

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 (1ページ)
- ソフトウェアのアップグレード (3ページ)
- ソフトウェアのダウングレード (13ページ)
- システムリカバリの実行(25ページ)
- 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)

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)
 - $J J 325.0(1) \sim 25.0(2)$
- ・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。

- [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。
- [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。
- 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)
- $U U 325.0(1) \sim 25.0(2)$

(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。

• SSH \neq – (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。

^{• [}Password]

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1 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。

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

• [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 Cloud Formation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)。

Changes (4)							
Q Search char	nges				< 1 >		
Action	Logical ID	Physical ID	Resource type	Replacement			
Modify	rApicAdminFullAccess Policy	am:aws:iam::70289519 7007:policy/ApicAdmin FullAccess 🚺	AWS::IAM::ManagedPolicy	False			
Modify	rApicAdminReadOnly Role	ApicAdminReadOnly 🖸	AWS::IAM::Role	False			
Modify	rApicAdminRole	ApicAdmin 🔼	AWS::IAM::Role	False			
Modify	rCAPICInstance	i-0a767732513c1010c	AW5::EC2::Inst∯nce	True			

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。

- 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。

- 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。
 - [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。
 - 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。
 - 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1 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。
 - 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。
 - 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。

 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。

Key pairs (1/3) Info	Actions 🔺	Create key pair		
O Filter key pairs			Import key pair	
~ Ther key purs			Delete	
Name	⊽ Туре	\bigtriangledown	Manage tags	▽
capic_downgrade	rsa		e5:06:7b:0d:fd:f9:ff:4	4a:53:ef:70:5a:42:
capic_upgrade	rsa		d4:db:17:e2:ff:dc:f9:	ce:a0:da:12:39:13:
C cisco	rsa		f3:b0:47:b6:6e:42:55	:45:ef:5b:39:9f:f4:

- 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。

aws Services •			Q. Sea	rch for services	s, features, marketplace products, o	nd do	cs [O	otion+S]		\$ ada	nin/vemovva@cisco.com	@ 9210-0878-	1738 •	N. California 🔻 Su	port	•
New EC2 Experience ×	Lau	nch instance 👻	Connect	Actions ~										• 4 0	۰	0
EC2 Dashboard	Q	Filter by tags and attrit	buttes or search	h by keyword											2	н
Events		name	- Name		- Instance ID			Instance Type -	Availability Zone -	Instance State	Status Checks -	Alarm Statu	s	Public DNS (IPv4)	IP.	v4 Put
Tags		case_sanity_stack	Capic-	1	Connect	D P	4	m5.2xlarge	us-west-1a	🥥 running	Ø 2/2 checks	None	5	ec2-54-193-157-146.us	54	.193.1
Limits		case_sanity_stack	Capio-	1	Get Windows Password			m5.2xlarge	us-west-1a	terminated		None	2			
▼ Instances		case_sanity_stack	Capio-		Create Template From Instance Launch More Like This	ľ		m5.2xlarge	us-west-1a	terminated		None	2		•	
instances					Instance State											
Instance Types					Instance Settings		Stop									
Caunch remptates					Networking		Reboot									
Spor nequests					CloudWatch Monitoring		Terrigate									
Reserved Instances								_								
Dedicated Hosts																
Capacity Reservations																

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。

New VPC Experience Tel us what you think		Your	VPCs (1/4) Info									C	Actions	Create VP	РС
/PC Dashboard		9, 1	Titer VPCs											< 1 >	۲
C2 Global View www	4	•	Name		Ψ	VPC ID	v	State	V IPv4 CIDR	IPv6 CIDR		IPv6 po	ol	DHC	CP opti
Select a VPC			Default-VPC-MAI	N		vpc-074162198b	20dfc64	O Available	172.31.0.0/16	-		-		dop	t-d9540
			capic-bastion-vpc			vpc-09c4da8097	c83dcf6	O Available	10.10.5.0/24	-		-		dopt	rt-d954
RTUAL PRIVATE			context-[overlay-	1]-addr-[10.10.1.0/25]	vpc-0a1014922d	ce8c381	@ Available	10.10.1.0/25	-		-		dop	t-d954
sur VPCs			case-infra-vpc			vpc-005358d8dd	DeGece7	⊘ Available	172.35.0.0/16	-		-		dop	r-d954
ubnets															
sute Tables New															
lernet Gateways															
ress Only Internet															
alowaya															
HCP Options Sets															
HCP Options Sets lastic IPs															
HCP Options Sets lastic IPs Services New VPC Experience bit a shat you then.		Sub	nets (5) Info		Search for service	s, features, market	(piace products, s	and doos	[Option+5]	_	4) adminiv	C	Actions ¥	N. Galibrisa V	Support
HCP Options Sets tastic IPs Services V New VPC Experience Tet a shall you time. PC Dashboard		Sub	nets (5) mto		Search for service	s, fasturos, márko	(place products, a	and docs	(Option+5)		4ja sämmiv	movelicaco.com 6 10	Actions ¥	N. California V Create subr < 1 >	bupport Net
HCP Options Sets astic IPs Services • New VPC Experience in a what you tow. PC Dashboard C2 Global View teer try VPC:	4	Sub	nets (5) soto Filter subnets Name	v	Search for service	n, fastures, murket	(parce) products, a	nd docs	[Uption+b] PC	♥ IPv4 CIDR	↓ sämmive	C IPv6 CIDR	Actions V	N. Collorna V Create subr < 1 > Available IPv4 add	tessee ©
ICP Options Sets stic IPs Services ¥ New VPC Experience Int a whit you then PC Dashboard C2 Global View New er by VPC: § Select a VPC	4	Sub	nets (5) info Filter subnets Name -	v	Subnet ID subnet-06d49aab	a, fasturas, muntet ♥ 05711b32c	gaace products a State ⓒ Available	end docs The V V	[Option+5] PC pc-09c4da8097c83dcf6 cc	♥ IPv4 CIDR pl, 10.10.5.0/25	4 admente	IPv6 CIDR	Actions V	N: Celifornia V Create subin < 1 > Available IPv4 add 123	buppor Net © dresses
C Dathonard PC: L Select a VPC: L Select a VPC: L Select a VPC:	•	Sub:	nets (5) sofo Filter submets Name - -	v	Subnet ID subnet-06449aab	♥ 05711b32c 29c0f6d03	state State ② Available ③ Available	ind docs The V Vi Vi	[65500143] PC pc-09c4da80097c83dcf6 [cl pc-074162198b20df664 [Cl	 ✓ IPv4 CIDR pl 10.10.5.0/25 wf 172.31.0.0/20 	kja admente ⊽	C IPv6 CDR -	Actions V	K Caltonia Create subn < 1 > Available IPv4 add 123 4091	Net ©
C Dashboard C Sober V PC C Dashboard C Sober V PC C Dashboard C Sober V PC S Sober 2 V PC S Sober 2 V PC S Sober 2 V PC S Sober 2 V PC	4	Sub	nets (5) Into Filter subnets Name - -	~	Subnet ID subnet-O6d49aab subnet-O6d49aab	x (astarca, yransa ♥ 05711552c 29c0f6d03 21f1c1d83	state State O Available O Available O Available	and doos ए V भा भा भा	PC pc-09c4da8097c83dcf6 [ci pc-09c4da8097c83dcf6 [ci pc-074162198b320dfc64 [Ci	 IPv4 CIDR ID-10.5.0/25 172.31.16.0/20 	4) administ	C IPv6 CIDR - -	Actions V	N. California Create subin Create subin Create subin Create subin Available IPv4 add 123 4091 4091	net ©
Cor Options Sets astic IPs Services New VPC Experience te us shar you from Coashboard 22 Global View www er by VPC: Services VIPC Instruct, PRIVATE LOUD VFOS	4	Suba	nets (5) Info Filter submets Name - - - submet-[10.10.1.	v 16	Subnet ID subnet-06649aab subnet-0772babd subnet-056b9b57	 ▼ 2015/000 (000/00) ▼ 05711b52c 29c0f6d03 21f1c1d83 rc905d0c52 	State Available Available Available Available Available	জ V জ V মা মা মা মা মা	PC PC 0-09-04640976354565 [0 0-07-1631980204564] 0-07-1631980204564] 0-01-1014922068581]	 IPv4 CIDR ID-10.5.0/25 IT-2.31.00/20 IT-2.31.16.0/20 ID-10.1.16/28 	4) atmos	IPv6 CIDR - - -	Actions V	N californi V Create subn < 1 > Available IPv4 add 123 4091 10	Support Set
CP Options Sets astic IPs CP Options Sets astic IPs CP Options Sets astic IPs CP Options Sets CP Options C	4	Subo	nets (5) sele Filter subnets - - - subnet-[10.10.1 subnet-[10.10.1)		Subnet ID subnet-0649aab subnet-0649aab subnet-032babd subnet-046bb subnet-046bb subnet-046bb	♥ 05711b32c 29c0f6d03 21f1c1d83 (<905d0c32 69ef58af7	State State State Available Available Available Available	स्त doos ज् प प प प प प प प	PC pc-09c4da8097c83dc46 (c pc-09c4da8097c83dc46 (c pc-074162198b20dc64 (c pc-074162198b20dc64 (c pc-074162198b20dc64 (c pc-074162198b20dc64 (c	 ♥ IP+4 CIDR □0.105.0/25 ■f 172.31.0.0/20 ■f 10.10.1.16/28 □0.10.1.012/8 	4) atmos	IPv6 CIDR - - -	Actions V	N. Cashona Create subm Create subm (1) Available IPv4 add 123 4091 4091 10 10	Support et O
CPC Popons Sets astic IPs CPC Popons Sets astic IPs CPC Popons Sets astic IPs CPC Pathoard C2 Global View now ere by VPC: CPC Instruct Private CPC Instruct Private CPC Instruct Instr	4	Subi	Name Name	⊽ 16 0/	Subnet ID subnet-06449aab subnet-06449aab subnet-06449aab subnet-064649aab subnet-064649ab subnet-06669457 subnet-0a18a90cc	v 05711b32c 29c0f6d3 211fc1d83 cr05d0c32 06ef5lar7	State O Available O Available O Available O Available	स्य विद्या च ् ् य य य य य य य	PC PC pc-09-0448097(d3dcf6) (d pc-074162198020dc64) (d pc-074162198020dc64) (d pc-074162198020dc64) (d pc-0410149220dc81) (d pc-0410149220dc81) (d	 ♥ IPv4 CDR pl 10.10.5.0/25 ef 172.31.0/20 er 10.10.1.6/28 	 administrative v 	C IPv6 CDR - - - -	Actions V	A Castona V Create sole < 1 > Available IPv4 add 123 4091 10 10	wet To dresses

- **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。

Stacks (1)				C	Delete Update Stack actio	Create stack V
Q. Filter by stack name			Active	٣	View nested	< 1 > @
Stack name	Status	Created time	Ŧ	Descripti	ion	
O capic-1	CREATE_COMPLETE	2021-09-08 18:30	:10 UTC-0700	This temp	plate creates the environment to launch a cloud	d APIC cluster in an AWS

[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。

CloudFormation > Stacks >	apic-1 > Update stack		
Step 1 Specify template	Update stack		
Step 2 Specify stack details	Prerequisite - Prepare template		
Step 3	Prepare template Every stack is based on a template. A template is a JSON or YAML file that contain	is configuration information about the AWS resou	rces you want to include in the stack.
Configure stack options	Use current template Replace current	c Ed	it template in designer
Step 4 Review	•		Cancel Next

[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。

aws	Services 🔻	Q. Search for services, features, marketplace products, and docs.	[Option+S]	۵.	admin/verriovva@ci
=		pExtNw	0.0.0.0/0		
		pFabricName	Cloud-APIC		
		pInfraVPCPool	10.10.1.0/24		
		plostanceType	m5.2xtarge		
		pKeyName	case-ssh-key-2		
		pPassword	Use existing value		
		Tags (1)			
		Tags (1)			
		A SHIFT IDIA			
		Key	Value		· •
		name	case_sanity_stack		
		Permissions			

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。

CloudFormation ×	CloudFormation > Stacks > capic-1				
Stacks Stack details Drifts	C Stacks (1) C .	capic-1 Stack info Events Resources	Outputs Parameters	Delete Template Change se	Update Stack actions V Create stack V
StackSets Exports	Active View nested	Events (82)			a
Designer	capic-1 2021-09-08 18:36:10 UTC-0700 ⊘ UPDATE_COMPLETE	Q. Search events			۲
		Timestamp Ÿ	Logical ID	Status	Status reason
Public extensions		2021-09-08 19:03:38 UTC-0700	capic-1	O UPDATE_COMPLETE	
Activated extensions		2021-09-08 19:03:38 UTC-0700	rCAPICInstance	O DELETE_COMPLETE	
Publisher		2021-09-08 19:03:21 UTC-0700	rCAPICInstance	DELETE_IN_PROGRESS	3
		2021-09-08 19:03:20 UTC-0700	capic-1	O UPDATE_COMPLETE_CLE ANUP_IN_PROGRESS	
-		2021-09-08 19:03:17 UTC-0700	rCAPICInstance	O UPDATE_COMPLETE	
Feedback		2021-09-08 19:03:09 UTC-0700	rCAPICInstance	UPDATE_IN_PROGRESS	Resource creation Initiated
		2021-09-08 19:03:07 UTC-0700	rCAPICInstance	UPDATE_IN_PROGRESS	Requested update requires the creation of a new physical resource; hence creating one.
		2021-09-08 19:02:59 UTC-0700	capic-1	UPDATE_IN_PROGRESS	User Initiated

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。
 - 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。

- 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
 - 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

CSR Routers are incompatible with the current version of Cloud APIC and need to be updated to version 17.3.2. Upgrade CSRs						
Ŧ	cisco Cloud APIC avs	Q 🔊 🔍 A 😂 🖓 💶				
Dashboard	Dashboard	Last Updated: a few seconds ago				
Topology	Dashbuara					

- 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>

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

```
<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>
```