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

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 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 （4 ページ）

- CCR のアップグレードのトリガー （32 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 （4 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 （32 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 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、の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 （5 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 （5 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 （32 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 （19 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 （5 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 （32 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 （5 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 （32 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

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 （8 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=ACI-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=0X7EEFFFFFFFFF--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]の行を見つけ、[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 （6 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 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 （5 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]フィールドにパスフレーズを入力して、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フレーズ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 （9 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 （10 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 （6 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も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 （6 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ものと同じリソース 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 （6 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 （8 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。
- Fabric Name：前に使用したものと同じファブリック名を入力します。Fabric Name（ファブリック名） （7 ページ）
- [インフラVNETプール（Infra VNET Pool）]：前に使用したも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 （8 ページ）
- **[外部サブネット（External Subnet）]**：外部サブネット （8 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 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）]：前に使用したも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 （9 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 （13 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 （10 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と仮想マシンへのロール割り当ての追加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 （9 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 （9 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 （9 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す。

（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） （18 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」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、の手順に従います。VNet ピアリングへの移行（オプション） （18 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、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 （13 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）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 クレデンシャル/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 クレデンシャル/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 （19 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 （5 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 （21 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 （21 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 （21 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 （20 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 （23 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（23 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 （25 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 （25 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）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。

2. 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。
3. 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。

これの手順により、次のシナリオを想定しています。

1. 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 （9 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。
2. 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 （9 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。

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。

- **[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 （27 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 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 （6 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も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 （6 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ものと同じリソース 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 （6 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 （8 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。
  - Fabric Name：前に使用したものと同じファブリック名を入力します。Fabric Name（ファブリック名） （7 ページ）
  - [インフラVNETプール（Infra VNET Pool）]：前に使用したも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 （8 ページ）
  - **[外部サブネット（External Subnet）]**：外部サブネット （8 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 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）]：前に使用したも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 （9 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 **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

ダウングレード後の手順の実行 （30 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 （27 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と 仮想マシンへのロール割り当ての追加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 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 （9 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 （9 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 （9 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。

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 （5 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

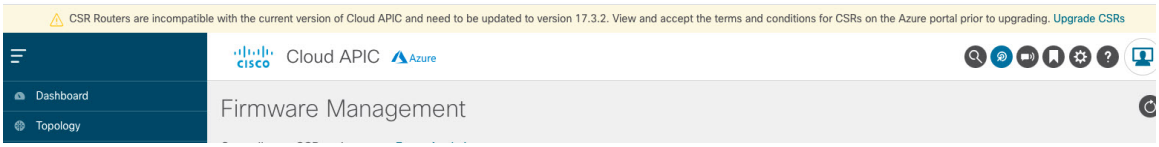
アップグレードとは関係なく、CCR のアップグレードをトリガーし、それらの CCR のアップグレードをモニタできます。これは、管理プレーン（Cisco Cloud APIC）とデータプレーン（CCR）のアップグレードを分割できるため、トラフィック損失を削減するのに役立ちます。

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 （34 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 （36 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 （32 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 （32 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>
```