



Cisco Cloud APIC Azure のインストールガイド、リリース 25.0(x)

初版：2021年9月20日

最終更新：2021年12月17日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



目次

はじめに :	Trademarks iii
--------	-----------------------

第 1 章	新機能および変更された機能に関する情報 1
	新機能および変更された機能に関する情報 1

第 2 章	概要 5
	Cisco ACI ファブリックをパブリック クラウドに拡張する 5
	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 6
	サポートされているクラウド コンピューティング プラットフォームと接続オプション 9
	ポリシーの用語 11
	テナント、ID、およびサブスクリプションについて 11
	Cisco Cloud APIC ライセンシング 14
	Cisco Cloud APIC 関連のマニュアル 16

第 3 章	Cisco Cloud APIC のインストールの準備 19
	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 19
	オンプレミス データ センターの要件 19
	Azure パブリック クラウドの要件 20
	Cisco Cloud APIC 通信ポート 24
	Cisco Cloud APIC のインストール ワークフロー 24

第 4 章	Azure でのクラウド APIC の導入 27
	CCR のサブスクリライブ 27
	Cisco Cloud Services Router 1000V への登録 27

Cisco Cloud Router 8000V への登録	29
必要なリソースプロバイダーの登録	30
Azure でのアプリケーションの作成	32
AzureのSSHキーペアの生成	33
Windows での SSH キー ペアの生成	33
Linux または MacOS での SSH キー ペアの生成	36
Azure でのクラウド APIC の導入	37
インフラサブネットとのサブネット競合問題の解決	42
ロール割り当ての追加	44
仮想マシンへのロール割り当ての追加	44
アプリへのロール割り当ての追加	47

第 5 章	セットアップ ウィザードを使用した Cisco Cloud APIC の設定	51
	サイト間接続の設定と展開	51
	オンプレミス設定情報の収集	52
	サイト、リージョン、および CCR の数の制限について	52
	クラウドリソースの命名	54
	命名ルールに使用できる変数	55
	命名ルールのガイドラインと制限事項	58
	クラウド APIC IP アドレスの特定	59
	セットアップ ウィザードを使用した Cisco Cloud APIC の設定	60
	Cisco Cloud APIC セットアップ ウィザードの設定の確認	71

第 6 章	マルチサイトを通じた Cisco Cloud APIC の管理	73
	Cisco Cloud Network Controller とマルチサイトについて	73
	マルチサイトへの Cisco Cloud APIC サイトの追加	74
	サイト間インフラストラクチャの設定	75
	Cisco Cloud APIC と ISN デバイス間の接続の有効化	76
	Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成	80
	テナントの設定	81
	スキーマの作成	83

アプリケーションプロファイルと EPG の設定	84
ブリッジドメインの作成と VRF への関連付け	84
コントラクトのフィルタの作成	85
コントラクトの作成	86
サイトをスキーマに追加する	87
エンドポイントセレクタの追加	88
マルチサイト構成の確認	92

第 7 章

Cisco Cloud APIC GUI について	95
Cisco Cloud APIC GUI の操作	95
Cisco Cloud APIC GUIを使用したテナントの作成	96
Cisco Cloud APIC コンポーネントの設定	96

第 8 章

システムのアップグレード、ダウングレード、またはリカバリの実行	97
特記事項	97
ソフトウェアのアップグレード	100
ソフトウェアのアップグレードに関する注意事項と制約事項	101
移行ベースのアップグレード	101
既存のクラウドAPIC設定情報の収集	101
既存設定のバックアップ	105
リカバリ テンプレートのダウンロードと展開	106
アップグレード後の手順の実行	109
VNet ピアリングへの移行 (オプション)	114
ポリシーベースのアップグレード	115
イメージのダウンロード中	116
ポリシーベースのアップグレードプロセスを使用したソフトウェアのアップグレード	117
ソフトウェアのダウングレード	122
ソフトウェアのダウングレードの前提条件	122
ソフトウェアのダウングレード	123
ダウングレード後の手順の実行	126

システム リカバリの実行	128
CCR のアップグレードのトリガー	128
CCR のアップグレードのトリガー	128
Cisco Cloud APIC GUI を使用した CCR のアップグレードのトリガー	130
REST API を使用した CCR のアップグレードのトリガー	132

付録 A :

SSH を介したクラウド APIC へのログイン	133
SSH キーを使用したクラウド APIC へのログイン	133
SSHパスワード認証を使用したクラウドAPICへのログイン	135



第 1 章

新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

新機能および変更された機能に関する情報

次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 1: Cisco Cloud APIC のリリース 25.0(3) の新機能と変更された動作

機能または変更	説明	参照先
Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V への移行	Cisco Cloud APIC は、リリース 25.0(3) 以降、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。	
Cisco Cloud Services Router 1000v および Cisco Catalyst 8000V で使用される用語	<p>上記の 2 種類のルータには、次の用語が使用されます。</p> <ul style="list-style-type: none">• CSR : クラウドサービス ルータの省略語です。シスコ クラウドサービス ルータ 1000v を指し、リリース 25.0(3) より前のリリースで使用されました。• CCR : Cisco Cloud ルータの略。リリース 25.0(3) 以降で使用される Cisco Catalyst 8000V を指します。 <p>さらに、このドキュメント全体で、CCR は、リリースに応じて、上記のいずれかのルータの総称として使用されます。</p>	

機能または変更	説明	参照先
マルチサイト オーケストレータの名前の変更	Cisco ACI マルチサイト Orchestrator (MSO) は、2021年8月15日のMSOリリース3.4.1からCisco Nexus Dashboard Orchestrator (NDO)に変更されました。このCisco Cloud APIC ドキュメントでは、MSOのすべてのインスタンスがNDOになりました。	

表 2: Cisco クラウド APIC リリース 25.0(1)の新機能と変更された動作

機能または変更	説明	参照先
Cisco Cloud APIC のリリース番号の変更	リリース 25.0(1) 以降では、Cisco Cloud APIC のリリース番号が変更されています。Cisco Cloud APIC のリリース順序は次のとおりです。 <ul style="list-style-type: none"> • 4.1(x) (AWS のみのサポート) • 4.2(x) • 5.0(x) • 5.1(x) • 5.2(x) • 25.0(x) (このリリース) 	
外部接続オプションの更新	リリース 25.0(1) 以降、インフラ VPC/VNet CCR およびクラウドネイティブルータから任意の外部デバイス(別のクラウドネイティブルータを含む)へのIPv4接続がサポートされるようになりました。さらに、同じクラウド内のクラウドネイティブルータ間、または2つの異なるクラウドベンダー間の外部接続のサポートも利用できます。	

機能または変更	説明	参照先
ルーティングとセキュリティポリシーを個別に構成するためのサポート	リリース 25.0(1) より前のリリースでは、ルーティング ポリシーとセキュリティ ポリシーはコントラクトによって緊密に結合されていました。リリース 25.0(1) 以降、ルーティングとセキュリティ ポリシーを個別に構成するためのサポートが利用できるようになりました。	



第 2 章

概要

- [Cisco ACI ファブリックをパブリッククラウドに拡張する \(5 ページ\)](#)
- [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コンポーネント \(6 ページ\)](#)
- [サポートされているクラウドコンピューティングプラットフォームと接続オプション \(9 ページ\)](#)
- [ポリシーの用語 \(11 ページ\)](#)
- [テナント、ID、およびサブスクリプションについて \(11 ページ\)](#)
- [Cisco Cloud APIC ライセンシング \(14 ページ\)](#)
- [Cisco Cloud APIC 関連のマニュアル \(16 ページ\)](#)

Cisco ACI ファブリックをパブリッククラウドに拡張する

Cisco Application Centric Infrastructure (ACI) プライベートクラウドを所有しているお客様は、パブリッククラウドでワークロードの一部を実行することがあります。ただし、ワークロードをパブリッククラウドに移行するには、別のインターフェイスを操作し、接続を設定してセキュリティポリシーを定義するさまざまな方法を学習する必要があります。これらの課題に対処すると、運用コストが増加し、一貫性が失われる可能性があります。

Cisco Application Policy Infrastructure Controller (APIC) リリース4.1(1)以降では、Cisco ACI を使用してマルチサイトファブリックを Amazon Web Services (AWS) パブリッククラウドに拡張できます。

APIC リリース4.2(1)以降では、Cisco ACI を使用して、マルチサイトファブリックを Microsoft Azure パブリッククラウドに拡張することもできます。

Cisco Cloud APIC とは

Cisco Cloud APIC は、クラウドベースの仮想マシン (VM) に導入できる Cisco APIC のソフトウェアコンポーネントです。Cisco Cloud APICは次の機能を提供します。

- Amazon AWSまたはMicrosoft Azureパブリッククラウドと対話するための既存のインターフェイスと同様のインターフェイスを提供します。Cisco APIC
- クラウド接続の展開と設定を自動化します。

- クラウド ルータ コントロール プレーンを設定します。
- オンプレミス Cisco ACI ファブリックとクラウドサイト間のデータ パスを設定します。
- Cisco ACI ポリシーをクラウド ネイティブ ポリシーに変換します。
- エンドポイントを検出します。

Cisco ACI Extension からパブリック クラウドへのメリットを享受するには

Cisco Cloud APIC は、パブリック クラウドへの拡張の重要な部分です。Cisco ACI Cisco Cloud APIC は、オンプレミスのデータセンターまたはパブリック クラウドの両方またはいずれかに展開されたワークロードに対して一貫したポリシー、セキュリティ、および分析を提供します。

パブリック クラウドへの Cisco ACI 拡張は、オンプレミスのデータセンターとパブリック クラウド間の自動接続を提供し、プロビジョニングとモニタリングを容易にします。また、オンプレミスのデータセンターとパブリック クラウド間、またはクラウド サイト間でポリシーを管理、監視、およびトラブルシューティングするための単一のポイントを提供します。

Azure ガバメント サポート

リリース 4.2(3) 以降では、オンプレミスからクラウドへの接続（ハイブリッドクラウドおよびハイブリッドマルチクラウド）、クラウドサイトからクラウドへの接続（マルチクラウド）、およびシングルクラウドの構成（クラウドファースト）について、Azure Government をサポートしています。

Cisco Cloud APIC は次の Azure 政府リージョンをサポートします。

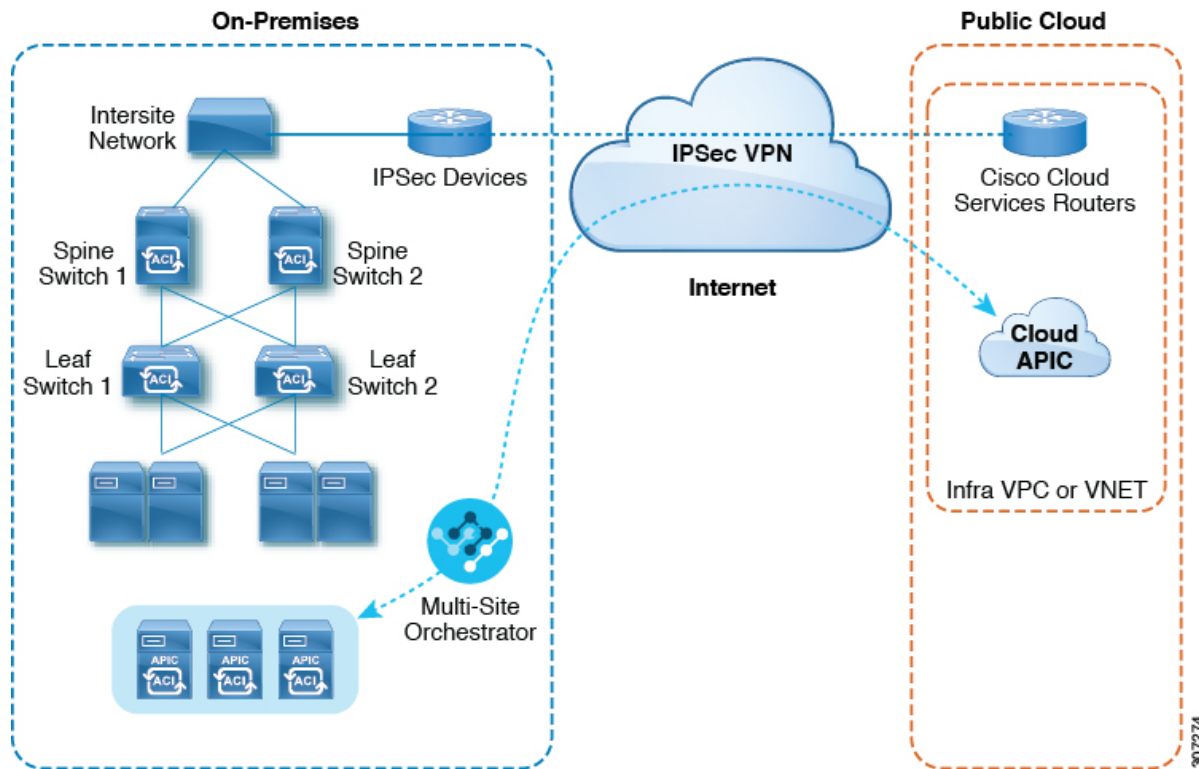
- US DoD セントラル
- US DoD 東部
- 米国政府、アリゾナ州
- 米国政府、テキサス州
- 米国政府、バージニア州

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

マルチサイト ファブリックを Microsoft Azure パブリック クラウドに拡張するには、それぞれに固有のロールを持つ複数のコンポーネントが必要です。

次の図は Cisco Cloud APIC のアーキテクチャの内容を示しています。

図 1: Cisco Cloud APICのアーキテクチャ



オンプレミスデータセンターコンポーネント

Cisco ACI ファブリックおよび Cisco APIC

Cisco ACI では、アプリケーション要件でネットワークを定義できます。このアーキテクチャにより、アプリケーションの導入ライフサイクル全体がシンプルになって最適化され、短時間で完了します。Cisco Application Policy Infrastructure Controller (APIC) の主要コンポーネントです。Cisco ACI これにより、アプリケーションは、ネットワーク、コンピューティング、およびストレージ機能を含むセキュアで共有された高性能リソースプールに直接接続できます。

マルチサイト およびマルチサイト オーケストレータ/Cisco Nexus Dashboard Orchestrator

マルチサイトは、プログラムを利用してアプリケーションがネットワーク要件を定義することを可能にするアーキテクチャです。このアーキテクチャにより、アプリケーションの展開が簡素化・最適化され、そして促進されます。Cisco Cloud APIC を使用してファブリックをパブリッククラウドに拡張するには、マルチサイトをインストールする必要があります。

詳細については、Cisco.com の [マルチサイトのマニュアル](#) およびこのガイドのマルチサイトの構成情報を参照してください。

Cisco Nexus Dashboard Orchestrator (NDO) は、複数のファブリック (サイト) で複数の Cisco Application Policy Infrastructure Controller (APIC) のインスタンスを管理します。

Cisco ACI ファブリックをパブリッククラウドに拡張すると、Cisco Nexus Dashboard Orchestrator はオンプレミスのデータセンターとパブリッククラウド間の接続を作成します。マルチサイト

を使用して、オンプレミスのデータセンターとパブリッククラウド全体にテナントを作成します。



- (注) オンプレミス Cisco ACI ファブリックを設定する必要があります。ファブリック外部接続ポリシーを作成し、マルチサイトに必要なオーバーレイTEPおよびその他の情報を定義します。また、マルチサイトアーキテクチャにオンプレミス Cisco ACI ファブリックを追加する必要があります。Cisco.com で『[Cisco ACI マルチサイト構成ガイド](#)』を参照してください。

詳細については、Cisco.com の [マルチサイトのマニュアル](#) およびこのガイドのマルチサイトの構成情報を参照してください。

IP セキュリティ (IPSec) ルータ

Microsoft Azure のオンプレミスサイトとクラウドサイトの間でIPsec接続を確立するには、インターネットプロトコルセキュリティ (IPsec) 対応のルータが必要です。

Azureパブリッククラウドコンポーネント

Cisco Cloud APIC

Cisco Cloud APIC は次のアクションを実行します。

- パブリッククラウド上のサイトを定義し、クラウドインフラ仮想ネットワーク (VNET) をプロビジョニングし、すべてのリージョンで CCR を管理します。
- パブリッククラウドでポリシーモデルをレンダリングし、クラウドの健全性を管理します。Cisco ACI

詳細については、『[Cisco Cloud APIC Release Notes](#)』を参照してください。

CCR

CCR は、仮想およびクラウド環境で包括的な WAN ゲートウェイとネットワークサービスを提供します。CCR により、企業は WAN をプロバイダーがホストするクラウドに拡張できます。Cisco Cloud APIC ソリューションには 2 つの CCR が必要です。

Cisco Cloud APIC で使用する CCR のタイプは、リリースによって異なります。

- 25.0(3) までのリリースでは、Cisco Cloud APIC では **CSR 1000v** をクラウドサービスルータとして使用します。この CCR の詳細については、[Cisco CSR 1000v のマニュアル](#) を参照してください。
- リリース 25.0(3) 以降、Cisco Cloud APIC では **Cisco Catalyst 8000V** をクラウドサービスルータとして使用します。この CCR の詳細については、[Cisco CSR 8000v のマニュアル](#) を参照してください。

Microsoft Azure パブリッククラウド

Microsoft Azure は、コンピューティング、ストレージ、ネットワーク、データベースなどのオンデマンドサービスを提供するクラウドベースのプラットフォームです。Azure のサブスクラ

イバは、ワークロードを実行できる仮想コンピュータにインターネット経由でアクセスできません。

詳細については、Microsoft Azure の Web サイトのマニュアルを参照してください。

オンプレミスデータセンターとパブリッククラウド間の接続

IPsec VPN

パブリックにルーティング可能なIPアドレスを含み、Microsoft Azure接続に十分な帯域幅を持つ、IPsecルータからのVPNとのインターネット接続が必要です。

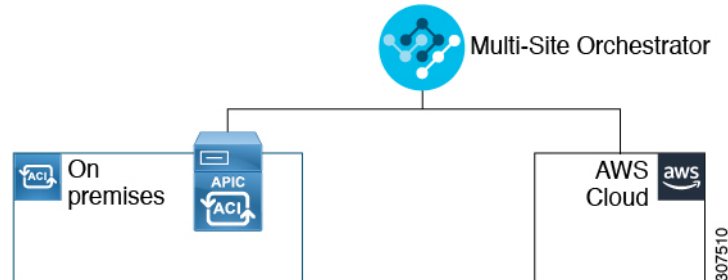
管理接続

オンプレミスのデータセンターの Nexus Dashboard Orchestrator と Microsoft Azure パブリッククラウドの Cisco Cloud APIC の間に管理接続が必要です。

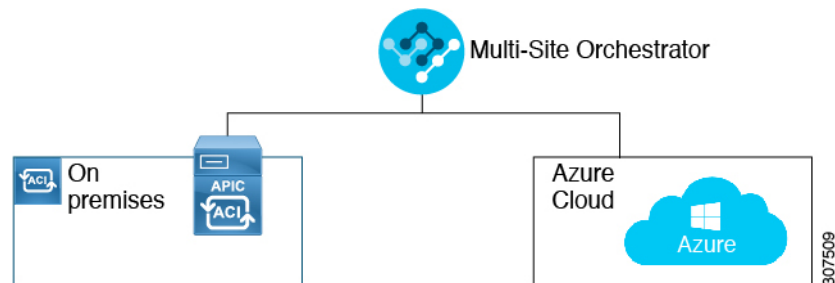
サポートされているクラウドコンピューティングプラットフォームと接続オプション

Cisco Cloud Network Controller は、次のクラウドコンピューティングプラットフォームをサポートしています。

- リリース 4.1(1) の Cisco Cloud Network Controller の初期リリースの一部として、オンプレミスからクラウドへの接続、またハイブリッド-クラウドに対するサポートが提供されており、シスコ Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを拡張することができます。



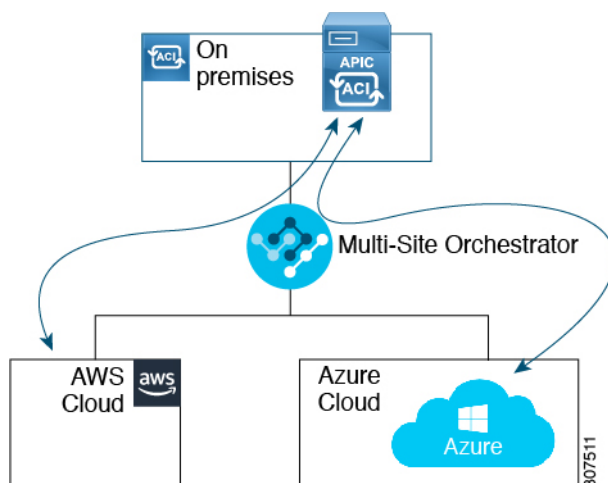
- リリース 4.2(1) 以降、Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Microsoft Azure パブリッククラウドに拡張できるようになりました。



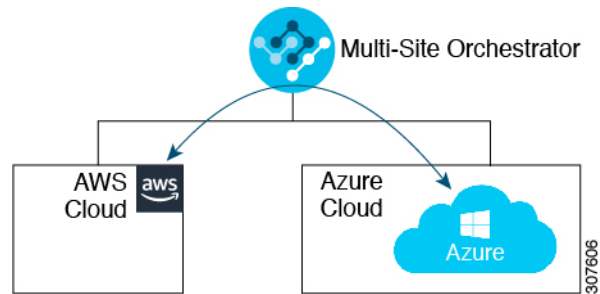
- Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Google Cloud パブリック クラウドに拡張するためのサポートを利用できます。

Cisco Nexus Dashboard Orchestrator を使用して、次のコンポーネント間の接続を確立することもできます。

- オンプレミスからクラウドへの接続 :
 - 次のパブリッククラウドサイトの接続 :
 - オンプレミス Cisco ACI および Amazon AWS パブリック クラウド サイト
 - オンプレミスおよび Microsoft Azure パブリッククラウドサイト Cisco ACI
 - オンプレミス Cisco ACI と Google Cloud パブリック クラウド サイト
 - オンプレミスからシングルクラウドサイトへの接続 (ハイブリッドクラウド)
 - オンプレミスから複数のクラウドサイトへの接続 (ハイブリッドマルチクラウド)



- クラウドサイト間接続 (マルチクラウド) :
 - Amazon AWSパブリッククラウドサイト間 (Amazon AWSパブリッククラウドサイトからAmazon AWSパブリッククラウドサイト)
 - Microsoft Azureパブリッククラウドサイト間 (Microsoft AzureパブリッククラウドサイトからMicrosoft Azureパブリッククラウドサイト)
 - Google Cloud パブリック クラウド サイト間 (Google Cloud パブリック クラウド サイトから Google Cloud パブリック クラウド サイトへ)
 - Amazon AWS、Microsoft Azure、および Google Cloud パブリック クラウド サイト間



さらに、シングルクラウド設定（Cloud First）もサポートされます。

ポリシーの用語

Cisco Cloud APICの主要な機能は、パブリッククラウドのネイティブコンストラクトへのCisco Application Centric Infrastructure（ACI）ポリシーの変換です。

Cisco ACI と Microsoft Azure 間のポリシー マッピング

次の表に、Microsoft Azure のポリシー用語と同等の用語を示します。Cisco ACI

Cisco ACI	Azure
テナント（リージョン、VRF）	リソース グループ
Virtual Routing and Forwarding（VRF）	仮想ネットワーク
BD サブネット	サブネット
契約、フィルタ	アウトバウンドルール、インバウンドルール
EP から EPG へのマッピング	アプリケーションセキュリティグループ（ASG）、ネットワークセキュリティグループ（NSG）
エンドポイント	VM インスタンスのネットワーク アダプタ

テナント、ID、およびサブスクリプションについて

AzureにはActive Directory構造があります。最上位レベルの構造は組織であり、その下にディレクトリ（Azureテナントとも呼ばれます）があります。ディレクトリ内には、1つ以上のAzureサブスクリプションを設定できます。

特定のAzureコンポーネント間の関係は次のとおりです。

テナントサブスクリプションリソースグループリソース >>>

それぞれの説明は次のとおりです。

- 1つのテナントは複数のサブスクリプションを持つことができますが、各サブスクリプションは1つのテナントにのみ属することができます。
- 1つのサブスクリプションに複数のリソースグループを含めることができますが、各リソースグループは1つのサブスクリプションにのみ属することができます。
- 1つのリソースグループは複数のリソースを持つことができますが、各リソースは1つのサブスクリプションにのみ属することができます。

次のセクションでは、これらのコンポーネントについて詳しく説明します。

- [Azure と Cisco Cloud APIC Component のマッピング \(12 ページ\)](#)
- [Azureサブスクリプションについて \(12 ページ\)](#)
- [テナントとアイデンティティについて \(12 ページ\)](#)

Azure と Cisco Cloud APIC Component のマッピング

Cisco Cloud APIC, では、各 Azure リソース グループは 1 つの Cisco Cloud APIC テナントにマッピングされ、1 つの Cisco Cloud APIC テナントが複数の Azure リソース グループを持つことができます。

特定の Cisco Cloud APIC コンポーネント間の関係は次のとおりです。

テナントVRFリージョン >>

Cisco Cloud APIC で VRF を作成すると、新しいリソース グループも Azure に作成されます。

Azureサブスクリプションについて

Azureサブスクリプションは、Azureクラウドサービスの支払いに使用されます。Azureサブスクリプションには、Azure Active Directory (Azure AD) との信頼関係があり、Azure ADを使用してユーザ、サービス、およびデバイスを認証します。複数のサブスクリプションは同じAzure ADを信頼できますが、各サブスクリプションは1つのAzure ADのみを信頼できます。

Azureでは、同じAzureサブスクリプションIDを複数のACIファブリックテナントに使用できません。これは、1つのAzureサブスクリプションを使用してインフラテナントを設定し、同じサブスクリプションで複数のユーザテナントを設定できることを意味します。ACIテナントはAzureサブスクリプションに関連付けられています。

テナントとアイデンティティについて

Azureおよび Cisco Cloud APIC で使用できるさまざまなタイプのテナントとアイデンティティを次に示します。



(注) リリース5.2 (1) より前のリリースでは、管理対象アイデンティティのみがインフラテナントのアクセスタイプとしてサポートされ、管理対象アイデンティティとサービスプリンシパルの両方がユーザテナントのアクセスタイプとしてサポートされていました。

リリース5.2 (1) 以降、マネージドアイデンティティとサービスプリンシパルの両方が、インフラテナントとユーザテナントのアクセスタイプとしてサポートされるようになりました。

マネージドアイデンティティ

マネージドアイデンティティは、Azure AD認証をサポートするリソースに接続するときに使用するアプリケーションのアイデンティティを提供します。アプリケーションは管理対象IDを使用してAzure ADトークンを取得できます。たとえば、開発者が安全な方法でクレデンシャルを保存したり、ストレージアカウントにアクセスしたりするために、アプリケーションでマネージドアイデンティティを使用してAzure KeyVaultなどのリソースにアクセスできます。

<https://docs.microsoft.com/en-us/azure/key-vault/general/overview>

管理対象IDを使用する利点は次のとおりです。

- クレデンシャルにはアクセスできないため、クレデンシャルを管理する必要はありません。
- マネージドIDを使用して、独自のアプリケーションを含むAzure AD認証をサポートする任意のリソースを認証できます。
- マネージドIDは追加コストなしで使用できます。

Azureの管理対象アイデンティティの詳細については、以下を参照してください。

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

管理対象アイデンティティを使用して Cisco Cloud APIC でテナントを構成する場合は、Azureポータルと Cisco Cloud APIC で次の構成を行います。

1. Azureポータルで、仮想マシンのロール割り当てを追加します。このオプションは、Azureサブスクリプションが（同じ組織の）同じAzureディレクトリにある場合に使用します。



(注) Azureサブスクリプションが異なるディレクトリにあり、マネージドIDを使用してテナントを設定する場合は、Azureコンソールに移動し、各サブスクリプションをクリックして同じAzureディレクトリの下にサブスクリプションを移動できます。これは、（異なるサブスクリプションを含む）ディレクトリが同じ親組織の子である場合にのみ実行できます。

仮想マシンのAzureにロール割り当てを追加する手順については、[を参照してください。仮想マシンへのロール割り当ての追加](#)（44 ページ）

2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するときに、**[自分自身の管理対象アイデンティティを作成する (Create Your Own Managed Identity)]** オプションを選

択します。このオプションは、[テナントの設定 \(81 ページ\)](#) の手順を使用して Cisco Cloud APIC GUI で設定します。

サービス プリンシパル (Service Principal)

Azure サービスプリンシパルは、Azure リソースにアクセスするためのアプリケーション、ホステッドサービス、および自動化ツールで使用するために作成された ID です。異なるサブスクリプションでテナントを設定する場合は、サービスプリンシパル ID を使用します。サブスクリプションが同じ組織内の異なる Azure ディレクトリ (Azure テナント) にあるか、サブスクリプションが異なる組織にある可能性があります。

サービス プリンシパルを使用して Cisco Cloud APIC でテナントを構成する場合は、Azure ポータルと Cisco Cloud APIC で次の構成を行います。

1. Azure ポータルで、**アプリケーション**のロール割り当てを追加します。この場合、クラウドリソースは特定のアプリケーションを介して管理されます。

アプリに Azure のロール割り当てを追加する手順については、[を参照してください。アプリへのロール割り当ての追加 \(47 ページ\)](#)

2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するときに、**サービス プリンシパル** オプションを選択します。このページに入力するサブスクリプションは、同じ組織内の異なる Azure ディレクトリ (Azure テナント) に配置することも、異なる組織に配置することもできます。このオプションは、[テナントの設定 \(81 ページ\)](#) の手順を使用して Cisco Cloud APIC GUI で構成します。

共有テナント

Azure サブスクリプションを上記の2つの方法のいずれかにすでに関連付けており、そのサブスクリプションにさらにテナントを作成する場合は、このオプションを選択します。

Cisco Cloud APIC でテナントを**共有テナント**として構成する場合は、Azure ポータルと Cisco Cloud APIC で次の構成を行います。

1. 上記の2つの方法のいずれかで Azure サブスクリプションをすでに関連付けているため、Azure で共有テナント専用の設定を行う必要はありません。共有テナントでは、既存のサブスクリプションにさらにテナントを作成します。
2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するときに **[共有]** オプションを選択します。このオプションは、[テナントの設定 \(81 ページ\)](#) の手順を使用して Cisco Cloud APIC GUI で構成します。

Cisco Cloud APIC ライセンシング

ここでは、Cisco Cloud Application Policy Infrastructure Controller (Cisco Cloud APIC) を使用するためのライセンス要件をリストします。

Cisco Cloud APIC と Cisco Cloud Router



- (注) このセクションのライセンス情報は、リリース 25.0(3) より前のリリースで使用されていた Cisco Cloud Services Router 1000v に特に適用されます。リリース 25.0(3) 以降で使用される Cisco Catalyst 8000V のライセンス情報については、[Cisco Catalyst 8000V \(16 ページ\)](#) を参照してください。

シスコは、管理する仮想マシン (VM) インスタンスごとに Cisco Cloud APIC のライセンスしています。Cisco Cloud APIC バイナリ イメージは Microsoft Azure ポータルで利用可能で、Bring Your Own License (BYOL) モデルをサポートしています。

Essentials Cloud 階層には、パブリッククラウド上の単一のポリシー ドメイン用または単一の Cisco Cloud APIC インスタンス用のライセンスが含まれています。Cisco Cloud APIC の複数のインスタンスを展開する場合は、Cisco Cloud APIC が管理する VM インスタンスごとに Advantage Cloud ライセンスを購入します。

ライセンスの詳細は、『[Cisco Application Centric Infrastructure Ordering Guide](#)』を参照してください。

1 つ以上の Cisco Cloud APIC ライセンスを取得することに加えて、Cisco Smart Software Licensing に Cisco Cloud APIC を登録する必要があります。

シスコのスマート ライセンスは、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。スマートソフトウェアライセンスの詳細については、<https://www.cisco.com/go/smartlicensing> を参照してください。

Cisco Cloud APIC および CCR を登録するには、次の手順を実行します。

1. 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。
2. スマートアカウントにログインします。
 1. Smart Software Manager : <https://software.cisco.com/>
 2. Smart Software Manager サテライト:
<https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html>
3. 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。
4. 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。



- (注) Cisco Cloud APIC は、Cisco Cloud APIC セットアップウィザードの [ルータの処理量 (Throughput of the routers)] フィールドで選択した設定に基づいて、適切なサイズの CCR を展開します。



(注) 将来のある時点で展開から CCR を削除すると (Cisco Cloud APIC GUI またはクラウドコンソールまたはポータルを使用して CCR を削除することにより)、CCR スマートライセンスサーバがその CCR から切断されます。削除された CCR インスタンスは 90 日間は失効としてマークされ、その期間は他の新しい CCR によってライセンスを再利用できません。

この状況を回避するには、「[Cisco CSR 1000v ライセンスの再ホスト](#)」の手順を使用して、CSR 1000v ライセンスを再ホストします。

Cisco Catalyst 8000V

Cisco Catalyst 8000V は、サブスクリプションベースのライセンスをサポートしています。

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、[Cisco Catalyst 8000V Edge ソフトウェア](#)を参照してください。
- 層に基づくさまざまなスループットの詳細については、[Azure パブリッククラウドの要件 \(20 ページ\)](#) を参照してください。

Cisco Cloud APIC は、「Cisco DNA Advantage」サブスクリプションを利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、[Cisco DNA ソフトウェア SD-WAN およびルーティング マトリックス](#)を参照してください。

オンプレミスの Cisco ACI ライセンス

1 つ以上のクラウドサイトを持つ単一のオンプレミス Cisco ACI サイトがある場合は、Essential、Advantage、Premier のいずれかのライセンスレベルでオンプレミス Cisco ACI ファブリックを実行できます。

Microsoft Azure

リリースに応じて、Microsoft Azure Marketplace から登録する必要があります。

- リリース 25.0(3) までのリリースでは、[Cisco Cloud Services Router \(CSR\) 1000V-BYOL for Maximum Performance](#) に登録します。
- リリース 25.0(3) 以降では、[Cisco Catalyst 8000V Edge Software - BYOL](#) に登録します。

Microsoft Azure Marketplace からサブスクライブするには、[この手順に従ってください](#)。CCR のサブスクライブ (27 ページ)

Cisco Cloud APIC 関連のマニュアル

Cisco Cloud APIC (APIC)、マルチサイト、および Microsoft Azure に関する情報は、さまざまなリソースから入手できます。

シスコのドキュメント

Cisco.com でシスコ製品のマニュアルを参照してください。

- [『Cisco Application Policy Infrastructure Controller Release Notes』](#)

他の Cisco Cloud APIC ドキュメントのリストが含まれています。

- [Cisco Cloud APIC のドキュメント](#)

ビデオ、リリースノート、基礎、インストール、設定、およびユーザガイドが含まれています。

- [マルチサイトのドキュメント](#)

ビデオ、リリースノート、インストール、設定、およびユーザガイドが含まれています。

- [CCR のドキュメント](#)

リリースノート、コマンドリファレンス、データシート、インストール、アップグレード、および設定ガイドが含まれています。

Microsoft Azure のマニュアル

Microsoft Azure Web サイトで、ユーザガイド、FAQ、ケーススタディ、ホワイトペーパーなどのドキュメントを検索できます。



第 3 章

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](#) (19 ページ)
- [Cisco Cloud APIC 通信ポート](#) (24 ページ)
- [Cisco Cloud APIC のインストール ワークフロー](#) (24 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する必要があります。
- Cisco SMART Licensing アカウントと Leaf Advantage ライセンス。Cisco ACI
オンプレミスサイト上のすべてのリーフには、リーフライセンスが必要です。Cisco ACI
- 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 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、Release 4.0 (1)』の「Multipod」の章を参照してください。
- 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。[Cisco Cloud APIC 通信ポート \(24 ページ\)](#)

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。

The screenshot shows the 'Usage + quotas' page in the Azure portal. The table displays the following data:

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 5000
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 10000
Peerings per Virtual Network	Microsoft.Network	West US	0% 0 of 500
Premium Storage Managed Disks	Microsoft.Compute	West US	0% 0 of 50000
PremiumStorageSnapshots	Microsoft.Compute	West US	0% 0 of 50000
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 1000
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 1000
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 オファァへのアクセス。Azure Marketplace で Cisco Cloud APIC オファァを探し、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
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（30ページ）](#)」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 クラウド APIC

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

Cisco Cloud APIC 通信ポート

Cisco 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 Cisco 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）

Cisco 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（60 ページ）](#) の最初に Cisco Cloud APIC にログインするために使用するものと同じ Cisco 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 Cisco Cloud APIC 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（75 ページ）](#) 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 APIC によって展開された CCR を接続および管理する場合は、各 CCR のパブリック IP アドレスへのポート TCP 22 のインバウンド/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 \(19 ページ\)](#)」を参照してください。

2. Azure での Cisco Cloud APIC の展開

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 APIC 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 でのクラウド APIC の導入 \(27 ページ\)](#)」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た Cisco Cloud APIC を構成します。

このタスクには、Cisco Cloud APIC へのログインと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) ピアリング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 \(51 ページ\)](#)」を参照してください。

4. マルチサイトを使用して Cisco Cloud APIC を設定します。

- 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 \(73 ページ\)](#)」を参照してください。

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

「[Cisco Cloud APIC GUI の操作 \(95 ページ\)](#)」および「[Cisco Cloud APIC コンポーネントの設定 \(96 ページ\)](#)」の項を参照してください。



第 4 章

Azure でのクラウド APIC の導入

- [CCR のサブスクリプション](#) (27 ページ)
- [必要なリソースプロバイダーの登録](#) (30 ページ)
- [Azure でのアプリケーションの作成](#) (32 ページ)
- [Azure の SSH キーペアの生成](#) (33 ページ)
- [Azure でのクラウド APIC の導入](#) (37 ページ)
- [ロール割り当ての追加](#) (44 ページ)

CCR のサブスクリプション

Cisco Cloud Services Router (CSR) に登録する手順は、Cisco Cloud APIC ソフトウェアのリリースによって異なります。

- 25.0(3) までのリリースでは、Cisco Cloud APIC はクラウド サービス ルータとして **CSR 1000v** を使用するため、[Cisco Cloud Services Router 1000V への登録](#) (27 ページ) の手順を参照してください。
- 25.0(3) より後のリリースでは、Cisco Cloud APIC はクラウド サービス ルータとして **CSR 8000v** を使用するため、[Cisco Cloud Router 8000V への登録](#) (29 ページ) の手順を参照してください。

Cisco Cloud Services Router 1000V への登録

最大パフォーマンスを得るには、Cisco Cloud Services Router (CSR) 1000V-Bring Your Own License (BYOL) に登録する必要があります。Microsoft Azure Marketplace でサブスクリプションするには、次の手順を実行します。

ステップ 1 [Azure Marketplace](#) の検索テキスト フィールドに、*Cisco Cloud Services Router (CSR) 1000V* と入力し、表示されるオプションを選択します。

Cisco Cloud Services Router (CSR) 1000V オプションが検索候補として表示されます。

ステップ 2 [**Cisco Cloud Services Router (CSR) 1000V**] オプションをクリックします。

Microsoft Azure Marketplace の **Cisco Cloud Services Router (CSR) 1000V** ページにリダイレクトされます。

ステップ 3 [ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューを開きます。

メイン ページに [ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューが表示されない場合、[プラン+価格設定 (Plans + Pricing)] タブをクリックしてください。このオプションが使用可能であれば、[ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューにアクセスします。

ステップ 4 [ソフトウェアプランの選択 (Select a software plan)] ドロップダウンメニューで、[Cisco CSR 1000V Bring Your Own License] オプションがリストされている領域を見つけます。

```

CISCO CSR1000V- AX Pkg. Max Performance- XE 17.2.1
Cisco CSR1000V-AX Pkg. Max Performance-XE 16.12.4a
Cisco CSR1000V-AX Pkg. Max Performance-XE 17.3.2
Cisco CSR 1000V Bring Your Own License - XE 16.9
Cisco CSR 1000V Bring Your Own License - XE 16.7
Cisco CSR 1000V Bring Your Own License - XE 16.10
Cisco CSR 1000V Bring Your Own License - XE 16.12
Cisco CSR 1000V Bring Your Own License - XE 17.1
Cisco CSR 1000V Bring Your Own License - XE 17.2.1
Cisco CSR 1000V Bring Your Own License -XE 17.3.1a
Cisco CSR 1000V Bring Your Own License-XE 16.12.4a
Cisco CSR 1000V Bring Your Own License -XE 17.3.2

```

ステップ 5 Cisco Cloud APIC ソフトウェアリリースに応じて、適切なオプションを選択します。

クラウドAPICリリースの場合	この特定のオプションを選択します
リリース 4.2x	Cisco CSR 1000V Bring Your Own License-XE 16.12
リリース 5.0(1)	Cisco CSR 1000V Bring Your Own License-XE 16.12
Release 5.0(2)	Cisco CSR 1000V Bring Your Own License-XE 17.1
<ul style="list-style-type: none"> • リリース 5.1(2) • リリース 5.2(1) • リリース 25.0(1) • リリース 25.0(2) 	Cisco CSR 1000V Bring Your Own License-XE 17.3.1 (a)

- ステップ6 プログラマビリティを導入しますか？ フィールドを特定し [開始 (Get Started)] をクリックします。
- ステップ7 [プログラマビリティ導入の設定 (Configure Programmability Deployment)] ページでサブスクリプションまでスクロールし、[ステータス (Status)] 列でサブスクリプションのステータスを [無効 (Disable)] から [有効 (Enable)] に変更します。
- ステップ8 [保存 (Save)] をクリックします。

次のタスク

「[必要なリソースプロバイダーの登録 \(30 ページ\)](#)」に進みます。

Cisco Cloud Router 8000V への登録

最大パフォーマンスを得るには、Cisco Cloud Router (CCR) 8000V-Bring Your Own License (BYOL) に登録する必要があります。Microsoft Azure Marketplaceでサブスクライブするには、次の手順を実行します。

- ステップ1 [Azure Marketplace](#) の検索テキスト フィールドに、*Cisco Catalyst 8000V Edge Software* と入力し、表示されるオプションを選択します。

[Cisco Catalyst 8000V Edge Software] オプションが検索候補として表示されます。

- ステップ2 [Cisco Catalyst 8000V Edge Software] オプションをクリックします。

Microsoft Azure Marketplace の [Cisco Catalyst 8000V Edge Software] ページにリダイレクトされます。

- ステップ3 [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューを開きます。

メインページに [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューが表示されない場合、[プラン+価格設定 (Plans + Pricing)] タブをクリックしてください。このオプションが使用可能であれば、[ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューにアクセスします。

- ステップ4 [ソフトウェアプランの選択 (Select a software plan)] ドロップダウンメニューで、Cisco Cloud APIC ソフトウェアリリースに応じて適切なオプションを選択します。

クラウドAPICリリースの場合	この特定のオプションを選択します
25.0(3)	Cisco Catalyst 8000V Edge ソフトウェア -BYOL- 17.7.1

- ステップ5 プログラマビリティを導入しますか？ フィールドを特定し [開始 (Get Started)] をクリックします。
- ステップ6 [プログラマビリティ導入の設定 (Configure Programmability Deployment)] ページでサブスクリプションまでスクロールし、[ステータス (Status)] 列でサブスクリプションのステータスを [無効 (Disable)] から [有効 (Enable)] に変更します。
- ステップ7 [保存 (Save)] をクリックします。

次のタスク

「必要なリソースプロバイダーの登録 (30 ページ)」に進みます。

必要なリソースプロバイダーの登録

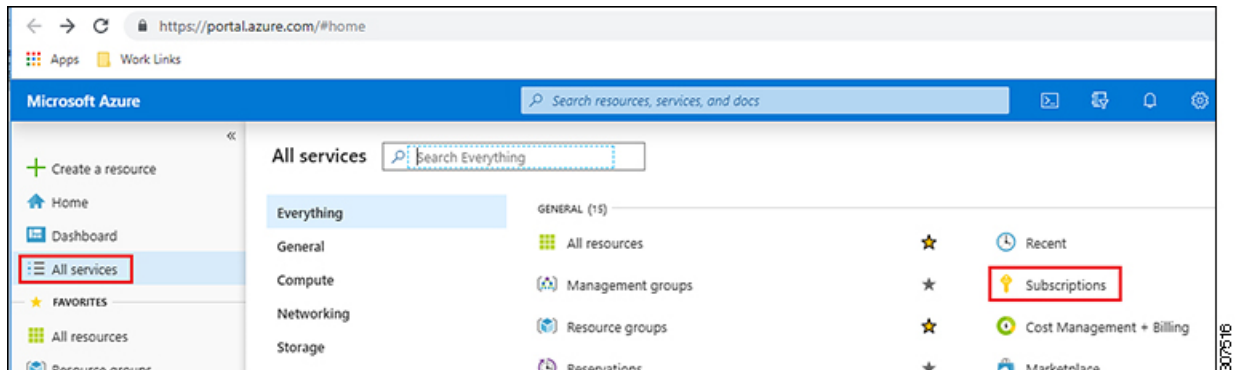
Cisco Cloud APIC で使用するすべてのサブスクリプションについて、後で追加する可能性のあるサブスクリプションがあるテナントを含めて、次のリソースプロバイダーを登録する必要があります。

- microsoft.insights
- Microsoft.EventHub
- Microsoft.Logic
- Microsoft.ServiceBus

これらの手順では、サブスクリプションに必要なこれらのリソースプロバイダーを登録する方法について説明します。

ステップ 1 リソースプロバイダーを表示できる Azure の領域にアクセスします。

- 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。

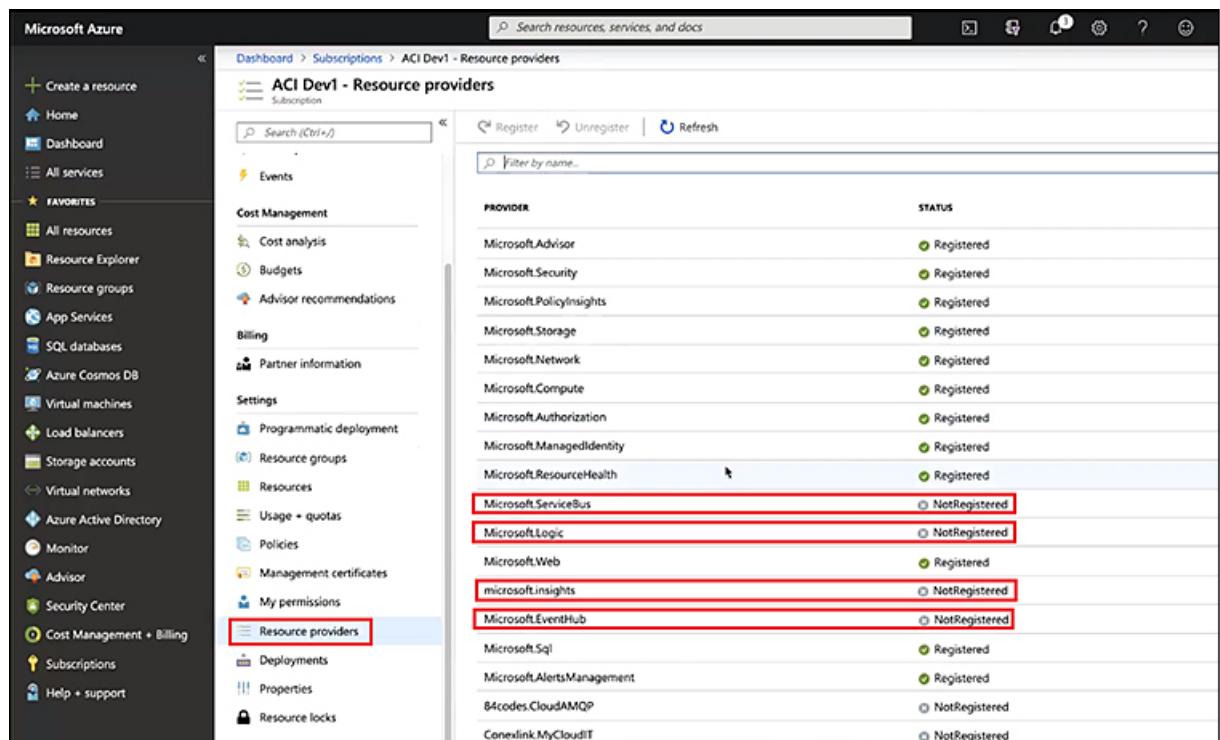


- b) Azure 管理ポータル の [サブスクリプション (Subscriptions)] ページで、Microsoft アカウントのサブスクリプションアカウントをクリックします。

そのサブスクリプションの概要情報が表示されます。

- 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 [リソースプロバイダー] リソースリンクを見つけ、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 [リソースプロバイダー (Resource Providers)] ページが表示されます。

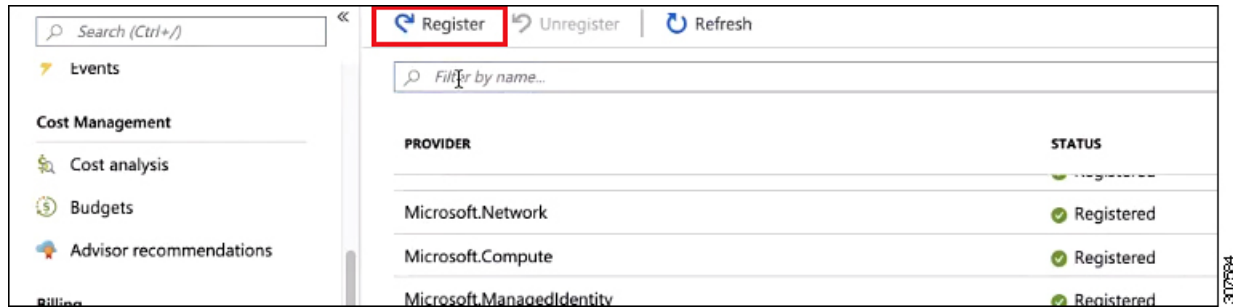


ステップ 2 前のスクリーンショットに示すように、プロバイダーのリストで次の4つのリソースプロバイダーを見つけます。

- microsoft.insights
- Microsoft.EventHub
- Microsoft.Logic
- Microsoft.ServiceBus

ステップ 3 4つすべてのリソースプロバイダーがRegisteredまたはNotRegistered状態であるかどうかを確認します。

- 4つすべてのリソースプロバイダーが[登録済み (Status)]列に[登録済み (Registered)]と表示されている場合、このサブスクリプションにこれらのリソースプロバイダーを登録するためにこれ以上何もする必要はありません。
- [ステータス (Status)]列に[未登録 (NotRegistered)]と表示されているすべてのリソースプロバイダーについて、次の手順を実行します。
 1. NotRegisteredと表示されている特定のリソースプロバイダーをクリックします。
 2. 画面上部の[登録 (Register)]をクリックして、そのリソースプロバイダーを登録します。



登録プロセスが完了すると、ステータスがNotRegisteredからRegisteringに変わり、Registeredに変わります。

- NotRegisteredと表示されているすべてのリソースプロバイダーについて、4つのリソースプロバイダーがすべてRegisteredと表示されるまで、これらの手順を繰り返します。

Azure でのアプリケーションの作成

必要に応じて、次の手順に従ってAzureでアプリケーションを作成します。テナントの新しいサブスクリプションを作成し、特定のアプリケーションを介してクラウドリソースを管理するために[管理対象外ID (Unmanaged Identity)]を選択する場合は、次の手順が必要です。



(注) Azureのアプリケーションは、サービスプリンシパルとも呼ばれます。

ステップ 1 まだログインしていない場合は、Cisco Cloud APIC インフラ テナントの Azure アカウントにログインし、Azure 管理コンソールに移動します。

<https://portal.azure.com/#home>

ステップ 2 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にある[Azure Active Directory]リンクをクリックし、[App registrations]リンクをクリックします。

ステップ 3 [アプリケーションの登録 (App registrations)] ページで、[+ New registration] をクリックします。

ステップ 4 [アプリケーションの登録 (Register an application)] ページに必要な情報を入力します。

- Name
- [サポートされるアカウントのタイプ (Supported Account Types)]: 最初のオプションを選択します (この組織ディレクトリ内のアカウントのみ)
- (オプション) リダイレクト URI

[登録 (Register)] をクリックします

このアプリケーションの概要ページが表示されます。

ステップ 5 左側のナビゲーションバーで **[Certificates & secrets]** をクリックし、**[Add a client secret]** 領域に必要な情報を入力して **[追加 (Add)]** をクリックします。

これにより、これらの手順の後半でアプリケーションシークレットフィールドに必要な情報が生成されます。

ステップ 6 テキストファイルを開き、必要な情報をテキストファイルにコピーアンドペーストします。

- **[Client Secret]** : **[Clients & Secrets]**ページの**[Client Secrets]**領域の**[Value]**フィールドのテキストをコピーします。
- **アプリケーションID** : ホームアプリケーション登録に移動します<application-name>、**[概要 (Overview)]** ページで、**[アプリケーション (クライアント) ID (Application (client) ID)]** フィールドからテキストをコピーします。 > >
- **Azure Active Directory ID** : **[Home App registrations]**に移動します。 <application-name>、**[概要 (Overview)]** ページで、**[ディレクトリ (テナント) ID]**フィールドからテキストをコピーします。 > >

ステップ 7 テキストファイルを保存し、その場所をメモします。

このドキュメントの後半の手順を実行するときに、この情報を参照します。 [テナントの設定 \(81 ページ\)](#)

AzureのSSHキーペアの生成

Cisco Cloud APIC セットアップ プロセスの一環として、管理者公開キー (SSH公開キー) を Cisco Cloud APIC の Azure リソース マネージャ (ARM) テンプレートに入力するように求められます。次の項では、WindowsまたはLinuxシステムでSSH公開キーと秘密キーのペアを生成する手順について説明します。

Windows での SSH キー ペアの生成

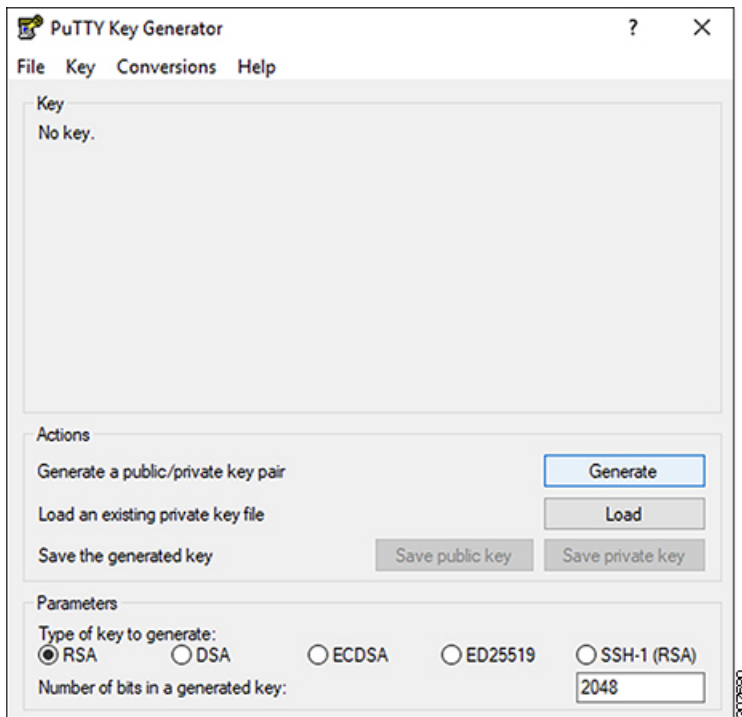
次の手順では、WindowsでSSH公開キーと秘密キーのペアを生成する方法について説明します。LinuxでSSH公開キーと秘密キーのペアを生成する手順については、[を参照してください。Linux または MacOS での SSH キー ペアの生成 \(36 ページ\)](#)

ステップ 1 PuTTYキージェネレーター (puttygen) をダウンロードしてインストールします。

<https://www.puttygen.com/download-putty>

ステップ 2 Windowsの > **[スタート]メニュー** > **[すべてのプログラム]** > **[PuTTY]** > **[PuTTYgen]** に移動して、PuTTY キージェネレーターを実行します。

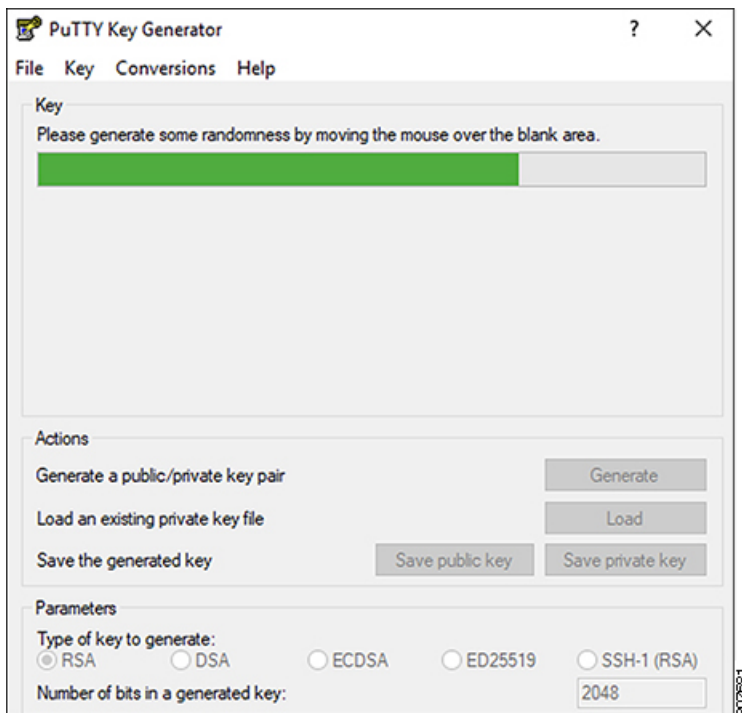
画面にPuTTYキージェネレーターのウィンドウが表示されます。



ステップ 3 [生成 (Generate)] をクリックします。

公開キーを生成するために空白領域にマウスを移動するように求める画面が表示されます。

ステップ 4 空白領域の周囲にカーソルを移動して、公開キーのランダムな文字を生成します。



ステップ 5 公開キーを保存します。

- a) 公開キーファイルを保存するラップトップ上のフォルダに移動し、この公開キーのテキストファイルを作成します。
- b) PuTTYキージェネレータの情報をコピーします。

次の内容を含めて、ウィンドウに公開キー情報をコピーします。

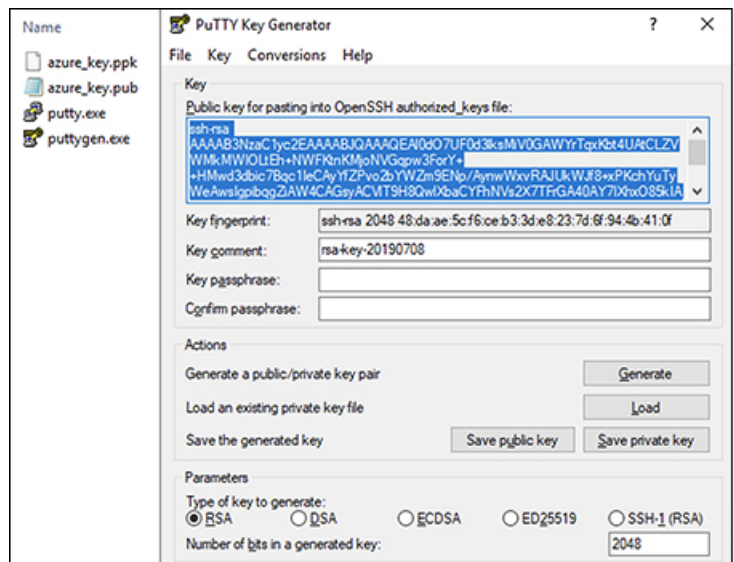
- 公開キーの先頭にssh-rsaテキストを含める。
- 末尾の次のテキスト文字列を除外します。

```
== rsa-key-<date-stamp>
```

== rsa-key-を含まないようにキーを切り捨てます。<date-stamp>末尾のテキスト文字列。

(注) 次の一連の手順では、公開キー情報を Azure ARM テンプレートに貼り付けます。フォームがこの形式のキーを受け入れない場合は、キーの末尾に==を追加します。一部の地域ではこの形式が必要になるためです。

キーが正しい形式でない場合、Cloud APICはインストールを完了しません。



- c) で作成した公開キーテキストファイルに情報を貼り付け、ファイルを保存して、一意のファイル名を付けます。5.a (35 ページ)

この公開キーテキストファイルには、1行のテキストのキーが含まれています。次の一連の手順では、この公開キーテキストファイルの情報が必要になります。

(注) PuTTYキージェネレータの[公開キーの保存 (Save public key)]オプションを使用して公開キーを保存しないでください。これにより、複数行のテキストを含む形式でキーが保存されます。これは、クラウドAPIC導入プロセスと互換性がありません。

ステップ 6 秘密キーを保存します。

- a) [プライベートキーの保存 (Save private key)] をクリックします。

パスフレーズなしでファイルを保存するかどうかを確認する画面が表示されます。この画面で [はい (Yes)] をクリックします。

- b) ラップトップのフォルダに移動し、一意のファイル名を付けて秘密キーファイルを保存します。

(注) 秘密キーファイルは、インストールプロセスでは使用されません。ただし、で説明されているように、SSH を介して Cloud APIC にログインするなど、他の理由で必要になる場合があります。SSH を介したクラウド APIC へのログイン (133 ページ)

次のタスク

[Azure でのクラウド APIC の導入 \(37 ページ\)](#) の手順に従って Azure の設定プロセスを続行します。これには、Azure ARM テンプレートへの公開キー情報の貼り付けが含まれます。

Linux または MacOS での SSH キー ペアの生成

次の手順では、Linux または MacOS で SSH 公開キーと秘密キーのペアを生成する方法について説明します。Windows で SSH 公開キーと秘密キーのペアを生成する手順については、を参照してください。Windows での SSH キー ペアの生成 (33 ページ)

- ステップ 1** Linux 仮想マシンまたは Mac で、ssh-keygen を使用して公開キーと秘密キーのペアを作成し、出力をファイルに送信します。

```
# ssh-keygen -f filename
```

次に例を示します。

```
# ssh-keygen -f azure_key
```

次のような出力が表示されます。パスフレーズを入力するように求められたら、テキストを入力せずに Enter キーを押します (パスフレーズがないようにフィールドを空のままにします)。

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in azure_key.
Your public key has been saved in azure_key.pub.
The key fingerprint is:
SHA256:gTsQIIAadjgNsgcguifI1oh4XGpVWMdcXVV6U0dyBNs
...
```

- ステップ 2** 保存した公開キーファイルと秘密キーファイルを見つけます。

```
# ls
```

2つのファイルが表示されます。

- 拡張子が .pub のファイルには、公開キー情報が含まれています。
- 同じ名前でサフィックスのないファイルに秘密キー情報が含まれている

たとえば、出力を azure_key という名前のファイルに送信すると、次の出力が表示されます。

```
# ls
azure_key
azure_key.pub
```

その場合、次のようになります。

- azure_key.pub ファイルには、公開キー情報が含まれています。
- azure_key ファイルには秘密キー情報が含まれています。

ステップ 3 公開キーファイルを開き、そのファイルから公開キー情報をコピーします。末尾に username @ hostname 情報は含めません。

(注) 秘密キーファイルは、インストールプロセスでは使用されません。ただし、で説明されているように、SSH を介して Cloud APIC にログインするなど、他の理由で必要になる場合があります。
[SSH を介したクラウド APIC へのログイン \(133 ページ\)](#)

次のタスク

の手順に従って Azure の設定プロセスを続行します。これには、公開キー情報を公開キーファイルから Azure ARM テンプレートに貼り付けることが含まれます。[Azure でのクラウド APIC の導入 \(37 ページ\)](#)

Azure でのクラウド APIC の導入

始める前に

- 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 \(19 ページ\)](#) に示されている要件を満たしていることを確認します。たとえば、エラスティック IP アドレスの数が正しいこと、およびインスタンス展開の許可の制限をチェックしたことを確認します。

ステップ 1 まだログインしていない場合は、Cisco Cloud APIC インフラ テナントの Azure アカウントにログインし、Azure 管理コンソールに移動します。

<https://portal.azure.com/#home>

ステップ 2 Azure 管理ポータル のメインページで、検索テキストフィールドに「Cisco Cloud APIC」と入力します。

ステップ 3 [Cisco Cloud APIC] ページの [プランの選択 (Select a plan)] フィールドで、適切なリリースを選択し、[作成 (Create)] をクリックします。

[Cisco Cloud APIC] 画面の [Basics] ページが表示されます。

ステップ 4 [基本 (Basics)] ページの必要なフィールドに入力します。

- **[サブスクリプション (Subscription)]** : ドロップダウン リストから、Cisco Cloud APIC インフラ サブスクリプション アカウントを選択します。
- **[リソース グループ (Resource group)]** : ドロップダウン リストから既存のリソース グループを選択するか、**[新規作成 (Create new)]** をクリックして新しいリソース グループの名前を入力します。

Azure リソース グループは、Azure ソリューションの関連リソースを保持するコンテナです。

クラウド APIC 自体のリソース グループを除き、クラウド APIC によって作成されたほとんど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。ここで選択したリソースグループ名が正しいことを確認します。

- **[リリース (Region)]** : ドロップダウン リストからロケーションを選択し、Cisco Cloud APIC の仮想マシンを展開する場所を選択します。
- **仮想マシン名** : 仮想マシン名を入力します。このエントリは、この Cisco Cloud APIC の仮想マシンの名前になります。仮想マシン名は英数字のみである必要がありますが、ダッシュで区切ることができます (CloudAPIC など)。
- **[パスワード (Password)]** : 管理者パスワードを入力します。このエントリは、SSH アクセスを有効にした後に Cisco Cloud APIC にログインするために使用するパスワードです。

パスワードの特徴は次のとおりです。

- 長さは 12 ~ 72 文字にする必要があります
- 次の 3 つが必要です。
 - 小文字を 1 つ
 - 大文字
 - 数字を 1 つ
- 許容される次の特殊文字のいずれか :

@!%*#?&

- **[パスワードの確認 (Confirm Password)]** : 管理者パスワードを再度入力します。
- **SSH 公開キー** : 次のいずれかの手順の最後にコピーした公開キー情報を貼り付けます。
 - [Windows での SSH キー ペアの生成 \(33 ページ\)](#)
 - [Linux または MacOS での SSH キー ペアの生成 \(36 ページ\)](#)

Cisco Cloud APIC には、この SSH キー ペアを使用してログインします。ssh-rsa 文字列は、このフィールドに貼り付ける公開キー文字列の先頭にある必要があります。

(注) WindowsでSSHキーペアを生成した場合、PuTTYキージェネレータのキーは==rsa-key-で終わります。<date-stamp>。==rsa-key-が含まれないようにキーを切り捨てます。<date-stamp>。フォームがこの形式のキーを受け入れない場合は、キーの末尾に==を追加します。一部の地域ではこの形式が必要になるためです。

キーが正しい形式でない場合、Cloud APICはインストールを完了しません。

ステップ 5 このページのフィールドへの入力完了したら、[Next : ACI Settings]をクリックします。

[Cisco Cloud APIC]画面の[ACI Settings]ページが表示されます。

ステップ 6 [ACI設定 (ACI Settings)]ページの必要なフィールドに入力します。

- **[ACI ファブリック名 (ACI Fabric name):]**デフォルト値のままにしておくか、ファブリック名を入力します。このエントリは、この Cisco Cloud APIC の名前になります。ファブリック名は英数字のみにする必要がありますが、ダッシュで区切ることができます (ACI-Cloud-Fabricなど)。
- **仮想マシンのサイズ :** 仮想マシンのサイズは、Standard_D8s_v3のデフォルトの展開サイズに自動的に設定されます。デフォルトの仮想マシンサイズ設定は変更できません。
- **[イメージバージョン (Image Version)] :** このフィールドで適切なリリースを選択します。
- **[インフラサブネット (Infra Subnet)] :** Cisco Cloud APIC のインフラプール。このフィールドには、デフォルト値の 10.10.0.0/24 が、自動的に入力されます。デフォルト値がオンプレミスファブリックからのインフラプールと重複している場合は、このフィールドの値を変更します。このエントリは/24サブネットである必要があります。

(注) 172.17.0.0/16からのサブネット (たとえば、172.17.10.0/24) をインフラサブネットとして使用しないことをお勧めします。これは、[インフラサブネットとのサブネット競合問題の解決 \(42 ページ\)](#) で説明されているように、DockerブリッジIPサブネットとの競合を引き起こす可能性があるためです。

- **Public IP Address :** パブリックIPアドレスを静的に設定します。

1. [Public IP Address]フィールドで、[Create New]をクリックします。

(注) クラウドAPICにプライベートIPアドレスを割り当てるには、ドロップダウンリストから[none]を選択します。

[Create public IP address]フィールドがページの右側に表示されます。

2. [SKU]領域で、[Basic]または[Standard]SKUを選択します。

Basic SKUとStandard SKUの違いの詳細については、Microsoftのドキュメントサイトの『Public IP Addresses in Azure』ドキュメントを参照してください。

3. [Assignment]領域で、[Static]を選択します。

[Assignment]領域の設定を[Dynamic]のままにしないでください。

4. [Create public IP address]領域で[OK]をクリックします。

- **[パブリック IP アドレスの DNS プレフィックス (DNS Prefix for the public IP Address)]** : Cisco Cloud APIC DNS 名のプレフィックス。Cisco Cloud APIC が展開されると、DNS 名を使用して Cisco Cloud APIC にアクセスできます。

(注) Azure の制限により、このフィールドに入力する Cisco Cloud APIC DNS 名のプレフィックスにはピリオド (.) を使用できません。

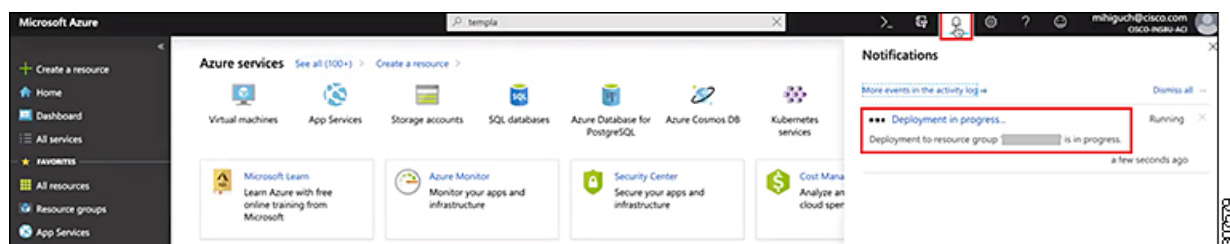
- **[外部サブネット (Access Control):]** Cisco Cloud APIC への接続を許可する外部ネットワークの IP アドレスとサブネットを入力します (たとえば、192.0.2.0/24)。このサブネットからの IP アドレスだけが、Cisco Cloud APIC への接続を許可されます。値 0.0.0.0/0 を入力すると、誰でも Cisco Cloud APIC への接続が許可されます。
- **[仮想ネットワーク名 (Virtual Network Name)]** : 必要に応じて、仮想ネットワーク名のデフォルトエントリをそのままにするか、このフィールドのエントリを変更します。
- **[Management NSG Name]** : 管理ネットワークセキュリティグループ名のデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。
- **[Management ASG Name]** : 管理アプリケーションセキュリティグループ名のデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。
- **サブネットプレフィックス** : サブネットプレフィックスのデフォルトエントリをそのままにするか、必要に応じてこのフィールドのエントリを変更します。

ステップ 7 このページのフィールドへの入力完了したら、**[Next : Review + create]** をクリックします。

[Cisco Cloud APIC] 画面の**[Review + create]** ページが表示されます。

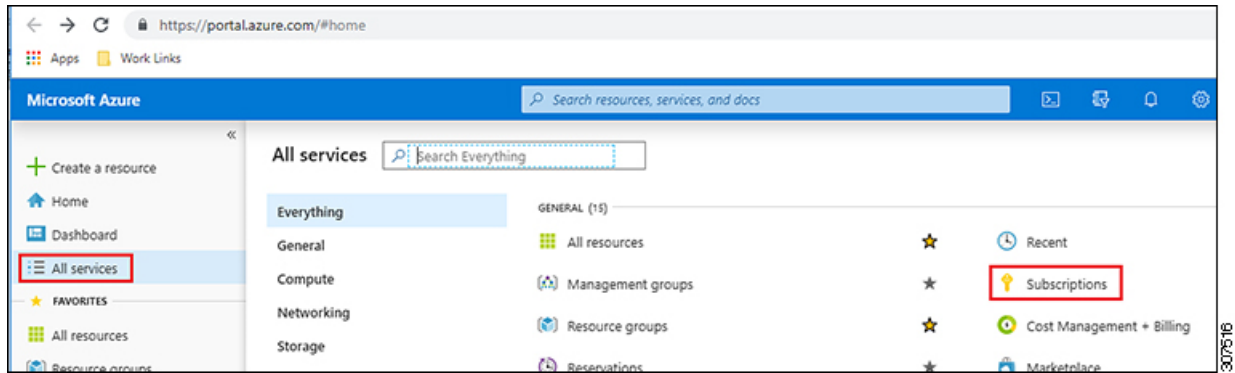
ステップ 8 **[Review + create]** ページで情報を確認し、**[Create]** をクリックします。

システムは、テンプレートに指定された情報を使用して Cisco Cloud APIC VM インスタンスを作成するようになりました。プロセスが完了するのに 5 ~ 10 分かかります。通知アイコン (ベル型のアイコン) をクリックして、Cisco Cloud APIC の展開のステータスを確認します。

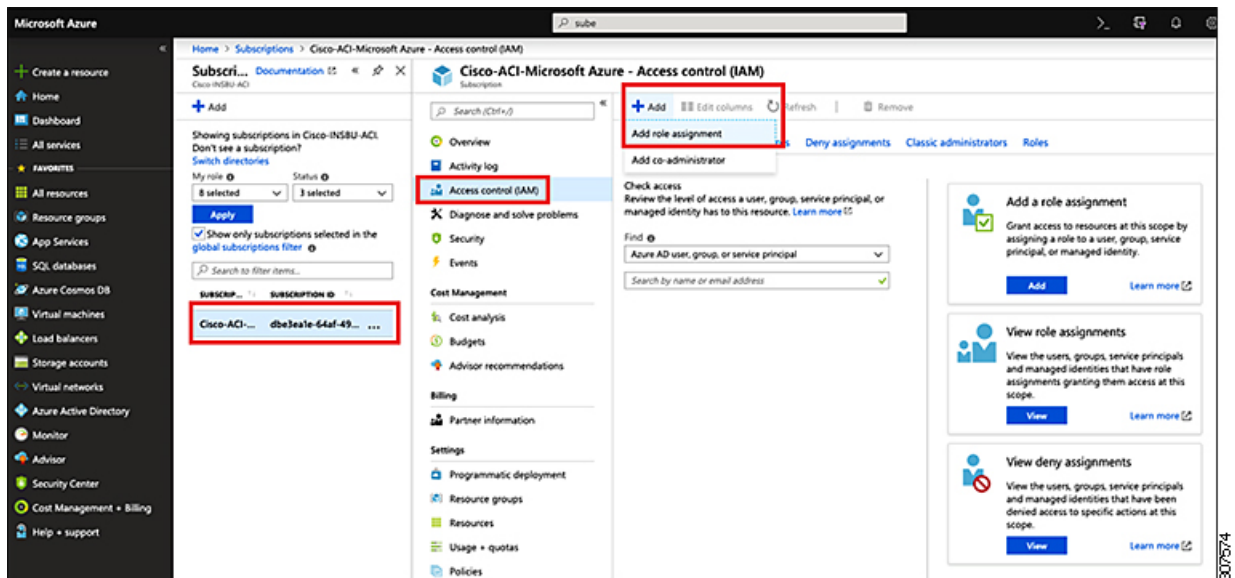


ステップ 9 展開が完了したら、ユーザアクセス管理者ロールの割り当てを追加します。

- a) Azure 管理ポータルメインページで、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 管理ポータル内の [サブスクリプション (Subscriptions)] ページで、Cisco Cloud APIC が展開され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。
- 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 [Access control (IAM)] 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 [アクセス制御 (Access Control)] ページが表示されます。
- d) [+ Add] をクリックし、ドロップダウンメニューから [Add role Assignment] を選択します。



- e) [ロール割り当ての追加 (Add role Assignment)] ページで、次の選択を行います。
- [ロール (Role)] フィールドで、ドロップダウンメニューから [管理者 (Administrator)] を選択します。
 - [Assign access to] フィールドで、[仮想マシン (Virtual Machine)] を選択します。
 - [サブスクリプション (Subscription)] フィールドで、Cisco Cloud APIC が展開されているサブスクリプションを選択します。

- Cisco Cloud APIC 仮想マシンを選択します。
- f) 画面の下部にある[保存 (Save)] をクリックします。

次のタスク

アクセスタイプに管理対象IDまたは管理対象外IDのロール割り当てを追加する必要があるかどうかを判断するには、に移動します。 [ロール割り当ての追加 \(44 ページ\)](#)

インフラサブネットとのサブネット競合問題の解決

状況によっては、Cisco Cloud APIC とのサブネットの競合に関する問題が発生することがあります。この問題は、次の条件が満たされた場合に発生する可能性があります。

- Cisco Cloud APIC はリリース 25.0(2) で実行されています
- Cisco Cloud APIC のインフラ サブネットは、172.17.0.0/16 CIDR 内に設定されています (たとえば、[Azure でのクラウド APIC の導入 \(37 ページ\)](#) の手順の一部として [インフラ サブネット] フィールドに 172.17.10.0/24 と入力した場合)。
- Cisco Cloud APIC のインフラ サブネットに使用している 172.17.0.0/16 CIDR と重複する何かが設定されています (たとえば、Docker ブリッジ IP サブネットが 172.17.0.0/16 で設定されている場合、Cisco Cloud APIC のデフォルトサブネット)。

この状況では、このサブネットの競合が原因で Cisco Cloud APIC が CCR プライベート IP アドレスに到達できない可能性があります、Cisco Cloud APIC は影響を受ける CCR に対して SSH 接続障害が発生させます。

root として Cisco Cloud APIC にログインし、`route -n` コマンドを入力することで、競合の可能性があるかどうかを判断できます。

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
```

以下のような出力が表示されることが想定されます。

```
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          172.17.0.17   0.0.0.0        UG    16     0      0 oobmgmt
169.254.169.0   0.0.0.0       255.255.255.0  U     0     0      0 bond0
169.254.254.0   0.0.0.0       255.255.255.0  U     0     0      0 lxcbr0
172.17.0.0      0.0.0.0       255.255.0.0    U     0     0      0 docker0
172.17.0.12     0.0.0.0       255.255.255.252 U     0     0      0 bond0
172.17.0.16     0.0.0.0       255.255.255.240 U     0     0      0 oobmgmt
```

この出力例では、強調表示されたテキストは、Docker ブリッジが 172.17.0.0/16 で構成されていることを示しています。

これは、Cisco Cloud APIC のインフラ サブネットに使用した 172.17.0.0/16 CIDR と重複するため、CCR への接続が失われ、CCR に SSH で接続できないという問題が発生する可能性があります

ます。CCR に ping を実行しようとする、ホストに到達できないというメッセージが表示されます（次の例では、172.17.0.84 が CCR のプライベート IP アドレスです）。

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
From 172.17.0.1 icmp_seq=1 Destination Host Unreachable
From 172.17.0.1 icmp_seq=2 Destination Host Unreachable
From 172.17.0.1 icmp_seq=3 Destination Host Unreachable
From 172.17.0.1 icmp_seq=5 Destination Host Unreachable
From 172.17.0.1 icmp_seq=6 Destination Host Unreachable
^C
--- 172.17.0.84 ping statistics ---
9 packets transmitted, 0 received, +5 errors, 100% packet loss, time 8225ms
pipe 4
[root@ACI-Cloud-Fabric-1 ~]#
```

この状況で競合を解決するには、次のような REST API 投稿を入力して、競合の原因となっている他の領域の IP アドレスを変更します。

```
https://{{apic}}/api/plgnhandler/mo/.xml
<apPluginPolContr>
  <apContainerPol containerBip="<new-IP-address>" />
</apPluginPolContr>
```

たとえば、上記のシナリオ例で示した 172.17.0.0/16 CIDR の下から Docker ブリッジの IP アドレスを移動するには、次のような REST API 投稿を入力します。

```
https://{{apic}}/api/plgnhandler/mo/.xml
<apPluginPolContr>
  <apContainerPol containerBip="172.19.0.1/16" />
</apPluginPolContr>
```

ここで、172.19.0.1/16 は Docker ブリッジの新しいサブネットです。これにより、Docker ブリッジの IP アドレスが 172.19.0.0/16 CIDR の下に移動し、172.17.0.0/16 CIDR 内で構成されている Cisco Cloud APIC のインフラサブネットとの競合がなくなります。

以前と同じコマンドを使用して、競合がなくなったことを確認できます。

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          172.17.0.17    0.0.0.0        UG    16     0      0 oobmgmt
169.254.169.0    0.0.0.0        255.255.255.0  U     0     0      0 bond0
169.254.254.0    0.0.0.0        255.255.255.0  U     0     0      0 lxcbr0
172.17.0.12      0.0.0.0        255.255.255.252 U     0     0      0 bond0
172.17.0.16      0.0.0.0        255.255.255.240 U     0     0      0 oobmgmt
172.19.0.0      0.0.0.0        255.255.0.0    U     0     0      0 docker0
```

この出力例では、強調表示されたテキストは、Docker ブリッジが IP アドレス 172.19.0.0 で構成されていることを示しています。Cisco Cloud APIC のインフラサブネットに使用している 172.17.0.0/16 CIDR との重複がないため、CCR との接続に問題はありません。

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
64 bytes from 172.17.0.84: icmp_seq=1 ttl=255 time=1.15 ms
64 bytes from 172.17.0.84: icmp_seq=2 ttl=255 time=1.01 ms
64 bytes from 172.17.0.84: icmp_seq=3 ttl=255 time=1.03 ms
```

```
64 bytes from 172.17.0.84: icmp_seq=4 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=5 ttl=255 time=1.09 ms
64 bytes from 172.17.0.84: icmp_seq=6 ttl=255 time=1.06 ms
64 bytes from 172.17.0.84: icmp_seq=7 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=8 ttl=255 time=1.05 ms
^C
--- 172.17.0.84 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7005ms
rtt min/avg/max/mdev = 1.014/1.061/1.153/0.046 ms
[root@ACI-Cloud-Fabric-1 ~]#
```

ロール割り当ての追加

追加するロール割り当てのタイプは、アクセスタイプに管理対象IDがあるかどうかによって異なります。

- アクセスタイプの管理対象IDがある場合は、ユーザテナントのロール割り当てを追加する必要があります。[仮想マシンへのロール割り当ての追加 \(44 ページ\)](#) に進みます。

このアクセスタイプは、このマニュアルで後述する手順で[アカウントの関連付け (Associate Account)] ページに情報を入力するときに、次のいずれかを選択した場合に適用されます。[テナントの設定 \(81 ページ\)](#)

- [Mode : Create Own] を選択し、[Associate Account] ページで [Managed Identity] を選択したか、または
 - [モード (Mode)] を選択し、[共有 (Shared)] を選択すると、インフラテナントと共有します。
 - アクセスタイプの管理対象外ID (サービスプリンシパル) がある場合、クラウドリソースは特定のアプリケーションを介して管理されます。[アプリへのロール割り当ての追加 \(47 ページ\)](#) に進みます。
- このアクセスタイプは、このマニュアルで後述する手順で[アカウントの関連付け (Associate Account)] ページで[管理対象外アイデンティティ (Unmanaged Identity)] (サービスプリンシパル) を選択した場合に適用されます。[テナントの設定 \(81 ページ\)](#)

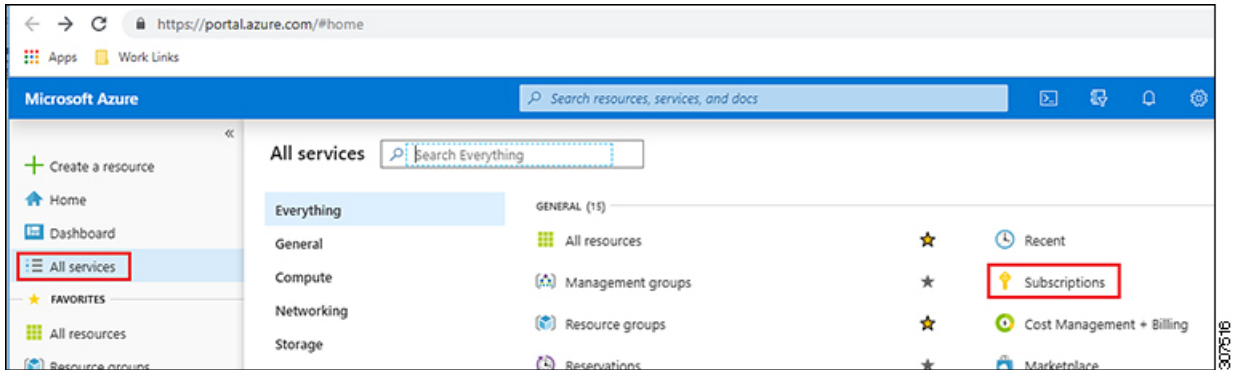
仮想マシンへのロール割り当ての追加

アクセスタイプの管理対象IDがある場合は、このセクションの手順に従います。ここで、ユーザテナントのロール割り当てを追加する必要があります。Azure サブスクリプションタイプとクラウド APIC テナントの関係の詳細については、[テナント、ID、およびサブスクリプションについて \(11 ページ\)](#) を参照してください。



-
- (注) クラウドリソースが特定のアプリケーションを介して管理されるアクセスタイプの管理対象外IDがある場合は、この手順に従います。[アプリへのロール割り当ての追加 \(47 ページ\)](#)
-

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。



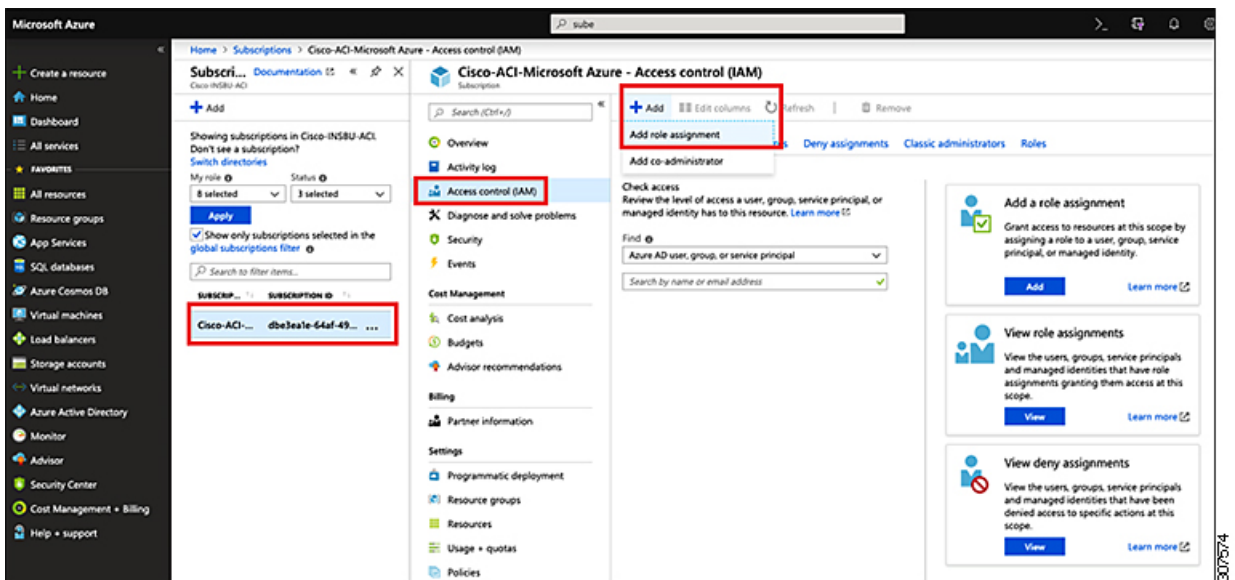
ステップ 2 Azure 管理ポータル [サブスクリプション (Subscriptions)] ページで、Cisco Cloud APIC が展開されたサブスクリプション アカウントをクリックします。

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 [Access control (IAM)] 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 [アクセス制御 (Access Control)] ページが表示されます。

ステップ 4 [+ Add] をクリックし、ドロップダウンメニューから [Add role Assignment] を選択します。



ステップ 5 貢献者 ロールの割り当てを追加します。

a) [ロール割り当ての追加 (Add role Assignment)] ページで、次の選択を行います。

- [ロール (Role)] フィールドで、ドロップダウンメニューから [貢献者 (Contributor)] を選択します。
- [Assign access to] フィールドで、[仮想マシン (Virtual Machine)] を選択します。
- [サブスクリプション (Subscription)] フィールドで、Cisco Cloud APIC が展開されているサブスクリプションを選択します。
- Cisco Cloud APIC 仮想マシンを選択します。

b) 画面の下部にある[保存 (Save)] をクリックします。

ステップ 6 [ユーザ アクセス管理者] ロールの割り当てを追加します。

a) [ロール割り当ての追加 (Add role Assignment)] ページで、次の選択を行います。

- [ロール (Role)] フィールドで、ドロップダウンメニューから [管理者 (Administrator)] を選択します。
- [Assign access to] フィールドで、[仮想マシン (Virtual Machine)] を選択します。
- [サブスクリプション (Subscription)] フィールドで、Cisco Cloud APIC が展開されているサブスクリプションを選択します。
- Cisco Cloud APIC 仮想マシンを選択します。

b) 画面の下部にある[保存 (Save)] をクリックします。

(注) ユーザテナントのサブスクリプションを共有している場合、新しいIAMロールの割り当てがAzureで有効になるまでに最大30分かかります。30分以上待つてから、次のセクションに進みます。

次のタスク

[セットアップウィザードを使用した Cisco Cloud APIC の設定 \(51 ページ\)](#) に移動して、Cisco Cloud APIC のセットアップを続行します。

アプリへのロール割り当ての追加

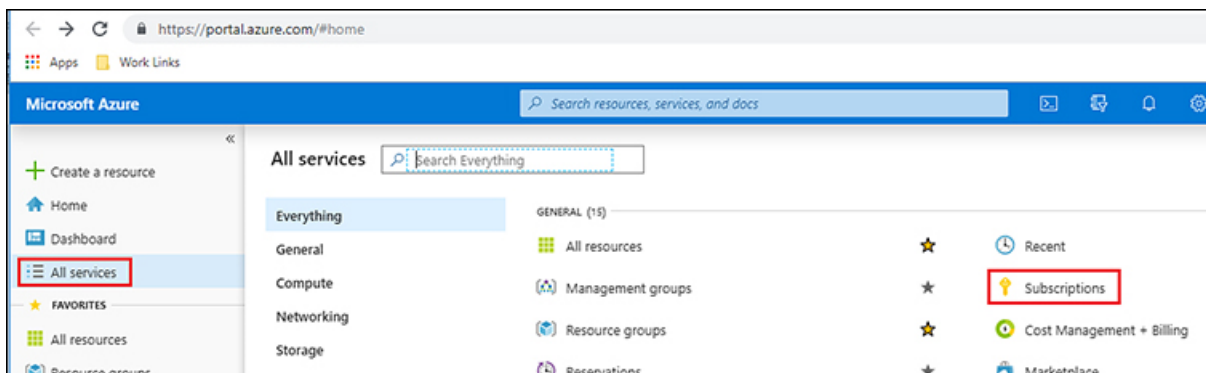
クラウドリソースが特定のアプリケーションを介して管理されるアクセスタイプの管理対象外 ID がある場合は、このセクションの手順に従います。Azure サブスクリプションタイプとクラウド APIC テナントの関係の詳細については、[を参照してください。テナント、ID、およびサブスクリプションについて \(11 ページ\)](#)



(注) ユーザテナントのロール割り当てを追加する必要があるアクセスタイプの管理対象アイデンティティがある場合は、[の手順に従います。仮想マシンへのロール割り当ての追加 \(44 ページ\)](#)

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。

アプリへのロール割り当ての追加



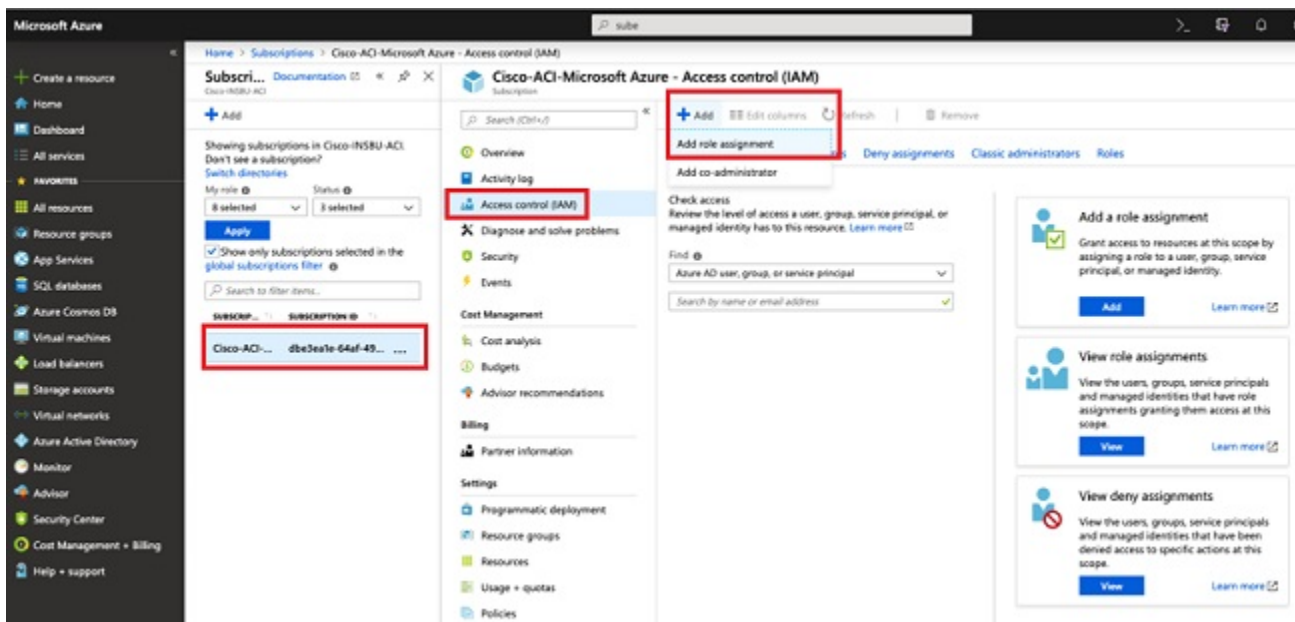
ステップ 2 Azure 管理ポータル内の [サブスクリプション (Subscriptions)] ページで、Cisco Cloud APIC が展開されたサブスクリプションアカウントをクリックします。

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 [Access control (IAM)] 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 [アクセス制御 (Access Control)] ページが表示されます。

ステップ 4 [+ Add] をクリックし、ドロップダウンメニューから [Add role Assignment] を選択します。



ステップ 5 貢献者 ロールの割り当てを追加します。

a) [ロール割り当ての追加 (Add role Assignment)] ページで、次の選択を行います。

- [ロール (Role)] フィールドで、ドロップダウンメニューから [貢献者 (Contributor)] を選択します。

- [Assign access to] フィールドで **Azure AD ユーザー、グループ、またはサービス プリンシパル** を選択します。
- [選択 (Select)] フィールドで、Azure アプリケーションに関連付けられているクレデンシャルを選択します。


Add role assignment ✕

Role ⓘ
Contributor ▼

Assign access to ⓘ
Azure AD user, group, or service principal ▼

Select ⓘ
App1 ✓

Selected members:

	App1	Remove
---	------	--------

Save Discard

b) 画面の下部にある[保存 (Save)]をクリックします。

ステップ 6 [ユーザ アクセス管理者] ロールの割り当てを追加します。

- a) [ロール割り当ての追加 (Add role Assignment)] ページで、次の選択を行います。
- [ロール (Role)] フィールドで、ドロップダウンメニューから [管理者 (Administrator)] を選択します。
 - [Assign access to] フィールドで Azure AD ユーザー、グループ、またはサービス プリンシパル を選択します。
 - [選択 (Select)] フィールドで、Azure アプリケーションに関連付けられているクレデンシヤルを選択します。
- b) 画面の下部にある[保存 (Save)] をクリックします。
- (注) 新しい IAM ロールの割り当てが Azure で有効になるまでに最大 30 分かかります。30 分以上待つてから次の章に進みます。Azure で IAM ロールの割り当てが有効になる前にセットアップ ウィザードを使用してクラウド APIC を設定しようとする、CCR の展開は失敗します。
-

次のタスク

セットアップ ウィザードを使用した [Cisco Cloud APIC の設定 \(51 ページ\)](#) に移動して、Cisco Cloud APIC のセットアップを続行します。



第 5 章

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 (51 ページ)
- オンプレミス設定情報の収集 (52 ページ)
- サイト、リージョン、および CCR の数の制限について (52 ページ)
- クラウドリソースの命名 (54 ページ)
- クラウド APIC IP アドレスの特定 (59 ページ)
- セットアップウィザードを使用した Cisco Cloud APIC の設定 (60 ページ)
- Cisco Cloud APIC セットアップウィザードの設定の確認 (71 ページ)

サイト間接続の設定と展開

Cisco Cloud APIC の構成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、マルチサイトとオンプレミス Cisco ACI を最初に構成して、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。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 Cisco Cloud APICi 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 \(6 ページ\)](#)」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 ACI <https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html> https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/Operating_ACI/guide/b_Cisco_Operating_ACI.html <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/basic-configuration/Cisco-APIC-Basic-Configuration-Guide-401.html>

- マルチサイト : 『Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide, Release 2.0(1)』などのマルチサイトのマニュアルから入手してください。
- 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 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に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 APIC 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)
 - 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) 移行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。

- Cisco 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〜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、Cisco Cloud APIC 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。

- `{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〜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〜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。

命名ルールに使用できる変数

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、Cisco Cloud APIC によって障害が発生します。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、Cisco Cloud APIC 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。

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、構成が拒否され、Cisco Cloud APIC リソースの作成に失敗したというエラーが発生します。その後、障害の詳細を確認し、命名規則を修正できます。Cisco Cloud APIC 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。

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 3: クラウドリソースでサポートされる変数

Azure のリソース	<code>\${tenant}</code>	<code>\${ctx}</code>	<code>\${ctxprofile}</code>	<code>\${subnet}</code>	<code>\${app}</code>	<code>\${epg}</code>	<code>\${contract}</code>	<code>\${region}</code>	<code>\${priority}</code>
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 4: 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}	#{deviceInterfaceID}
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1CIDR、オーバーレイ2CIDR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。

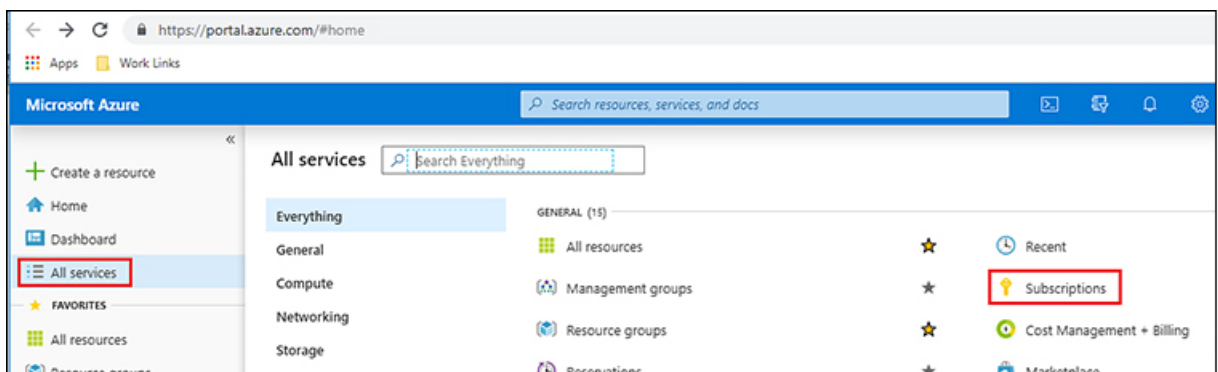
最初に命名規則を定義することをお勧めします。それからテナント設定も行ってください。

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 Cisco 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。

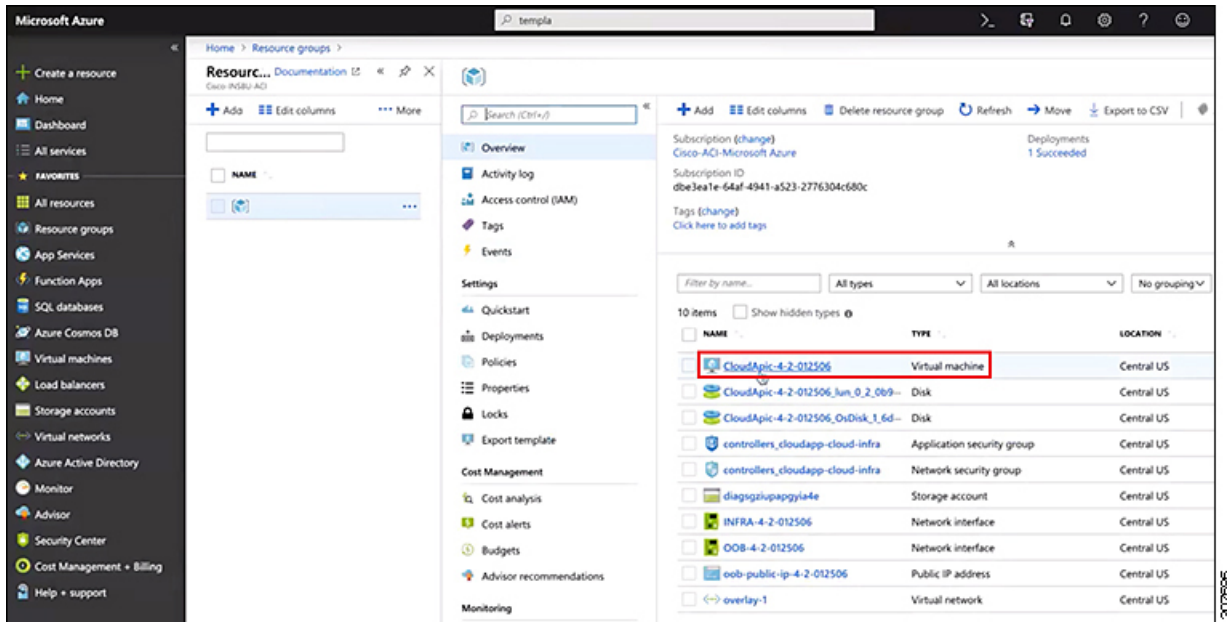
そのサブスクリプションのリソース グループが表示されます。

- ステップ 4** [Azure でのクラウド APIC の導入 \(37 ページ\)](#) で選択または作成したリソース グループを選択します。

そのリソース グループの概要情報が表示されます。

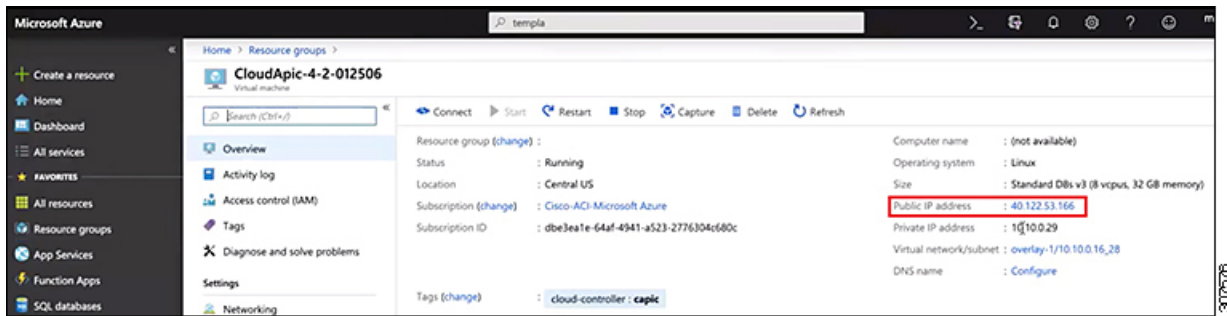
- ステップ 5** リソース グループの概要ページで、Cisco Cloud APIC VM インスタンス ([タイプ (TYPE)] 列の下に [仮想マシン (Virtual machine)] と表示) を見つけ、その VM インスタンスのリンクをクリックします。

セットアップウィザードを使用した Cisco Cloud APIC の設定



Cisco Cloud APIC VM 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、Cisco Cloud APIC へのログインに使用する Cisco Cloud APIC IP 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

Cisco Cloud APIC 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 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。

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 \(19 ページ\)](#) 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 \(27 ページ\)](#) 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 Cisco Cloud APIC の IP アドレスを見つけます。

手順については、[クラウド APIC IP アドレスの特定 \(59 ページ\)](#) 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 Cisco 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 Cisco 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。

[Cisco Cloud APIC へようこそ (Welcome to Cisco 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。

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 \(62 ページ\)](#) 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。

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 Cisco 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。

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、Cisco Cloud APIC が展開されるリージョン (Cisco Cloud APIC によって管理されるリージョン) で、[リージョン (Region)] 列に「Cloud APIC Deployed」というテキストが表示されます。

(注) **ステップ 10 (62 ページ)** で Azure VNetピアリングを有効にした場合は、Cisco Cloud API Chome ホームリージョンの[クラウドルータ (Cloud Router)] 列がオンになっていない場合は、それもオンにする必要があります。

ステップ 13 Cisco 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 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。

Cisco 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。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 Cisco Cloud APIC 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Cisco ACIにより単一のサイトと見なされます。

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 \(52 ページ\)](#)」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。

次の状況では、この手順で CCR のサブネットを追加します。

- Cisco 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 Cisco Cloud APIC により管理対象となる追加のリージョンを選択した場合：
 - 管理対象リージョンごとに 2~4 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 (66 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 (66 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 5~8 を入力した場合)。

例：

- 前のページで選択した Cisco Cloud APIC ホームリージョンのみがあり、Cisco Cloud APIC ホームリージョンに CCR 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 Cisco Cloud APIC の 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 (66 ページ)) で、各管理対象リージョンに展開する 2~4 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 (66 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 (Cisco Cloud APIC ホームリージョンと管理対象として選択した 2 つの追加リージョン) があり、Cisco Cloud APIC の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）
- Cisco 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。

- 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 1-65534 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、429496729 <http://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。

- Cisco Cloud APIC GUI の管理インターフェイスを介して 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。
- 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 \(52 ページ\)](#) 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) **[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 \(20ページ\)](#)」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ヤルを変更する前に、すべてのリージョンから展開解除する必要があります。

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。

- j) 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。

- k) [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 \(14 ページ\)](#)」を参照してください。

(注) プライベート IP アドレスを [15.e \(66 ページ\)](#) 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。

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 \(69 ページ\)](#) 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 ~ /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 \(54 ページ\)](#)

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。準備ができたなら、[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。

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 APIC を Cisco Smart Licensing に登録するには、以下のようになります。

- 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。

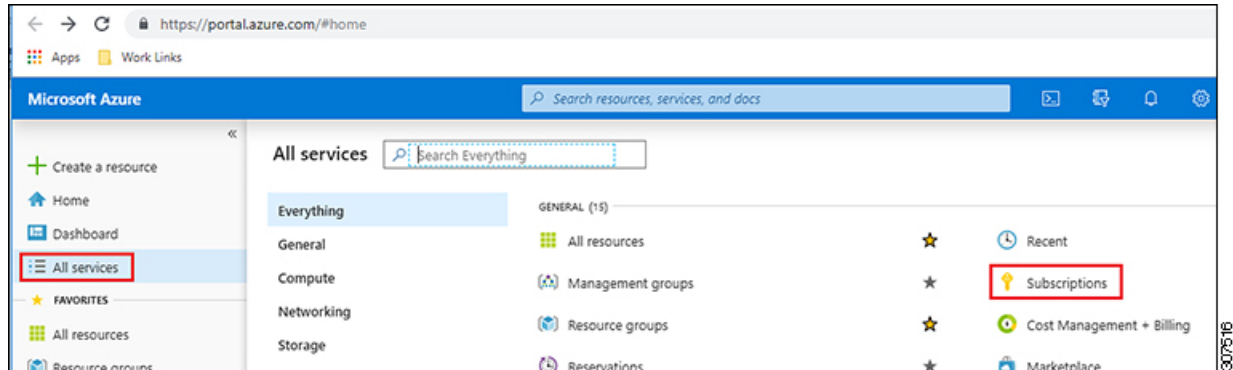
ステップ 25 [サマリ (Summary)] ページで情報を確認し、[完了 (Finish)] をクリックします。

この時点で、Cisco Cloud APIC の内部ネットワーク接続の設定は完了です。

Cisco 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 [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。

- 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 \(37 ページ\)](#)

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てみます。
 - [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（73 ページ）](#)
- 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（96 ページ）](#)

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（95 ページ）](#)」と「[Cisco Cloud APIC コンポーネントの設定（96 ページ）](#)」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 \(73 ページ\)](#)



第 6 章

マルチサイトを通じた Cisco Cloud APIC の管理

- [Cisco Cloud Network Controller とマルチサイトについて \(73 ページ\)](#)
- [マルチサイトへの Cisco Cloud APIC サイトの追加 \(74 ページ\)](#)
- [サイト間インフラストラクチャの設定 \(75 ページ\)](#)
- [Cisco Cloud APIC と ISN デバイス間の接続の有効化 \(76 ページ\)](#)
- [Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成 \(80 ページ\)](#)
- [テナントの設定 \(81 ページ\)](#)
- [スキーマの作成 \(83 ページ\)](#)
- [アプリケーションプロファイルと EPG の設定 \(84 ページ\)](#)
- [ブリッジドメインの作成と VRF への関連付け \(84 ページ\)](#)
- [コントラクトのフィルタの作成 \(85 ページ\)](#)
- [コントラクトの作成 \(86 ページ\)](#)
- [サイトをスキーマに追加する \(87 ページ\)](#)
- [エンドポイントセレクタの追加 \(88 ページ\)](#)
- [マルチサイト構成の確認 \(92 ページ\)](#)

Cisco Cloud Network Controller とマルチサイトについて

セットアップウィザードを使用して Cisco Cloud Network コントローラを設定するときに、[**サイト間接続 (Inter-Site Connectivity)**] オプションを [**リージョン管理 (Region Management)**] ページで選択した場合は、マルチサイトを使用して、オンプレミス サイトやクラウド サイトなどの別のサイトを Cisco Cloud APIC サイトとともに管理します。Cisco Cloud ネットワーク コントローラのセットアップウィザードで、[**クラウド ルータ (Cloud Routers)**] オプションだけを [**リージョン管理 (Region Management)**] ページで選択した場合、マルチサイトは必要ありません。

Cisco Cloud ネットワーク コントローラの管理専用で使用される、いくつかの新しいページが Cisco Nexus Dashboard Orchestrator に導入されています。この章のトピックでは、これらの新しい Cisco Cloud ネットワーク コントローラ管理ページについて説明します。これらの Cisco Cloud

ネットワーク コントローラ管理ページに必要な情報を入力すると、Cisco Cloud ネットワーク コントローラは、実質的に、マルチサイトを介して管理する別のサイトになります。

Cisco Cloud ネットワーク コントローラ サイトとともにオンプレミスサイトを管理している場合は、まだ設定していなければ、これらの手順を開始する前にオンプレミスサイトを設定しておくことを推奨します。これらの手順については、<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html> にある『ネットワーク コントローラ マルチサイト オークレーターのインストールとアップグレード』を参照してください。

マルチサイトへの Cisco Cloud APIC サイトの追加

ステップ 1 まだログインしていない場合は、Cisco Nexus Dashboard Orchestrator にログインします。

ステップ 2 メインメニューで [サイト] をクリックします。

ステップ 3 [サイト リスト] ページで、[サイトの追加 (ADD SITE)] をクリックします。

ステップ 4 [接続設定] ページで、次の操作を実行します。

- a) [名前 (NAME)] フィールドに、サイト名を入力します。

たとえば、cloudsite1です。

- b) (任意) [ラベル (LABELS)] フィールドで、ラベルを選択するか作成します。

- c) [APIC CONTROLLER URL] フィールドに、Cisco Cloud APIC の URL を入力します。これは、Azure によって割り当てられるパブリック IP アドレスです。これは、セットアップ ウィザードを使用して Cisco Cloud APIC を構成する手順の開始時にログインするために使用したのと同じパブリック IP アドレスです。

たとえば、https://192.0.2.1です。

- d) [ユーザ名 (USERNAME)] フィールドにユーザ名を入力します。

たとえば、adminとします。admin と同じ権限を持つ任意のアカウントに登録することもできます。

- e) [パスワード (PASSWORD)] フィールドに、パスワードを入力します。

- f) このフィールドが自動的に入力されていない場合は、[APIC SITE ID] フィールドに、一意のサイト ID を入力します。

サイト ID は、Cisco Cloud APIC サイトの固有識別子である必要があります。範囲は 1 ~ 127 です。

- g) [保存 (SAVE)] をクリックします。

ステップ 5 Cisco Cloud APIC サイトが正しく追加されたことを確認します。

複数のサイトを管理している場合は、Cisco Nexus Dashboard Orchestrator の [サイト (Sites)] 画面にすべてのサイトを表示する必要があります。Cisco Nexus Dashboard Orchestrator は、サイトがオンプレミスであるか、Cisco Cloud APIC サイトであるかを自動的に検出します。

次のタスク

「[サイト間インフラストラクチャの設定 \(75 ページ\)](#)」に進みます。

サイト間インフラストラクチャの設定

- ステップ 1** [サイト (Sites)] ビューで、[インフラの構築 (CONFIGURE INFRA)] をクリックします。
[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。
- ステップ 2** 左側のペインの [サイト (SITES)] の下で、クラウドサイトをクリックします。
クラウドサイト領域のほとんどすべての情報は自動的に入力され、次のステップで説明する [BGP パスワード (BGP Password)] フィールドを除き、変更できません。
- ステップ 3** オンプレミス サイトとクラウド サイト間でパスワードを設定するかどうかを決定します。
- オンプレミス サイトとクラウド サイトの間でパスワードを設定しない場合は、[ステップ 4 \(75 ページ\)](#) に進みます。
 - オンプレミス サイトとクラウド サイト間でパスワードを設定するには、次のようにします。
 - a) 右側のペインで、[BGP パスワード (BGP password)] フィールドをクリックして、パスワードを入力します。
 - b) [CloudSite] ウィンドウの右上隅にある [更新 (Refresh)] アイコンをクリックします。
すべてのクラウド プロパティは、Cisco Cloud APIC から自動的に取得されます。サイトが正常に更新されたことを示すメッセージが表示され、すべてのクラウド プロパティが Cisco Cloud APIC から正常に取得されたことを確認します。
- ステップ 4** クラウドサイトでマルチサイト接続を有効にするには、[マルチサイト (Multi-Site)] ボタンをクリックします。
- ステップ 5** サイト間インフラストラクチャを設定するために使用する展開のタイプを選択します。
画面の右上にある [展開 (Deploy)] ボタンをクリックすると、次のスクロールダウンメニューオプションが表示されます。
- **[展開のみ (Deploy Only):]** マルチクラウド (クラウドサイトからクラウドサイト) への接続を設定する場合は、このオプションを選択します。
このオプションは、クラウドサイトと Cisco Cloud APIC サイトに設定をプッシュし、クラウドサイト間のエンドツーエンドインターコネクト接続を有効にします。
 - **[展開 & IPN デバイス設定ファイルをダウンロード: (Deploy & Download IPN Device config files:)]** オンプレミスの APIC サイトと Cisco Cloud APIC サイトの両方に設定をプッシュし、オンプレミスとクラウドサイト間のエンドツーエンドインターコネクト接続を有効にします。さらに、このオプションでは、Azure に導入された Cisco Cloud Router (CCR) とオンプレミスの IPsec 終端デバイスとの間の接続を有効にするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定

ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[IPN デバイス設定ファイルのみをダウンロード (Download IPN Device config files only):]** Azure に展開された CCR とオンプレミスの IPsec 終端デバイス間の接続を有効にするために使用する、設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

Cisco Cloud APIC と ISN デバイス間の接続の有効化



- (注) このセクションの手順は、オンプレミスサイトとクラウドサイト間の接続を有効にしている場合にのみ実行してください。オンプレミスサイトがない場合は、これらの手順をスキップして、[Cisco Cloud APIC GUI を使用したセキュリティドメインの作成 \(80 ページ\)](#) に進みます。

Azure に展開された Cisco Cloud Router (CCR) とオンプレミスの IPsec 端末デバイス間の接続を手動で有効にするには、次の手順に従います。

デフォルトでは、Cisco Cloud APIC は冗長 CCR のペアを展開します。このセクションの手順では、2 つのトンネルを作成します。1 つはオンプレミスの IPsec デバイスからこれらの各 CCR に対する IPsec トンネルです。

次の情報は、オンプレミスの IPsec 端末デバイスとして CCR のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

ステップ 1 Azure に展開された CCR とオンプレミスの IPsec 端末デバイスとの間の接続を有効にするために必要な情報を収集します。

- [サイト間インフラストラクチャの設定 \(75 ページ\)](#) で示されている手順の一部として Cisco Nexus Dashboard Orchestrator で、**IPN デバイス設定ファイルを展開してダウンロードするか、IPN デバイス設定ファイルのみをダウンロードするように選択した場合**、ISN デバイスの設定ファイルが含まれている zip ファイルを見つけます。
- Azure に展開された CCR とオンプレミスの IPsec 端末デバイスとの間の接続を有効にするために必要な情報を手動で検索する場合は、『*Cisco Cloud APIC Installation Guide*』の付録で説明されているように、CSR とテナントの情報を収集します。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CCR のトンネルを構成します。

Cisco Nexus Dashboard Orchestrator を使用して、ISN デバイスの構成ファイルをダウンロードした場合は、最初の CCR の設定情報を見つけて、その構成情報を入力します。

最初の CCR の構成情報の例を次に示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-<first-CCR-tunnel-ID>
  pre-shared-key address <first-CCR-elastic-IP-address> key <first-CCR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<first-CCR-tunnel-ID>
  local-address <interface>
  match identity address <first-CCR-elastic-IP-address>
  keyring infra:overlay-1-<first-CCR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<first-CCR-tunnel-ID> esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-CCR-tunnel-ID>
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel <first-CCR-tunnel-ID>
  ip address <peer-tunnel-for-onprem-IPsec-to-first-CCR> 255.255.255.252
  ip virtual-reassembly
  tunnel source <interface>
  tunnel destination <first-CCR-elastic-IP-address>
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-<first-CCR-tunnel-ID>
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf <process-id> area <area-id>
  no shut
exit
```

それぞれの説明は次のとおりです。

- <first-CCR-tunnel-ID> は、このトンネルに割り当てられている一意のトンネル ID です。
- <first-CCR-tunnel-ID> は、最初の CCR の 3 番目のネットワーク インターフェイスの柔軟な IP アドレスです。
- <first-CCR-preshared-key> は、最初の CCR の事前共有キーです。
- <interface> は、Azure に展開された CCR への接続に使用されるインターフェイスです。
- <peer-tunnel-for-onprem-IPsec-to-first-CCR> は、最初のクラウド CCR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- <process-id> は OSPF プロセス ID です。
- <area-id> は、OSPF エリア ID です。

次に例を示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-1000
  pre-shared-key address 192.0.2.20 key 123456789009876543211234567890
exit

crypto isakmp profile infra:overlay-1-1000
  local-address GigabitEthernet1
  match identity address 192.0.2.20
  keyring infra:overlay-1-1000
exit

crypto ipsec transform-set infra:overlay-1-1000 esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-1000
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel 1000
  ip address 30.29.1.2 255.255.255.252
  ip virtual-reassembly
  tunnel source GigabitEthernet1
  tunnel destination 192.0.2.20
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-1000
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf 1 area 1
  no shut
exit
```

ステップ 4 2 番目の CCR のトンネルを構成します。

Cisco Nexus Dashboard Orchestrator を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、2 番目の CCR の設定情報を見つけて、その設定情報を入力します。

2 番目の CCR の構成情報の例を次に示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-<second-CCR-tunnel-ID>
  pre-shared-key address <second-CCR-elastic-IP-address> key <second-CCR-preshared-key>
```

```
exit

crypto isakmp profile infra:overlay-1-<second-CCR-tunnel-ID>
  local-address <interface>
  match identity address <second-CCR-elastic-IP-address>
  keyring infra:overlay-1-<second-CCR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<second-CCR-tunnel-ID> esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-<second-CCR-tunnel-ID>
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel <second-CCR-tunnel-ID>
  ip address <peer-tunnel-for-onprem-IPsec-to-second-CCR> 255.255.255.252
  ip virtual-reassembly
  tunnel source <interface>
  tunnel destination <second-CCR-elastic-IP-address>
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-<second-CCR-tunnel-ID>
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf <process-id> area <area-id>
  no shut
exit
```

例 :

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-1001
  pre-shared-key address 192.0.2.21 key 123456789009876543211234567891
exit

crypto isakmp profile infra:overlay-1-1001
  local-address GigabitEthernet1
  match identity address 192.0.2.21
  keyring infra:overlay-1-1001
exit

crypto ipsec transform-set infra:overlay-1-1001 esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-1001
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel 1001
  ip address 30.29.1.6 255.255.255.252
```

```

ip virtual-reassembly
tunnel source GigabitEthernet1
tunnel destination 192.0.2.21
tunnel mode ipsec ipv4
tunnel protection ipsec profile infra:overlay-1-1001
ip mtu 1476
ip tcp adjust-mss 1460
ip ospf 1 area 1
no shut
exit

```

ステップ 5 構成する必要があるその他の CCR について、これらの手順を繰り返します。

ステップ 6 オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

次に例を示します。

```

ISN_CCR# show ip interface brief | include Tunnel
Interface          IP-Address      OK? Method Status          Protocol
Tunnel1000         30.29.1.2       YES manual up              up
Tunnel1001         30.29.1.4       YES manual up              up

```

両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

Cisco Cloud APIC GUI を使用したセキュリティドメインの作成

セキュリティドメインは、追加するセキュリティドメインにテナントを制限します。セキュリティドメインを追加しない場合、すべてのセキュリティドメインがこのテナントにアクセスできます。この手順を使用して共有テナントを設定する場合は、これらのセキュリティドメインを選択できます。[テナントの設定 \(81 ページ\)](#)

このセクションでは、クラウド APIC GUI を使用してセキュリティドメインを作成する方法について説明します。

ステップ 1 クラウド APIC システムにログインします。

ステップ 2 インテント アイコンをクリックします。[**インテント (Intent)**] メニューが表示されます。

ステップ 3 [Intent] 検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative] を選択します。

[Intent] メニューに管理オプションのリストが表示されます。

ステップ 4 [Intent] メニューの [Administrative] リストで、[Create Security Domain] をクリックします。[**セキュリティドメインの作成 (Create Security Domain)**] ダイアログ ボックスが表示されます。

ステップ 5 [名前 (Name)] フィールドに、セキュリティドメインの名前を入力します。

ステップ6 [説明 (Description)] フィールドに、セキュリティ ドメインの説明を入力します。

ステップ7 設定が終わったら [Save] をクリックします。

テナントの設定

オンプレミスサイトと Cisco Cloud API サイト間で共有されるテナントを設定するには、この項の手順に従います。Azure サブスクリプションタイプとクラウド APIC テナントの関係の詳細については、[テナント、ID、およびサブスクリプションについて \(11 ページ\)](#) を参照してください。

ステップ1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ2 左側のナビゲーションメニューで、[Tenants] をクリックします。

ステップ3 メイン ペインで、[テナントの追加(Add Tenants)] をクリックします。

ステップ4 [テナントの追加 (Add Tenant)] ウィンドウで、テナントの名前を入力します。

テナントの説明を入力することもできます。

ステップ5 テナントをオンプレミスサイトに展開する必要がある場合は、[関連付けられたサイト (Associated Sites)] 領域の横にあるチェックボックスをオンにしてオンプレミスサイトを選択します。

(オプション) サイトのドロップダウンリストからセキュリティドメインを選択することもできます。

ステップ6 Azureクラウドサイトをテナントに追加するには、[関連付けられたサイト (Associated Sites)] 領域の横にあるチェックボックスをオンにして、Azureクラウドサイトを選択します。

Azureクラウドサイトをテナントに関連付ける場合は、Azureサブスクリプション情報も提供する必要があります。

ステップ7 Azureサイトを確認したら、ドロップダウンリストからセキュリティドメインを選択し (該当する場合)、その横にある[アカウントの関連付け (Associate Account)] をクリックします。

ステップ8 Azureアカウントのモードを選択します。

- テナントを新しいAzureサブスクリプションに関連付ける場合は、[Mode : Create Own] を選択し、次のフィールドに情報を入力します。

1. [Azure Subscription ID] フィールドに、AzureサブスクリプションのIDを入力します。

Azureアカウントにログインし、ホームサブスクリプションに移動することで、サブスクリプションIDを取得できます。 > Azureポータルにリストされているサブスクリプション名ではなく、サブスクリプションIDを使用する必要があります。

2. (オプション) このセキュリティアカウントを他のセキュリティドメインと共有する場合は、[セキュリティドメイン (Security Domain)] フィールドでクラウドアカウントの下のセキュリティドメインを選択します。

詳細については、「[Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成 \(80 ページ\)](#)」を参照してください。

3. **[アクセス タイプ (Access Type)]** フィールドで、Cisco Cloud API VM とテナント間のアクセス タイプを選択します。

(注) リリース 5.2 (1) より前のリリースでは、管理対象アイデンティティのみがインフラテナントのアクセスタイプとしてサポートされ、管理対象アイデンティティと管理対象外アイデンティティ/サービスプリンシパルの両方がユーザテナントのアクセスタイプとしてサポートされていました。アンマネージドアイデンティティ/サービスプリンシパルは、リリース 5.2 (1) より前のリリースのインフラテナントのアクセスタイプとしてサポートされていませんでした。

リリース 5.2 (1) 以降、マネージドアイデンティティとアンマネージドアイデンティティ/サービスプリンシパルの両方が、インフラテナントとユーザテナントのアクセスタイプとしてサポートされるようになりました。

- 特定のアプリケーションを介してクラウドリソースを管理するには、**[Unmanaged Identity]** を選択します。

これは、異なるサブスクリプションでテナントを設定する場合に使用できます。サブスクリプションが同じ組織内の異なる Azure ディレクトリ (Azure テナント) にあるか、サブスクリプションが異なる組織にある可能性があります。

この場合、アプリケーションのクレデンシャルも Cisco Cloud API に提供する必要があります。の手順の最後に保存した情報を参照してください。[Azure でのアプリケーションの作成 \(32 ページ\)](#)

- **アプリケーション ID** : Azure アプリケーションのアプリケーション ID を入力します。この ID は、ホームアプリケーション登録にリストされます。<application-name> [アプリケーション (クライアント) ID (Application (client) ID)] フィールドに入力します。>>
- **[Client Secret]** : アプリケーションシークレットを入力します。ホームアプリケーションの登録でシークレットを作成できます。<application-name> Certificates & secrets 新しいクライアントシークレット。>>>>
- **Azure Active Directory ID** : Azure アプリケーションのアプリケーションディレクトリ ID を入力します。この ID は、ホームアプリケーション登録にリストされます。<application-name>、[Directory (tenant) ID] フィールドに入力します。>>

(注) この場合、アプリケーションのロール割り当ても追加する必要があります。これらの手順については、[アプリへのロール割り当ての追加 \(47 ページ\)](#) を参照してください。

- **[管理対象アイデンティティ (Managed Identity)]** を選択して、Cisco Cloud API VM がクラウドリソースを管理できるようにします。

これは、Azure サブスクリプションが (同じ組織の) 同じディレクトリにある場合に使用できます。

(注) この場合、VMのロール割り当ても追加する必要があります。これらの手順については、[仮想マシンへのロール割り当ての追加 \(44 ページ\)](#) を参照してください。

- [モードの選択 (Choose Mode)] : 既存のテナントと共有されている既存のサブスクリプションを使用する場合は、[共有 (Shared)]を選択します。

Azureでは、同じサブスクリプションを使用して複数のテナントを作成できます。

[共有の選択 (Select Shared)]を選択した場合は、ドロップダウンリストからクラウドアカウントを選択できます。ドロップダウンリストで使用可能なクラウドアカウントは、選択したセキュリティドメインに基づいています。[ステップ 7 \(81 ページ\)](#) 新しいテナントは、選択したアカウントと同じAzureサブスクリプションに関連付けられます。

- (注) セキュリティドメインを設定した場合は、選択したクラウドアカウントが、テナント用に選択したものと同一セキュリティドメインと共有されている必要があります。同じAzureサブスクリプションを共有するすべてのテナントは、同じセキュリティドメインに存在する必要があります。

ステップ 9 必要に応じて、[Associated Users]領域で、テナントにアクセスできるユーザを選択します。

ステップ 10 (オプション) 整合性チェッカを有効にします。

このテナントのスケジュール済み整合性チェッカを有効にすることもできます。整合性チェックの詳細については、『[設定ガイド](#)』を参照してください。マルチサイト

ステップ 11 [保存 (Save)]をクリックしてテナントを追加します。

次のタスク

[スキーマの作成 \(83 ページ\)](#) に移動してスキーマを作成します。

スキーマの作成

Cisco Cloud APIC に固有ではない一般的な Multi-Site 手順がいくつかありますが、Multi-Site を介してオンプレミスサイトと Cisco Cloud APIC サイトを管理している場合は Cisco Cloud APIC の全体的なセットアップの一部として実行する必要があります。ここでは、APICのCisco Cloud 全体的なセットアップの一部である Multi-Site の一般的な手順について説明します。

Cisco Cloud APIC サイトの新しいスキーマを作成する場合は、この項の手順に従ってください。

Cisco Cloud APIC サイトに使用するスキーマがすでにある場合は、これらの手順をスキップして、[サイトをスキーマに追加する \(87 ページ\)](#) に移動することができます。

ステップ 1 メインメニューで[スキーマ]をクリックします。

ステップ 2 [スキーマ] ページで、[スキーマの追加]をクリックします。

- ステップ 3** [無題スキーマ] ページで、ページの上にあるテキスト 無題スキーマを、作成するスキーマの名前 (たとえば、`Cloudbursting` スキーマ) に置き換えます。
- ステップ 4** 左側のペインで [ロール (Roles)] をクリックします。
- ステップ 5** 中央のペインで、スキーマを作成するエリアをクリックしてテナントを選択してくださいをクリックしてください。
- ステップ 6** [テナントの選択] ダイアログ ボックスにアクセスし、ドロップダウン メニューから [テナントの設定 \(81 ページ\)](#) で作成したテナントを選択します。

アプリケーション プロファイルと EPG の設定

この手順では、アプリケーション プロファイルを設定し、2 つの EPG を追加する方法について説明します。1 つはクラウドサイト用、もう 1 つは、プロバイダ コントラクトが 1 つの EPG に関連付けられており、コンシューマ コントラクトが他の EPG に関連付けられている場合です。

- ステップ 1** 中央のペインで、[アプリケーション プロファイル (Application Profile)] エリアを見つけて、[+ アプリケーション プロファイル (+ Application profile)] をクリックします。
- ステップ 2** 右側のペインで、[表示名 (DISPLAY NAME)] フィールドにアプリケーション プロファイルの名前を入力します。
- ステップ 3** 中央のペインで、[+ EPG の追加 (+ ADD EPG)] をクリックして、クラウドサイトの EPG を作成します。
- ステップ 4** 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば `epg1`)。
- ステップ 5** オンプレミスサイトの EPG を作成する場合には、中央のペインで、[+ EPG の追加 (+ ADD EPG)] をクリックします。
- ステップ 6** 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば `epg2`)。
- ステップ 7** VRF を作成します。
- 中央のペインで、[VRF] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。
 - 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば `vrf1`)。
- ステップ 8** [保存 (SAVE)] をクリックします。

ブリッジ ドメインの作成と VRF への関連付け

この項の手順に従って、オンプレミスサイトのブリッジ ドメインを作成し、それを VRF に関連付けます。これらの手順は、クラウドのみのスキーマには必要ではないことに注意してください。

-
- ステップ 1 中央のペインで、**[EPG]** まで上にスクロールして戻り、以前にオンプレミスサイト用に作成した EPG をクリックします。
 - ステップ 2 右側のペインの**[オンプレミス プロパティ (ON-PREMPROPERTIES)]** エリアの**[ブリッジドメイン (BRIDGE DOMAIN)]** の下で、フィールドに名前を入力し (たとえば、bd1)、**[作成 (create)]** エリアをクリックして新しいブリッジドメインを作成します。
 - ステップ 3 中央のペインで、今作成したブリッジドメインをクリックします。
 - ステップ 4 **[仮想ルーティング/フォワーディング (Virtual Routing & Forwarding)]** フィールドで、[アプリケーションプロファイルと EPG の設定 \(84 ページ\)](#) で作成した VRF を選択します。
 - ステップ 5 **[サブネット (SUBNETS)]** エリアまで下にスクロールし、**[GATEWAY (ゲートウェイ)]** 見出しの下の**[サブネット (SUBNET)]** の横にある + をクリックします。
 - ステップ 6 **[サブネットの追加 (Add Subnet)]** ダイアログで、**[ゲートウェイ IP (Gateway IP)]** アドレスと、追加する予定のサブネットの説明を入力します。このゲートウェイ IP アドレスは、オンプレミスのサブネットのものです。
 - ステップ 7 **[範囲 (Scope)]** フィールドで、**[外部にアドバタイズ (Advertised Externally)]** を選択します。
 - ステップ 8 **[保存 (SAVE)]** をクリックします。
-

コントラクトのフィルタの作成

- ステップ 1 中央のペインで、**[コントラクト (Contract)]** エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。
 - ステップ 2 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドにフィルタの名前を入力します。
 - ステップ 3 **[+ 入力 (+ Entry)]** をクリックして、**[エントリの追加 (Add Entry)]** ディスプレイ上のスキーマフィルタについての情報を入力します。
 - a) **Name** フィールド (**Add Entry** ダイアログ) のスキーマフィルタ エントリの名前を入力します。
 - b) オプション。 **Description** フィールドにフィルタの説明を入力します。
 - c) EPG の通信のフィルタ処理を行うために、必要に応じて詳細を入力します。

たとえば、フィルタを通過する HTTPS トラフィックを許可するエントリを追加するには、次のように選択します。

TYPE: IP、IP PROTOCOL: TCP、および DESTINATION PORT RANGE FROM および DESTINATION PORT range TO: https。
 - d) **[保存 (SAVE)]** をクリックします。
-

コントラクトの作成

-
- ステップ 1** 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。
- ステップ 2** 右側のペインで、[表示名 (DISPLAY name)] フィールドにコントラクトの名前を入力します。
- ステップ 3** [範囲 (SCOPE)] エリアで、VRF の選択をそのままにします。
- ステップ 4** [フィルタ チェーン (FILTER CHAIN)] エリアで、[+ フィルタ (+ FILTER)] をクリックします。
[フィルタ チェーンの追加 (Add Filter Chain)] 画面が表示されます。
- ステップ 5** [名前 (NAME)] フィールドで、[コントラクトのフィルタの作成 \(85 ページ\)](#) で作成したフィルタを選択します。
- ステップ 6** 中央のペインで、[EPG] までスクロールして戻り、クラウドサイト用に作成した EPG をクリックします。
- ステップ 7** 右側のペインで、[+コントラクト (+ CONTRACT)] をクリックします。
[コントラクトの追加] 画面が表示されます。
- ステップ 8** [コントラクト (contract)] フィールドで、この手順で以前に作成したコントラクトを選択します。
- ステップ 9** [タイプ (TYPE)] フィールドで、[コンシューマ](#)または[プロバイダ](#)のいずれかを選択します。
- ステップ 10** [クラウドのプロパティ (CLOUD PROPERTIES)] エリアまでスクロールし、[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)] エリアで、[アプリケーションプロファイルと EPG の設定 \(84 ページ\)](#) で作成した VRF を選択します。
- ステップ 11** [保存 (SAVE)] をクリックします。
- ステップ 12** 中央のペインで、[EPG] までスクロールして戻り、オンプレミスサイト用に作成した EPG をクリックします。
- ステップ 13** 右側のペインで、[+コントラクト (+ CONTRACT)] をクリックします。
[コントラクトの追加] 画面が表示されます。
- ステップ 14** [コントラクト (contract)] フィールドで、この手順で以前に作成したコントラクトを選択します。
- ステップ 15** [タイプ (TYPE)] フィールドで、[[コンシューマ \(CONSUMER\)](#)] または [[プロバイダ \(PROVIDER\)](#)] を選択します。これは、前の EPG に選択しなかったものです
たとえば、最初の EPG に [[プロバイダ \(PROVIDER\)](#)] を選択した場合は、2番目の EPG の [[コンシューマ \(CONSUMER\)](#)] を選択します。
- ステップ 16** [クラウドのプロパティ (CLOUD PROPERTIES)] エリアまでスクロールし、[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)] エリアで、[アプリケーションプロファイルと EPG の設定 \(84 ページ\)](#) で作成したものと同一 VRF を選択します。
-

サイトをスキーマに追加する

ステップ 1 左側のペインで、[**サイト (Sites)**] の横にある + をクリックします。

ステップ 2 [**サイトの追加 (Add Sites)**] ページで、それぞれの横にあるボックスをオンにして、オンプレミスおよびクラウドサイトをスキーマに追加し、[**保存 (Save)**] をクリックします。

ステップ 3 左側のペインのクラウドサイトの下にあるテンプレートをクリックして、テンプレートのサイトローカルプロパティを設定します。

ステップ 4 中央のペインで、VRF をクリックします。

ステップ 5 右側のペインの [**サイト ローカル プロパティ (SITE LOCAL PROPERTIES)**] 領域で、次の情報を入力します。

- a) [**リージョン (region)**] フィールドで、この VRF を導入する Azure リージョンを選択します。
- b) **CIDR** フィールドで、+**CIDR** をクリックします。

[**クラウド CIDR の追加 (ADD CLOUD CIDR)**] ダイアログボックスが表示されます。次の情報を入力します。

- **CIDR**: VNET CIDR 情報を入力します。たとえば、11.11.0.0/16 とします。

CIDR には、Azure VNET で使用可能になるすべてのサブネットの範囲が含まれています。

(注) このフィールドに入力した VPC CIDR 情報は、インフラプールと重複させることはできません。このフィールドに入力した CIDR 情報が、[Azure でのクラウド APIC の導入 \(37 ページ\)](#) の [ステップ 6 \(39 ページ\)](#) の [**インフラ サブネット (Infra Subnet)**] フィールドに入力したインフラプール情報と重複していないことを確認します。

- [**CIDR タイプ (CIDR TYPE)**]: [プライマリ (Primary)] または [セカンダリ (Secondary)] を選択します。これが最初の CIDR の場合は、CIDR タイプとして [プライマリ (Primary)] を選択します。
- [**サブネット追加 (ADD SUBNETS)**]: サブネット情報を入力し、チェックマークをクリックします。たとえば、11.11.1.0/24 とします。

Cisco Cloud APIC の場合、サブネットはサブネットマスク付きの有効なサブネットであり、サブネットマスク付きの IP アドレスではありません。たとえば、11.11.0.0/24 は有効なサブネットおよびサブネットマスクですが、11.11.0.1 は IP アドレスおよびサブネットマスクですが、Cisco Cloud APIC で使用する有効なサブネットではありません。

(注) VGW 専用のサブネットを 1 つ追加する必要があります。この特定のサブネットに対して [Used by VGW] を選択します。

- c) ウィンドウで [**保存 (Save)**] をクリックします。

エンドポイントセレクタの追加

Cisco Cloud APIC では、クラウド EPG は、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウド EPG は、1 つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウド EPG に割り当てるために使用される、エンドポイントセレクタと呼ばれる機能があります。エンドポイントセレクタは、基本的に言って、Cisco ACI によって管理される Azure VNET に割り当てられたクラウドインスタンスに対して実行される一連のルールです。エンドポイントインスタンスに一致するエンドポイントセレクタルールは、そのエンドポイントをクラウド EPG に割り当てます。エンドポイントセレクタは、Cisco ACI で使用可能な属性ベースのマイクロセグメンテーションに似ています。

エンドポイントセレクタは、Cisco Cloud APIC GUI または Cisco Nexus Dashboard Orchestrator GUI のいずれかを使用して設定できます。2 つの GUI 間で使用可能なオプションにはわずかな違いがありますが、エンドポイントセレクタを追加するための一般的な概念と全体的な手順は、基本的にこの 2 つの間で同じです。

このセクションの手順では、Cisco Nexus Dashboard Orchestrator GUI を使用してエンドポイントセレクタを設定する方法について説明します。Cisco Cloud APIC GUI を使用したエンドポイントセレクタの設定の詳細については、『Cisco Cloud APIC User Guide、リリース 4.2 (x)』を参照してください。

ステップ 1 Cisco Cloud APIC のエンドポイントセレクタに使用できる Azure サイトから、必要な情報を収集します。

(注) これらの手順は、最初に Azure でインスタンスを設定してから、その後に Cisco Cloud APIC のエンドポイントセレクタを追加することを前提としています。ただし、最初に Cisco Cloud APIC のエンドポイントセレクタを追加してから、これらのエンドポイントセレクタの手順の最後に、この Azure インスタンスの設定手順を実行することもできます。

ステップ 2 ログインしていない場合は、Cisco Nexus Dashboard Orchestrator にログインします。

ステップ 3 左側のペインで、[スキーマ (schema)] をクリックし、以前に作成したスキーマを選択します。

ステップ 4 エンドポイントセレクタを作成する方法を決定します。

- 今後追加される、任意のクラウドサイトに適用できるエンドポイントセレクタを作成するには、次の手順を実行します。

1. 左側のペインで、テンプレートを選択したままにします。

これらの手順で特定のサイトを選択しないでください。

2. 中央のペインで、クラウドサイト用に作成した EPG を選択します。

3. 右側のペインの [クラウドのプロパティ (CLOUD PROPERTIES)] 領域で、+ ([セレクタ (SELECTORS)]) の横にあるものをクリックして、エンドポイントセレクタを設定します。

4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。
 5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタのタイプを選択します。
このように作成されたエンドポイントセレクタの場合、**[キー (Key)]** フィールドで使用できるオプションは **[EPG]** のみです。
 6. **ステップ 5 (90 ページ)** に進みます。
- このクラウドサイト専用のエンドポイント セレクタを作成するには、次の手順を実行します。
1. 左ペインで、クラウドサイトを選択します。
 2. 中央のペインで、クラウドサイト用に作成した EPG を選択します。
 3. 右側のペインの **[サイトのローカルのプロパティ (SITE LOCAL PROPERTIES)]** 領域の **[セレクタ (SELECTOR)]** 領域で、**+** (**[セレクタ (SELECTOR)]** の横にあるもの) をクリックして、エンドポイント セレクタを設定します。
 4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。
たとえば、IP サブネット分類のエンドポイントセレクタの場合は、**[IP-Subnet-EPSelector]** などの名前を使用できます。
 5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタで使用するキーを選択します。
 - **[IP アドレス (IP Address)]**: IP アドレスまたはサブネットによって選択するために使用されます。エンドポイントセレクタとしてのIPアドレスの値は、CIDRで作成されたユーザサブネットに属します。[サイトをスキーマに追加する \(87 ページ\)](#)
さらに、特にAzureスケールセットVMの場合、エンドポイントセレクタとしてのIPアドレスの値は、そのスケールセットが存在する場所で設定された完全なサブネットである必要があります。[サイトをスキーマに追加する \(87 ページ\)](#) サブネット内のIPアドレスは使用できません。
たとえば、AzureスケールセットVMのこれらのフィールドで次の値を使用した場合。
 - CIDR : 10.1.0.0/16
 - Subnet : 10.1.0.0/24エンドポイントセレクタとしてのIPアドレスの有効な値は10.1.0.0/24です。10.1.0.1/32または10.1.0.0/16のエントリは、AzureスケールセットVMのエンドポイントとしてのIPアドレスの有効な値ではありません。
(注) IPv6はAzureではCisco Cloud APICに対してサポートされていません。このフィールドには有効なIPv4アドレスを使用する必要があります。
 - **[リージョン (Region)]**: エンドポイントの Azure リージョンで選択するために使用されます。

- エンドポイントセレクトアのカスタムタグを作成する場合は、**[検索または作成のために入力 (Type to search or create)]** フィールドで入力を開始してカスタム タグまたはラベルを入力し、新しいフィールドで **[作成 (Create)]** をクリックして、新しいカスタム タグまたはラベルを作成します。

Azure にタグを追加するときに、これらの手順の前の例を使用すると、以前に Azure で追加したロケーションタグと一致するように、このフィールドにカスタム タグのロケーションを作成できます。

ステップ 5 **[演算子 (Operator)]** フィールドで、エンドポイント セレクトアに使用する演算子を選択します。

次のオプションがあります。

- **[等しい (Equals)]**: [値 (value)] フィールドに 1 つの値がある場合に使用します。
- **[等しくない (Not Equals)]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある (In)]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にある (Not In)]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ (Has Key)]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 6 **[値 (value)]** フィールドで、2 つ前のフィールドに対して行った選択に基づいて、エンドポイントセレクトアに使用する値を選択します。**[値 (Value)]** フィールドには、複数のカンマ区切りのエントリを含めることができます。このフィールドのエントリの間には論理 OR があるものとみなされます。

(注) **[キーを持つ (Has Key)]** または **[キーの不在 (Key Not Exist)]** を選択していない場合には、**[演算子 (Operator)]** フィールドは表示されません。

たとえば、エンドポイントセレクトアに、westus など特定の Azure リージョンがある場合には、この画面で次の項目を選択します。

- **[キー (Key):]** Region
- **[演算子 (Operator):]** Equals
- 値 : westus

別の例として、これらのフィールドで次の値を使用したとします。

- **[キー (Key):]** IP
- **[演算子 (Operator):]** Has Key
- **[値 (Value):]** は、演算子 (Operator) フィールドで [Has Key] が使用されているため、使用できません。

EPG ルールは、この状況で IP アドレスを持つすべてのエンドポイントに適用されます。

最後の例として、これらのフィールドで次の値を使用したとします。

- [キー (Key):] custom tag: Location
- [演算子 (Operator):] Has Key
- [値 (Value):]は、演算子 (Operator) フィールドで [Has Key] が使用されているため、使用できません。

この場合、EPGルールは、Azure タグ キーとして Location を持つすべてのエンドポイントに、ロケーションの値に関係なく適用されます。

ステップ 7 このエンドポイントセレクタ式の作成が完了したら、チェックマークをクリックします。

ステップ 8 追加のエンドポイントセレクタ式を作成するかどうかを決定します。

単一のエンドポイントセレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイントセレクタ 1、式 1:
 - [キー (Key):] Region
 - [演算子 (Operator):] Equals
 - 値 : eastus
- エンドポイントセレクタ1、式 2:
 - [キー (Key):] IP
 - [演算子 (Operator):] Equals
 - [値 (Value):] 192.0.2.1/24

この場合、これらの式の両方が真になる場合 (regionが eastus で、IP アドレスがサブネット 192.0.2.1/24 に属している場合) に、そのエンドポイントはクラウド EPG に割り当てられます。

このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックします。

ステップ 9 このエンドポイントセレクタの式の作成が完了したら、[保存 (SAVE)] をクリックします。これは [新しいエンドポイントセレクタの追加 (Add New End Point selector)] の右下隅にあります。

EPGの下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイントセレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイントセレクタを作成したとします。

- エンドポイントセレクタ 2、式 1:
 - [キー (Key):] Region
 - [演算子 (Operator):] In
 - 値 : centralus、eastus2

その場合、次のようになります。

- リージョンが **eastus** で、IP アドレスが 192.0.2.1/24 サブネットに属している (エンドポイント セレクタ 1 の式)

または

- リージョンが **centralus** または **eastus2** (エンドポイント セレクタ 2 の式) のいずれかである

その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 10 エンドポイント セレクタの作成が完了したら、右上隅の **[保存 (SAVE)]** をクリックします。

ステップ 11 画面の右上隅にある **[サイトに展開 (DEPLOY TO SITES)]** ボタンをクリックして、スキーマをサイトに展開します。

[正常に展開 (Successfully Deployed)] されたというメッセージが表示されます。

次のタスク

[マルチサイト構成の確認 \(92 ページ\)](#) の手順を使用して、マルチサイトエリアが正しく設定されていることを確認します。

マルチサイト構成の確認

このトピックの手順を使用して、Cisco Nexus Dashboard Orchestrator に入力した設定が正しく適用されていることを確認します。

ステップ 1 Cisco Cloud APIC にログインし、次のことを確認します。

- [ダッシュボード (Dashboard)] をクリックしサイト間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を使用して、次のことを確認します。
 - トンネルは、Azure 上の Cisco Cloud Services Router 1000V から、オンプレミスの ISN (IPsec 終端ポイント)、およびユーザー VNet の VGW に対して動作しています。
 - OSPF ネイバーが CCR と ISN オンプレミス デバイスの間で起動していることを示します。
 - VRF の BGP EVPN ルートにはクラウドとオンプレミスのルートが表示され、クラウドルートは ACI スパイン スイッチの BGP EVPN を介して入力されます。
- [アプリケーション管理 (Application Management)] → [テナント] をクリックし、テナントが正しく設定されていることを確認します。
- [アプリケーション管理 (Application Management)] → [アプリケーションプロファイル] をクリックし、アプリケーションプロファイルが正しく設定されていることを確認します。
- [アプリケーション管理 (Application Management)] → [EPG] をクリックし、EPG が正しく設定されていることを確認します。

- e) [アプリケーション管理 (Application Management)] → [コントラクト] をクリックし、契約が正しく設定されていることを確認します。
- f) [アプリケーション管理 (Application Management)] → [VRF] をクリックし、VRF が正しく設定されていることを確認します。
- g) [アプリケーション管理 (Application Management)] → [クラウド コンテキスト Cloud プロファイル] をクリックし、クラウド コンテキスト プロファイルが正しく設定されていることを確認します。
- h) [クラウドリソース (Cloud Resources)] → [リージョン] をクリックし、リージョンが正しく設定されていることを確認します。
- i) [クラウドリソース (Cloud Resources)] → [VNETs] をクリックし、VNETs が正しく設定されていることを確認します。
- j) [クラウドリソース (Cloud Resources)] → [クラウドエンドポイント] をクリックし、クラウドエンドポイントが正しく設定されていることを確認します。
- k) [クラウドリソース (Cloud Resources)] → [ルータ] をクリックし、CCR が正しく設定されていることを確認します。

ステップ 2 オンプレミスの APIC サイトにログインし、APIC のスキーマを確認します。

Cisco Nexus Dashboard Orchestrator で設定した共有テナントが APIC のテナントエリアに表示され、Cisco Nexus Dashboard Orchestrator スキーマから展開された VRF と EPG がオンプレミス APIC で設定されていることが確認できます。

ステップ 3 コマンドラインから、Azure の CCR で VRF が正しく作成されていることを確認します。

show vrf

テナント t1 と VRF v1 が Cisco Nexus Dashboard Orchestrator から展開されている場合、CCR の出力は次のようになります。

Name	Default RD	Protocols	Interfaces
t1:v1	64514:3080192	ipv4	BD1 Tu4 Tu5

ステップ 4 コマンドラインから、Azure の CCR と ISN オンプレミス デバイスの間でトンネルがアップしていることを確認します。

Azure の CCR または ISN オンプレミスのデバイスで、次のコマンドを実行できます。

show ip interface brief | inc Tunnel

以下のような出力が表示されます。

Interface	IP-Address	OK?	Method	Status	Protocol
Tunnel1	1.2.3.22	YES	manual	up	up
Tunnel2	1.2.3.30	YES	manual	up	up
Tunnel3	1.2.3.6	YES	manual	up	up
Tunnel4	1.2.3.14	YES	manual	up	up

ステップ 5 コマンドラインから、Azure の CCR と ISN オンプレミス デバイスの間で OSPF ネイバーがアップしていることを確認します。

show ip ospf neighbor

以下のような出力が表示されます。

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.200.10.201	0	FULL/ -	00:00:36	1.2.3.13	Tunnel4
20.30.40.50	0	FULL/ -	00:00:36	1.2.3.29	Tunnel2
10.202.101.202	0	FULL/ -	00:00:38	1.2.3.5	Tunnel3

ステップ6 コマンドラインから、オンプレミスの BGP EVPN ネイバーが CCR に存在することを確認します。

```
show bgp l2vpn evpn summary
```

以下のような出力が表示されます。

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.2	4	100	139	137	99	0	0	01:30:36	6

ステップ7 コマンドラインから、VRF の BGP ルートにクラウドとオンプレミスの両方のルートが表示されていることを確認します。

(注) 現在、Cisco Cloud APIC のワークフローでは、VRF は、対応する VNET が Azure で作成されるまで、CCR で構成されません。

```
show ip route vrf t1:v1
```

以下のような出力が表示されます。

```
B 129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1
B 130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```



第 7 章

Cisco Cloud APIC GUI について

- [Cisco Cloud APIC GUI の操作 \(95 ページ\)](#)
- [Cisco Cloud APIC GUIを使用したテナントの作成 \(96 ページ\)](#)
- [Cisco Cloud APIC コンポーネントの設定 \(96 ページ\)](#)

Cisco Cloud APIC GUI の操作

Cisco Cloud APIC をインストール後、それを使用して Cisco Application Centric Infrastructure (ACI) ポリシーを Amazon Web Services (AWS) または Microsoft Azure パブリック クラウドに拡張するために使用できます。これを行うには、Cisco Cloud APIC GUI を使用します。

Cisco Cloud APIC GUI では、テナントを作成し、アプリケーションプロファイル、エンドポイントグループ (EPG)、コントラクト、フィルタ、および VRF を設定できます。Cisco Cloud APIC トポロジ、設定、およびリソースを表示することもできます。

を使用して設定手順を実行します。インテント機能。インテント機能の使用方法については、[Cisco Cloud APIC コンポーネントの設定 \(96 ページ\)](#) を参照してください。『*Cisco Cloud APIC User Guide*』の「Understanding the Cisco Cloud APIC GUIアイコン」の項も参照してください。

Cisco Cloud APIC の基本的なタスクを実行する手順は、通常の Cisco APIC の手順とは異なりません。ただし、テナントの機能、アプリケーションプロファイル、および Cisco APIC のその他の要素は同じです。詳細については、Cisco.com の『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

左側のナビゲーションペインで設定やその他の情報を表示します。[Dashboard] (デフォルトビュー)、[Topology]、[Application Management]、[Cloud Resources]、[Operations]、[Infrastructure]、および [Administrative] を選択できます。

アイコンの詳細については、Cisco.comの『*Cisco Cisco Cloud APIC User Guide*』の「Understanding the Cisco Cloud APIC GUI Icons」の項を参照してください。

Cisco Cloud APIC GUIを使用したテナントの作成

次の項では、Cisco Cloud APIC GUI を使用してテナントを作成する方法について説明します。

Cisco Cloud APIC コンポーネントの設定

このセクションでは、テナント、アプリケーションプロファイル、およびエンドポイントグループ (EPG) の作成を含む、Cisco Cloud APIC で主要なタスクの実行の概要について説明します。

始める前に

Cisco Cloud APIC をインストールしておく必要があります。このガイドの前のインストールの項を参照してください。

ステップ 1 Cisco Cloud APIC にログインします。

ステップ 2 [ダッシュボード (Dashboard)] ペインの右上で、ブルズアイを指す矢印の付いたアイコンをクリックします。

このアイコンは、**インテント** アイコンまたは機能と呼ばれることがあります。

ステップ 3 [何をしますか] ウィンドウに用語を入力して、オプションのリストを表示します。

たとえば、テナントを設定する場合は、検索ウィンドウに `tenant` と入力します。検索は、テナントの作成と設定に関連するタスクのリストを返します。

ステップ 4 タスクをクリックし、開いたウィンドウで設定手順を実行します。

次のタスク

左側のナビゲーションペインで設定を確認できます。[ダッシュボード (Dashboard)] ペインの左上にあるハンバーガーアイコンをクリックして、ペインを展開します。該当する見出しを展開して設定を表示します。

たとえば、テナントを設定した場合は、[アプリケーション管理 (Application Management)] を展開し、[テナント (Tenants)] をクリックします。中央の作業ウィンドウにテナントに関する情報が表示されます。



第 8 章

システムのアップグレード、ダウングレード、またはリカバリの実行

- [特記事項 \(97 ページ\)](#)
- [ソフトウェアのアップグレード \(100 ページ\)](#)
- [ソフトウェアのダウングレード \(122 ページ\)](#)
- [システム リカバリの実行 \(128 ページ\)](#)
- [CCR のアップグレードのトリガー \(128 ページ\)](#)

特記事項

リリース 25.0(3) に関する特記事項

リリース 25.0(3) のインストール、アップグレード、またはダウングレード手順に関する特記事項を次に示します。

- Cisco Catalyst 8000V は、サブスクリプションベースのライセンスをサポートしています。25.0(3) より前のリリースからリリース 25.0(3) にアップグレードする前に、まず階層ベースの Cisco Catalyst 8000V ライセンスのいずれかをサブスクライブする必要があります。
 - ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、[Cisco Catalyst 8000V Edge ソフトウェア](#) を参照してください。
 - 層に基づくさまざまなスループットの詳細については、[Azure パブリッククラウドの要件 \(20 ページ\)](#) を参照してください。

Cisco Cloud APIC は、「Cisco DNA Advantage」サブスクリプションを利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、[Cisco DNA SoftwareSD-WAN およびルーティング マトリックス](#) を参照してください。

- Cisco Cloud APIC をリリース 25.0(3) にアップグレードする場合は、Cisco Cloud APIC のアップグレード後できるだけ早く CCR をアップグレードする必要があります。手順については、以下を参照してください。
 - [ソフトウェアのアップグレード \(100 ページ\)](#)

- [CCR のアップグレードのトリガー \(128 ページ\)](#)

以下は、これらのアップグレードプロセスを実行する方法の例です。

- **単一サイトのアップグレード**：通常、単一サイトの Azure の展開には CCR があります。Cisco Cloud APIC がリリース 25.0(3) へのアップグレードを完了し、準備完了状態に達したら、構成の変更を行う前に、古い CCR (Cisco Cloud Services Router 1000v) から新しい CCR (Cisco Catalyst 8000V) へのアップグレードを開始する必要があります。
- **マルチクラウド/ハイブリッドクラウドアップグレード**：このアップグレードプロセスの例として、次の設定があると仮定します。
 - サイト 1：AWS
 - サイト 2：Azure
 - サイト 3：オンプレミス サイト

次に、これらのサイトを次の方法でアップグレードします。

1. Nexus Dashboard Orchestrator を 3.7(1) リリースにアップグレードします。
2. [ソフトウェアのアップグレード \(100 ページ\)](#) の手順を使用して、サイト 1 (AWS サイト) を Cisco Cloud APIC リリース 25.0(3) にアップグレードします。

このアップグレードが安定した状態になるまで待ってから、次の手順に進みます。

3. [CCR のアップグレードのトリガー \(128 ページ\)](#) の手順を使用して、サイト 1 (AWS サイト) の CCR を古い CCR (Cisco Cloud Services Router 1000v) から新しい CCR (Cisco Catalyst 8000V) にアップグレードします。

CCR が新しい Cisco Catalyst 8000V に完全にアップグレードされるまで待ってから、次の手順に進みます。

4. サイト 1 (AWS サイト) の CCR が完全にアップグレードされたら、サイト 2 (Azure サイト) に対してこれらの手順を繰り返します。最初に Cisco Cloud APIC ソフトウェアをリリース 25.0(3) にアップグレードします。アップグレードが安定した状態に達したら、サイト 2 の CCR を新しい Cisco Catalyst 8000V にアップグレードします。

- Cisco Cloud APIC リリース 25.0(3) より前の古い Cisco Cloud Services Router 1000v ルータは、[Azure パブリック クラウドの要件 \(20 ページ\)](#) で説明されているように、番号ベースのスループットで設定されていました。Cisco Catalyst 8000V ルータは階層ベースのスループット オプションのみをサポートするため、リリース 25.0(3) へのアップグレード中に、Cisco Cloud APIC は、古い Cisco Cloud Services Router 1000v ルータで使用される数値ベースのスループットからのスループット値を新しい Cisco Catalyst 8000V ルータで使用される階層ベースのスループットにマッピングします。

次の表は、アップグレード中の古い Cisco Cloud Services Router 1000v ルータから新しい Cisco Catalyst 8000V ルータへのスループットのマッピングを示しています。

Cisco クラウド サービス ルータ 1000v	Cisco Catalyst 8000V のスループット
10 M	T0 (最大 15M のスループット)
5,000 万人	T1 (最大 100M のスループット)
1 億	T1 (最大 100M のスループット)
2 億 5000 万	T2 (最大 1G のスループット)
5 億	T2 (最大 1G のスループット)
1G	T2 (最大 1G のスループット)
2.5G	T3 (最大 10G のスループット)
5G	T3 (最大 10G のスループット)
7.5G	T3 (最大 10G のスループット)
10G	T3 (最大 10G のスループット)

アップグレード中に古い Cisco Cloud Services Router 1000v ルータから新しい Cisco Catalyst 8000V ルータに移行する場合、Cisco Cloud APIC は、上記のように同等の帯域幅を移行します。これらの Cisco Catalyst 8000V ルータが起動すると、その帯域幅をスマート ライセンス アカウントに登録しようとします。スマート ライセンス サーバーにこれらのライセンスがない場合、Cisco Catalyst 8000V はデフォルトの帯域幅にフォールバックし、既存のワークロードトラフィックを処理できなくなります。したがって、アップグレード時に古い Cisco Cloud Services Router 1000v ルータから新しい Cisco Catalyst 8000V ルータに移行する前に、必要な Cisco Catalyst 8000V ライセンスをスマート アカウントで調達してプロビジョニングする必要があります。

- 同様に、リリース 25.0(3) から以前のリリースにダウングレードする場合、Cisco Cloud APIC は、新しい Cisco Catalyst 8000V ルータで使用される階層ベースのスループットから、古い Cisco Cloud Services Router 1000v ルータで使用される数値ベースのスループットにスループット値をマッピングします。

次の表は、新しい Cisco Catalyst 8000V ルータから、ダウングレード中に古い Cisco Cloud Services Router 1000v ルータで使用される数値ベースのスループットへのスループットのマッピングを示しています。

Cisco Catalyst 8000V のスループット	Cisco Cloud Services Router 1000v のスループット
T0 (最大 15M のスループット)	10 M
T1 (最大 100M のスループット)	1 億

Cisco Catalyst 8000V のスループット	Cisco Cloud Services Router 1000v のスループット
T2 (最大 1G のスループット)	1G
T3 (最大 10G のスループット)	10G



- (注) Cisco Cloud APIC と CCR が非互換モードの場合は、構成を変更しないでください。リリース 25.0(3) にアップグレードする場合は、構成を変更する前に、Cisco Cloud APIC と CCR の両方がその最新リリースにアップグレードされていることを確認してください。

ソフトウェアのアップグレード

次のセクションでは、移行ベースのアップグレードまたはポリシーベースのアップグレードのいずれかを使用した Cisco Cloud APIC ソフトウェアのアップグレードについて説明します。Cisco Cloud APIC ソフトウェアをアップグレードする前に、[このリンク](#)で情報を確認してください。[ソフトウェアのアップグレードに関する注意事項と制約事項 \(101 ページ\)](#)

Cisco Cloud APIC ソフトウェアのアップグレードに使用する方法は、状況によって異なります。

- 5.0(x) より前のリリースからリリース 5.1(2) にアップグレードする場合は、移行ベースのプロセスを使用してソフトウェアをアップグレードします。これらの指示については、[移行ベースのアップグレード \(101 ページ\)](#) にアクセスしてください。



- (注) で説明したように、アップグレードに使用したのと同じ移行ベースの手順をシステムリカバリにも使用できます。[システムリカバリの実行 \(128 ページ\)](#)

- リリース 5.0(x) からリリース 5.1(2) にアップグレードする場合は、ポリシーベースのプロセスを使用してソフトウェアをアップグレードします。これらの指示については、[ポリシーベースのアップグレード \(115 ページ\)](#) にアクセスしてください。



- (注) リリース 5.0(x) からリリース 5.1(2) へのポリシーベースのアップグレードが何らかの理由で機能しない場合は、[移行ベースのアップグレード \(101 ページ\)](#) で説明されている移行ベースのプロセスを使用して、リリース 5.0(x) からリリース 5.1(2) にアップグレードできます。

CCR のアップグレード

Cisco Cloud APIC ソフトウェアのアップグレードに使用する方法に関係なく、クラウド APIC ソフトウェアをアップグレードするたびに、クラウドルータ (CCR) もアップグレードする必要があります。

- リリース 5.2(1) より前のリリースでは、Cisco Cloud APIC のアップグレードをトリガーするたびに CCR が自動的にアップグレードされます。
- リリース 5.2(1) 以降では、Cisco Cloud APIC のアップグレードとは関係なく、CCR のアップグレードをトリガーし、それらの CCR のアップグレードをモニタできます。これは、管理プレーン (Cisco Cloud APIC) とデータプレーン (CCR) のアップグレードを分割できるため、トラフィック損失を削減するのに役立ちます。

詳細については、「[CCR のアップグレードのトリガー \(128 ページ\)](#)」を参照してください。

ソフトウェアのアップグレードに関する注意事項と制約事項

次に、Cisco Cloud APIC ソフトウェアをアップグレードする前に知っておく必要がある注意事項と制限事項を示します。

リリース 5.0(2) 以降、[Cisco Cloud APIC for Azure ユーザー ガイド](#)、リリース 5.0(x) 以降の「構成のばらつき」の章で説明されているように、構成のばらつき機能が使用可能になりました。Cisco Cloud APIC をアップグレードした後、アップグレード前に構成のばらつきを有効にしていた場合、アップグレードの完了後に構成のばらつき機能が再起動されます。機能を再起動すると、以前の構成のばらつき分析はクリアされ (アップグレード後に構成のばらつきは表示されません)、アップグレード後に機能を再起動すると、構成のばらつきの新しい分析が開始されます。これは想定されている動作です。

移行ベースのアップグレード

次の手順に従って、移行ベースのプロセスを使用してソフトウェアをアップグレードします。

このセクションの手順を実行する前に、に記載されている情報を確認してください。[ソフトウェアのアップグレードに関する注意事項と制約事項 \(101 ページ\)](#)



- (注) アップグレードに使用されるこれらの移行ベースの手順は、で説明されているように、システムリカバリにも使用できます。[システムリカバリの実行 \(128 ページ\)](#)

既存のクラウド APIC 設定情報の収集

Cisco Cloud APIC ソフトウェアをアップグレードまたはダウングレードする前に、このトピックの手順に従って特定のフィールドの既存の設定情報を検索し、これらの各フィールドのエントリを書き留めます。リカバリ テンプレートをを使用して Cisco Cloud APIC をアップグレードする場合は、次の手順の後の手順で、これらのフィールドに同じエントリを使用します。

次の各フィールドについて、で実行した元の導入の一部として入力したエントリをメモします。[Azure でのクラウド APIC の導入 \(37 ページ\)](#)

- [サブスクリプション \(102 ページ\)](#)
- [リソース グループ \(102 ページ\)](#)
- [ロケーション \(102 ページ\)](#)
- [Fabric Name \(ファブリック名\) \(103 ページ\)](#)
- [外部サブネット \(104 ページ\)](#)
- [Virtual Machine Name \(104 ページ\)](#)
- [インフラVNETプール \(104 ページ\)](#)
- [ストレージ アカウント名 \(105 ページ\)](#)

サブスクリプション

1. [アプリケーション管理 (Application Management)] > [テナント (Tenants)] の順に移動します。
2. [Name]列の名前の下にinfraがあるテナントの行を見つけます。
3. [Azure Subscription]列の値をメモします。
これは、Cisco Cloud APIC のサブスクリプション エントリです。

リソース グループ

1. [クラウド リソース仮想マシン]に移動します。
[仮想マシン] ウィンドウが表示されます。
2. VM リストで Cisco Cloud APIC VM を見つけてメモします。
VMの値は通常、次の形式で表示されます。
 - 「vm_name」は、で説明されているように、仮想マシン名です。[Virtual Machine Name \(104 ページ\)](#)
 - (<resource_group>) は、Cisco Cloud APIC のリソース グループエントリです。

ロケーション

1. [クラウド リソース仮想マシン]に移動します。
[仮想マシン] ウィンドウが表示されます。
2. VM リストで Cisco Cloud APIC VM を見つけます。
3. VM リストで Cisco Cloud APIC VMの値をクリックします。

Cisco Cloud APIC VMの詳細が記載されたナビゲーションパネルが画面の右側から表示されます。

4. [General]領域で、[Region]フィールドの値を見つけてメモします。

これは、Cisco Cloud APIC のロケーション エントリです。

Fabric Name (ファブリック名)

1. CLI を介して Cisco Cloud APIC に SSH で接続します。

```
# ssh admin@<cloud_apic_ip_address>
```

プロンプトが表示されたら、パスワードを入力します。

2. 次の CLI を入力します。

```
ACI-Cloud-Fabric-1# acidiag avread
```

3. 出力でFABRIC_DOMAIN領域を見つけます。

```
Local appliance ID=1 ADDRESS=10.100.0.13 TEP ADDRESS=10.100.0.12/30 ROUTABLE IP
ADDRESS=0.0.0.0
CHASSIS_ID=afe36d66-042a-11eb-ab21-7b2dc494b182

Cluster of 1 lm(t):1(zeroTime) appliances (out of targeted 1
lm(t):1(2020-10-01T21:15:48.743+00:00))
with FABRIC_DOMAIN name=ACTI-Cloud-Fabric set to version=5.0(2i)
lm(t):1(2020-10-01T21:15:48.746+00:00);
discoveryMode=PERMISSIVE lm(t):0(zeroTime); drrMode=OFF lm(t):0(zeroTime);
kafkaMode=OFF lm(t):0(zeroTime)


appliance id=1 address=10.100.0.13 lm(t):1(2020-10-01T21:14:23.001+00:00) tep
address=10.100.0.12/30
lm(t):1(2020-10-01T21:14:23.001+00:00) routable address=0.0.0.0 lm(t):1(zeroTime)
oob address=10.100.0.29/28 lm(t):1(2020-10-01T21:14:26.723+00:00) version=5.0(2i)
lm(t):1(2020-10-01T21:14:26.841+00:00) chassisId=afe36d66-042a-11eb-ab21-7b2dc494b182

lm(t):1(2020-10-01T21:14:26.841+00:00) capabilities=0X7EEEEEEEEEE--0X2020--0X1
lm(t):1(2020-10-01T21:20:27.483+00:00) rK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) aK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobrK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobaK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) cntrlSbst=(APPROVED, E8E6DDB1D800)
lm(t):1(2020-10-01T21:14:26.841+00:00) (targetMbSn= lm(t):0(zeroTime),
failoverStatus=0 lm(t):0(zeroTime)) podId=1 lm(t):1(2020-10-01T21:14:23.001+00:00)
commissioned=YES lm(t):1(zeroTime) registered=YES
lm(t):1(2020-10-01T21:14:23.001+00:00)
standby=NO lm(t):1(2020-10-01T21:14:23.001+00:00) DRR=NO lm(t):0(zeroTime) apicX=NO

lm(t):1(2020-10-01T21:14:23.001+00:00) virtual=YES
lm(t):1(2020-10-01T21:14:23.001+00:00)
active=YES(2020-10-01T21:14:23.001+00:00) health=(applnc:255
lm(t):1(2020-10-01T21:16:16.514+00:00) svc's)
-----
clusterTime=<diff=-1 common=2020-10-02T07:46:19.717+00:00
local=2020-10-02T07:46:19.718+00:00
pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):1(2020-10-01T21:15:50.026+00:00)>>
-----
```

これは、Cisco Cloud APIC のファブリック名エントリです。

外部サブネット


1. [アプリケーション管理] > [EPG s] の順に移動します。
2. ext-networks という名前の EPG を見つけ、その EPG をクリックします。
画面の右側からナビゲーションパネルがスライドします。
3. ナビゲーションパネルで、[詳細 (Details)] アイコン () をクリックします。  この EPG の概要ページが表示されます。
4. [Endpoints] 領域で、[ext-Network1] の行を見つて、[Subnet] 列の値を確認します。
これは Cisco Cloud APIC の外部サブネットエントリです。値 0.0.0.0/0 は、誰でも Cisco Cloud APIC への接続が許可されることを意味します。

Virtual Machine Name

1. [クラウド リソース 仮想マシン] に移動します。
[仮想マシン] ウィンドウが表示されます。
2. リストで Cisco Cloud APIC VM を見つけてメモします。
VM の値は通常、次の形式で表示されます。 <vm_name>(<resource_group>)
 - <vm_name> は、Cisco Cloud APIC の仮想マシン名エントリです。
 - (<resource_group>) は、で説明されているリソースグループです。 [リソース グループ \(102 ページ\)](#)

インフラ VNET プール

インフラ VNET プールの場合、複数のインフラ サブネットプールがある可能性があるため、[Azure でのクラウド APIC の導入 \(37 ページ\)](#) の手順の一部として、ARM テンプレートを使用して元の Cisco Cloud APIC を起動したときに使用したインフラサブネットの情報を確認してください。

1. Cisco Cloud APIC GUI で、[インテント (Intent)] アイコン () をクリックし、[cAPIC セットアップ (cAPIC Setup)] を選択します。
2. [リージョン管理 (Region Management)] エリアで、[設定の編集 (Edit Configuration)] をクリックします。
[管理するリージョン (Regions to Manage)] ウィンドウが表示されます。
3. [Next] をクリックします。
[一般接続 (General Connectivity)] ウィンドウが表示されます。

4. [一般 (General)] の下の [クラウドルータのサブネットプール (Subnet Pools for Cloud Routers)] 領域で、[作成者 (Created By)] 列に [システム内部 (System Internal)] 値がある行を見つけ、[サブネット (Subnet)] 列の値をメモします。

これはの Cisco Cloud APIC の **Infra VNET** プール エントリです。

ストレージアカウント名

Cisco Cloud APIC が以前に展開されたリソース グループの下にある Azure の [ストレージアカウント (Storage accounts)] ページに移動します。

1. まだログインしていない場合は、Cisco Cloud APIC インフラ テナントの Azure アカウントにログインし、Azure 管理コンソールに移動します。

<https://portal.azure.com/#home>

2. [サービス (Services)] の [ストレージアカウント (Storage accounts)] を選択します。
[ストレージアカウント (Storage accounts)] ページが表示されます。

3. Cisco Cloud APIC リソース グループのストレージアカウント名を見つけてメモします。
これはのストレージアカウント名エントリです。

既存設定のバックアップ

後で何らかの理由で以前のリリースにロールバックすることにした場合に備えて、移行ベースのアップグレードを実行する前に、既存の構成をバックアップすることをお勧めします。

始める前に

これらの手順に進む前に、[既存のクラウドAPIC設定情報の収集 \(101 ページ\)](#) の手順を完了してください。

ステップ 1 バックアップを実行する前に、グローバル AES 暗号化を有効にします。

- a) Cisco Cloud APIC GUI で、[インフラストラクチャ > システム設定 (Infrastructure System Configuration)] に移動します。

デフォルトでは、[一般 (General)] タブが表示されます。そうでない場合は、[一般 (General)] タブをクリックします。

- b) [Global AES Encryption] 領域の右上にある鉛筆アイコンをクリックします。

[Global AES 暗号 Settings] ウィンドウが表示されます。

- c) [Encryption : Enabled] 領域の横にあるボックスをクリックし、[Passphrase / Confirm Passphrase] フィールドにパスワードを入力して、ウィンドウの下部にある [Save] をクリックします。

バックアップの復元プロセスの一部として必要になるため、この手順で入力したパスワードを書き留めておきます。

ステップ 2 既存の設定をバックアップします。

- a) [操作 (Operations)] > [バックアップと復元 (Backup & Restore)] に移動します。
- b) [バックアップ プロファイル (Backup Profiles)] タブをクリックします。
- c) [アクション (Actions)] > [バックアップ設定の作成 (Create Backup Configuration)] をクリックします。
- d) 既存の設定をバックアップします。

バックアップの構成の作成で使用できるオプションの詳細については、『Azure ユーザー ガイド用 Cisco Cloud APIC』の「Cisco Cloud APIC GUI を使用してバックアップの構成を作成する」の手順を参照してください。

ステップ 3 Cisco Cloud APIC VM を削除します。

- a) Microsoft Azure ポータルで、[Services > Virtual Machines] に移動します。
- b) [仮想マシン (Virtual Machines)] ウィンドウで Cisco Cloud APIC VM を見つけ、[Cloud APIC VM] をクリックします。
この Cisco Cloud APIC VM の概要ページが表示されます。
- c) [削除 (Delete)] をクリックし、このアクションの確認を求められたら [はい (Yes)] をクリックします。
[通知 (Notifications)] 領域で削除プロセスを確認できます。

リカバリ テンプレートのダウンロードと展開

始める前に

これらの手順に進む前に、[既存設定のバックアップ \(105 ページ\)](#) の手順を完了してください。

ステップ 1 Cisco Cloud APIC のリリースに適したリカバリ テンプレートをダウンロードします。

Cisco TAC に連絡して、適切な回復テンプレートを入手してください。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

ステップ 2 Azure ポータルにリカバリ テンプレートを展開します。

- a) Azure ポータルで、[All Services] ページに移動します。
<https://portal.azure.com/#allservices>
- b) [General] 領域で、[Templates] をクリックします。
- c) [テンプレート (Templates)] ページで、[追加 (Add)] をクリックします。
[テンプレートの追加] ページが表示されます。
- d) [テンプレートの追加 (Add Template)] ページに必要な情報を入力します。

- **Name** : このテンプレートをリリース固有のリカバリ テンプレートとして識別する一意の名前を入力します(たとえば、リリース 25.0(1) リカバリ テンプレートの場合、リリース固有の一意の名前として `template-2501-recovery` を使用できます)。
- [説明 (Description)] : 必要に応じて、このテンプレートの説明テキストを入力します。

e) **OK** をクリックします。

[ARM テンプレート (ARM template)] ページが表示されます。

- f) [ARM テンプレート (ARM Template)] ページで、テンプレートに自動的に追加されるデフォルトのテキストを削除します。
- g) [ステップ 1 \(106 ページ\)](#) のリカバリ テンプレートをダウンロードした領域に移動します。
- h) テキストエディタを使用して、リカバリテンプレートを開き、テンプレートの内容をコピーします。
- i) Azureポータルウィンドウで、[ARMテンプレート (ARM Template)] ページに内容を貼り付けます。
- j) **OK** をクリックします。

[テンプレートの追加] ページが再度表示されます。

k) [追加 (Add)] をクリックします。

新しいリカバリ テンプレートが [テンプレート (Templates)] ページに追加されます。[テンプレート (Templates)] ページに新しいリカバリ テンプレートが表示されない場合は、[更新 (Refresh)] をクリックしてページを更新します。

ステップ 3 リカバリ テンプレートを使用して、同じリソース グループに Cisco Cloud APIC VM を展開します。

- a) [テンプレート (Templates)] ページで、追加した新しいリカバリ テンプレートをクリックします。
- b) [展開 (Deploy)] をクリックします。

[カスタムの展開 (Custom Deployment)] ページが表示されます。

c) リカバリ テンプレートに必要な情報を入力します。

• **基本** :

- [サブスクリプション (Subscription)] : [サブスクリプション \(102 ページ\)](#) の説明どおりに、Cisco Cloud APIC を最初に展開したときに使用したのと同じサブスクリプションを選択します。
- [リソース グループ (Resource Group)] : [リソース グループ \(102 ページ\)](#) で説明したように、Cisco Cloud APIC を最初に展開したときに使用したのと同じリソース グループを選択する必要があります。
- [ロケーション (Location)] : [ロケーション \(102 ページ\)](#) の説明に従って、Cisco Cloud APIC を最初に展開したときに使用したのと同じリージョンを選択します。

(注) 同じリソース グループを使用している場合、[ロケーション (Location)] オプションは使用できない場合があります。

• [設定] :

- [Vm Name] : 前に使用したのと同じVM名を入力します。 [Virtual Machine Name \(104 ページ\)](#)
- Vm Size : VMのサイズを選択します。
- [イメージ SKU (Image SKU)] : 適切なイメージ SKU を選択します。たとえば、リリース 25.0(1) の場合は、25_0_1_byol を選択します。
- [Admin Username] : このフィールドのデフォルトエントリはそのままにします。Cisco Cloud APIC が起動すると、管理者ユーザー名のログインが機能します。
- [Admin Password or Key] : 管理者パスワードを入力します。
- [管理者公開キー (Admin Public Key)] : 管理者公開キー (sshキー) を入力します。
- FabricName : 前に使用したのと同じファブリック名を入力します。 [FabricName \(ファブリック名\) \(103 ページ\)](#)
- [インフラVNETプール (Infra VNET Pool)] : 前に使用したのと同じインフラサブネットプールを入力します。 [インフラVNETプール \(104 ページ\)](#)
- [外部サブネット (External Subnet)] : [外部サブネット \(104 ページ\)](#) の説明に従って、Cisco Cloud APIC にアクセスするために以前に使用された外部ネットワークの IP アドレスとサブネットを入力します。これは、[Azure でのクラウド APIC の導入 \(37 ページ\)](#) で実行した元の展開の一部として入力した Cisco Cloud APIC のアクセスと同じ外部サブネットプールです。
- [ストレージアカウント名 (Storage Account Name)] : 前に使用したのと同じストレージアカウント名を入力します (の説明を参照) 。 [ストレージアカウント名 \(105 ページ\)](#)
- [仮想ネットワーク名 (Virtual Network Name)] : このフィールドの仮想ネットワーク名が、Cisco Cloud APIC の開発に最初に使用された仮想ネットワーク名と一致することを確認します。
- [Mgmt Nsg Name] : このフィールドの管理ネットワーク セキュリティ グループ名が、Cisco Cloud APIC の展開に最初に使用された管理ネットワーク セキュリティ グループ名と一致することを確認します。
- [Mgmt Asg Name] : このフィールドの管理アプリケーションセキュリティ グループ名が、Cisco Cloud APIC の展開に最初に使用された管理アプリケーションセキュリティ グループ名と一致することを確認します。
- サブネットプレフィックス : このフィールドのエントリは、自動的に設定されるインフラサブネットに使用する必要があるサブネットプレフィックスになります。

このフィールドのサブネットプレフィックスが、Cisco Cloud APIC の展開に最初に使用されたサブネットプレフィックスと一致することを確認します。Cisco Cloud APIC 仮想ネットワーク上のサブネット名の形式を調べることで、そのプレフィックスを確認できます。たとえば、サブネット名がサブネット **10.10.0.0_28** であることが示されている場合、このフィールドのサブネットプレフィックスは **subnet-** である必要があります。このフィールドのサブネットプレフィックスが、Cisco Cloud APIC の展開に最初に使用されたサブネットプレフィックスと一致することを確認します。Cisco Cloud APIC 仮想ネットワーク上のサブネット名の形式を調

べることで、そのプレフィックスを確認できます。たとえば、サブネット名がsubnet-10.10.0.0_28の場合、このフィールドのサブネットプレフィックスはsubnet-である必要があります。

- d) 契約書の横にあるボックスをクリックし、[購入 (Purchase)] をクリックします。

[Azure services] ウィンドウが開き、[Deployment in progress] という小さなポップアップウィンドウが表示されます。[通知 (Notifications)] アイコンをクリックして、展開の進行状況の監視を続行します。通常、展開には約5分かかります。

しばらくすると、[Deployment successful] ウィンドウが表示されます。

次のタスク

[アップグレード後の手順の実行 \(109 ページ\)](#) の手順を実行します。

アップグレード後の手順の実行

始める前に

これらの手順に進む前に、[リカバリテンプレートのダウンロードと展開 \(106 ページ\)](#) の手順を完了してください。

ステップ 1 インフラ サブスクリプションの Cisco Cloud APIC VM に貢献者ロールを付与します。

- a) Microsoft Azureポータルでの[Services]で、[Subscription]を選択します。
- b) Cisco Cloud APIC が展開されたサブスクリプションを選択します。
- c) [アクセス制御 (IAM) (Access control (IAM))] を選択します。
- d) 上部のメニューで、[追加 (Add)] [追加 (Add role role)] をクリックします。 >
- e) [Role]フィールドで、[Contributor]を選択します。
- f) [Assign access to] フィールドで、[仮想マシン (Virtual Machine)] を選択します。
- g) [サブスクリプション (Subscription)] フィールドで、Cisco Cloud APIC が展開されているサブスクリプションを選択します。
- h) [選択 (Select)] で、Cisco Cloud APIC 仮想マシンをクリックします。
- i) [保存 (Save)] をクリックします。

(注) また、ユーザーテナントを管理している場合は、Cisco Cloud APIC VMに貢献者ロールを付与します。これは、ユーザーテナントの展開に使用されるユーザサブスクリプションで行う必要があります。詳細については、[テナント、ID、およびサブスクリプションについて \(11 ページ\)](#) と [仮想マシンへのロール割り当ての追加 \(44 ページ\)](#) を参照してください。

ステップ 2 同じ暗号化パスフレーズが使用可能です。

- a) Microsoft Azureポータルでの[Services]で、[Virtual Machines]を選択します。
- b) [仮想マシン (Virtual machine)] ウィンドウで、Cisco Cloud APIC をクリックします。

この Cisco Cloud APIC の概要ページが表示されます。

- c) [パブリックIPアドレス (Public IP address)]フィールドを見つけて、IPアドレスをコピーします。
- d) 別のブラウザウィンドウで、IPアドレスを入力し、Return :

```
https://<IP_address>
```

 初めてログインすると、[クラウドAPICへようこそ (Welcome to Cloud APIC)]画面が表示されます。
- e) [初回セットアップの開始 (Begin First Time Setup)]をクリックします。
 [Let's Configure the Basics]ウィンドウが表示されます。右上隅の[X]をクリックしてこのウィンドウを終了し、同じ暗号化パスフレーズを有効にする手順に進みます。
- f) Cisco Cloud APIC GUIで、[インフラストラクチャ>システム設定 (Infrastructure System Configuration)]に移動します。
 デフォルトでは、[General]タブの下にあります。そうでない場合は、[General]タブをクリックします。
 最初のログイン後、ウェルカム画面が表示されます。[初回セットアップの開始 (Begin first time setup)]をクリックします。初回セットアップページが開き、初回セットアップページを閉じてから、パスフレーズの設定に進みます。
- g) [Global AES Encryption]領域で、[Global AES Encryption]領域の右上にある鉛筆アイコンをクリックします。
 [Global AES 暗号 Settings] ウィンドウが表示されます。
- h) [Encryption : Enabled]領域の横にあるボックスをクリックし、[Passphrase / Confirm Passphrase]フィールドに同じパスフレーズを入力してから、ウィンドウの下部にある[Save]をクリックします。 [既存設定のバックアップ \(105 ページ\)](#)

ステップ 3 リリース 25.0(1) への移行ベースのアップグレードを実行している場合は、以前にバックアップした設定をインポートする前に、Python スクリプトを実行して必要な設定をクリーンアップします。

Cisco TACに連絡し、[CSCvy42684](#)で発生した問題に対処するPythonスクリプトを入手して、必要な設定をクリーンアップします。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

ステップ 4 バックアップした設定をインポートします。 [既存設定のバックアップ \(105 ページ\)](#)

設定のバックアップ時にリモートロケーションを設定した場合は、バックアップにアクセスするためにリモートロケーションを再度作成する必要があります。

- a) Cisco Cloud APIC GUIで、[操作 (Operations)] > [Backup & Restore]に移動します。
- b) [Backup & Restore]ウィンドウで、[Backups]タブをクリックします。
- c) [Actions]スクロールダウンメニューをクリックし、[Restore Configuration]を選択します。
 [復元の設定 (Restore Configuration)]ウィンドウが表示されます。
- d) バックアップした設定を復元するために必要な情報を入力します。 [既存設定のバックアップ \(105 ページ\)](#)

次の設定を使用します。

- [復元タイプ (Restore Type)] フィールドで、[結合 (Merge)] を選択します。
- [Restore Mode] フィールドで、[Best Effort] を選択します。

このウィンドウに必要な情報を入力したら、[Restore Configuration] をクリックします。

- e) 復元プロセスが完了してから、次のステップに進みます。

[Backup & Restore] ウィンドウの [Job Status] タブをクリックして、復元プロセスのステータスを取得し、復元プロセスが成功したことを確認します。

ステップ 5 命名ポリシーを確認します。

- a) Cisco Cloud APIC GUI で、[インテント (Intent)] アイコン (🔗) をクリックし、[Cloud APIC セットアップ (Cloud APIC Setup)] を選択します。
- b) [リージョン管理 (Region Management)] エリアで、[設定の編集 (Edit Configuration)] をクリックします。

[管理するリージョン (Regions to Manage)] ウィンドウが表示されます。

- c) 移行前の選択内容がバックアップインポートで正常に転送されたことを確認し、[次へ (Next)] をクリックします。

(注) この時点では、管理対象リージョンまたは CCR の構成を変更しないでください。

- d) セットアップの最後のページに移動し、[Cloud Resource Naming Rules] 領域の情報を確認します。

クラウドリソースの命名規則が、Cisco Cloud APIC を展開するために最初に使用されたクラウドリソースの命名規則と一致することを確認します。

[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)] の横にあるボックスをクリックし、この画面の情報を確認してから [保存して続行 (Save and Continue)] をクリックします。命名ルールが確認され、承認されるまで、リソースはクラウドに展開されません。

プロセスのこの時点で、非ホームリージョンの CCR が新しい CCR イメージで自動的に展開されません。

(注) 次のステップに進む前に、Cisco Cloud APIC がすべての障害をクリアするまでしばらく待ちます。詳細については、『Cisco Cloud APIC for Azure User Guide』の「Viewing Health Details Using the Cisco Cloud APIC GUI」を参照してください。

ステップ 6 非ホームリージョンの CCR がクラウドで起動するのを待ち、すべての VGW トンネルが新しく作成された CCR で起動し、構成の調整が完了することを確認します。

さらに、CCR のアップグレードが必要な場合は、プロセスのこの時点でホームリージョンの CCR が削除され、再作成されることがあります。これらのアクションと、結果として表示される可能性のある障害は無視してください。これらのアクションは、この手順の次の手順を完了すると解消されます。

この場合、ホームリージョンの CCR が最新の CCR バージョンにアップグレードされるまで待ちます。

ステップ 7 (任意) サイト間接続があり、サイト間トラフィックの完全なドロップを回避する場合は、次のステップでホームリージョンの CCR を停止する前に、非ホームリージョンのサイト間トンネルを再構成し、Cisco Nexus Dashboard Orchestrator を介してトンネルを起動します。

この手順は、サイト間接続がない場合、またはサイト間接続があるが、トラフィックの損失を気にしない場合は必要ありません。

- a) Cisco Nexus Dashboard Orchestrator [サイト (Sites)] ビューで、[インフラの構築 (CONFIGURE INFRA)] をクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

- b) 左側のペインの [サイト (SITES)] の下で、クラウドサイトをクリックします。
- c) [サイトデータのリロード (Reload Site Data)] をクリックします。
- d) 新しい CCR が UI に追加されたことを確認します。
- e) 画面の右上にある [展開 (Deploy)] ボタンをクリックし、[IPN デバイスの展開およびダウンロード config ファイル (Deploy & Download IPN Device config files)] オプションを選択します。

このアクションは、オンプレミスの APIC サイトと Cisco Cloud API サイトの両方に設定をプッシュし、オンプレミスとクラウドサイト間のエンドツーエンドインターコネクト接続を有効にします。さらに、このオプションでは、Azure に導入された CCR とオンプレミスの IPsec 終端デバイスとの間の接続を有効にするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

(注) この手順で Cisco Cloud APIC からクラウド CCR でサイト間トンネルを削除して再作成し、オンプレミスの IPsec 終端デバイスで新しいキーをプログラムする必要がある場合は、同じパブリック IP アドレスのキーを変更します。クラウド CCR の場合は、最初にオンプレミスの IPsec 終端デバイス上の既存のキーを手動で削除し、新しいキーを追加する必要があります。オンプレミスの IPsec 終端デバイスの特定のクラウド CCR 宛先 IP アドレスに一致する IPsec 事前共有キーは 1 つだけです。

ステップ 8 ホームリージョンの CCR を展開解除します。

- a) Cisco Cloud APIC GUI で、[インテント (Intent)] アイコン (🔗) をクリックし、[cAPIC セットアップ (cAPIC Setup)] を選択します。
- b) [リージョン管理 (Region Management)] エリアで、[設定の編集 (Edit Configuration)] をクリックします。

[管理するリージョン (Regions to Manage)] ウィンドウが表示されます。

- c) ホームリージョン ([Cloud APIC Deployed] というテキストがあるリージョン) を見つけ、そのホームリージョンの [Cloud Routers] カラムのボックスを選択解除します。
- d) [Save] をクリックします。

これにより、ホームリージョンの古い CCR が削除されます。

- e) ホームリージョンの CCR VM、CCR NIC、および CCR パブリック IP アドレスがクラウドで削除されるのを待ちます。

ホームリージョンの CCR VM、CCR NIC、および CCR パブリック IP アドレスがクラウドで削除されると、ホームリージョンに CCR を再展開できます。

ステップ 9 ホームリージョンの CCR を再展開します。

この手順では、以前に構成したホームリージョンの CCR が削除され、新しいホームリージョンの CCR が再作成されます。

- a) **[戻る (Previous)]** をクリックして **[管理対象リージョン (Regions to Manage)]** 画面に戻り、ホームリージョンの **[クラウドルータ (Cloud Routers)]** 列のボックスをクリックして、ホームリージョンの CCR を再度有効にします。
- b) **[保存 (Save)]** をクリックします。

ステップ 10 (任意) サイト間接続が必要な場合は、この手順の手順を実行します。

- サイト間接続が不要な場合は、この手順の手順を実行する必要はありません。その場合は [VNet ピアリングへの移行 \(オプション\) \(114 ページ\)](#) にスキップします。
- サイト間接続が必要な場合は、次の手順を実行します。

- a) 新しいホームリージョンの CCR が表示されたら、Cisco Nexus Dashboard Orchestrator の **[サイト (Sites)]** 画面で **[インフラストラクチャの構成 (CONFIGURE INFRA)]** をクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

- b) 左側のペインの **[サイト (SITES)]** の下で、クラウドサイトをクリックします。
- c) **[サイトデータのリロード (Reload Site Data)]** をクリックします。
- d) 新しい CCR が UI に追加されたことを確認します。
- e) 画面の右上にある **[展開 (Deploy)]** ボタンをクリックし、**[IPN デバイスの展開およびダウンロード config ファイル (Deploy & Download IPN Device config files)]** オプションを選択します。
- f) ダウンロードした IPN 設定を使用して、オンプレミス CCR の IPN IPsec トンネルを再設定します。

[「Cisco Cloud APIC と ISN デバイス間の接続の有効化 \(76 ページ\)」](#) を参照してください。

(注) いかなる理由でも Cisco Cloud APIC からクラウド CCR でサイト間トンネルを削除して再作成し、オンプレミスの IPsec 終端デバイスで新しいキーをプログラムする必要がある場合は、同じパブリック IP アドレスのキーを変更します。クラウド CCR の場合は、最初にオンプレミスの IPsec 終端デバイス上の既存のキーを手動で削除し、新しいキーを追加する必要があります。オンプレミスの IPsec 終端デバイスの特定のクラウド CCR 宛先 IP アドレスに一致する IPsec 事前共有キーは 1 つだけです。

次のタスク

VNet間接続のために Azure VNet ピアリングに移行する場合は、この手順に従います。 [VNet ピアリングへの移行 \(オプション\) \(114 ページ\)](#)

VNet ピアリングへの移行（オプション）


CCR を介した従来のトンネルベースの VPN 接続を使用するのではなく、VNet 間接続のために Azure VNet ピアリングに移行する場合は、このタスクの手順に従います。VNet ピアリング機能の詳細については、『Configuring VNet Peering for Cloud APIC for Azure』ドキュメントを参照してください。



(注) VNet ピアリング モードへの移行は中断を伴う操作です。プロセス中にトラフィック損失が発生することに注意してください。

始める前に

これらの手順に進む前に、この手順を完了してください。[アップグレード後の手順の実行（109 ページ）](#)

-
- ステップ 1** Cisco Cloud APIC GUI で、[インテント (Intent)] アイコン () をクリックし、[cAPIC セットアップ (cAPIC Setup)] を選択します。
- ステップ 2** [リージョン管理 (Region Management)] エリアで、[設定の編集 (Edit Configuration)] をクリックします。
- [管理するリージョン (Regions to Manage)] ウィンドウが表示されます。
- ステップ 3** [内部ネットワークの接続性 (Connectivity for Internal Network)] 領域を見つけ、仮想ネットワーク ピアリングが使用可能であることを確認します。
- ステップ 4** [仮想ネットワークピアリング (Virtual Network Peering)] をクリックして、Azure VNet ピアリング機能を有効にします。
- これにより、Cisco Cloud APIC レベルで VNet ピアリングが可能になり、インフラ VNet 内の CCR を持つすべてのリージョンに NLB が導入されます。
- Cisco Cloud APIC レベルで VNet ピアリングを有効にした後、各ユーザークラウドコンテキストプロファイルで、**VNet ピアリングオプション** を有効にし、**VNet ゲートウェイ ルータ オプション** を無効にする必要があります。
- (注) 次の手順では、Cisco Cloud APIC GUI を使用して各クラウドコンテキストプロファイルで VNet ピアリングを有効にする方法について説明します。必要に応じて、次の手順を実行することもできます。Cisco Nexus Dashboard Orchestrator
- ステップ 5** 左側のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [クラウドコンテキスト プロファイル (Cloud Context Profiles)] に移動します。
- 既存のクラウドコンテキストプロファイルが表示されます。
- ステップ 6** [アクション (Actions)] をクリックし、[クラウドコンテキスト プロファイル) Create Cloud Context Profile] を選択します。

[クラウド コンテキスト プロファイルの作成 (Create Cloud Context Profile)] ダイアログ ボックスが表示されます。

- ステップ 7** [VNet ゲートウェイ ルータ (VNet Gateway Router)] フィールドを見つけて、[VNet Gateway Router] チェックボックスのチェックを外し (無効) します。
- ステップ 8** [VNet ペアリング (VNet Peering)] フィールドを見つけて、[VNet ペアリング] チェックボックスにチェック (有効) します。
- ステップ 9** 設定が終わったら [保存 (Save)] をクリックします。
- ステップ 10** インフラサブスクリプションとユーザテナントサブスクリプションの両方にネットワーク貢献者ロールを設定します。

たとえば、次のようなケースがあるとします。

- インフラ テナントはアクセス クレデンシアル/サービス プリンシパル **C1** でサブスクリプション **S1** を使用しています
- ユーザテナントは、アクセス クレデンシアル/サービス プリンシパル **C2** でサブスクリプション **S2** を使用しています

この状況では、ユーザ テナントと infra VNet の間でピアリングが機能するように、次を設定する必要があります。

- ハブ ツー スポーク ピアリングリンクの S2 に C1 ネットワーク 投稿者ロール権限を付与する必要があります。
 - ハブ ピアリングリンクへのスポークのアクセス許可を S1 に付与する必要があります。
- a) 表示される黄色のウィンドウで、指定された **az** コマンドをコピーします。
- ユーザテナントのネットワーク投稿者ロールを設定している場合は、[ユーザサブスクリプション用に実行するコマンド (Command to run)] のテキストをコピーします。
 - インフラテナントのネットワーク投稿者ロールを設定している場合は、[インフラサブスクリプション用に実行するコマンド (Command to run)] 領域のテキストをコピーします。
- b) Azure 管理ポータルに戻り、左側のナビゲーションバーで [登録 (Registrations)] をクリックします。
- c) クラウドシェルをオープンします。
- d) [Bash] を選択します。
- e) コピーした **az** コマンドを貼り付けます。 [10.a \(115 ページ\)](#)

ポリシーベースのアップグレード

以下のシナリオの手順を使用して、Cisco Cloud APIC ソフトウェアのポリシーベース アップグレードを実行します。

このセクションの手順を実行する前に、[ソフトウェアのアップグレードに関する注意事項と制約事項（101 ページ）](#)に記載されている情報を確認してください。

イメージのダウンロード中

ステップ 1 Cisco Cloud APIC にログインしていない場合は、それにログインします。

ステップ 2 [Navigation]メニューから、[Operations] [Firmware Management]を選択します。 >

[ファームウェア管理] ウィンドウが表示されます。

ステップ 3 [ファームウェア管理] ウィンドウの [イメージ (Images)] タブをクリックします。

ステップ 4 [Actions]をクリックし、スクロールダウンメニューから[Add Firmware Image]を選択します。

[ファームウェア イメージを追加] ポップアップが表示されます。

ステップ 5 ファームウェア イメージをローカルまたはリモート ロケーションから追加するかを決めます。

- ローカル ロケーションからファームウェア イメージを追加する場合は、[イメージの場所 (Image Location)] フィールドの [ローカル] ラジオ ボタンをクリックします。 [ファイルの選択 (Choose File)] ボタンをクリックし、インポートするファームウェア イメージがあるローカルシステムのフォルダに移動します。「[ステップ 6（117 ページ）](#)」に進みます。
- リモートロケーションからファームウェアイメージをインポートする場合は、[イメージの場所 (Image Location)] フィールドの [リモート (Remote)] オプション ボタンをクリックし、次の操作を実行します。
 - a) [プロトコル (Protocol)] フィールドで、[HTTP] または [SCP] のどちらかのオプション ボタンをクリックします。
 - b) [URL] フィールドに、イメージのダウンロード元の URL を入力します。
 - 前の手順で [HTTP] オプション ボタンを選択した場合は、ソフトウェア イメージのダウンロードに使用する http ソースを入力します。URL の例は **10.67.82.87:/home/<username>/ACI/aci-capic-dk9.25.0.2f.iso** です。「[ステップ 6（117 ページ）](#)」に進みます。
 - 前の手順で [SCP] オプション ボタンを選択した場合は、<SCP サーバ>:/<パス> の形式を使用して、ソフトウェア イメージのダウンロードに使用する Secure Copy Protocol (SCP) ソースを入力します。URL の例は**10.67.82.87:/home/<username>/ACI/aci-capic-dk9.25.0.2f.iso** です。
 - c) [Username] フィールドに、セキュア コピーのユーザー名を入力します。
 - d) [認証タイプ (Authentication Type)] フィールドで、ダウンロードの認証タイプを選択します。次のタイプを選択できます。
 - [Password]
 - SSH キー (SSH Key)

デフォルトは、「Password」です。

- e) [パスワード (Password)] を選択した場合は、[パスワード (Password)] フィールドにセキュアコピーのパスワードを入力します。「[ステップ 6 \(117 ページ\)](#)」に進みます。
- f) [SSH 公開/秘密キー ファイルを使用 (Use SSH Public/Private Key Files)] を選択した場合は、次の情報を入力します。
- [SSH キー コンテンツ (SSH Key Contents)] : SSH キー コンテンツを使用して SSH キー ファイルを作成します。SSH キー ファイルは、ダウンロード用のリモートロケーションの作成時に必要です。
 - (注) 公開キーは、転送時に生成されます。転送後、バックグラウンドで生成されたキー ファイルは削除されます。一時的なキー ファイルが、APIC の dataexport ディレクトリに保存されます。
 - [SSH キー パスフレーズ (SSH Key Passphrase)] : SSH キー パスフレーズを使用して SSH キー ファイルを作成します。SSH キー ファイルは、ダウンロード用のリモートロケーションの作成時に必要です。
 - (注) [パスフレーズ (Passphrase)] フィールドは空白にしておくことができます。

ステップ 6 [選択 (Select)] をクリックします。

Cisco Cloud APIC のファームウェア イメージがダウンロードされるのを待ちます。

ポリシーベースのアップグレードプロセスを使用したソフトウェアのアップグレード

以下のシナリオの手順を使用して、Cisco Cloud APIC ソフトウェアのポリシーベース アップグレードを実行します。

始める前に

- の手順を使用してイメージをダウンロードしました。[イメージのダウンロード中 \(116 ページ\)](#)

ステップ 1 CCR の正しいイメージをサブスクライブします。

- リリース 25.0(3) 以前のリリースについては、「**Cisco Cloud Services Router (CSR) 1000V-Bring Your Own License (BYOL)**」のイメージをサブスクライブしてください：
 - a) [Azure Marketplace](#) の検索テキスト フィールドに、*Cisco Cloud Services Router (CSR) 1000V* と入力し、表示されるオプションを選択します。

Cisco Cloud Services Router (CSR) 1000V オプションが検索候補として表示されます。
 - b) [**Cisco Cloud Services Router (CSR) 1000V**] オプションをクリックします。Microsoft Azure Marketplace の **Cisco Cloud Services Router (CSR) 1000V** ページにリダイレクトされます。

- c) [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューを開きます。
- メイン ページに [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューが表示されない場合、[プラン+価格設定 (Plans + Pricing)] タブをクリックしてください。このオプションが使用可能であれば、[ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューにアクセスします。
- d) [ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューで、[Cisco CSR 1000V Bring Your Own License] オプションを選択します。
- e) プログラマビリティを導入しますか? フィールドを特定し [開始 (Get Started)] をクリックします。
- f) [プログラマビリティ導入の設定 (Configure Programmability Deployment)] ページでサブスクリプションまでスクロールし、[ステータス (Status)] 列でサブスクリプションのステータスを [無効 (Disable)] から [有効 (Enable)] に変更します。
- g) [保存 (Save)] をクリックします。
- リリース 25.0(3) 以降では、Cisco Catalyst 8000V Edge Software-Bring Your Own License (BYOL) のイメージをサブスクライブします。
- a) Azure Marketplace の検索テキスト フィールドに、Cisco Catalyst 8000V Edge Software と入力し、表示されるオプションを選択します。
- [Cisco Catalyst 8000V Edge Software] オプションが検索候補として表示されます。
- b) [Cisco Catalyst 8000V Edge Software] オプションをクリックします。
- Microsoft Azure Marketplace の [Cisco Catalyst 8000V Edge Software] ページにリダイレクトされます。
- c) [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューを開きます。
- メイン ページに [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューが表示されない場合、[プラン+価格設定 (Plans + Pricing)] タブをクリックしてください。このオプションが使用可能であれば、[ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューにアクセスします。
- d) [ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューで、[Cisco Catalyst 8000V Edge Software-BYOL-17.7.1] オプションを選択します。
- e) プログラマビリティを導入しますか? フィールドを特定し [開始 (Get Started)] をクリックします。
- f) [プログラマビリティ導入の設定 (Configure Programmability Deployment)] ページでサブスクリプションまでスクロールし、[ステータス (Status)] 列でサブスクリプションのステータスを [無効 (Disable)] から [有効 (Enable)] に変更します。
- g) [保存 (Save)] をクリックします。

ステップ 2 リリース 5.0(1) からアップグレードする場合は、ホーム リージョンを除くすべてのリージョンから CCR を削除します。

(注) リリース 5.0(2) 以降からアップグレードする場合は、CCR を削除しないでください。その場合は [ステップ 3 \(119 ページ\)](#) に移動します。

この時点では、ホーム リージョンから CCR を削除しないでください。この時点では、ホーム リージョンの CCR を削除すると、停止が発生します。

- a) クラウド APIC GUI で、[インターネット (Intent)]アイコン (🌐) をクリックし、[cAPIC セットアップ (cAPIC Setup)]を選択します。
- b) [リージョン管理 (Region Management)]エリアで、[設定の編集 (Edit Configuration)]をクリックします。

[管理するリージョン (Regions to Manage)] ウィンドウが表示されます。

- c) [クラウド ルータ (Cloud Routers)]列でボックスが選択されているリージョンをメモします。
次の手順で[クラウドルータ (Cloud Routers)]列のボックスの選択を解除します。そのため、この手順の最後に、どの領域を再度選択する必要があるかを確認してください。
- d) ホームリージョン (テキスト **Cloud APIC Deployed** を含むリージョン) を除くすべてのリージョンの [クラウドルータ (Cloud Routers)]列で、チェックボックスをオフにします。
- e) [次へ (Next)]をクリックし、次のページに必要な情報を入力して、[保存して続行 (Save and Continue)]をクリックします。

CCR の削除プロセスには約 30 分かかる場合があります。Azure ポータルでリソースグループの仮想マシンを確認することで、CCR の削除プロセスを監視できます。

必要な CCR が完全に削除されるまで、次の手順に進まないでください。

ステップ 3 [移動 (Navigation)]メニューから、[オペレーションズ (Operations)]>[ファームウェア管理 (Firmware Management)]を選択します。

[ファームウェア管理] ウィンドウが表示されます。

ステップ 4 [アップグレードのスケジュール設定] をクリックします。

[アップグレードのスケジュール設定] ポップアップが表示されます。

ファブリックに障害があることを示すメッセージが表示された場合は、アップグレードを実行する前にこれらの障害を解決することを推奨します。詳細については、『Cisco Cloud APIC for Azure User Guide』の「Viewing Health Details Using the Cisco Cloud APIC GUI」を参照してください。

ステップ 5 [ターゲットファームウェア (Target Firmware)]フィールドで、スクロールダウンメニューからファームウェアイメージを選択します。

ステップ 6 [Upgrade Start Time]フィールドで、アップグレードを今すぐ開始するか、後で開始するかを決定します。

- 今すぐアップグレードをスケジュールする場合は、[Now]をクリックします。「[ステップ 7 \(119 ページ\)](#)」に進みます。
- 後で日付または時刻にアップグレードをスケジュールする場合は、[後で (Later)]をクリックし、スケジュールされたアップグレードの日時をポップアップカレンダーから選択します。

ステップ 7 互換性チェック機能を無効にするように特に指示されている場合を除き、[互換性チェックを無視 (Ignore Compatibility check)] フィールドでは設定をデフォルトの [オフ (off)] のままにします。

クラウド APIC 内では、システムの現在稼働中のバージョンから特定の新しいバージョンへのアップグレードパスがサポートされているか否かを確認する互換性チェック機能が存在します。[互換性チェック

を無視]設定はデフォルトでは[オフ]に設定されているため、システムは可能なアップグレードの互換性をデフォルトで自動的にチェックします。

(注) **[互換性チェックを無視]** フィールドの隣のボックスにチェック マークを入力して互換性チェック機能を無効に設定することを選択する場合、システム内でサポートされていないアップグレードを発生させるリスクを生じ、これにより使用不能な状態を引き起こす可能性があります。

ステップ 8 **[アップグレードをスケジュール (Schedule Upgrade)]** をクリックします。

[Upgrade Status]領域のメインの[Firmware Management]ウィンドウで、アップグレードの進行状況をモニタできます。

ステップ 9 リリース**5.0 (1)** からアップグレードする場合は、アップグレードが完了したら、必要な CCR を再度追加します。

(注) この手順は、**リリース 5.0 (1)** からアップグレードする場合にのみ必要です。**リリース 5.0(2)** からアップグレードする場合は、このセクションでこれ以上の手順を実行する必要はありません。

他のリージョンにCCRを再度追加する前に、ホームリージョンのCCRが安定していることを確認します。

- a) クラウド APIC GUI で、[インターネット (Intent)]アイコン (🌐) をクリックし、**[cAPIC セットアップ (cAPIC Setup)]** を選択します。
- b) [リージョン管理 (Region Management)]エリアで、**[設定の編集 (Edit Configuration)]** をクリックします。
[管理するリージョン (Regions to Manage)] ウィンドウが表示されます。
- c) CCRが含まれていたすべてのリージョンを特定し、それらの各リージョンの**[クラウドルータ (Cloud Routers)]** 列のボックスをオンにして、CCR を再度追加します。
- d) [次へ (Next)] をクリックし、次のページに必要な情報を入力して、**[保存して続行 (Save and Continue)]** をクリックします。

ステップ 10 すべてのCCR (ホームリージョンのCCRと非ホームリージョンのCCR) がリリース 17.7.1 になっていることを確認します。

すべてのCCRがリリース 17.7.1 になるまで、Cisco Cloud APIC VM の電源をオフにしないでください。

ステップ 11 リリース 5.0(1)からリリース 5.1(2)にアップグレードする場合は、CSRを介した従来のトンネルベースのVPN接続を使用するのではなく、VNet間接続のために Azure VNetピアリングに移行するかどうかを決定します。

VNetピアリング機能の詳細については、『Configuring VNet Peering for Cloud APIC for Azure』ドキュメントを参照してください。

(注) VNetピアリングモードへの移行は中断を伴う操作です。プロセス中にトラフィック損失が発生することに注意してください。

VNetピアリング機能を有効にするには、次の手順を実行します。

- a) クラウド APIC GUI で、[インターネット (Intent)] アイコン (🌐) をクリックし、[cAPIC セットアップ (cAPIC Setup)] を選択します。
- b) [リージョン管理 (Region Management)] エリアで、[設定の編集 (Edit Configuration)] をクリックします。

[管理するリージョン (Regions to Manage)] ウィンドウが表示されます。

- c) [内部ネットワークの接続性 (Connectivity for Internal Network)] 領域を見つけ、仮想ネットワーク ピアリングが使用可能であることを確認します。
 - 仮想ネットワーク ピアリングが使用可能な場合、ホーム リージョン CCR は基本 SKU から標準 SKU にすでに正常に移行されています。その場合は [11.i \(121 ページ\)](#) に移動します。
 - 仮想ネットワーク ピアリングが使用できない場合、ホーム リージョンの CCR は、更新された標準SKUではなく基本SKUに設定されたままになります。ホームリージョンのCSRを標準SKUに移行するために、[11.d \(121 ページ\)](#) に続行します。

- d) ホームリージョン (「Cloud APIC Deployed」というテキストがあるリージョン) を検索し、ホームリージョンの[Cloud Routers]カラムのボックスを選択解除します。
- e) [Save] をクリックします。

このアクションにより、ホーム リージョンの基本 SKU を持つ CCR が削除されます。

- f) [戻る (Previous)] をクリックして [管理対象リージョン (Regions to Manage)] 画面に戻り、ホームリージョンの [クラウドルータ (Cloud Routers)] 列のボックスをクリックして、ホームリージョンの CCR を再度有効にします。
- g) [保存 (Save)] をクリックします。

この操作により、CCR がホーム リージョンの標準 SKU に追加されます。

- h) [Previous] をクリックして [Regions to to Manage] 画面に戻り、[Connector for Internal Network] 領域を見つけて、仮想ネットワークピアリングが使用可能であることを確認します。
- i) [仮想ネットワークピアリング (Virtual Network Peering)] をクリックして、Azure VNet ピアリング機能を有効にします。

これにより、Cloud APIC レベルで VNet ピアリングが可能になり、インフラ VNet 内の CCR を持つすべてのリージョンに NLB が導入されます。

(注) CCR 経由の VPN 接続オプションは、VNet ピアリングを使用する代わりに、CCR と Azure VPN ゲートウェイ ルータ間のオーバーレイ IPsec トンネルを介した従来の VPN 接続を有効にするために使用されます。

クラウドAPICレベルでVNetピアリングを有効にした後、各ユーザクラウドコンテキストプロファイルで、VNetピアリングオプションを有効にし、VNetゲートウェイルータオプションを無効にする必要があります。

- j) 左側のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [クラウドコンテキスト プロファイル (Cloud Context Profiles)] に移動します。

既存のクラウドコンテキストプロファイルが表示されます。

- k) [アクション (Actions)] をクリックし、[クラウドコンテキスト プロファイル) **Create Cloud Context Profile**] を選択します。
[クラウド コンテキスト プロファイルの作成 (Create Cloud Context Profile)] ダイアログ ボックスが表示されます。
- l) [VNet ゲートウェイ ルータ (VNet Gateway Router)] フィールドを見つけて、[VNet Gateway Router] チェックボックスのチェックを外し (無効) します。
- m) [VNet ペアリング (VNet Peering)] フィールドを見つけて、[VNet ペアリング] チェックボックスにチェック (有効) します。
- n) 設定が終わったら [Save] をクリックします。

ソフトウェアのダウングレード

次の項では、Cisco Cloud APIC ソフトウェアを正常にダウングレードするために必要な情報を提供します。

ソフトウェアのダウングレードの前提条件

次に、Cisco Cloud APIC ソフトウェアをダウングレードする前に従う必要がある前提条件を示します。

- Cisco Cloud APIC が Cisco マルチサイト ACI ファブリックの一部であり、Cisco マルチサイトと連携している場合は、Cisco Nexus Dashboard Orchestrator ソフトウェアをダウングレードする前に、まず同等またはそれ以前のリリースに Cisco Cloud APIC ソフトウェアをダウングレードする必要があります。つまり、Cisco Nexus Dashboard Orchestrator ソフトウェアのリリースは、常に Cisco Cloud APIC ソフトウェアのリリース以降である必要があります。
- Cisco Nexus Dashboard Orchestrator ソフトウェアのリリース日を確認するには、ソフトウェア ダウンロード サイトの [Multi-Site Software](#) に移動し、左側のナビゲーションバーで該当するリリースを選択して、そのリリースのリリース日を確認します。
- ソフトウェアのリリース日を確認するには、ソフトウェア ダウンロード サイトの [Cloud Application Policy Infrastructure Controller](#) に移動し、左側のナビゲーションバーで該当するリリースを選択して、そのリリースのリリース日を確認します。

たとえば、リリース 5.0(2i) にダウングレードする場合は、次のようになります。

1. ソフトウェアダウンロードサイト (この場合は、25-Sep-2020) の [クラウドアプリケーションポリシーインフラストラクチャコントローラ](#) の情報を使用して、リリース 5.0(2i) のリリース日を確認し、ソフトウェア ダウンロード サイトの [ACI Multi-Site Software](#) に移動します。Cisco Nexus Dashboard Orchestrator ソフトウェアの同等またはそれ以降のリリース (この場合、マルチサイト リリース 3.0 (2k) は、2020 年 10 月 2 日にリリースされました) を検索します。

- 最初に、このドキュメントの手順に従って、Cisco Cloud APIC ソフトウェアを Cisco Cloud APIC リリース 5.0(2i) にダウングレードします。
- ソフトウェアをダウングレードしたら、Cisco Nexus Dashboard Orchestrator ソフトウェアをマルチサイト リリース 3.0 (2k) にダウングレードします。これらの手順については、『[Multi-Site Orchestrator Installation and Upgrade Guide, Release 3.1\(x\)](#)』を参照してください。

ソフトウェアのダウングレード

これらの手順では、ソフトウェアをダウングレードする方法について説明します。

この手順により、次のシナリオを想定しています。

- 以前のある時点で、リリース 5.2(1) などのソフトウェアの 1 つのバージョンを実行していて、リリース 25.0(2) などの後のリリースにアップグレードすることにしました。ただし、そのアップグレードを実行する前に、[既存設定のバックアップ \(105 ページ\)](#) で説明されているように既存の構成をバックアップし、バックアップした構成ファイルを保存しました。
- その後、ソフトウェアのアップグレードを実行し、後である時点で、以前のリリースに戻すことにしました。

これらの手順では、以前のリリースに戻す方法について説明していますが、これらのダウングレード手順を機能させるには、その以前のリリース用にバックアップした設定ファイルが必要です。

ステップ 1 [既存設定のバックアップ \(105 ページ\)](#) で説明されているように、以前のリリースからバックアップされた構成ファイルがあることを確認します。

以前のリリースからバックアップされた構成ファイルがない場合は、ソフトウェアをダウングレードするためにこれらの手順を使用しないでください。これらのダウングレード手順では、そのバックアップ設定ファイルが必要になります。

ステップ 2 Cisco Cloud APIC のリカバリ テンプレートをダウンロードします。

Cisco TAC に連絡して、リカバリ テンプレートを入手します。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

ステップ 3 Azureポータルにリカバリ テンプレートを展開します。

- Azureポータルで、[All Services]ページに移動します。

<https://portal.azure.com/#allservices>

- [General]領域で、[Templates]をクリックします。

- [テンプレート (Templates)]ページで、[追加 (Add)]をクリックします。

[テンプレートの追加] ページが表示されます。

- d) [テンプレートの追加 (Add Template)] ページに必要な情報を入力します。
- [名前 (Name)] : このテンプレートをリカバリテンプレートとして識別する一意の名前を入力します (template-512-recovery など)。
 - [説明 (Description)] : 必要に応じて、このテンプレートの説明テキストを入力します。
- e) **OK** をクリックします。
- [ARM テンプレート (ARM template)] ページが表示されます。
- f) [ARM テンプレート (ARM Template)] ページで、テンプレートに自動的に追加されるデフォルトのテキストを削除します。
- g) [ステップ 2 \(123 ページ\)](#) のリカバリ テンプレートをダウンロードした領域に移動します。
- h) テキストエディタを使用して、リカバリテンプレートを開き、テンプレートの内容をコピーします。
- i) Azureポータルウィンドウで、[ARMテンプレート (ARMTemplate)] ページに内容を貼り付けます。
- j) **OK** をクリックします。
- [テンプレートの追加] ページが再度表示されます。
- k) [追加 (Add)] をクリックします。
- 新しいリカバリ テンプレートが [テンプレート (Templates)] ページに追加されます。[テンプレート (Templates)] ページに新しいリカバリ テンプレートが表示されない場合は、[更新 (Refresh)] をクリックしてページを更新します。

ステップ 4 リカバリ テンプレートを使用して、同じリソース グループに Cisco Cloud APIC VM を展開します。

- a) [テンプレート (Templates)] ページで、追加したばかりの新しいリカバリテンプレートをクリックします。
- b) [展開 (Deploy)] をクリックします。
- [カスタムの展開 (Custom Deployment)] ページが表示されます。
- c) リカバリ テンプレートに必要な情報を入力します。
- **基本 :**
 - [サブスクリプション (Subscription)] : [サブスクリプション \(102ページ\)](#) の説明どおりに、Cisco Cloud APIC を最初に展開したときに使用したのと同じサブスクリプションを選択します。
 - [リソース グループ (Resource Group)] : [リソース グループ \(102 ページ\)](#) で説明したように、Cisco Cloud APIC を最初に展開したときに使用したのと同じリソース グループを選択する必要があります。
 - [ロケーション (Location)] : [ロケーション \(102ページ\)](#) の説明に従って、Cisco Cloud APIC を最初に展開したときに使用したのと同じリージョンを選択します。
- (注) 同じリソース グループを使用している場合、[ロケーション (Location)] オプションは使用できない場合があります。

• [設定] :

- [Vm Name] : 前に使用したのと同じVM名を入力します。 [Virtual Machine Name \(104 ページ\)](#)
- Vm Size : VMのサイズを選択します。
- イメージ SKU : 適切な画像 SKU (たとえば、5_2_1_byol) を選択します。
- [Admin Username] : このフィールドのデフォルトエントリはそのままにします。 Cisco Cloud APIC が起動すると、管理者ユーザー名のログインが機能します。
- [Admin Password or Key] : 管理者パスワードを入力します。
- [管理者公開キー (Admin Public Key)] : 管理者公開キー (sshキー) を入力します。
- FabricName : 前に使用したのと同じファブリック名を入力します。 [FabricName \(ファブリック名\) \(103 ページ\)](#)
- [インフラVNETプール (Infra VNET Pool)] : 前に使用したのと同じインフラサブネットプールを入力します。 [インフラVNETプール \(104 ページ\)](#)
- [外部サブネット (External Subnet)] : [外部サブネット \(104 ページ\)](#) の説明に従って、Cisco Cloud APIC にアクセスするために以前に使用された外部ネットワークの IP アドレスとサブネットを入力します。これは、[Azure でのクラウド APIC の導入 \(37 ページ\)](#) で実行した元の展開の一部として入力した Cisco Cloud APIC のアクセスと同じ外部サブネットプールです。
- [ストレージアカウント名 (Storage Account Name)] : 前に使用したのと同じストレージアカウント名を入力します (の説明を参照) 。 [ストレージアカウント名 \(105 ページ\)](#)
- [仮想ネットワーク名 (Virtual Network Name)] : このフィールドの仮想ネットワーク名が、Cisco Cloud APIC の展開に最初に使用された仮想ネットワーク名と一致することを確認します。
- [Mgmt Nsg Name] : このフィールドの管理ネットワーク セキュリティ グループ名が、Cisco Cloud APIC の展開に最初に使用された管理ネットワーク セキュリティ グループ名と一致することを確認します。
- [Mgmt Asg Name] : このフィールドの管理アプリケーション セキュリティ グループ名が、Cisco Cloud APIC の展開に最初に使用された管理アプリケーション セキュリティ グループ名と一致することを確認します。
- サブネットプレフィックス : このフィールドのエントリは、自動的に設定されるインフラサブネットに使用する必要があるサブネットプレフィックスになります。

このフィールドのサブネットプレフィックスが、Cisco Cloud APIC の展開に最初に使用されたサブネットプレフィックスと一致することを確認します。Cisco Cloud APIC 仮想ネットワーク上のサブネット名の形式を調べることで、そのプレフィックスを確認できます。たとえば、サブネット名が `subnet-10.10.0.0_28` と表示されている場合、このフィールドのサブネットプレフィックスは `subnet-` である必要があります。このフィールドのサブネットプレフィックスが、Cisco Cloud APIC の展開に最初に使用されたサブネットプレフィックスと一致することを確認します。Cisco Cloud APIC 仮想ネットワーク上のサブネット名の形式を調べるこ

で、そのプレフィックスを確認できます。たとえば、サブネット名がsubnet-10.10.0.0_28の場合、このフィールドのサブネットプレフィックスはsubnet-である必要があります。

- d) 契約書の横にあるボックスをクリックし、[購入 (Purchase)] をクリックします。

[Azure services] ウィンドウが開き、[Deployment in progress] という小さなポップアップウィンドウが表示されます。[通知 (Notifications)] アイコンをクリックして、展開の進行状況の監視を続行します。通常、展開には約5分かかります。

しばらくすると、[Deployment successful] ウィンドウが表示されます。

次のタスク

[ダウングレード後の手順の実行 \(126 ページ\)](#) の手順を実行します。

ダウングレード後の手順の実行

始める前に

これらの手順に進む前に、[ソフトウェアのダウングレード \(123 ページ\)](#) の手順を完了してください。

ステップ 1 インフラ サブスクリプションの Cisco Cloud APIC VM に貢献者ロールを付与します。

- a) Microsoft Azure ポータルの [Services] で、[Subscription] を選択します。
- b) Cisco Cloud APIC が展開されたサブスクリプションを選択します。
- c) [アクセス制御 (IAM) (Access control (IAM))] を選択します。
- d) 上部のメニューで、[追加 (Add)] [追加 (Add role role)] をクリックします。 >
- e) [Role] フィールドで、[Contributor] を選択します。
- f) [Assign access to] フィールドで、[仮想マシン (Virtual Machine)] を選択します。
- g) [サブスクリプション (Subscription)] フィールドで、Cisco Cloud APIC が展開されているサブスクリプションを選択します。
- h) [選択 (Select)] で、Cisco Cloud APIC 仮想マシンをクリックします。
- i) [保存 (Save)] をクリックします。

(注) また、ユーザーテナントを管理している場合は、Cisco Cloud APIC VM に貢献者ロールを付与します。これは、ユーザテナントの展開に使用されるユーザサブスクリプションで行う必要があります。詳細については、[テナント、ID、およびサブスクリプションについて \(11 ページ\)](#) と [仮想マシンへのロール割り当ての追加 \(44 ページ\)](#) を参照してください。

ステップ 2 リリース 25.0(3) から以前のリリースにダウングレードする場合は、古いシスコクラウドサービスルーター 1000v への CCR ダウングレードをトリガーします。

25.0(3) へのアップグレードの一環として、古いシスコ クラウド サービスルータ 1000v から新しい Cisco Catalyst 8000V にも移動しました。したがって、25.0(3) から以前のリリースにダウングレードするには、CCR を古いシスコ クラウド サービスルータ 1000v にダウングレードする必要があります。

そのダウングレードが完了すると、システムは CCR が Cisco Cloud APIC と互換性がなくなったことを認識します。CCR と Cisco Cloud APIC に互換性がなく、Cisco Cloud APIC 用に設定された新しいポリシーは、CCR をダウングレードするまで CCR に適用されないことを示すメッセージが表示されます。

次の2つの方法のいずれかを使用して、CCR ダウングレードのトリガープロセスを開始できます。どちらの方法でもメニュー オプションは **CCR のアップグレード** として表示されますが、実際にはこのオプションを選択することで、この状況で CCR をダウングレードしていることに注意してください。

- 最初に Cisco Cloud APIC にログインしたときに表示される画面上部のバナーで、**[CCR のアップグレード (Upgrade CCRs)]** リンクをクリックします。
- 次のように移動することで、**[ファームウェアの管理 (Firmware Management)]** ページの **[CCR]** 領域を使用します。

[オペレーション (Operations)] > **[ファームウェア管理]**

[CCR] タブをクリックし、**[CCR のアップグレード (Upgrade CCRs)]** を選択します。

ステップ 3 同じ暗号化パスフレーズが使用可能です。

- a) Microsoft Azure ポータルの **[Services]** で、**[Virtual Machines]** を選択します。
- b) **[仮想マシン (Virtual machine)]** ウィンドウで、Cisco Cloud APIC をクリックします。
この Cisco Cloud APIC の **概要** ページが表示されます。
- c) **[パブリック IP アドレス (Public IP address)]** フィールドを見つけて、IP アドレスをコピーします。
- d) 別のブラウザウィンドウで、IP アドレスを入力し、Return :
`https://<IP_address>`
初めてログインすると、**[クラウド APIC へようこそ (Welcome to Cloud APIC)]** 画面が表示されます。
- e) **[初回セットアップの開始 (Begin First Time Setup)]** をクリックします。
[Let's Configure the Basics] ウィンドウが表示されます。右上隅の **[X]** をクリックしてこのウィンドウを終了し、同じ暗号化パスフレーズを有効にする手順に進みます。
- f) Cisco Cloud APIC GUI で、**[インフラストラクチャ > システム設定 (Infrastructure System Configuration)]** に移動します。
デフォルトでは、**[General]** タブの下にあります。そうでない場合は、**[General]** タブをクリックします。
最初のログイン後、ウェルカム画面が表示されます。**[初回セットアップの開始 (Begin first time setup)]** をクリックします。初回セットアップページが開き、初回セットアップページを閉じてから、パスフレーズの設定に進みます。
- g) **[Global AES Encryption]** 領域で、**[Global AES Encryption]** 領域の右上にある鉛筆アイコンをクリックします。

[Global AES 暗号 Settings] ウィンドウが表示されます。

- h) [Encryption : **Enabled**]領域の横にあるボックスをクリックし、[Passphrase / Confirm Passphrase]フィールドに同じパスワードを入力してから、ウィンドウの下部にある[Save]をクリックします。[既存設定のバックアップ \(105 ページ\)](#)

ステップ4 バックアップした設定をインポートします。[既存設定のバックアップ \(105 ページ\)](#)

設定のバックアップ時にリモートロケーションを設定した場合は、バックアップにアクセスするためにリモートロケーションを再度作成する必要があります。

- Cisco Cloud APIC GUIで、[操作 (Operations)] > [Backup & Restore]に移動します。
- [Backup & Restore]ウィンドウで、[Backups]タブをクリックします。
- [Actions]スクロールダウンメニューをクリックし、[Restore Configuration]を選択します。

[復元の設定 (Restore Configuration)]ウィンドウが表示されます。

- バックアップした設定を復元するために必要な情報を入力します。[既存設定のバックアップ \(105 ページ\)](#)

次の設定を使用します。

- [復元タイプ (Restore Type)]フィールドで、[結合 (Merge)]を選択します。
- [Restore Mode]フィールドで、[Best Effort]を選択します。

このウィンドウに必要な情報を入力したら、[Restore Configuration]をクリックします。

- 復元プロセスが完了してから、次のステップに進みます。

[Backup & Restore]ウィンドウの[Job Status]タブをクリックして、復元プロセスのステータスを取得し、復元プロセスが成功したことを確認します。

システム リカバリの実行

システム リカバリを実行する手順は、移行ベースのアップグレードを実行する手順と同じです。これらの手順については、セクション [移行ベースのアップグレード \(101 ページ\)](#) を参照してください。

CCR のアップグレードのトリガー

次のトピックでは、CCRのアップグレードをトリガーするための情報と手順について説明します。

CCR のアップグレードのトリガー

リリース 5.2(1) より前のリリースでは、Cisco Cloud APIC のアップグレードをトリガーするたびに CCR が自動的にアップグレードされます。リリース 5.2(1)以降では、Cisco Cloud APIC の

アップグレードとは関係なく、CCR のアップグレードをトリガーし、それらの CCR のアップグレードをモニタできます。これは、管理プレーン（Cisco Cloud APIC）とデータプレーン（CCR）のアップグレードを分割できるため、トラフィック損失を削減するのに役立ちます。

リリース 5.2(1) 以降、この機能はデフォルトで有効になっています。デフォルトの前提は、Cisco Cloud APIC へのアップグレードをトリガーした後に CCR へのアップグレードをトリガーすることです。この機能を有効にすると、無効にすることはできません。

この機能を有効にすると、Cisco Cloud APIC と CCR の適切なアップグレードシーケンスは次のようになります。



(注) 次に、CCR へのアップグレードをトリガーするための全体的なプロセスを説明する上位レベルの手順を示します。具体的な手順については、[を参照してください](#)。 [Cisco Cloud APIC GUI を使用した CCR のアップグレードのトリガー（130 ページ）](#)

1. この章の手順に従って Cisco Cloud APIC をアップグレードします。
2. Cisco Cloud APIC のアップグレード手順が完了するまで待ちます。そのアップグレードが完了すると、システムは CCR が Cisco Cloud APIC と互換性がなくなったことを認識します。CCR と Cisco Cloud APIC に互換性がなく、Cisco Cloud APIC 用に構成された新しいポリシーは、CCR をアップグレードするまで CCR に適用されないことを示すメッセージが表示されます。



3. Azure ポータルで CCR の契約条件を確認し、同意します。
4. CSRアップグレードをトリガーして、Cisco Cloud APIC の互換バージョンになるようにします。

次の 2 つの方法のいずれかを使用して、CCR アップグレードのトリガープロセスを開始できます。

- 画面上部のバナーで、**[CCR のアップグレード (Upgrade CCRs)]** リンクをクリックします。
- **[ファームウェアの管理 (Firmware Management)]** ページの **[CCR]** 領域を使用します。次の順に選択：
[オペレーション (Operations)] > **[ファームウェア管理]**
[CCR] タブをクリックし、**[CCR のアップグレード (Upgrade CCRs)]** を選択します。

また、REST API を使用して CCR のアップグレードをトリガーすることもできます。手順については、[REST API を使用した CCR のアップグレードのトリガー（132 ページ）](#) を参照してください。

ガイドラインと制約事項

- Cisco Cloud APIC をアップグレードした後、CCR と Cisco Cloud APIC に互換性がないというメッセージが表示されない場合は、そのメッセージを表示するためにブラウザを更新する必要がある場合があります。
- Cisco Cloud APIC をアップグレードした後、CCR へのアップグレードをトリガーします。Cisco Cloud APIC をアップグレードする前に、CCR へのアップグレードをトリガーしないでください。
- CCR へのアップグレードをトリガーすると、停止することはできません。
- CCR へのアップグレードをトリガーした後にエラーが表示された場合は、それらのエラーを確認して解決します。これらの CCR アップグレードエラーが解決されると、CCR アップグレードが自動的に続行されます。

Cisco Cloud APIC GUI を使用した CCR のアップグレードのトリガー

このセクションでは、Cisco Cloud APIC GUI を使用した CCR へのアップグレードをトリガーする方法を示します。詳細については、[CCR のアップグレードのトリガー \(128ページ\)](#) を参照してください。

ステップ 1 CSR ソフトウェアバージョンが Cisco Cloud APIC ソフトウェアバージョンと互換性がない場合は、まず Azure ポータルで CCR の契約条件を確認し、同意します。

- リリース 25.0(3) 以前のリリースについては、**Cisco Cloud Services Router (CSR) 1000V-Bring Your Own License (BYOL)** :
 - a) [Azure Marketplace](#) の検索テキストフィールドに、*Cisco Cloud Services Router (CSR) 1000V* と入力し、表示されるオプションを選択します。
Cisco Cloud Services Router (CSR) 1000V オプションが検索候補として表示されます。
 - b) **[Cisco Cloud Services Router (CSR) 1000V]** オプションをクリックします。
Microsoft Azure Marketplace の **Cisco Cloud Services Router (CSR) 1000V** ページにリダイレクトされます。
 - c) **[ソフトウェア プランの選択 (Select a software plan)]** ドロップダウンメニューを開きます。
メイン ページに **[ソフトウェア プランの選択 (Select a software plan)]** ドロップダウンメニューが表示されない場合、**[プラン+価格設定 (Plans + Pricing)]** タブをクリックしてください。このオプションが使用可能であれば、**[ソフトウェア プランの選択 (Select a software plan)]** ドロップダウンメニューにアクセスします。
 - d) **[ソフトウェア プランの選択 (Select a software plan)]** ドロップダウンメニューで、**[Cisco CSR 1000V Bring Your Own License]** オプションを選択します。
 - e) **プログラマビリティを導入しますか？** フィールドを特定し **[開始 (Get Started)]** をクリックします。

- f) [プログラマビリティ導入の設定 (Configure Programmability Deployment)] ページでサブスクリプションまでスクロールし、[ステータス (Status)] 列でサブスクリプションのステータスを [無効 (Disable)] から [有効 (Enable)] に変更します。
- g) [保存 (Save)] をクリックします。
 - リリース 25.0 (3) 以降、Cisco Catalyst 8000V Edge ソフトウェア : Bring Your Own License (BYOL) :
 - a) Azure Marketplace の検索テキスト フィールドに、Cisco Catalyst 8000V Edge Software と入力し、表示されるオプションを選択します。
[Cisco Catalyst 8000V Edge Software] オプションが検索候補として表示されます。
 - b) [Cisco Catalyst 8000V Edge Software] オプションをクリックします。
Microsoft Azure Marketplace の [Cisco Catalyst 8000V Edge Software] ページにリダイレクトされます。
 - c) [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューを開きます。
メイン ページに [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューが表示されない場合、[プラン+価格設定 (Plans + Pricing)] タブをクリックしてください。このオプションが使用可能であれば、[ソフトウェア プランの選択 (Select a software plan)] ドロップダウンメニューにアクセスします。
 - d) [ソフトウェア プランの選択 (Select a software plan)] ドロップダウン メニューで、[Cisco Catalyst 8000V Edge Software-BYOL-17.7.1] オプションを選択します。
 - e) プログラマビリティを導入しますか? フィールドを特定し [開始 (Get Started)] をクリックします。
 - f) [プログラマビリティ導入の設定 (Configure Programmability Deployment)] ページでサブスクリプションまでスクロールし、[ステータス (Status)] 列でサブスクリプションのステータスを [無効 (Disable)] から [有効 (Enable)] に変更します。
 - g) [保存 (Save)] をクリックします。

ステップ 2 互換性のある CSR バージョンへの CCR アップグレードをトリガーするプロセスを開始します。

次の 2 つの方法のいずれかを使用して、CCR アップグレードのトリガー プロセスを開始できます。

- 画面上部のバナーで、[CCR のアップグレード (Upgrade CCRs)] リンクをクリックします。
- [ファームウェアの管理 (Firmware Management)] ページの [CCR] 領域を使用します。次の順に選択：
[オペレーション (Operations)] > [ファームウェア管理]
[CCR] タブをクリックし、[CCR のアップグレード (Upgrade CCRs)] を選択します。

[CCR のアップグレード (Upgrade CCRs)] をクリックすると、CCR をアップグレードすると CCR がリブートし、トラフィックが一時的に中断する可能性があることを示す警告が表示されます。

ステップ 3 この時点で CCR をアップグレードし、トラフィックが一時的に中断された場合は、警告メッセージで [アップグレードの確認 (Confirm Upgrade)] をクリックします。
CCR ソフトウェアのアップグレードが開始されます。CCR のアップグレードが進行中であることを示すバナーが画面の上部に表示されます。メッセージ内の [CCR アップグレード ステータスの表示 (View CCR upgrade status)] をクリックして、CCR アップグレードのステータスを表示します。

ステップ 4 CCR のアップグレード中に発生する可能性のある障害を修正します。

アップグレード中に障害が発生した場合は、次の場所に移動して障害の詳細情報を取得できます。

Operations Event Analytics Faults > >

REST API を使用した CCR のアップグレードのトリガー

このセクションでは、REST API を使用した CCR へのアップグレードをトリガーする方法を示します。詳細については、[CCR のアップグレードのトリガー \(128 ページ\)](#) を参照してください。

クラウドテンプレートで `routerUpgrade` フィールドの値を「true」に設定し、REST API を介して CCR へのアップグレードをトリガーします (`routerUpgrade = "true"`)。

```
<polUni>
<fvTenant name="infra">
  <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
    <cloudtemplateProfile name="defaultxyz" routerUsername="SomeFirstName"
routerPassword="SomePass" routerUpgrade="true">
      </cloudtemplateProfile>
      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="westus"/>
        <cloudRegionName provider="azure" region="westus2"/>
      </cloudtemplateIntNetwork>
      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="aws" region="us-west-2"/>
        <cloudtemplateVpnNetwork name="default">
          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />
          <cloudtemplateOspf area="0.0.0.1"/>
        </cloudtemplateVpnNetwork>
        <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
/>
      </cloudtemplateExtNetwork>
    </cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```



付録 **A**

SSH を介したクラウド APIC へのログイン

通常、セットアップウィザードを使用した Cisco Cloud APIC の設定 (60 ページ) で説明されているように、ブラウザを介して Cisco Cloud APIC にログインします。ただし、何らかの理由で SSH 経由で Cisco Cloud APIC にログインする必要がある場合は、前のセクションで生成した SSH キーまたは SSH パスワード認証を使用して Cisco Cloud APIC にログインする方法について説明します。

- SSH キーを使用したクラウド APIC へのログイン (133 ページ)
- SSH パスワード認証を使用したクラウド APIC へのログイン (135 ページ)

SSH キーを使用したクラウド APIC へのログイン

ステップ 1 まだログインしていない場合は、Cisco Cloud APIC インフラ テナントの Azure アカウントにログインし、Azure 管理コンソールに移動します。

<https://portal.azure.com/#home>

ステップ 2 Azure 管理ポータル 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、[仮想マシン (Virtual Machines)] リンクをクリックします。

ステップ 3 [仮想マシン (Virtual Machines)] ページでクラウド APIC システムを見つけ、[パブリック IP アドレス (Public IP address)] 列に表示されている IP アドレスを見つけます。

ステップ 4 SSH キーを使用してクラウド APIC にログインします。

- Linux システムの場合は、次を入力して Cloud APIC にログインします。

```
# ssh -i private-key-file admin@public-IP-address
```

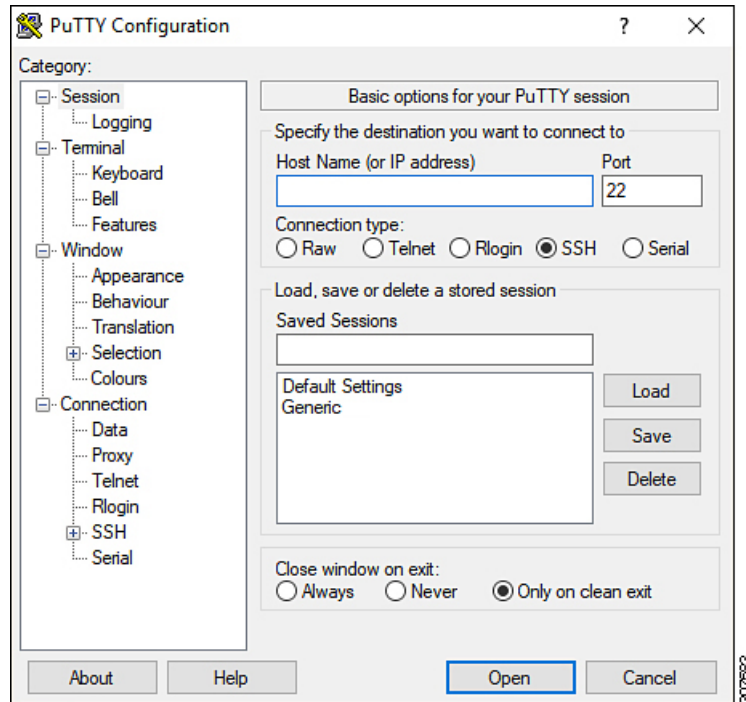
ここで、private-key-file は作成した秘密キーファイルです。Linux または MacOS での SSH キーペアの生成 (36 ページ)

次に例を示します。

```
# ssh -i azure_key admin@192.0.2.1
```

- Windows システムの場合、PuTTY を使用して Cloud APIC にログインします。

1. Windowsの[スタート]メニューの[すべてのプログラム] [PuTTY PuTTY]に移動して、PuTTY設定プログラムを実行します。 > > > >
2. 左側のナビゲーションバーで[セッション (Session)]をクリックし、クラウドAPICのパブリックIPアドレスを入力します。



3. 左側のナビゲーションバーで、[Connection SSH Auth]をクリックします。 > >
4. [Authentication parameters]領域で、[Private key file for authentication]フィールドを見つけ、[Browse ...]ボタンをクリックします。
5. で作成した秘密キーファイルに移動し、[Open]をクリックします。 [Windows での SSH キー ペアの生成 \(33 ページ\)](#)
6. PuTTYのメインウィンドウで[開く (Open)]をクリックして、クラウドAPICにログインします。ログインプロンプトが表示されます。
7. クラウド APIC に admin としてログインします。

SSHパスワード認証を使用したクラウドAPICへのログイン

公開キーを使用するSSHとは異なり、SSHパスワード認証はデフォルトで無効になっています。ユーザ名とパスワードを使用してクラウドAPICにSSH接続できるように、次の手順を使用してSSHパスワード認証を有効にします。

-
- ステップ 1** 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://192.0.2.1`です。
- ステップ 2** Cloud APICのログインページに次の情報を入力します。
- [Username] : 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 (Domain)] : [ドメイン (Domain)]フィールドが表示される場合は、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 3** ページの下部にある [ログイン] をクリックします。
- ステップ 4** [Infrastructure System Configuration]に移動し、[System Configuration]ページの[Management Access]タブをクリックします。 >
- ステップ 5** SSH設定を編集するには、画面の右上隅にある鉛筆アイコンをクリックします。
- SSH用の設定ページが表示されます。
- ステップ 6** [パスワード 認証ステータス (Password Authentication State) フィールドで、[有効 (Enabled)] を選択します。

SSH Settings

Settings

Admin State
 Enabled

Password Authentication State
 Enabled

Port
22

SSH Ciphers
 aes128-ctr aes192-ctr aes256-ctr

SSH MACs
 hmac-sha1 hmac-sha2-256 hmac-sha2-512

Cancel Save

ステップ7 **[Save]** をクリックします。

これで、公開キーファイルと秘密キーファイルにアクセスしなくても、クラウドAPICにSSH接続できます。

```
# ssh admin@192.0.2.1
```

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。

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。