セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

サイト間接続の設定と展開

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、Cisco Cloud Network Controller の構成と展開を開始する前に、マルチサイト とオンプレミスの Cisco ACI を構成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。また、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 Cisco Cloud Network Controller によって展開された クラウド サービス ルータ 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 Dashboard のマニュアル：Nexus Dashboard のマニュアルで入手できます。Multi-Site Orchestrator 設置およびアップグレード ガイドなどがあります。
- 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 Network Controller 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 Network Controller 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 Network Controller 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

Cisco Cloud Network Controller を使用できるサイトの合計数は、セットアップする構成のタイプによって異なります。

- **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）
  - BGP IPv4 展開モードの 3 つのクラウド サイト（AWS、Azure、Google Cloud）

Google Cloud から Google Cloud への接続は、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**：**単一クラウド構成**：マルチサイト マルチクラウド展開は、単一のクラウド サイト（AWS、Azure または GCP）をサポートします。

地域

サポートされるリージョンの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 Google Cloud 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。

（注） 管理対象リージョンあたりの CCR 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 CCR がサポートされ（クラウドサイトごとに合計 16 の CCR）、Azure では 8 つの CCR がサポートされます。（クラウドサイトあたり合計 32 の CCR）。

- Cisco Cloud Network Controller による Google Cloud での CCR 展開はまだサポートされていません。

Cisco Cloud Network Controller の IP アドレスの特定

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

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

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

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 Cisco Cloud Network Controller 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。

これは、Cisco Cloud Network Controller へのログインに使用する Cisco Cloud Network Controller の IP アドレスです。

（注） また、**CloudFormation** ページに戻り、Cisco Cloud Network Controller 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、Cisco Cloud Network Controller の IP アドレスを取得できます。Cisco Cloud Network Controller の IP アドレスは **[値（Value）]** 列に表示されます。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

Cisco Cloud Network Controller のクラウドインフラストラクチャ構成をセットアップするには、このトピックの手順に従ってください。Cisco Cloud Network Controller は、必要な AWS コンストラクトと必要な CCR 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 Network Controller のクラウド形成テンプレート情報の構成 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、Cisco Cloud Network Controller の IP アドレスを取得します。

手順については、Cisco Cloud Network Controller の IP アドレスの特定 （3 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 Network Controller の構成

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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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 での Cisco Cloud Network Controller の展開
- **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。

[Cisco Cloud Network Controller へようこそ（Welcome to Cisco Cloud Network Controller）] 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**
- **詳細設定**
- **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。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

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。

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、Cisco Cloud Network Controller のホーム 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 での Cisco Cloud Network Controller の展開これは、Cisco Cloud Network Controller が展開されるリージョン（Cisco Cloud Network Controller によって管理されるリージョン）で、[リージョン（Region）] 列に「`Cisco Cloud Network Controller`」というテキストが表示されます。

ステップ 12 Cisco Cloud Network Controller で追加のリージョンを管理します。他のリージョンでVPC 間通信と Hybrid-Cloud、Hybrid Multi-Cloud、または Multi-Cloud 接続を行うように CCR を展開する場合は、追加のリージョンを選択します。

CCRは、Cisco Cloud Network Controller が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。

Cisco Cloud Network Controller 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。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 ACICisco Cloud Network Controller 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 Cisco ACI から単一のサイトと見なされます。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

ステップ 13 リージョンにローカルにクラウド ルータを展開するには、そのリージョンの **Catalyst 8000Vs** チェック ボックスにチェック マークをつけるためにクリックします。

VPC 間通信を行うには、少なくとも 1 つのリージョンに Catalyst 8000V 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 Catalyst 8000V 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。

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.f （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。

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) AWS Transit Gateway Connect 機能を追う使用する場合は、**[TGW Connect]** フィールドで**[有効化]** の隣のチェック ボックスをクリックします。

詳細については、*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。

e) **[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。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

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。

f) CCR 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のアドレスは、最初の 2 つのリージョンの後に追加された、Cisco Cloud Network Controller で管理する必要がある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） Cisco クラウド Network Controller 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。

g) **[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。

h) 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。

i) **[CCR]** エリアでは、**[CCR の BGP 自律システム番号（BGP Autonomous System Number for CCRs）]** フィールドに値を入力します。

BGP ASN の範囲は 1 ー 65534 です。

（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。

j) **[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 アドレスを Catalyst 8000V インターフェイスに割り当てるかどうかを決定します。

プライベート IP アドレスは、デフォルトで Catalyst 8000V インターフェイスに割り当てられます。**[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）]** オプションは、パブリック IP アドレスを Catalyst 8000V インターフェイスにも割り当てるかどうかを決定します。

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。これは、Catalyst 8000V 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。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

- *[パブリック（public）]* IP アドレスを Catalyst 8000V 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アドレスのみをCatalyst 8000V に割り当てるには、オプションを無効化するために **[有効（Enabled）]** の横にあるチェックボックスをオフにします。

Catalyst 8000V 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） Catalyst 8000V 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。Catalyst 8000V にパブリック IP アドレスが割り当てられていない場合は、プライベート IP アドレスだけが表示されます。

k) **[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 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。

（注） 各リージョンで使用される CCR の数を増減させるためにフィールドの値変更する場合、またフィールドの値を変更する前にスマート ライセンス サーバーの登録が正しく同期するようオペレーションが完了するまで待ちます。

- CCR の数を減らす場合、フィールドの値をまた変更する前にそれらの CCR が削除されるまで待ちます。
- CCR の数を増やす場合、フィールドの値をまた変更する前にそれらの CCR が展開されるまで待ちます。

l) **[ユーザー名（Username）]** に、CCR のユーザー名を入力します。

m) **[パスワード（Password）]** フィールドに CCR のパスワードを入力します。

n) **[価格タイプ（Pricing Type）]** 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） AWS 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 Network Controller 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、CCR のスループットを選択します。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

Cisco Catalyst 8000V は、ティアベース（T0/T1/T2/T3）のスループット オプションをサポートしています。次の表に、Cisco Catalyst 8000V 向けのさまざまなルータ スループット設定に使用される AWS EC2 インスタンスを示します。

CCR スループット	AWS EC2 インスタンス
T0 (最大 15M のスループット)	c5.xlarge
T1 (最大 100M のスループット)	c5.xlarge
T2 (最大 1G のスループット)	c5.xlarge
T3 (最大 10G のスループット)	c5.9xlarge

Tier2（T2）は、Cisco Cloud Network Controller でサポートされるデフォルトのスループットです。

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。

（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 **[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、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、「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。

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。

   [TCP MSS] オプションを使用すれば TCP 最大セグメントサイズ（MSS）を構成できます。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。

3. **[ライセンス トークン（License Token）]** フィールドに、CCR 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 > >

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

（注） 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場合、パブリック IP アドレスが 15.j （8 ページ） の CCR 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（**[管理用（Administrative）]> > [スマート ライセンス（Smart Licensing）]**に移動して使用可能です）。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。

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

1. **[VM タイプ（VM Type）]** フィールドで、要件に応じて AWS EC2 インスタンスの 1 つを選択します。

   Cisco Cloud Network Controller は Cisco Catalyst 8000V 仮想ルータを使用し、クラウド ネットワーキングのニーズに合わせて一定範囲の AWS EC2 コンピュート インスタンスをサポートします。以下の表は、AWS 上の Cisco Cloud Network Controller でサポートされているクラウド インスタンス タイプを示しています。

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
c5.xlarge	最大 5 ギガビット スループット	4	8 GiB
c5.2xlarge	最大 10 ギガビット スループット	8	16 GiB
c5.4xlarge	最大 10 ギガビット スループット	16	32 GiB
c5.9xlarge	最大 10 ギガビット スループット	36	72 GiB
c5n.xlarge	最大 25 ギガビット スループット	4	10.5 GiB
c5n.2xlarge	最大 25 ギガビット スループット	8	21 GiB
c5n.4xlarge	最大 25 ギガビット スループット	16	42 GiB
c5n.9xlarge	最大 50 ギガビット スループット	36	96 GiB

   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。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

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。

   [TCP MSS] オプションを使用すれば TCP 最大セグメントサイズ（MSS）を構成できます。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 [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 **[詳細設定（Advanced Settings）]** 行で、**[構成の編集（Edit Configuration）]** をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 18 **[詳細設定（Advanced Settings）]** ページで必要な構成を行います。

- **[コントラクト ベースのルーティング]** コントラクト ベースのルーティング設定は、現在の内部 VRF ルート リーク ポリシーを反映しています。これは、インフラ テナントの下のグローバル ポリシーであり、ブール フラグを使用して、コントラクトがルートマップがない場合にルートを駆動できるかどうかを示します：
  - **オフ（はい**ボックスにチェックが入っていない）：デフォルト設定。ルートがコントラクトに基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。
  - **オン（On）（はい**ボックスにチェックが入っている）：ルートマップが存在しない場合に、契約に基づいてルートが漏洩していることを示します。有効にすると、ルート マップが構成されていないときにコントラクトがルーティングを駆動します。ルートマップが存在する場合、ルート マップは常にルーティングを駆動します。

- **[クラウド ネットワーク コントローラ アクセス権限（Cloud Network Controller Access Privilege）]**：デフォルトで **[ルーティングとセキュリティ（Routing & Security）]** に設定されています。

  アクセス ポリシーを変更する場合は、**[Cisco クラウド ネットワーク コントローラ アクセス権限（Cisco Cloud Network Controller Access Privilege）]** フィールドのスクロール ダウン メニューをクリックし、VPC (クラウド コンテキスト プロファイル) レベルで適用するアクセス ポリシーの 1 つを選択します。
  - **ルーティングとセキュリティ**：デフォルトのアクセスポリシー。Cisco Cloud ネットワーク コントローラにアクセス ポリシーを割り当てない場合、Cisco Cloud ネットワーク コントローラには、デフォルトでルーティングとセキュリティのアクセス ポリシーが適用されます。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

ルーティングとセキュリティ アクセス ポリシーを Cisco Cloud ネットワーク コントローラに割り当てることは、ルーティングとセキュリティを制御できる完全な権限を持っていることを意味します。

- **ルーティングのみ**：ルーティングのみのアクセス ポリシーを Cisco Cloud ネットワーク コントローラに割り当てることは、ルーティング ポリシーとネットワーク接続のみを制御できることを意味します。

ステップ 19 [保存して続行（Save and Continue）] をクリックします。

[基本を構成しましょう（Let's Configure the Basics）]ページに戻ります。

ステップ 20 **[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 21 **[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 Cisco Cloud Network Controller 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 22 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 23 [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、Cisco Cloud Network Controller の内部ネットワーク接続の設定は完了です。

Cisco Cloud Network Controller 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 Network Controller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 Network Controller 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、マルチサイトを介した Cisco Cloud Network Controller の管理 に移動します。
- Cisco Cloud Network Controller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構成をセットアップする場合は、追加の構成に Cisco Cisco Nexus Dashboard Orchestrator を使用する必要はありません。ただし、この場合、Cisco Cloud Network Controller GUIで追加の設定を実行する必要があります。Cisco Cloud Network Controller GUIの [グローバル作成（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 Network Controller GUI のナビゲート」と「Cisco Cloud Network Controller コンポーネントの構成」を参照してください。

Cisco Cloud Network Controller セットアップ ウィザードの構成の確認

このトピックの手順に従って、Cisco Cloud Network Controller セットアップ ウィザードに入力した構成情報が正しく適用されていることを確認します。

Cisco Cloud Network Controller 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。マルチサイトを介した Cisco Cloud Network Controller 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。