



Cisco Cloud Network Controller 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](#) (1 ページ)
- [Cisco Cloud Network Controller の通信ポート](#) (6 ページ)
- [Cisco Cloud Network Controller のインストールワークフロー](#) (7 ページ)

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。



(注) Cisco Nexus pre-EX リーフ スイッチはサポートされていますが、「Cisco Nexus 9372PX および 9372TX スイッチの販売終了およびサポート終了のお知らせ」で説明されているように、これらの古い pre-EX リーフ スイッチのサポート終了が発表されているため、EX または FX リーフ スイッチなどの新しい世代のリーフ スイッチを使用することをお勧めします。

- リリース 4.1 以降および Cisco Nexus Dashboard Orchestrator (NDO) 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 Cisco Application Policy Infrastructure Controller (APIC)。
- 基本設定で展開された Cisco Nexus Dashboard 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します。
- オンプレミス サイトのすべてのリーフスイッチに適切な Cisco ACI ライセンスがあることを確認します。
 - Cisco ACI オンプレミス サイトが単一サイトの場合、オンプレミス リーフスイッチには Essentials ライセンス階層 (またはそれ以上) を使用します。
 - Cisco ACI オンプレミス サイトがマルチサイトの場合、オンプレミス リーフスイッチには Advantage ライセンス階層 (またはそれ以上) を使用します。



(注) オンプレミス データセンターのこれらのライセンス要件は、パブリック クラウドに展開された Cisco Cloud Network Controller の数とは無関係です。Cisco Cloud Network Controller のライセンス要件については、Cisco Cloud Network Controller およびオンプレミス ACI ライセンスの概要を参照してください。

- 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』の「Multipod」の章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>
- 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 Network Controller

の HTTPS アクセス、各 Azure CCR の IPsec ポート、Azure CCR 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。[Cisco Cloud Network Controller の通信ポート \(6 ページ\)](#)

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。



(注) インフラ アカウントで実行できる Cloud Network Controller は 1 つだけです。同じインフラ アカウントで複数の Cloud Network Controller を実行することはサポートされていません。

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。

| QUOTA | PROVIDER | LOCATION | USAGE |
|---|-------------------|----------|--------------------|
| Network Intent Policies | Microsoft Network | West US | 0% 0 of 200 |
| Network Interfaces | Microsoft Network | West US | 0% 0 of 65536 |
| Network Security Groups | Microsoft Network | West US | 0% 0 of 3020 |
| Network Watchers | Microsoft Network | West US | 0% 0 of 1 |
| Outbound Rules per Load Balancer | Microsoft Network | West US | 0% 0 of 5 |
| Packet Captures | Microsoft Network | West US | 0% 0 of 10200 |
| Peerings per Virtual Network | Microsoft Network | West US | 0% 0 of 500 |
| Premium Storage Managed Disks | Microsoft Compute | West US | 0% 0 of 50200 |
| PremiumStorageSnapshots | Microsoft Compute | West US | 0% 0 of 50200 |
| Private Endpoint Redirect Maps | Microsoft Network | West US | 0% 0 of 2147483647 |
| Private Endpoints | Microsoft Network | West US | 0% 0 of 65536 |
| Private Link Services | Microsoft Network | West US | 0% 0 of 32 |
| Public IP Addresses | Microsoft Network | West US | 0% 0 of 1020 |
| Public ip Prefixes | Microsoft Network | West US | 0% 0 of 2147483647 |
| Route filter rules per Route Filter | Microsoft Network | West US | 0% 0 of 1 |
| Route Filters | Microsoft Network | West US | 0% 0 of 1020 |
| Route Filters per Express route BGP Peer... | Microsoft Network | West US | 0% 0 of 1 |
| Route Tables | Microsoft Network | West US | 0% 0 of 200 |
| Routes per Network Intent Policy | Microsoft Network | West US | 0% 0 of 200 |
| Routes per Route Table | Microsoft Network | West US | 0% 0 of 400 |
| Secondary IP Configurations per Network... | Microsoft Network | West US | 0% 0 of 256 |

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 Network Controller オファーを探し、そのページの手順に従います。
- 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 |
| 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 |

| リソース名 | Resource Type | 最小要件 |
|-------------------------------|---------------|------|
| 仮想マシン | コンピューティング | 3 |
| 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

Cisco Cloud Network Controller 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](#)」を参照してください。

CCR

使用可能なライセンス モデルには次の 2 種類があります。

- BYOL (Bring your own license、独自ライセンス使用)
- PAYG (Pay as You Go、従量制)

BYOL

Cisco Cloud Network Controller の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 CCR を展開します。

ルータのスループットの値によって、展開する CCR 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。CCR ライセンスは、Cisco Cloud Network Controller の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構成に基づきます。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。

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、シスコ クラウド サービス ルータ 8000v のさまざまなルータ スループット設定に必要な Azure VM のサイズを示します。

| CCR スループット | Azure VMサイズ |
|----------------------|-------------|
| T0 (最大 15M のスループット) | DS3_v2 |
| T1 (最大 100M のスループット) | DS3_v2 |
| T2 (最大 1G のスループット) | DS3_v2 |
| T3 (最大 10G のスループット) | F16s_v2 |

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。

PAYG

Cisco Cloud Network Controller 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 | メモリー | vCPU の数 | NetworkBw |
|-----------------|-------|---------|---------------|
| 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 |

初回セットアップ時に、[VM タイプ (VM Type)] 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。

Cisco Cloud Network Controller

Cisco Cloud Network Controller は、Standard_D8s_v3 を使用して展開されます。

Cisco Cloud Network Controller の通信ポート

Cisco Cloud Network Controller 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を注意してください。

- Cisco Nexus Dashboard Orchestrator と Cisco Cloud Network Controller の間の通信用：HTTPS (TCP ポート 443 インバウンド/アウトバウンド)

Cisco Cloud Network Controller には、[セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成](#)の最初に Cisco Cloud Network Controller にログインするために使用するものと同じ Cisco Cloud Network Controller 管理 IP アドレスを使用します。

- オンプレミスの IPsec デバイスと、Azure で Cisco Cloud Network Controller によって展開された CCR 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）
2 つの Azure CCR については、[サイト間インフラストラクチャの設定](#) の手順を使用して ISN デバイス構成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。
- Azure で Cisco Cloud Network Controller によって導入された CCR を接続して管理する場合は、各 CCR のパブリック IP アドレスへのポート TCP 22 インバウンド/アウトバウンドを許可します。
- 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 Network Controller のインストール ワークフロー

このセクションでは、Cisco Cloud Network Controller 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、Cisco Cloud Network Controller セットアップウィザード、および Cisco Application Centric Infrastructure (ACI) Nexus Dashboard Orchestrator を使用して実行します。

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 \(1 ページ\)](#)」を参照してください。

2. Azure に Cisco Cloud Network Controller を展開します。

このタスクには、CCR 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 Cisco Cloud Network Controller 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。

セクション「[Azure での Cisco Cloud Network Controller の展開](#)」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 Network Controller を構成します。

このタスクには、Cisco Cloud Network Controller へのログインと、パブリック クラウドに接続するため Cisco Cloud Network Controller により管理されるファブリックの構成が含まれます。Azure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어링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 Network Controller の構成](#)」を参照してください。

4. Nexus Dashboard Orchestrator を使用して Cisco Cloud Network Controller を構成します。

- 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、Cisco Nexus Dashboard 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。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、Cisco Nexus Dashboard Orchestrator GUI へのログイン、クラウドサイトの追加、Nexus Dashboard オプションの有効化、および構成を展開する際の **[展開のみ (Deploy Only)]** オプションの選択が含まれます。

セクション「[マルチサイトを介した Cisco Cloud Network Controller の管理](#)」を参照してください。

5. Cisco ACI ポリシーを Azure パブリック クラウドに拡張するため、Cisco Cloud Network Controller を使用します。

「[Cisco Cloud Network Controller GUI を使用したテナントの作成](#)」および「[Cisco Cloud Network Controller コンポーネントの構成](#)」の項を参照してください。

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。