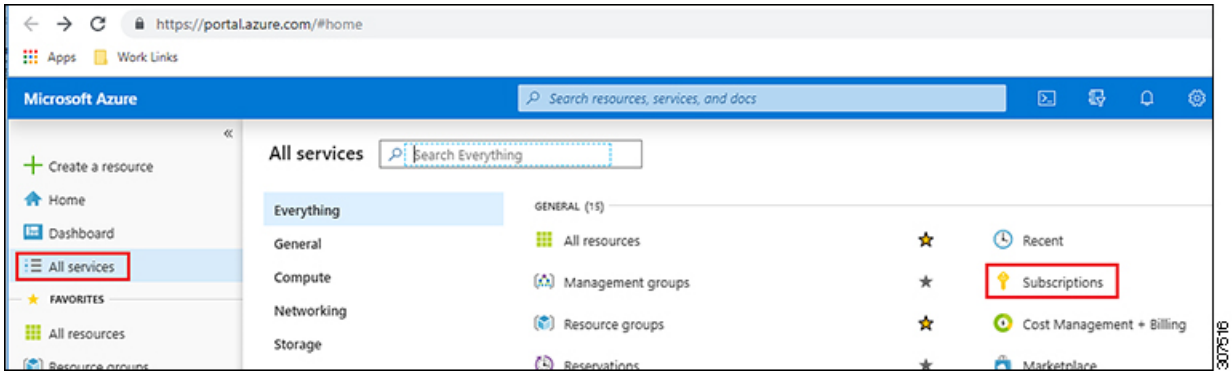
ステップ 25 **[サマリ（Summary）]** ページで情報を確認し、**[完了（Finish）]** をクリックします。

この時点で、Cloud APIC 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。

ステップ 26 CCR 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。

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

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

そのリソースグループの概要情報が表示されます。

e) リソース グループの概要ページで、CCR VMインスタンス（[TYPE] 列の下に **[仮想マシン（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。

CCR 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 CCR カウントです。

例：ct_routerp_centralus_0_0またはct_routerp_centralus_1_0

CCR 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、CCR 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、CCR 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）。マルチサイトを通じた Cisco Cloud APIC の管理
- 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を使用する必要はありません。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

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」と「Cisco Cloud APIC コンポーネントの設定」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。マルチサイトを通じた Cisco Cloud APIC の管理

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。