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

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重要な注意事項を次に示します。Cisco Cloud APIC

- リリース 5.0（x）から以前のリリースにダウングレードすると、CSR が下位のリリースにダウングレードされるため、CSR で一部のトンネルが「ダウン」状態になることがあります。これは、AWS アカウントの古い VPN リソースがクリーンアップされなかったために発生する可能性があります。

  この問題を修正するには、古い VPN 接続を手動でクリーンアップします。

- に記載されているように、リリース 5.0（x）以降では、導入でサポートされるインスタンスタイプが変更されています。AWS パブリック クラウドの要件Cisco Cloud APIC

  - リリース 5.0(x) より前のリリースでは、Cisco Cloud APIC は M4.2xlarge インスタンスを使用して展開されます。

  - リリース 5.0(x) 以降では、Cisco Cloud APIC は M5.2xlarge インスタンスを使用して展開されます。

  4.2（x）リリースからリリース 5.0（x）以降にアップグレードする場合、ポリシーベースのアップグレードはサポートされません。これは、ポリシーベースのアップグレードではインスタンスタイプを変更できないためです。代わりに、これらのアップグレードでは、に示す移行手順を使用してアップグレードする必要があります。移行ベースのアップグレード （3 ページ）

- 4.2（x）リリースからリリース5.0（x）以降にアップグレードする場合、atomic での replace オプションを使用した設定のインポートはサポートされません。手順のこの時点で、**[復元設定（Restore Configuration）]**領域で次のように選択します。
  - **[復元タイプ（Restore Type）]** フィールドで、**[結合（Merge）]** を選択します。
  - **[復元モード（Restore Mode）]** フィールドで、**[ベスト エフォート（Best Effort）]** を選択します。

  この制限は、4.2（x）リリースからリリース 5.0（x）以降へのアップグレードにのみ適用されます。リリース5.0（x）から以降のリリースにアップグレードする場合、これらの制限は適用されません。

ソフトウェアのアップグレード

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

- 4.2（x）リリースからリリース 5.0（x）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 （3 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 （13 ページ）

- リリース 5.0(1) からリリース 5.0(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 （9 ページ） にアクセスしてください。

  注 リリース 5.0(1) からリリース 5.0(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、に記載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(1) からリリース 5.0(2) にアップグレードできます。移行ベースのアップグレード （3 ページ）

CSR 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、クラウドサービスルータ（CSR）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 CSR 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、CSR のアップグレードをトリガーし、それらの CSR 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（CSR）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、「クラウド サービス ルータのアップグレードのトリガー （13 ページ）」を参照してください。

移行ベースのアップグレード

次の項では、トラフィック フローを失わずに 4.2(x) リリースからリリース5.0(x) 以降にアップグレードできる移行手順について説明します。

移行手順を使用したクラウドAPICソフトウェアのアップグレード

この項では、の4.2（x）リリースからリリース5.0（x）以降にアップグレードする場合に使用する移行手順を示します。Cisco Cloud APICこの移行によるトラフィックへの影響はありません。

ステップ 1 暗号化パスフレーズ制御が有効になっていない場合は、有効にします。

a) クラウドAPIC GUI で、**[インフラストラクチャシステム設定（Infrastructure System Configuration）]**

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

b) 暗号化されたパスフレーズ制御がすでに有効になっているかどうかを確認します。

- [Global AES Encryption]領域で、[Encryption]フィールドと[Key Configured]フィールドの下に[Yes]と表示されている場合は、暗号化されたパスフレーズ制御がすでに有効になっています。ステップ 2 （3 ページ） に進みます。
- [Encryption]フィールドと[Key Configured]フィールドの下に[Yes]と表示されない場合は、次の手順を実行します。

1. [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。

2. [Encryption：Enabled]エリア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。

ステップ 2 既存の Cloud APIC 設定をバックアップします。

クラウドAPICの設定をバックアップするには、さまざまな方法があります。詳細については、『Cloud APIC for AWS Users Guide』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/products-installation-and-configuration-guides-list.html リモートバックアップを使用する場合は、最初にリモートロケーションを追加する必要があることに注意してください。

ステップ 3 AWS infraアカウントからCloud APIC EC2インスタンスを終了します。

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

https://signin.aws.amazon.com/

https://console.aws.amazon.com/

b) AWS 管理コンソールの EC2 ダッシュボードの**インスタンス**に移動します。

c) クラウドAPICインスタンスを見つけます。

クラウドAPICのインスタンスタイプとして**m4.2xlarge**が表示されます。これは5.0(1)より前のリリースでは正しいインスタンスタイプです。

d) Cloud APICインスタンスの横にあるチェックボックスをオンにして選択し、[Actions Instance State Terminate]をクリックします。

[Terminate Instances]ポップアップウィンドウで、[Yes、Terminate]を選択してこのインスタンスを終了します。

[Instances]ウィンドウが再表示され、クラウドAPICインスタンスの[Instance State]行のステータスが「shutting-down」に変わります。ここでCloud APICインスタンスを終了しても、Cloud APICのトラフィックはドロップされません。

ステップ 4 AWS Marketplace の Cloud APIC ページに移動します。

http://cs.co/capic-aws

ステップ 5 **[引き続きサブスクライブする（Continue to Subscribe）]** をクリックして登録します。

ステップ 6 [Subscribe to this software]ページで、[Continue to Configuration]ボタンをクリックします。

[このソフトウェアを設定 (Configure this software)] ページが表示されます。

ステップ 7 以下のパラメータを選択します。

- **[デリバリー方法（Delivery Method）:]** Cisco Cloud APIC クラウド形成テンプレート (デフォルトで選択)
- ソフトウェアバージョン：Cloud APICソフトウェアの適切なバージョンを選択します（例：5.0.1k）。
- **[リージョン (Region):]** クラウド APIC が展開されるリージョン

ステップ 8 **[続行して起動 (Continue to Launch)]** ボタンをクリックします。

[**このソフトウェアの起動 (Launch this software**)] ページが表示され、設定の概要が表示され、クラウド形成テンプレートを起動できます。

ステップ 9 **[アクションの選択（Choose Action）]** フィールドで、**[CloudFormation の起動（Launch CloudFormation）]** を選択し、**[起動（Launch）]** をクリックすると、すでに正しい Amazon S3 テンプレート URL が入力さ

れている適切なリージョン内の [CloudFormation サービス] にダイレクトに移動します。**[テンプレートの指定（Specify Details）]** ページが、**[スタックの作成（Create stack）]** ページ内に表示されます。

ステップ 10 [テンプレートの指定（Specify template）]ページで、次の選択を行います。

- 前提条件-[テンプレートの準備（Prepare template）]フィールド：デフォルトの[テンプレートの準備（Template is ready）]オプションを選択したままにします。
- テンプレート領域の指定：
  - [テンプレートソース（Template source）]フィールドで、デフォルトのAmazon S3 URLオプションを選択したままにします。
  - [Amazon S3 URL]フィールドで、自動的に生成されたエントリをそのままにします。
  - [デザイナーで表示（View in Designer）]をクリックします。

ステップ 11 画面の下半分のtemplate1領域：

- [**テンプレート言語**の選択]を[**JSON**]のままにします。
- 1行目のテキスト文字列の先頭にカーソルを置き、Shiftキーを押しながらウィンドウの一番下までスクロールして、ウィンドウ内のテキスト文字列全体を選択し、このウィンドウ内のすべてのテキストをコピーします（Ctrl + Cを押すか、右クリックして **[コピー（Copy）]** を選択します）。

ステップ 12 ローカルコンピュータで、適切なフォルダに移動し、一意の名前を付けてテキストファイルを作成し、コピーしたテキスト文字列をテキストファイルに貼り付けます。

これはリリース5.0（1）のCloud APIC CFTで、M5.2xlargeインスタンスタイプがあります。

ステップ 13 テキストファイルを保存してテキストエディタを終了します。

ステップ 14 リリース5.0（1）のCloud APIC CFTをAWSにアップロードします。

a) AWS CloudFormation コンソールにログインします。

https://console.aws.amazon.com/cloudformation

b) AWS CloudFormationダッシュボードで、既存のCloud APICスタックをクリックし、[**Update**]をクリックします。

c) **Update Stack**ウィザードの **[Prepare template]** 画面で、**[Replace current template]** を選択します。

[テンプレート領域の指定（Specify template area）] が表示されます。

d) **Update Stack**ウィザードの[**Specify template**]領域で、**[Upload a template file]** を選択します。

[テンプレート ファイルのアップロード（Upload a template file）] のオプションが表示されます。

e) [Upload a template file]オプションの下にある[Choose file]をクリックし、リリース5.0（1）用のCloud APIC CFTを作成した領域に移動します。

f) リリース5.0（1）のCloud APIC CFTを選択し、[**Next**]をクリックします。

g) [**スタックの詳細の指定**（Specify stack details）]画面で、画面下部の[**その他のパラメータ**（Other parameters）]領域に表示されるインスタンスタイプが**m5.2xlarge**に正しく設定されていることを確認し、[次へ（**Next**）]をクリックします。

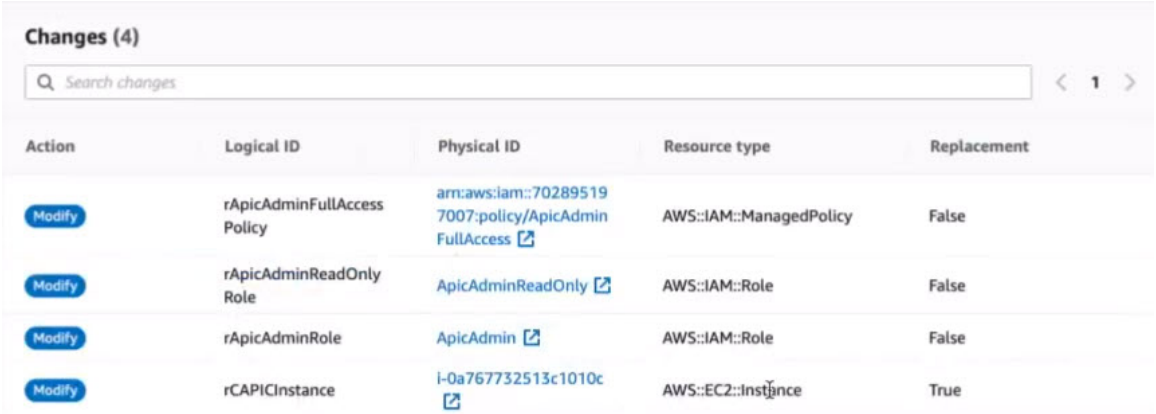
この手順では、インスタンスタイプを**m4.2xlarge**に変更しないでください。

h) **[スタック オプションの設定（Configure stack options）]**画面で、**[次へ（Next）]**をクリックします。

i) [**Review**]画面で、[**Update stack**]をクリックします。

この時点で、次のアクションが実行されます。

- AWS infraは、更新される3つのIAMリソースを検出します（[Replacement]列に[False]と表示されます）。
- AWS infraは、置き換えられるEC2インスタンスを1つ検出します（[Replacement]列に[True]と表示されます）。



これにより、以前と同じパブリックIPアドレスを使用して、リリース5.0（1）イメージの新しいCloud APICインスタンスが起動します。AWS Management ConsoleのEC2ダッシュボードで[インスタンス（Instances）]に戻ることで、新しいクラウドAPICインスタンスの起動の進行状況を確認できます。

ステップ 15 **インスタンスの状態**が[**実行**中（Running）]に変化した場合は、以前に行ったようにクラウドAPICにログインできます。

クラウドAPICは、この時点で設定なしで起動します。

（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。ログインするためにページを更新する必要がある場合もあります。

ステップ 16 同じ暗号化パスフレーズが使用可能です。

a) クラウド 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。

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。ステップ 1 （3 ページ）

ステップ 17 リリース5.2（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 18 バックアップした設定をインポートします。ステップ 2 （3 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) クラウドAPIC GUIで、[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。ステップ 2 （3 ページ）

4.2（x）リリースからリリース5.0（x）以降にアップグレードする場合は、この特定のバックアップの復元に、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。[バックアップと復元（Backup & Restore）]ウィンドウの[ジョブステータス（Job Status）]タブをクリックして、バックアップ復元のステータスを取得します。

ステップ 19 CapicTenantRole更新を実行して、すべての信頼できるテナントのセットを変更します。

a) テナントロールCFTを見つけます。

テナントロール CFT は、Cisco Cloud APIC インフラ テナントの AWS アカウントの S3 バケットにあります。S3 バケットの名前は「capic-common-[capicAccountId]-data」で、テナント ロールの CFT オブジェクトはそのバケット内の tenant-cft.json です。CapicAccountId は、Cisco Cloud APIC インフラ テナントの AWS アカウント番号です。これは、クラウド APIC が展開されているアカウントです。

b) テナントロールCFTリンクをクリックします。

このテナントロールCFTの[**概要**（Overview）]ページが表示されます。

c) [**Overview**]ページのtenant-cft.jsonエントリの横にあるボックスをクリックします。

このJSON形式のテナントロールCFTのスライドインペインが表示されます。

d) **[ダウンロード]** をクリックしてテナント ロール CFT をコンピュータ上の場所にダウンロードします。

セキュリティ上の理由から、AWS でのこの S3 バケットへのパブリック アクセスは許可されていないため、このファイルをダウンロードしてテナント アカウントで使用する必要があります。

e) AWSで、信頼できるテナントのユーザアカウントに移動し、[**CloudFormation**]をクリックします。

f) AWS CloudFormationダッシュボードで、信頼できるテナントスタックを見つけ、その信頼できるテナントのスタック名をクリックします。

この特定のスタックのスタックプロパティページが表示されます。

g) **[Change set]** タブをクリックします。

h) [Change set]領域で、[Create change set]をクリックします。

i) このスタックの[Create change set]ウィンドウで、[Replace current template]をクリックします。

j) **[テンプレートの指定（Specify template）]** 領域で、**[テンプレート ファイルにアップロード（Upload a Template File）]** の横にある円をクリックし、**[ファイルの選択（Choose File）]** ボタンをクリックします。

k) テナントロールCFTをダウンロードしたコンピュータ上の場所に移動し、そのテンプレートファイルを選択します。

l) このスタックの[Change set set]ウィンドウで[**Next**]をクリックします。

[Create Change Set]ポップアップが表示されます。

m) [Create Change Set]ポップアップウィンドウで[Create Change Set]をクリックします。

ステータスは、しばらくの間、**CREATE_PENDING**と表示され、その後、**CREATE_COMPLETE**に変わります。

n) 信頼できるテナントごとにこれらの手順を繰り返します。

信頼できる各テナントで、このtenant-cft.jsonファイルを使用して変更セットを作成し、その変更セットを実行します。

ステップ 20 クラウドAPIC GUIで、移行前にクラウドAPICに対して行ったすべての設定が存在することを確認します。

5.2（1）より前のリリースでは、CSRも16.xバージョンから17.xバージョンに自動的にアップグレードされます。これを確認するには、AWS Management ConsoleのEC2ダッシュボードで[インスタンス（Instances）]に移動し、CSRインスタンスを見つけて、それらもアップグレードされていることを確認します。

リリース5.2（1）以降では、のアップグレード時にCSRが自動的にアップグレードされないため、のアップグレードが完了した後にCSRアップグレードを個別にトリガーする必要があります。Cisco Cloud APICCisco Cloud APIC詳細については、「クラウド サービス ルータのアップグレードのトリガー （13 ページ）」を参照してください。

ポリシーベースのアップグレード

リリース5.0(1) からリリース 5.0(2) にアップグレードする場合は、次の項の手順を使用して、Cisco Cloud APIC ソフトウェアのポリシーベースのアップグレードを実行します。

イメージのダウンロード中

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

ステップ 2 **[移動]** メニューから、**[オペレーションズ]** > **[ファームウェア管理]**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 **[アクション（Actions）]** をクリックし、スクロールダウン メニューから **[ファームウェア イメージを追加（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 （10 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-apic-dk9.1.0.2j.iso`** です。ステップ 6 （10 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-apic-dk9.1.0.2j.iso`** です。

c) **[Username]** フィールドに、セキュア コピーのユーザ名を入力します。

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 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 （10 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 ファイルは、Cisco Cloud 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

リリース 5.0(1) からリリース 5.0(2) にアップグレードする場合は、次の項の手順を使用して、ソフトウェアのポリシーベースのアップグレードを実行します。Cisco Cloud APIC

始める前に

- イメージのダウンロード中 （9 ページ） の手順を使用してイメージをダウンロードしました。

ステップ 1 GUI で、[移動（Navigation）] メニューから [ファームウェア管理のオペレーション（Operations Firmware Management）] を選択します。Cloud APIC

[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 2 **[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 AWS 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 3 **[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 4 **[開始時間のアップグレード（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、**[今すぐ（Now）]** をクリックします。ステップ 5（11 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付と時刻をポップアップカレンダーから選択します。

ステップ 5 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 6 **[アップグレードのスケジュール設定]** 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。

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

始める前に

5.0（2）から 5.0（2）より前のリリースにダウングレードする場合は、次の前提条件が適用されます。

- Cisco Cloud APIC が常にリリース 5.0（2）で実行されている場合（5.0（2）より前のリリースからリリース 5.0（2）にアップグレードしたことがない場合）、リリース 5.0（2）より前のリリースにダウングレードすることはできません。）。Cisco Cloud APIC が以前のリリースで実行されなかった 5.0（2）より前のリリースへのダウングレードはサポートされていません。
- Cisco Cloud APIC をリリース 5.0（2）にアップグレードし、その後に特定のリリース 5.0（2）固有の設定を完了し、リリース 5.0（2）より前のリリースにダウングレードする場合は、5.0（2）ダウングレード前の固有の設定を削除する必要があります。

ステップ 1 必要に応じて、ダウングレードする前に 5.0（2）固有の設定を削除します。

ステップ 2 イメージのダウンロード中 （9 ページ） で説明している手順を使用して、ダウングレードのイメージをダウンロードします。

ステップ 3 イメージが完全にダウンロードされたら、**[Navigation]** メニューから **[Operations > Firmware Management]**

[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存在することを示すメッセージが表示された場合は、ダウン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 AWS 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 **[開始時間のアップグレード（Upgrade Start Time）]** フィールドで、ダウン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。

- ダウングレードを今すぐスケジュールする場合は、**[今すぐ（Now）]** をクリックします。ステップ 7（12 ページ） に進みます。
- ダウングレードを後の日付または時刻に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ダウン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ダウングレード 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、システムは可能なダウン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ダウン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 **[アップグレードのスケジュール設定]** をクリックします。

[ステータスのアップグレード（Upgrade Status）] 領域のメインの **[ファームウェア管理（Firmware Management）]** ウィンドウで、ダウングレードの進行状況をモニタできます。

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 （3 ページ） を参照してください。

クラウド サービス ルータのアップグレードのトリガー

次のトピックでは、クラウド サービス ルータ（CSR）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。

クラウド サービス ルータのアップグレードのトリガー

リリース 5.2(1) より前は、Cisco Cloud APIC のアップグレードをトリガーするたびに、クラウド サービス ルータ（CSR）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、CSR のアップグレードをトリガーし、Cisco Cloud APIC アップグレードとは無関係に CSR 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（CSR）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減らすのに役立ちます。

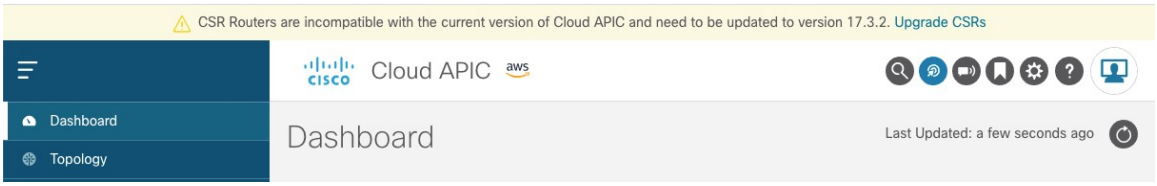
リリース 5.2(1) 以降、この機能はデフォルトで有効になっています。デフォルトの前提は、Cisco Cloud APIC へのアップグレードをトリガーした後に CSR へのアップグレードをトリガーすることです。この機能を有効にすると、無効にすることはできません。

この機能を有効にすると、Cisco Cloud APIC と CSR 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、CSR 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、GUI を使用したクラウドサービスルータのアップグレードのトリガーCisco Cloud APIC （15 ページ） を参照してください。

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 CSR が Cisco Cloud APIC と互換性がなくなったことを認識します。その後、CSR と Cisco Cloud APIC に互換性がなく、Cisco Cloud APIC に設定された新しいポ

リシーは CSR をアップグレードするまで CSR 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. AWS ポータルで CSR の利用規約を確認し、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、CSR 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、**[CSR のアップグレード（Upgrade CSRs）]** リンクをクリックします。
   - [ファームウェア管理（Firmware Management）] ページの [CSRs] 領域を使用します。次のとおりに移動します。

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

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

また、REST API を使用して CSR 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 を使用したクラウドサービスルータのアップグレードのトリガー（15 ページ） を参照してください。

注意事項と制約事項

- Cisco Cloud APIC をアップグレードした後、CSR と Cisco Cloud APIC に互換性がないことを示す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ります。
- Cisco Cloud APIC をアップグレードした後、CSR 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、CSR へのアップグレードをトリガーしないでください。
- CSR 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。
- CSR 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 CSR アップグレード エラーが解決されると、CSR アップグレードが自動的に続行されます。

GUI を使用したクラウド サービス ルータのアップグレードのトリガー Cisco Cloud APIC

ここでは、GUI を使用してクラウド サービス ルータ（CSR）へのアップグレードをトリガーする方法について説明します。Cisco Cloud APIC詳細については、「クラウド サービス ルータのアップグレードのトリガー （13 ページ）」を参照してください。

ステップ 1 互換性のある CSR バージョンへの CSR 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、CSR 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、**[CSR のアップグレード（Upgrade CSRs）]** リンクをクリックします。
- **[ファームウェア管理（Firmware Management）]** ページの **[CSRs]** 領域を使用します。次のとおりに移動します。

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

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

[CSR のアップグレード（Upgrade CSRs）]をクリックすると、CSR をアップグレードすると CSR 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 2 この時点で CSR 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 [Confirm Upgrade] をクリックします。
CSR ソフトウェアのアップグレードが開始されます。CSR 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 [CSR アップグレード ステータス（View CSR upgrade status）] をクリックして、CSR アップグレードのステータスを表示します。

ステップ 3 CSR 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。

[オペレーション（Operations)] > **[イベント 分析（ Event Analytics）]** > **[失敗（Faults）]**

REST API を使用したクラウド サービス ルータのアップグレードのトリガー

ここでは、REST API を使用してクラウド サービス ルータ（CSR）へのアップグレードをトリガーする方法について説明します。詳細については、「クラウド サービス ルータのアップグレードのトリガー （13 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 CSR 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="aws" region="us-west-1"/>
            <cloudRegionName provider="aws" region="us-west-2"/>
        </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>
```