



Cisco Cloud APIC 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 \(1 ページ\)](#)
- [Cloud APIC 通信ポート \(6 ページ\)](#)
- [Cisco Cloud APIC 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 Cloud APIC の数とは無関係です。Cloud APIC のライセンス要件については、[Cisco Cloud APIC 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 APIC の HTTPS ア

アクセス、各 Azure CCR の IPsec ポート、および 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。[Cloud APIC 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。

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 30200
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
Peering 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 Redress 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 10200
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 10200
Route filters per Express route BGP Peeri...	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 APIC オファーを探し、そのページの手順に従います。

<https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-aci-cloud-apic>

- 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

クラウド APIC 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

Cisco Cloud APIC 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 APIC 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 クラウドサービスルータ 1000v

次の表に、シスコクラウドサービスルータ 1000v 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。

CSR スループット	Azure VM サイズ	Premium Storage	Accelerated Networking
最大 1 GB	DS3_v2	対応	点灯
1 GB - 5 GB	DS4_v2	対応	点灯

リリース 5.1(2) 以降では、シスコクラウドサービスルータ 1000v のバージョン 17.3 CSR で最大 40G のスループットがサポートされています。CSR がサポートする最大スループットは、イ

インスタンスタイプによって異なります。40Gのスループットを実現するには、少なくとも8つのCSRが必要です。

次の表に、40Gスループットを達成するために必要なCSRの数とインスタンスタイプを示します（リージョンごと）。

CSR あたりのスループット	CSR インスタンス タイプ	CSR の数
5 Gbps	F16s_v2	8

Cisco Catalyst 8000V

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 APIC でサポートされるデフォルトのスループットです。

Cisco Cloud APIC

Cisco Cloud APIC はStandard_D8s_v3を使用して展開されます。

Cloud APIC 通信ポート

Cloud APIC 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 Cloud APIC 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）

Cloud APIC には、[セットアップウィザード](#)を使用した [Cisco Cloud APIC の設定](#) の開始時に Cloud APIC にログインするために使用するものと同じ Cloud APIC 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Cloud APICによって導入された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 Cloud APIC 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 APIC のインストール ワークフロー

このセクションでは、Cisco Cloud APIC 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、Cloud APIC Setup Wizard、および (ACI) Multi-Site を使用して実行します。Cisco Application Centric Infrastructure

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 に導入します。Cisco Cloud APIC

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。Cisco Cloud APIC

セクション「[Azure でのクラウド APIC の導入](#)」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 APIC を設定します。

このタスクには、パブリッククラウドに接続するための Cisco Cloud ACI ファブリックへのログインと設定が含まれます。Cisco Cloud APIC 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 APIC の設定](#)」を参照してください。

4. マルチサイトを使用して Cisco Cloud APIC 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、ACI Multi-Site オプションの有効化、および設定を展開する際の **[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「[マルチサイトを通じた Cisco Cloud APIC の管理](#)」を参照してください。

5. Azureパブリッククラウドにポリシーを拡張するために使用します。Cisco Cloud APIC Cisco ACI

「[Cisco Cloud APIC GUI の操作](#)」および「[Cisco Cloud APIC コンポーネントの設定](#)」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。