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、AWS で Cloud APIC 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。詳細については、「Components of Extending Cisco ACI Fabric to the Public Cloud」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 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 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

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**：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。

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。

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。

注 管理対象リージョンあたりの CSR の数は、AWS と Azure で異なります。AWS ではリージョンごとに 4 つの CSR がサポートされ（クラウド サイトごとに合計 16 の CSR）、リリース5.1(2) 以降の場合は Azure で 8 つの CSR がサポートされます。（クラウド サイトあたり合計 32 の CSR）。

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

クラウド APIC IP アドレスの特定

次の手順では、AWS サイトからの IP アドレスを見つける方法について説明します。Cloud APIC

ステップ 1 インフラ テナントの AWS アカウントに移動します。Cloud APIC

ステップ 2 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[EC2]** リンクをクリックします。

[EC2 ダッシュボード (EC2 Dashboard)] 画面が表示されます。

ステップ 3 [EC2 ダッシュボード (EC2 Dashboard)] 画面の **[リソース (Resources)]** 領域には、実行中のインスタンスの数を示すテキストが表示されます (たとえば、**[1 つの実行インスタンス (1 Running Instances)]**)。この実行中のインスタンスのリンクをクリックします。

[インスタンス (Instances)] 画面が表示されます。

ステップ 4 [Capic-1] という名前のインスタンスを選択し、IPv4 パブリック IP 列に表示されている IP アドレスをコピーします。Cloud APIC

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

（注） また、CloudFormation ページに戻り、Cisco Cloud APIC の横にあるボックスをクリックして [出力（Outputs）] タブをクリックすることでも、IP アドレスを取得できます。Cloud APIC[値（Value）] 列に Cisco Cloud APIC の IP アドレスが表示されます。

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

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 AWS コンストラクトと必要な CSR を自動的に展開します。

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。
- Cisco Cloud APIC のクラウド形成テンプレート情報の設定 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 AWS サイトで IP アドレスを取得します。Cloud APIC

手順については、クラウド APIC IP アドレスの特定 （4 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）]：手順の [詳細の指定（Specify Details）] ページで指定したパスワードを入力します。12AWS で Cloud APIC を導入する
- **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。

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

[クラウド 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 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 サーバー**
- **リージョン管理**
- **スマート ライセンス**

ステップ 6 [DNS Servers] 行で、[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。

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 （6 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 AWS Transit Gateway を使用するかどうかを決定します。

Transit Gateway を使用して、リージョン内および TGW ピアリングがサポートされているリージョン間の接続に VPN トンネルを使用しないようにします。詳細については、ドキュメント「*AWS* トランジット ゲートウェイまたは *AWS* トランジット ゲートウェイ コネクトを使用した *VPC* 間の帯域幅の増加」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

AWS Transit Gateway を使用する場合は、**[Transit Gateway の使用（Use Transit Gateway）]** 領域で、**[有効（Enable）]** の横にあるチェックボックスをクリックします。

ステップ 11 **[管理するリージョン（Regions to Manage）]** 領域で、Cloud APIC ホーム リージョンが選択されていることを確認します。

2 で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。AWS で Cloud APIC を導入するこれは、Cloud APIC が展開されている地域（によって管理される地域）であり、[地域（Region）] 列にテキスト cAPICが表示されます。Cloud APIC

ステップ 12 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 VPC 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。

CSR は、展開されているホームリージョンを含む 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クラスタが 2 つのリージョンを管理する場合、これらの 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

ステップ 13 クラウド ルータをこのリージョンにローカルに展開するには、そのリージョンの [Cloud Routers] チェック ボックスをオンにします。

VPC 間または VNET 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 （2 ページ）」を参照してください。

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。

- ステップ 10 （6 ページ） で AWS Transit Gateway Connect 機能を有効にした場合、このウィンドウで [ハブ ネットワーク（Hub Network）] フィールドを使用できます。「15.a （7 ページ）」に進みます。
- ステップ 10 （6 ページ） で AWS Transit Gateway Connect 機能を有効にしていない場合は、15.e （8 ページ） にスキップしてください。

a) **[ハブ ネットワーク（Hub Network）]** 領域で、**[ハブ ネットワークの追加（Add Hub Network）]** をクリックします。

[ハブ ネットワークの追加（Add Hub Network）] ウィンドウが表示されます。

b) **[名前（Name）]** フィールドにハブ ネットワークの名前を入力します。

c) [BGP Autonomous System Number] フィールドに、AWS でゼロを入力して番号を選択するか、各ハブネットワークの値を 64512 ー 65534 の範囲で入力し、フィールドの横にあるチェック マークをクリックします。

独自の BGP 自律番号を設定するには、各ハブネットワークに 64512 ー 65534 の値を入力します。

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

AWS トランジット ゲートウェイのインスタンスごとに異なる番号を使用することをお勧めします。

d) **[CIDR]** 領域で、**[Add CIDR]** をクリックします。

これは、AWS トランジット ゲートウェイ接続 CIDR ブロックで、トランジット ゲートウェイ側の接続ピア IP アドレス（GRE 外部ピア IP アドレス）として使用されます。

1. **[Region]** フィールドで、適切な地域を選択します。
2. **[CIDR Block Range]** フィールドに、中継ゲートウェイ側の接続ピア IP アドレスとして使用される CIDR ブロックを入力します。
3. この CIDR ブロックのこれらの値を受け入れるには、チェック マークをクリックします。
4. AWS トランジット ゲートウェイ接続機能を使用するすべての管理対象リージョンに対して、これらの管理対象リージョンのそれぞれに使用する CIDR ブロックを追加します。

e) CSR のサブネット プールを追加するには、**[クラウド ルータのサブネット プールを追加する（Add Subnet Pool for Cloud Router）]** をクリックし、テキスト ボックスにサブネットを入力します。

最初の 2 つのリージョンの最初のサブネット プールが自動的に入力されます。3 つ以上のリージョンを選択した場合は、追加の 2 つのリージョンのリストにクラウド ルータのサブネットを追加する必要があります。このサブネット プールからのアドレスは、最初の 2 つのリージョンの後にクラウド 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。これはマスク /24 の有効な Ipv4 サブネットである必要があります。

（注） クラウド APIC の導入時に提供される /24 サブネットは、最大 2 つのクラウド サイトに十分です。3 つ以上のクラウドサイトを管理する必要がある場合は、さらにサブネットを追加する必要があります。

f) **[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。

g) 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。

h) **[CSR]** 領域では、**[CSR の BGP 自律システム番号（BGP Autonomous System Number for CSRs）]** フィールドに値を入力します。

BGP ASN の範囲は 1 ー 65534 です。

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

（注） このフィールドでは、自律システム番号として **64512** を使用しないでください。

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

- パブリック IP アドレスを CSR インターフェイスに割り当てるには、**[有効（Enabled）]** チェック ボックスをオンのままにします。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。
- パブリック IP アドレスを CSR インターフェイスに割り当てるには、**[有効]** チェック ボックスをオンのままにします。この場合、接続にはプライベート IP アドレスが使用されます。

（注） パブリック IP アドレスの無効化または有効化は中断を伴う操作であり、トラフィック損失の原因となる可能性があります。

リリース 5.2(1) 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。

j) **[リージョンごとのルータ数（Number of Routers Per Region）]** フィールドで、各リージョンで使用する Cisco 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 （2 ページ）

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

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

m) [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。

（注） 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。

また、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、「AWS パブリック クラウドの要件」を参照してください。

（注） 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。

n) 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

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

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。

o) [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>>

（注） 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場合、パブリック IP アドレスが CSR に対して無効になっている場合、サポートされる唯一のオプションは、AWS Direct Connect または Azure Express Route to Cisco Smart Software Manager（CSSM）です（Administrative Smart Licensing に移動して使用可能））。15.i （9 ページ）この場合、AWS Direct Connect または Azure Express Route を介して CSSM への到達可能性を提供する必要があります。パブリック IP アドレスが無効になっている場合、プライベート IP アドレスが使用されているため、パブリック インターネットは使用できません。したがって、接続には AWS Direct Connect または Azure Express Route であるプライベート接続を使用する必要があります。

ステップ 16 [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 17 **[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 18 **[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。

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 19 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 20 [Summary] ページで情報を確認し、[Close] 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。

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サイト（オンプレミス サイトまたはクラウド サイト）をマッピングしている場合、Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 に移動します。
- Cisco Cloud APIC サイトとともに他のサイトを管理していないクラウド ファースト設定を設定する場合は、追加の設定に Cisco ACI マルチサイト オーケストレータ 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。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。
- [インフラストラクチャ（Infrastructure）]で、[オンプレミス接続（On Premises 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