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

- Cisco Cloud APIC は、次のアップグレード パスのポリシーベースのアップグレードをサポートしています。
  - リリース 5.2(1) から 25.0(2)
  - リリース 25.0(1) ～ 25.0(2)
- 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 （8 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。
  - [Restore Mode]フィールドで、[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。

- アップグレードプロセスには、リリース 5.2(1g) からそれ以降のリリースへのアップグレードが失敗するという問題があります。

  この問題を回避するには、**[互換性チェックを無視（Ignore Compatibility Check）]** オプションを有効にします。

  1. **[アップグレードのスケジュール（Ignore Compatibility Check）]** ウィンドウの **[互換性チェックを無視（Schedule Upgrade）]** 手順に到達するまで、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 （6 ページ） に示されている通常のアップグレード手順に従います。
  2. **[互換性チェックを無視（Ignore Compatibility Check）]** 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、**[互換性チェックを無視（Ignore Compatibility Check）]** オプションを有効にします。

     [互換性チェックを無視（Ignore Compatibility Check）] オプションを有効にすると、この特定のアップグレードを正常に続行できます。
  3. 5.2(1g) 以降のリリースへのアップグレードを完了します。
  4. 5.2(1g) 以降のリリースへのアップグレードが完了したら、**[アップグレードのスケジュール（Schedule Upgrade）]** ウィンドウに戻り、**[互換性チェックを無視する（Ignore Compatibility Check）]** フィールドの横にあるボックスのチェック マークを外します。

     これにより、このフィールドのデフォルト設定である **[互換性チェックを無視する（Ignore Compatibility Check）]** オプションが無効になります。

- 前の箇条書きで説明した問題のため、リリース 5.2(1) より前のリリースから 5.2(1) リリースにアップグレードする場合は、リリース 5.2(1 **h**) に直接アップグレードすることをお勧めします（リリース 5.2(1 **g**) ではない）。

ソフトウェアのアップグレード

次のセクションでは、ポリシーベースのアップグレードまたは移行ベースのアップグレードを使用した 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 は、次のアップグレードパスのポリシーベースのアップグレードをサポートします。

- リリース 5.2(1) から 25.0(2)
- リリース 25.0(1) ～ 25.0(2)

（注） 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 （8 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アップグレードできます。

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) より前は、Cisco Cloud APIC のアップグレードをトリガするたびに CSR が自動的にアップグレードされました。
- 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（）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。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 （25 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

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。

既存設定のバックアップ

次のポリシーベースのアップグレードを実行する前に、既存の設定をバックアップすることをお勧めします。

- リリース 5.2(1) からリリース 25.0(1) または 25.0(2) へのアップグレード

- リリース 25.0(1) からリリース 25.0(2) へのアップグレード

ソフトウェアのダウングレード （13 ページ） で提供されている手順を使用して、その後のある時点で以前のリリースにダウングレードすることにした場合、ダウングレードを正常に実行するためにバックアップされた設定ファイルが必要になります。

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 スタックの展開中に設定したインフラ VPC プールを書き留めます。

インフラ VPC 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、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。

a) インフラ テナントの AWS アカウントに移動します。

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

b) 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[CloudFormation]** リンクをクリックします。

[CloudFormation] 画面が表示されます。

c) 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ます。

Cloud APIC スタックの **[スタックの詳細（Stack details）]** ウィンドウが表示されます。

d) **[スタックの詳細（Stack details）]** ウィンドウの **[パラメータ（Parameters）]** タブをクリックします。

e) **[パラメータ（Parameters）]** テーブルで **pInfraVPCPool** 行を見つけます。

pInfraVPCPool 行のエントリを書き留めます。これは、スタックの展開中に設定したインフラ VPC プールです。

ステップ 3 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。

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

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 [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 （6 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 （6 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 （6 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

以下のセクションの手順を使用して、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

イメージのダウンロード中 （5 ページ） で説明された手順を使用して、イメージをダウンロードしたことを確認します。

ステップ 1 ポリシーベースのアップグレードを実行する前に、既存の設定をバックアップしてください。

ポリシーベース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 （3 ページ） で提供されている情報を使用して、既存のリリースの設定をバックアップすることをお勧めします。

ポリシーベースのアップグレードが完了した後、ソフトウェアのダウングレード （13 ページ） で説明されている手順を使用して、ある時点で以前のリリースにダウングレードする場合は、ダウングレードを正常に実行するために、以前のリリースからバックアップされた設定ファイルが必要になります。

ステップ 2 **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。
conref="../../../../../../../commoncollectionfiles/g_common_names_and_phrases.xml#ditaVar/Cloud_APIC_ShortName"

[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 **[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 4 **[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 5 [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 6 （7 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 6 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 7 **[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。

移行ベースのアップグレード

次のセクションは、トラフィック フローがなくなることなくアップグレードが可能な移行ベース アップグレード手順を提供します。

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

このセクションでは、Cisco Cloud APIC の移行ベースのアップグレード手順について説明します。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）]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) 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 （8 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]が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]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。

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**：クラウド APIC ソフトウェアの適切なバージョンを選択します。
- **[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、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 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) **[テンプレート ファイルのアップロード（Upload a template file）]** オプションの下にある **[ファイルの選択（Choose file）]** をクリックし、Cloud APIC CFT を作成した領域に移動します。

f) Cloud APIC CFT を選択し、**[次へ（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。

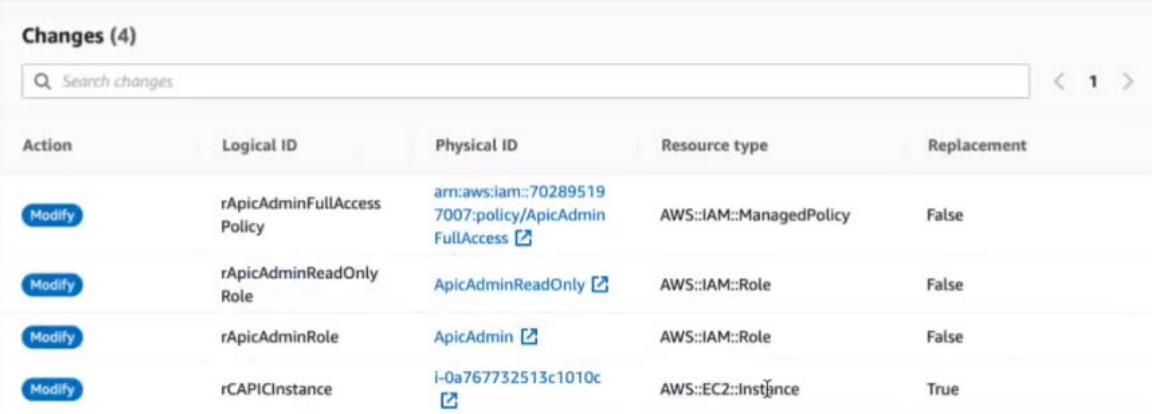
この手順では、インスタンスタイプを**m4.2xlarge**に変更しないでください。

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 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。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。

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 （8 ページ）

ステップ 17 バックアップした設定をインポートします。ステップ 2 （8 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 （8 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。[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 18 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 19 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 （25 ページ）」を参照してください。

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：リリース 25.0(1) から 5.2(1)

これらの手順では、ソフトウェアをリリース 25.0(1) からリリース 5.2(1) に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) を実行していて、リリース 25.0(1) 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、リリース 5.2(1) の設定をバックアップし、そのバックアップした設定ファイルを保存しました。
2. 次に、リリース 25.0(1) へのポリシーベースのアップグレードを実行し、その後ある時点で、リリース 5.2(1) に戻すことにしました。

これらの手順では、リリース 5.2(1) 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、バックアップしたリリース 5.2(1) 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 （3 ページ） の説明に従って、バックアップされたリリース 5.2(1) 設定ファイルがあることを確認します。

バックアップされたリリース 5.2(1) の設定ファイルがない場合は、これらの手順を使用してリリース 25.0(1) からダウングレードしないでください。これらのダウングレード手順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 非ホーム リージョン CSR が構成されていることを確認します。

ステップ 3 ホーム リージョンから CSR を削除します。

ホーム リージョンの CSR が削除され、トラフィック フローが非ホーム リージョンの CSR に切り替わる間、約 3 ～ 5 分間サイト間トラフィックが失われます。

a) クラウド APIC GUI で、[インテント（Intent）] アイコン（複数の円を指す矢印の付いたアイコン）をクリックし、**[クラウド APIC 設定（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) ホーム リージョンの **[クラウド ルータ（Cloud Routers）]** 列で選択解除（ボックスからチェックをオフにする）します（テキスト「**Cloud APIC 展開済み**」があるリージョン）。

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。

CSR の削除プロセスには約 5 ～ 10 分かかる場合があります。AWS ポータルの仮想マシンを確認することで、CSR 削除プロセスをモニタできます。

（注） ホーム リージョンの CSR 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 4 AWS ポータルのインフラ アカウントから、ホーム リージョン VPC とリモート リージョン VPC 間のすべてのインフラ VPC ピアリング接続を手動で削除します。

a) ナビゲーション ペインで、**[ピアリング接続（Peering connections）]** を選択します。

b) VPC ピアリング接続を選択し、**[アクション（Actions）]** > **[VPC ピアリング接続の削除（Delete VPC peering connection）]** の順に選択します。

c) **[VPC ピアリング接続の削除（Delete VPC peering connection）]** ダイアログ ボックス内で接続の詳細を確認し、**[関連するルート テーブル エントリを削除する（Delete related route table entries）]** チェックボックスをオンにして必要なルートを削除し、**[はい、削除します（Yes, Delete）]** を選択して選択した VPC ピアリング接続を削除します。

リモート リージョン VPC から他のリモート リージョン VPC への VPC ピアリング接続を変更しないでください。

ステップ 5 残りの設定が自動的に削除されるまで 10 ～ 15 分待ちます。

次の設定は、10 ～ 15 分後に自動的に削除されます。

- トランジット ゲートウェイの接続ピアは、ホーム リージョンのアタッチメントを接続します。

- トランジットゲートウェイ接続アタッチメント
- インフラ VPC へのトランジット ゲートウェイのアタッチメント

自動的に削除されない場合は、次のように手動で削除してください。

a) ホーム リージョンのトランジット ゲートウェイ接続アタッチメントの場合、接続ピアを削除します。

1. ナビゲーションペインで、**[Transit Gateway の添付ファイル（Transit Gateway Attachments）]** を選択します。
2. [接続（Connect）] 添付ファイルを選択します。
3. **[ピアに接続（Connect peers）]** タブで、Transit Gateway Connect ピアを選択し、**[アクション（Actions）] > [接続ピアの削除（Delete Connect peer）]** を選択します。
4. 確認のダイアログボックスで **[はい、削除します（Yes, Delete）]** をクリックします。
5. これらの手順を繰り返して、ホーム リージョンのトランジット ゲートウェイ接続アタッチメントの追加の接続ピアを削除します。

b) トランジット ゲートウェイ接続の添付ファイルを削除します。

1. ナビゲーションペインで、**[Transit Gateway の添付ファイル（Transit Gateway Attachments）]** を選択します。
2. [接続（Connect）] 添付ファイルを選択します。
3. **[アクション（Actions）] > [削除（Delete）]** を選択します。
4. 確認を求められたら、**[削除（Delete）]** を選択します。

c) インフラ VPC へのトランジット ゲートウェイのアタッチメントを削除します。

1. ナビゲーションペインで、**[Transit Gateway の添付ファイル（Transit Gateway Attachments）]** を選択します。
2. インフラ VPC アタッチメントのみを選択します。

   他のユーザ VPC アタッチメントがある可能性があるため、この手順ではインフラ VPC アタッチメントを選択していることを確認してください。
3. **[アクション（Actions）] > [削除（Delete）]** を選択します。
4. 確認を求められたら、**[削除（Delete）]** を選択します。

ステップ 6 スタックを削除します。

a) AWS コンソールで、**[サービス（Services）] > [CloudFormation] > [スタック（Stacks）]**に移動します。
b) 削除するスタックを選択します。
c) **[スタックの削除（Delete Stack）]** をクリックします。

これにより、Cisco Cloud APIC VM が削除され、他のリソースの削除が試行されます。

ステップ 7 スタックが削除されるまで 15 ～ 20 分待ちます。

スタックの削除が [削除中（Delete in Progress）] のままになっている場合は、ホーム リージョンでインフラ VPC を手動で削除します。

a) AWS コンソールで、**[サービス（Services）]** > **[仮想プライベート クラウド（Virtual Private Cloud）]** > **[VPC（Your VPCs）]** に移動します。
b) インフラ VPC を選択します。
c) **[アクション（Actions）]** > **[VPC の削除（Delete VPC）]** を選択します。
[VPC の削除（Delete VPC）] ウィンドウが表示されます。
d) 削除を確認するには、フィールド領域に **delete** と入力し、**[削除（Delete）]** をクリックします。

ステップ 8 ダウンロード先のリリース イメージのクラウド形成テンプレートを使用して、新しいスタックを再作成します。

（注） または、以下の手順の代わりに AWS Marketplace からクラウド形成テンプレートをデプロイできます。

a) AWS コンソールで、**[サービス（Services）]** > **[CloudFormation]** > **[スタック（Stacks）]**に移動します。
b) **[新しいリソースで** > **スタックを作成（標準）（Create Stack With new resources (standard)）]** をクリックします。
[スタックの作成（Create stack）] ウィンドウが表示されます。
c) **[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。
d) 適切な JSON 形式テナント ロール CFT を使用してコントピュータの場所に移動して、テンプレート ファイルを選択し、**[次へ（Next）]** をクリックします。

[詳細の指定 (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。

e) **[詳細の指定 (Specify Details)]** ページに、必要な情報を入力します。

- **[スタック名 (Stack name):]** この Cloud APIC 設定の名前を入力します。
- **[ファブリック名 (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 Cloud APIC の名前になります。
- **インフラ VPC プール**：最初に Cloud APIC を展開したときと同じインフラ VPC プール情報を使用します。

  既存設定のバックアップ （3 ページ） の手順の一部として、このインフラ VPC プール情報を書き留めておく必要があります。
- **[可用性ゾーン (Availability Zone):]**スクロールダウン メニューから、 Cloud APICサブネットのアベイラビリティ ゾーンを選択します。
- **[インスタンス タイプ（Instance Type）]**：EC2 インスタンス タイプを選択します。

- **[パスワード/パスワードの確認 (Password/Confirm Password):]** 管理者パスワードを入力し、確認入力します。このエントリは、 SSH アクセスを有効にした後に Cloud APICにログインするために使用するパスワードです。
- **[SSH キー ペア（SSH Key Pair）]**：SSH キーペアの名前を選択します。

  Cloud APIC には、この SSH キーペアを使用してログインします。
- **[アクセス制御 (Access Control):]** 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、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 Cloud APIC への接続が許可されます。
- **パブリックIPアドレスの割り当て**：パブリック IP アドレスを Cloud APIC にアウトオブバンド（OOB）管理インターフェイスに割り当てるかどうかを選択します。

  リリース5.2（1）よりも前は、の管理インターフェイスにパブリックIPアドレスとプライベートIPアドレスが割り当てられていました。Cloud APICリリース5.2（1）以降、プライベートIPアドレスはの管理インターフェイスに割り当てられ、パブリックIPアドレスの割り当てはオプションです。Cloud APIC詳細については、『Cisco Cloud APIC for AWS User Guide、Release 5.2（1）』の「Private IP Address Support for Cisco Cloud APIC and Cisco Cloud Services Router」を参照してください。

  - true：パブリックIPアドレスをのアウトオブバンド（OOB）管理インターフェイスに割り当てます。Cloud APIC
  - false：パブリックIPアドレスを無効にし、プライベートIPアドレスをのアウトオブバンド（OOB）管理インターフェイスに割り当てます。Cloud APIC

f) 画面の下部にある **[次へ（Next）]** をクリックします。

[オプション (Option)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

g) **[オプション (Options)]** 画面ですべてのデフォルト値を受け入れ、**[オプション（Options）]** 画面の下部にある **[次へ（Next）]** をクリックします。

[レビュー (Review)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

h) **[レビュー (Review)]** ページのすべての情報が正しいことを確認します。

[レビュー (Review)] ページにエラーが表示された場合は、**[前へ (Previous)]** ボタンをクリックして、誤った情報を含むページに戻ります。

i) **[レビュー (Review)]** ページのすべての情報が正しいことを確認したら、 **[AWS CloudFormation が IAM リソースをカスタム名で作成することを認める (I acknowledge that AWS CloudFormation might create IAM resources with custom names)]** の隣にあるボックスをオンにします。

j) ページ下部にある **[スタックの作成 (Create stack)]** ボタンをクリックします。

[Cloudformation] ページが再び表示され、Cloud APIC作成したテンプレートが [ステータス (Status)] 列に **CREATE_IN_PROGRESS** というテキストとともに表示されます。

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。作成プロセスの進行状況をモニタするには、Cisco Cloud APIC テンプレートの名前の横にあるボックスをオンにし、[イベント (Events)] タブをクリックします。[イベント (Events)] タブの下の [ステータス (Status)] 列には、**CREATE_IN_PROGRESS** というテキストが表示されます。

k) **CREATE_COMPLETE**メッセージが表示されたら、続行する前にインスタンスの準備が整っていることを確認します。

1. 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[EC2]** リンクをクリックします。

   [EC2 ダッシュボード (EC2 Dashboard)] 画面が表示されます。

2. [EC2 ダッシュボード (EC2 Dashboard)] 画面の **[リソース (Resources)]** 領域には、実行中のインスタンスの数を示すテキストが表示されます (たとえば、**[1 つの実行インスタンス (1 Running Instances)]**)。この実行中のインスタンスのリンクをクリックします。

   [インスタンス (Instances)] 画面が表示されます。

3. 続行する前に、そのインスタンスの準備ができるまで待ちます。

   [スタータス チェック (Status Checks)] の下で、新しいインスタンスが **[初期化 (Initializing)]** ステージを経過するのを確認できます。続行する前に、**[スタータス チェック (Status Checks)]** の下で、**[2/2 のチェックをパス (Check Passed)]** というメッセージが表示されるまで待ちます。

ステップ 9 既存設定のバックアップ （3 ページ） で設定をバックアップしたときに書き留めたのと同じパスフレーズを使用して、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、**[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。

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) **[暗号化：有効（Encryption: Enabled）]** 領域の隣にあるボックスをクリックして、既存設定のバックアップ （3 ページ） （**[パスフレーズ/確認/パスフレーズの確認（Passphrase/Confirm Passphrase）]** で記載されているパスフレーズを入力します。

d) ウィンドウの下部にある **[保存（Save）]** をクリックします。

ステップ 10 リリース 25.0(1) にアップグレードする前にバックアップしたリリース 5.2(1) の設定をインポートし、以前の設定が収束することを確認します。

バックアップしたリリース 5.2(1) 設定をインポートするときは、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。

ホーム リージョン CSR 作成は、このステップの後に自動的に開始します。

ステップ 11 サイトが ACI マルチサイト オーケストレータ/Nexus ダッシュボード オーケストレータによって管理されている場合は、新しいCloud APIC VM の IP アドレスを更新します。

a) ACI マルチサイト オーケストレータ/Nexus ダッシュボードにログインします

b) サイトを編集し、登録します。

1. Nexus ダッシュボード オーケストレータで、**[サイト（Sites）]** に移動し、適切なサイトをクリックします。
2. [詳細（Details）] アイコンをクリックし、[概要（Overview）] ウィンドウを起動します。
3. 鉛筆アイコンをクリックし、このサイトの情報を編集します。
4. **[サイトの再登録（Re-register Site）]** の横にあるボックスをクリックし、必要な情報を入力して、新しい Cloud APIC VM の IP アドレスで更新します。
5. [保存（Save）] をクリックします。

c) ACI マルチサイト オーケストレータ/Nexus ダッシュボード オーケストレータに移動し、サイトが引き続き管理されていることを確認します。

1. Nexus ダッシュボード オーケストレータで、**[サイト（Sites）]** に移動します。
2. サイトに移動し、**[管理（Managed）]** が **[状態（State）]** 列に表示されていることを確認します。

d) クラウド サイト更新を実行します。

1. Nexus ダッシュボード オーケストレータで、**[インフラストラクチャ（Infrastructure）]** > **[インフラ設定（Infra Configuration）]** に移動し、**[インフラの設定（Configure Infra）]** をクリックします。
2. 左側のナビゲーション バーでサイトを選択し、**[更新（Refresh）]** をクリックします。

   確認ウィンドウで **[はい（Yes）]** をクリックして、クラウド サイトの更新を続行します。

e) **[展開（DEPLOY）]** > **[展開のみ（Deploy Only）]** をクリックして、インフラ設定を展開します。

ソフトウェアのダウングレード：リリース 25.0(2) から 25.0(1) または 5.2(1)

これらの手順では、ソフトウェアをリリース 25.0(2) から 25.0(1) または 5.2(1) に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 25.0(1) または 5.2(1) を実行していて、リリース 25.0(2) 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 （3 ページ） で説明されているようにリリース 25.0(1) または 5.2(1) の設定をバックアップし、バックアップした設定ファイルを保存しました。

2. 次に、リリース 25.0(2) へのポリシー ベースのアップグレードを実行し、その後、ある時点で、リリース 25.0(1) または 5.2(1) に戻すことを決定しました。

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 （3 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設定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設定ファイルがない場合は、これらの手順を使用してリリース 25.0(2) からダウングレードしないでください。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 同じ内容 (同じ公開鍵または秘密鍵) で SSH キーの複製を作成します。

a) https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
b) ナビゲーション ペインで、**[キー ペア（Key Pairs）]** を選択します。
c) **[キー ペアのインポート（Import key pair）]** を選択します。

d) **[名前（Name）]** に、公開鍵のわかりやすい名前を入力します。名前には、最大 255 文字の ASCII 文字を含めることができます。先頭または末尾のスペースを含めることはできません。

（注） EC2 コンソールからインスタンスに接続すると、コンソールは秘密鍵ファイルの名前としてこの名前を提案します。

e) **[参照（Browse）]** を選択して公開鍵に移動して選択するか、公開鍵の内容を **[公開鍵の内容（Public key contents）]** フィールドに貼り付けます。
f) **[キー ペアのインポート（Import key pair）]** を選択します。
g) インポートした公開鍵が鍵ペアのリストに表示されていることを確認します。

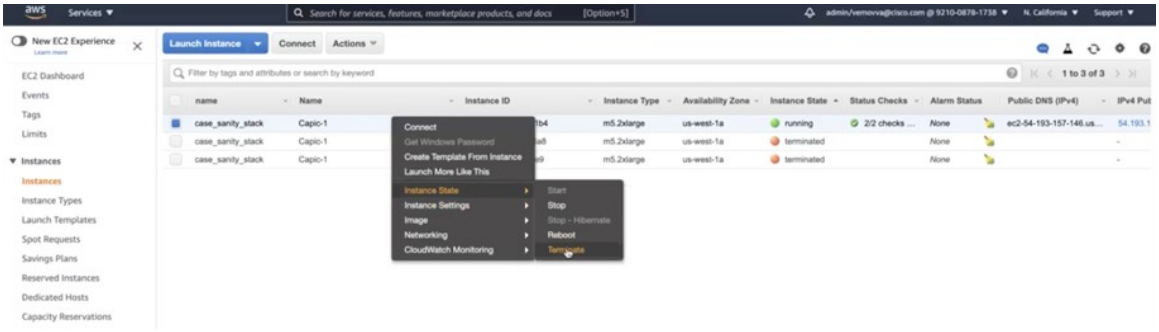
（注） 何らかの理由で**キーペアのインポート**プロセスが機能しない場合は、**[キーペアの作成（Create key pair）]** オプションを使用して新しいキーペアを作成し、必要に応じて ステップ 7 （22 ページ） でそれを使用できます。

ステップ 3 EC2 インスタンス領域に移動し、Cloud APIC VM インスタンスを終了します。

a) ナビゲーション ペインで、**[インスタンス（Instances）]** を選択します。
b) Cloud APIC VM インスタンスの横にあるチェックボックスをオンにします。

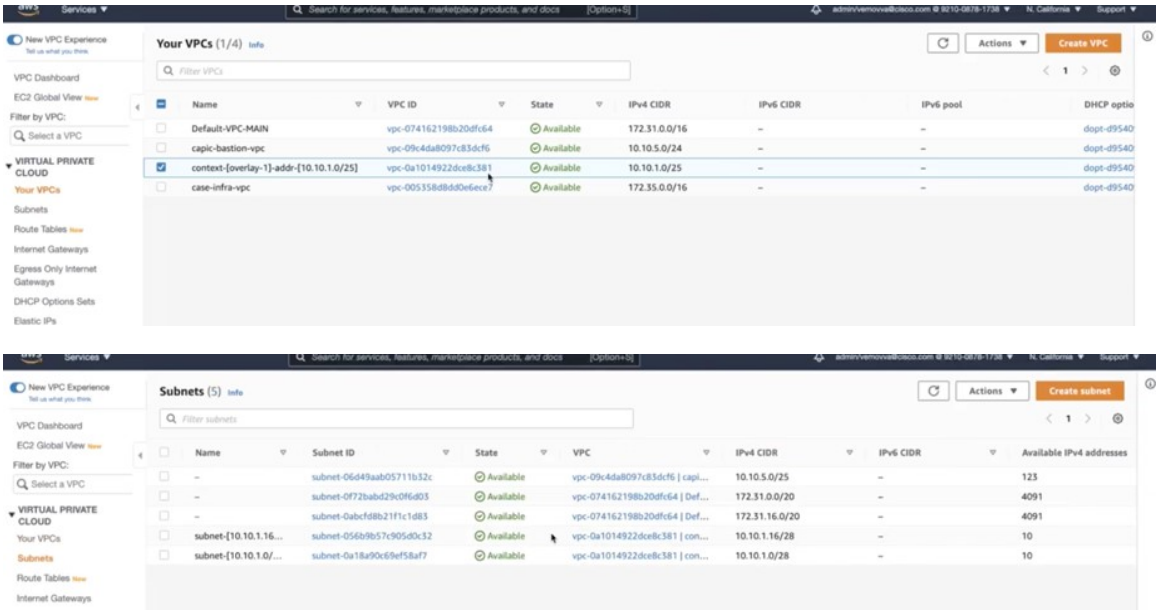
c) Cloud APIC VM インスタンスの行を右クリックし、**[インスタンス状態（Instance State）] > [端末（Terminate）]**を選択します。

Cloud APIC VM インスタンスが終了するまで数分かかります。



Cloud APIC VM インスタンスが終了すると、VM に関連付けられた 2 つのインターフェースがこの時点でハングします。アップグレードの一部として新しい VM が起動すると、同じインターフェイスに再接続されます。

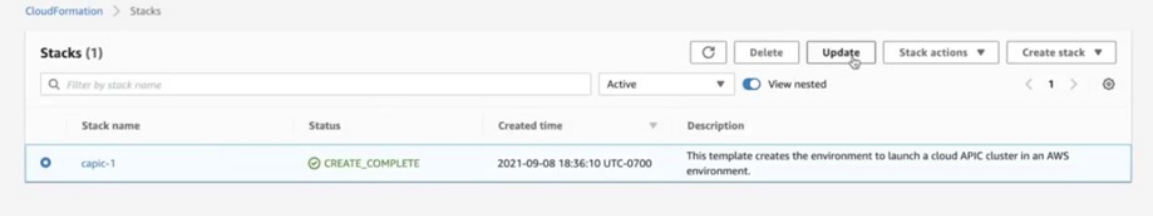
Cloud APIC VM の終了プロセスが完了すると、VPC やその他のネットワーク リソース (CIDR やサブネットなど) がそのまま残っていることがわかります。



ステップ 4 Cloud APIC VM の終了プロセスが完了したら、スタックに戻り、まだ実行状態であることを確認します。

CloudFormation エリアに移動し、Cloud APIC スタックがまだ実行状態であることを確認します。

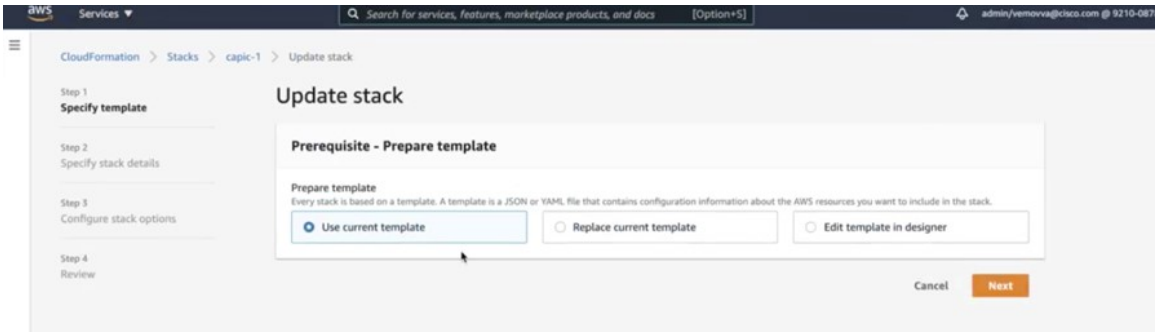
ステップ 5 Cloud APIC スタックの横にある円をクリックし、**[更新（Update）]** をクリックします。



[スタックの更新（Update stack）] ウィンドウが表示されます。

ステップ 6 **[現在のテンプレートを使用（Use current template）]** をクリックし、**[次へ（Next）]** をクリックします。

テンプレートでは何も変更しないため、このウィンドウで **[現在のテンプレートを使用（Use current template）]** オプションを選択します。

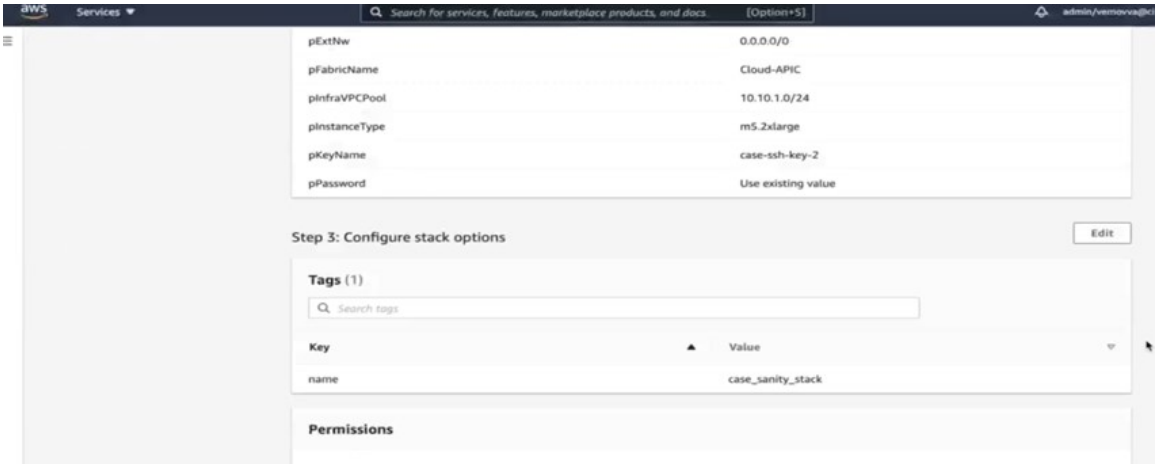


[スタック詳細の指定（Specify stack details）] ウィンドウが表示されます。

ステップ 7 **[スタックの詳細を指定（Specify stack details）]** ウィンドウで、**[SSH キー ペア（SSH Key Pair）]** フィールドを除くすべてのフィールドをそのままにします。

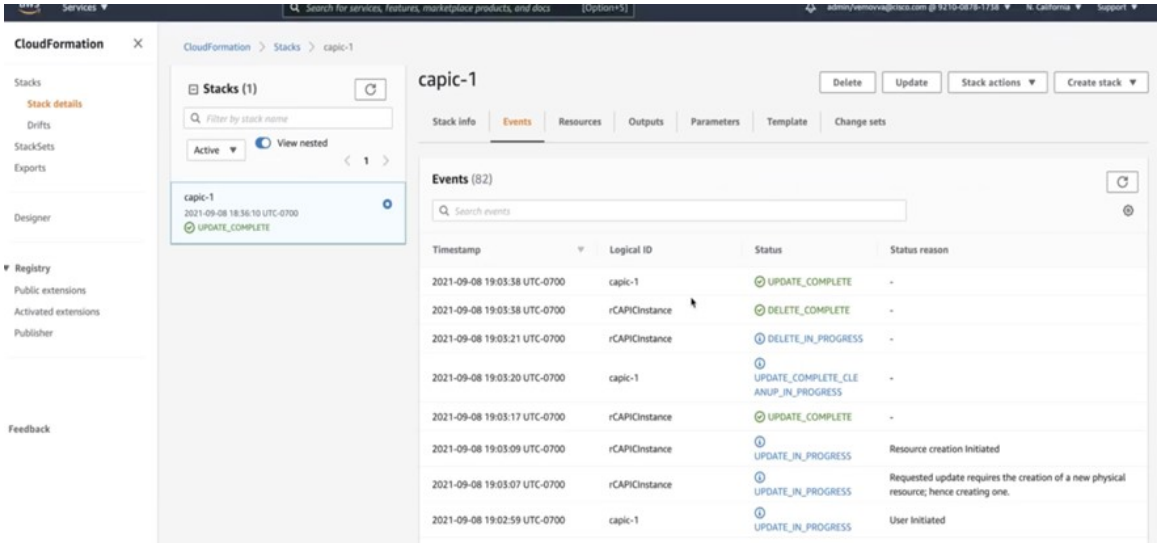
[SSH キー ペア（SSH Key Pair）] フィールドで、ステップ 2 （20 ページ） で設定した新しい SSH キー ファイル名を選択します。

ステップ 8 **[スタックの詳細を指定（Specify stack details）]** ウィンドウの下部にある **[次へ（Next）]** をクリックし、**[スタックの更新（Update stack）]** ウィンドウの残りのウィンドウに移動し、それらのウィンドウのフィールドに新しい SSH キー ファイル名が表示されていることを確認します。



ステップ 9 プロセスの最後にある **[スタックの更新（Update stack）]** をクリックします。

スタックの更新が開始されます。



ステップ 10 スタックの更新の進行状況を監視します。

スタックの更新は、次の段階を経ます。

- AWS は最初に新しい Cloud APIC VM を作成します。
- スタック更新の一環として、手動ですでに削除されている古い Cloud APIC VM の削除を試みます。
- Cisco Cloud APIC はスタックに投稿されます。

ステップ 11 **[スタック（Stacks）]** ウィンドウに **UPDATE_COMPLETE** メッセージが表示されるまで待ってから、**[インスタンス（Instances）]** ウィンドウに戻ります。

- Cloud APIC インスタンスは新しいインスタンス ID を持ち、新しい SSH キーを使用します。
- 古いインターフェースは新しいインスタンスに再接続され、CIDR とサブネットはすべて同じままです。
- Cloud APIC の管理 IP アドレスも同じになります。

ステップ 12 約 5 ～ 10 分後、Cloud APIC でバージョンが正しいことを確認します。

管理 IP アドレスを使用して Cloud APIC にログインします。リリース 25.0(2) にアップグレードする前に、以前に実行されていたリリースのバージョンが表示されます。

ステップ 13 既存設定のバックアップ （3 ページ） で設定をバックアップしたときに書き留めたのと同じパスフレーズを使用して、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、**[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。

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) **[暗号化：有効（Encryption: Enabled）]** 領域の隣にあるボックスをクリックして、既存設定のバックアップ （3 ページ） （**[パスフレーズ/確認/パスフレーズの確認（Passphrase/Confirm Passphrase）]** で記載されているパスフレーズを入力します。

d) ウィンドウの下部にある **[保存（Save）]** をクリックします。

ステップ 14 リリース 25.0(2) にアップグレードする前にバックアップした以前のリリースの設定をインポートし、以前の設定が収束することを確認します。

バックアップした以前のリリースの設定をインポートするときは、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。

この手順の後、ホーム リージョン CSR の作成が自動的に開始されます。

ステップ 15 サイトが ACI マルチサイト オーケストレータ/Nexus ダッシュボード オーケストレータによって管理されている場合は、新しいCloud APIC VM の IP アドレスを更新します。

a) ACI マルチサイト オーケストレータ/Nexus ダッシュボードにログインします

b) サイトを編集して再登録します。

1. Nexus ダッシュボードで、**[サイト（Sites）]** に移動し、正しいサイトをクリックします。
2. 「詳細」アイコンをクリックして、「概要」ウィンドウを表示します。
3. 鉛筆アイコンをクリックして、このサイトの情報を編集します。
4. **[サイトの再登録（Re-register Site）]** の横にあるボックスをクリックし、必要な情報を入力して、新しい Cloud APIC VM の IP アドレスで更新します。
5. [保存（Save）] をクリックします。

c) ACI マルチサイト オーケストレータ/Nexus ダッシュボード オーケストレータに移動し、サイトが引き続き管理されていることを確認します。

1. Nexus ダッシュボード オーケストレータで、**[サイト（Sites）] に移動します。**
2. サイトを見つけて、**[状態（State）]** 列に **[管理（Managed）]** が表示されていることを確認します。

d) クラウド サイトの更新を実行します。

1. Nexus ダッシュボード オーケストレータで、**[インフラストラクチャ（Infrastructure）]** > **[インフラ設定（Infra Configuration）]** に移動し、**[インフラの設定（Configure Infra）]** をクリックします。

2. 左側のナビゲーション バーでサイトを選択し、**[更新（Refresh）]** をクリックします。

   確認ウィンドウで **[はい（Yes）]** をクリックして、クラウド サイトの更新を続行します。

e) **[展開（DEPLOY）]** > **[展開のみ（Deploy Only）]** をクリックして、インフラ設定を展開します。

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 （8 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、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。Cisco Cloud APIC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、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。Cisco Cloud APICこれは、管理プレーン（）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。Cisco Cloud APIC

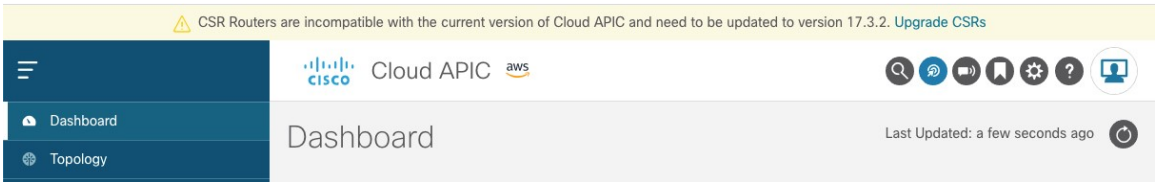
リリース5.2（1）以降、この機能はデフォルトで有効になっています。デフォルトの前提は、へのアップグレードをトリガーした後にCSRへのアップグレードをトリガーすることです。Cisco Cloud APICこの機能を有効にすると、無効にすることはできません。

この機能を有効にすると、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。Cisco Cloud APIC

（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、を参照してください。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 （27 ページ）

1. この章の手順に従ってアップグレードします。Cisco Cloud APIC
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がと互換性がなくなったことを認識します。Cisco Cloud APICその後、CSRとに互換性がなく、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。Cisco Cloud APICCisco Cloud APIC



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、の互換バージョンになるようにします。Cisco Cloud APIC

   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。
   - **[ファームウェアの管理（Firmware Management）]** ページの **[CSRs]** 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]**

     [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 （27 ページ） を参照してください。

ガイドラインと制約事項

- をアップグレードした後、CSRと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 APICCisco 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。Cisco Cloud APIC
- 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 （25 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。
- **[ファームウェアの管理（Firmware Management）]** ページの **[CSRs]** 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]**

  [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[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。

Operations Event Analytics 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 （25 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>
```