

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(6ページ)
- ソフトウェアのダウングレード(16ページ)
- システムリカバリの実行(34ページ)
- CCR のアップグレードのトリガー (34 ページ)

特記事項

- ・リリース 25.0(3) に関する特記事項 (1ページ)
- •一般的な特記事項(4ページ)

リリース 25.0(3) に関する特記事項

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

- Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V への移行のため、25.0(3) より前のリリースからリリース 25.0(3) 以降にアップグレードする前に、必要なポリシーを追加する必要があります。
- 1. AWS ポータルでインフラ テナントに移動します。
- 2. [IAM]>>[ポリシー (Policies)]をクリックします。
- **3.** [ポリシー (Policies)] ウィンドウで、[ApicAdminFullAccess] ポリシーをクリックします。

このポリシーの[サマリー (Summary)]ページが表示されます。

- 4. [ポリシーの編集(Edit Policy)]をクリックします。
- 5. [JSON] タブをクリックします。

6. 以下のエントリをコピーして、ポリシーに貼り付けます。

```
{
    "Effect": "Allow",
    "Action": "ssm:*",
    "Resource": "*"
}
```

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

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

- Cisco Cloud Network Controller をリリース 25.0(3) にアップグレードする場合は、Cisco Cloud Network Controller のアップグレード後できるだけ早く CCR をアップグレードする必要が あります。手順については、以下を参照してください。
 - ソフトウェアのアップグレード(6ページ)
 - CCR のアップグレードのトリガー (34 ページ)

以下は、これらのアップグレードプロセスを実行する方法の例です。

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

次に、これらのサイトを次の方法でアップグレードします。

1. Nexus Dashboard Orchestrator を 3.7(1) リリースにアップグレードします。

 ソフトウェアのアップグレード (6ページ) の手順に従って、サイト1 (AWS サイト) を Cisco Cloud Network Controller リリース 25.0(3) にアップグレードしま す。

このアップグレードが安定した状態になるまで待ってから、次の手順に進みま す。

 CCR のアップグレードのトリガー (34ページ) の手順を使用して、サイト1 (AWS サイト)の CCR を古い CCR (Cisco Cloud Services Router 1000v) から新 しい CCR (Cisco Catalyst 8000V) にアップグレードします。

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

- サイト1(AWSサイト)のCCRが完全にアップグレードされたら、サイト2 (Azureサイト)に対してこれらの手順を繰り返します。最初にCisco Cloud Network Controller ソフトウェアをリリース25.0(3)にアップグレードします。アップグレー ドが安定した状態に達したら、サイト2のCCRを新しいCisco Catalyst 8000Vに アップグレードします。
- Cisco Cloud Network Controller リリース 25.0(3) より前の古い Cisco Cloud Services Router 1000v ルータは、AWS パブリック クラウドの要件 で説明されているように、番号ベース のスループットで設定されていました。Cisco Catalyst 8000V ルータは階層ベースのスルー プット オプションのみをサポートするため、リリース 25.0(3) へのアップグレード中に、 Cisco Cloud Network Controller は、古い Cisco Cloud Services Router 1000v ルータで使用され る数値ベースのスループットからのスループット値を新しい Cisco Catalyst 8000V ルータで 使用される階層ベースのスループットにマッピングします。

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

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

Cisco クラウド サービス ルータ 1000v	Cisco Catalyst 8000V のスループット
10G	T3 (最大 10G のスループット)

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

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

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

Cisco Catalyst 8000V のスループット	Cisco Cloud Services Router 1000v のスループット
T0(最大 15M のスループット)	10 M
T1(最大 100M のスループット)	1億
T2(最大 1G のスループット)	1G
T3(最大 10G のスループット)	10G

*4

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

一般的な特記事項

一般的な特記事項は次のとおりです。

• Cisco Cloud Network Controller 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(5)
- リリース 25.0(1) から 25.0(5)
- リリース 25.0(2) から 25.0(5)
- リリース 25.0(3) から 25.0(5)
- ・リリース 25.0(4) から 25.0(5)
- 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、CCR が下位のリリースにダウングレードされるため、CCR 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。

- AWS パブリック クラウドの要件 に記載されているように、リリース 5.0(x) 以降では、 Cisco Cloud Network Controller の展開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。
 - リリース 5.0(x) より前のリリースでは、Cisco Cloud Network Controller 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 Network Controller 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、移行 ベースのアップグレード (11 ページ) 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。

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 (9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以降ベースのアップグレードの いずれかを使用した Cisco Cloud Network Controller ソフトウェアのアップグレードについて説 明します。



(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(11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。

CCRのアップグレード

Cisco Cloud Network Controller 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、Cisco Cloud Network Controller ソフトウェアをアップグレードするたびに、CCR もアップグレードす る必要があります。

- リリース 5.2(1) より前のリリースでは、Cisco Cloud Network Controller のアップグレードを トリガーするたびに CCR が自動的にアップグレードされます。
- リリース 5.2(1)以降では、Cisco Cloud Network Controllerのアップグレードとは関係なく、 CCRのアップグレードをトリガーし、それらのCCRのアップグレードをモニタできます。
 これにより、管理プレーン(Cisco Cloud Network Controller)とデータプレーン(CCR)の アップグレードを分離できるため、トラフィック不足を抑えるのに役立ちます。

i詳細については、「CCR のアップグレードのトリガー (34 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に従って、Cisco Cloud Network Controller 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

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

ソフトウェアのダウングレード(16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 Network Controller GUIで、[インフラストラクチャ(Infrastructure)]>[システム設定(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 Network Controller 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 Cisco Cloud Network Controller スタックをクリックし ます。

Cisco Cloud Network Controller 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。

バックアップ構成の作成で使用できるオプションの詳細については、Cisco Cloud Network Controller for AWS User Guide の *Cisco Cloud Network Controller GUI* を使用してバックアップ構成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 まだログインしていない場合は、Cisco Cloud Network Controller 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(9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>/cloud-network-controller-dk9.25.0.5f.iso で す。「ステップ6 (9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>/cloud-network-controller-dk9.25.0.5f.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 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(9ページ)」に進みます。
- f) [SSH 公開/秘密キー ファイルを使用(Use SSH Public/Private Key Files)]を選択した場合は、次の情報を入力します。
 - [SSH キー コンテンツ (SSH Key Contents)]: SSH キー コンテンツを使用して SSH キー ファイ ルを作成します。SSH キーファイルは、ダウンロード用のリモートロケーションの作成時に必要 です。
 - (注) 公開キーは、転送時に生成されます。転送後、バックグラウンドで生成されたキーファ イルは削除されます。一時的なキーファイルが、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller のファームウェア イメージがダウンロードされるのを待ちます。

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

以下のシナリオの手順に従って、Cisco Cloud Network Controller 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(8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(7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(16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 Cisco Cloud Network Controller GUI で、[移動(Navigation)] メニューから[オペレーション(Operations)]> [ファームウェア管理(Firmware Management)]を選択します。

[ファームウェア管理] ウィンドウが表示されます。

ステップ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 Network Controller 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(10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。

Cisco Cloud Network Controllerには、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 Cisco Cloud Network Controller 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 Network Controller 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) Cisco Cloud Network Controller GUIで、[インフラストラクチャ(Infrastructure)] > [システム設定 (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 (11 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 Cisco Cloud Network Controller 構成をバックアップします。

Cisco Cloud Network Controller の構成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、*Cisco Cloud Network Controller for AWS* ユーザーガイドを参照してください。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 Cisco Cloud Network Controller 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、Cisco Cloud Network Controller 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) Cisco Cloud Network Controller インスタンスを特定します。

- ・リリース 5.0(x) より前のリリースでは、Cisco Cloud Network Controller 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 Network Controller は m5.2xlarge インスタンスを使用して 展開されます。
- 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、[アクション(Actions)]> [インスタンスの状態(Instance State)]>[終了(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。

[インスタンス(Instances)]ウィンドウが再表示され、クラウドAPICインスタンスの[インスタンスの の状態(Instance State)]行のステータスが[シャットダウン中(shutting-down)]に変わります。こ こで Cisco Cloud Network Controller インスタンスを終了しても、Cisco Cloud Network Controller のトラ フィックがドロップすることはありません。

ステップ4 AWS Marketplace の Cisco Cloud Network Controller 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 (Software Version)]: Cisco Cloud Network Controller 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)]: Cisco Cloud Network Controller 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 Cisco Cloud Network Controller CFT で、m5.2xlarge インスタンス タイプです。

- **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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller スタックをクリックし、[更新(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、Cisco Cloud Network Controller CFT を作成した領域に移動します。
- f) Cisco Cloud Network Controller 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	AWS::EC2::Instignce	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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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(Instance State)]が[実行中(running)]に変化したら、以前のようにCisco Cloud Network Controller にログインできます。

この時点では、Cisco Cloud Network Controller には何も構成されていません。

- (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) Cisco Cloud Network Controller GUIで、[インフラストラクチャ(Infrastructure)] > [システム設定 (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 (11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(11ページ)

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

- a) Cisco Cloud Network Controller GUIで、[操作(Operations)]>[バックアップとレストア(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(11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 Network Controller 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-[cloud-network-controller-AccountId]-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。cloud-network-controller-AccountId は、Cisco Cloud Network Controller インフラ テナントの AWS アカウント番号です。これは、Cisco Cloud Network Controller 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。
- 1) 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** Cisco Cloud Network Controller GUIで、移行前に Cisco Cloud Network Controller に対して加えたすべての構成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、CCR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管理コンソールのEC2ダッシュボードで[インスタンス(Instances)] に移動し、CCR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、Cisco Cloud Network Controller のアップグレード時にCCRが自動的にアップグレードされないため、Cisco Cloud Network Controller のアップグレードが完了した後にCCRアップグレードを個別にトリガーする必要があります。詳細については、「CCR のアップグレードのトリガー(34 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 Network Controller ソフトウェアを正常にダウングレードするために 必要な情報について説明します。

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(7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 CCR 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 CCR を削除します。

ホーム リージョンの CCR 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 CCR 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) Cisco Cloud Network Controller 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、[Cisco Cloud Network Controller セットアップ(Cisco Cloud Network Controller 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)]列で選択解除をします(ボックスのチェッ クをオフにします)。ホームリージョンとは、Cisco Cloud Network Controller 展開済み(Cisco Cloud Network Controller Deployded]というテキストが表示されているがあるリージョンです。
- d) [次へ (Next)]をクリックし、次のページに必要な情報を入力して、[保存して続行 (Save and Continue)]をクリックします。

CCR 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、CCR 削除プロセスをモニタできます。

- (注) ホーム リージョンの CCR が完全に削除されるまで、次の手順に進まないでください。
- **ステップ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。
 - 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 Network Controller が削除され、他のリソースの削除も試行されます。

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 Cisco Cloud Network Controller 構成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 Cisco Cloud Network Controller の名前になります。
- •[インフラ VPC プール(Infra VPC Pool)]:最初に Cisco Cloud Network Controller 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 (7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。

- •[アベイラビリティ ゾーン (Availability Zone):]スクロールダウン メニューから、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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。

Cisco Cloud Network Controller 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):] Cisco Cloud Network Controller への接続を許可する外部ネット ワークの IP アドレスとサブネットを入力します(たとえば 192.0.2.0/24)。このサブネットか らの IP アドレスだけが、Cisco Cloud Network Controller への接続を許可されます。値として 0.0.0.0/0 を入力すると、誰でも Cisco Cloud Network Controller 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(Assign Public IP address)]: パブリック IP アドレスを Cisco Cloud Network Controller 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 るかどうかを選択します。

リリース5.2(1)よりも前は、Cisco Cloud Network Controller 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。リリース 5.1(1) 以降、 プライベート IP アドレスは Cisco Cloud Network Controller 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。詳細については、*Cisco Cloud Network Controller for AWS User Guide*、リリース 5.2 (1) の「Private IP Address Support for Cisco Cloud Network Controller and CCR」のトピックを参照してください。

- •[true]:パブリックIPアドレスをCisco Cloud Network Controller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。
- [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 Cisco Cloud Network Controller 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。
- 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、作成した Cisco Cloud Network Controller 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 Network Controller 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 Network Controller 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。
 - 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 (7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 Network Controller GUIで、[インフラストラクチャ(Infrastructure)] > [システム設定 (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(7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。

この手順の後、ホーム リージョン CCR の作成が自動的に開始されます。

- **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 Dashboard Orchestrator によって管理されている場合 は、新しい Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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。

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(7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 (7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	C	C Actions 🔺					
0	Filter key noirs			Import key pair				
-	< ritter key puirs			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:			
	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(25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、Cisco Cloud Network Controller 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) Cisco Cloud Network Controller 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) Cisco Cloud Network Controller 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)]>[終了(Terminate)]を選択します。

Cisco Cloud Network Controller VM インスタンスが終了するまで数分かかります。



Cisco Cloud Network Controller 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。

Cisco Cloud Network Controller 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 then		Your	VPCs (1/4) Infe								C Actions 🔻	Create VPC
VPC Dashboard		Q,	Filter VPCs									< 1 > @
EC2 Global View to Filter by VPC:	4	•	Name	v	VPC ID	v	State	v	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP optio
Q Select a VPC			Default-VPC-MAIN		vpc-074162198b20dfc64		⊘ Available		172.31.0.0/16	-	-	dopt-d9540
			capic-bastion-vpc		vpc-09c4da8097c83dcf6		⊘ Available		10.10.5.0/24		-	dopt-d9540
VIRTUAL PRIVATE			context-[overlay-1]-addr-[10.10.1.0/25	1	vpc-0a1014922dce8c381		⊘ Available		10.10.1.0/25	-	-	dopt-d9540
Your VPCs			case-infra-vpc		vpc-005358d8dd0e6ece7		⊘ Available		172.35.0.0/16	-	-	dopt-d9540
Subnets												
Route Tables New												
Internet Gateways												
Egress Only Internet Gateways												
DHCP Options Sets												
Elastic IDs												

Services V					C Search for services, features, i	narketj	olace products, a	nd doc	s [Option+5]			A adminis	emovva@cisco.com @ 92	10-0878-1738 •	N. California V Support V
New VPC Experience Tell us what you then		Sub	nets (5) Info										C	Actions ¥	Create subnet
VPC Dashboard		Q	Filter submets												< 1 > @
EC2 Global View New Filter by VPC:	4		Name	Ψ	Subnet ID	v	State		VPC	v	IPv4 CIDR	~	IPv6 CIDR	Ψ.	Available IPv4 addresses
Q. Select a VPC			-		subnet-06d49aab05711b32c		 Available 		vpc-09c4da8097c83dcf6 cap	si	10.10.5.0/25		-		123
			-		subnet-0f72babd29c0f6d03		O Available		vpc-074162198b20dfc64 De	đ	172.31.0.0/20		-		4091
VIRTUAL PRIVATE			-		subnet-0abcfd8b21f1c1d83		⊘ Available		vpc-074162198b20dfc64 De	đ	172.31.16.0/20		-		4091
Your VPCs			subnet-[10.10.1	1.16	subnet-056b9b57c905d0c32		O Available		vpc-0a1014922dce8c381 co	n	10.10.1.16/28		-		10
Subnets			subnet-[10.10.1	1.0/	subnet-0a18a90c69ef58af7		O Available		vpc-0a1014922dce8c381 co	n	10.10.1.0/28		-		10
Route Tables New															
Internet Gateways															

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

> [CloudFormation] エリアに移動し、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller スタックの横にある丸をクリックし、[更新(Update)]をクリックします。

Stack name	Status	Created time	v Descri	iption	
Q. Filter by stack name		Activ	re	View nested	< 1 > @
Stacks (1)			C	Delete Update Stack act	tions 🔻 Create stack 🔻

[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。

aws	Services 🔻	Q Search for services, features, mark	etplace products, and docs	[Option+S]	♦ admin/	removva@cisco.com @ 9210-08
=	CloudFormation > Stacks > capic-1	> Update stack				
	Step 1 Specify template	Update stack				
	Step 2 Specify stack details	Prerequisite - Prepare template				
	Services ▼ CloudFormation > Stacks > capic-1 Step 1 Specify template Step 2 Specify stack details Step 3 Configure stack options Step 4 Review	Prepare template Every stack is based on a template. A template is a JSON	or VAML file that contains configur	ation information about the AP	WS resources you want to include in the stack.	
	Configure stack options	O Use current template	 Replace current temp 	late	Edit 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 (23 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 pr	reducts, and docs. [Option+S]	A admin/ver	iovva@c
1		pExtNw	0.0.0/0		
		pFabricName	Cloud-APIC		
		pInfraVPCPool	10.10.1.0/24		
		pinstanceType	m5.2xlarge		
		pKeyName	case-ssh-key-2		
		pPassword	Use existing value		
		Tags (1)			
		Tags (1)			
		Q. Search togs			
		Кеу	▲ 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。

Services V	Q. Search for services, featu	res, marketplace products, and docs [Op	tion+5]	43. admin/vemov	wagicisco.com (8 9210-0878-1738 🖤 N. California 👻 Support 🛡
CloudFormation \times	CloudFormation > Stacks > capic-1				
Stacks	🗆 Stacks (1)	capic-1		Delete	Update Stack actions V Create stack V
Stack details Drifts	Q. Filter by stack name	Stack info Events Resource	s Outputs Parameters	Template Change se	ets
StackSets Exports	Active w View nested				
Designer	Capic-1 2021-09-08 18.56:10 UTC-0700 ⊘ UPDATE_COMPLETE	Q, Search events			C
		Timestamp 🖤	Logical ID	Status	Status reason
Public extensions		2021-09-08 19:03:38 UTC-0700	capic-1	@ 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	O DELETE_IN_PROGRESS	
		2021-09-08 19:03:20 UTC-0700	capic-1	O UPDATE_COMPLETE_CLE ANUP_IN_PROGRESS	2
Fredhad		2021-09-08 19:03:17 UTC-0700	rCAPICInstance	UPDATE_COMPLETE	
reedback		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 Cisco Cloud Network Controller VM を作成します。
- スタック更新の一環として、古い Cisco Cloud Network Controller VM の削除が試みられます。ただし、これは手動ですでに削除されています。
- Cisco Cloud Network Controller はスタックにポストされます。

- 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。
 - Cisco Cloud Network Controller インスタンスは新しいインスタンス ID を取得し、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。
 - Cisco Cloud Network Controller の管理 IP アドレスも同じです。
- ステップ12 約5~10分経過したら、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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(7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 Network Controller GUIで、[インフラストラクチャ(Infrastructure)] > [システム設定 (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(7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 CCR 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 Dashboard Orchestrator によって管理されている場合 は、新しい Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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。

ソフトウェアのダウングレード: リリース 25.0(3) から 25.0(2)、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(3) から 25.0(2)、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(2)、25.0(1)または5.2(1)を実行していて、リリース25.0(3) 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(7ページ)で説明されているようにリリース25.0(2)、25.0(1)ま たは5.2(1)の構成をバックアップし、バックアップした構成ファイルを保存しました。
- 2. 次に、リリース 25.0(3) 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(2)、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 (7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構成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(3)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#unique_68 unique_68 Connect_42_step_it2_mtz_yrb 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、Cisco Cloud Network Controller 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) Cisco Cloud Network Controller 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) Cisco Cloud Network Controller 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)]>[終了(Terminate)]を選択します。

Cisco Cloud Network Controller VM インスタンスが終了するまで数分かかります。

aws Services •		Q Search for services,	features, marketplace products, a	and doc	s [Op	tion+5]		∳ adm	in/vemovva@cisco.co	m @ 9210-0878-	1758 •	N. California 🕷 Sup	port ¥
New EC2 Experience X	Launch Instance 💌	Connect Actions ~										• 4 •	• •
EC2 Dashboard	Q. Filter by tags and attri	butes or search by keyword										Ø < < 1 to 3 of 3	> >1
Events	name	- Name	- Instance ID			Instance Type	Availability Zone -	Instance State +	Status Checks	Alarm Statu		Public DNS (IPv4) -	IPv4 Pu
Tags	case_sanity_stack	Capic-1	Connect	164		m5.2xlarge	us-west-1a	🧼 running	Ø 2/2 checks	None	2	ec2-54-193-157-146.us	54,193.
Limits	case_sanity_stack	Capio-1	Get Windows Password	ad		m5.2xlarge	us-west-1a	terminated		None	2		
♥ Instances	case_sanity_stack	Capio-1	Create Template From Instance Launch More Like This	•		m5.2xlarge	us-west-1a	terminated		None	2		÷.
Instances			Instance State										
Instance Types			Instance Settings		Stop								
Launch Templates			Image		Stop - Hiberr	uto							
Spot Requests			Networking Circultions Manifester		Rebool	-							
Savings Plans			Cloudwatch Monitoring	×	and the second								
Reserved Instances													
Dedicated Hosts													
Capacity Reservations													

Cisco Cloud Network Controller 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。

Cisco Cloud Network Controller 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 shat you think		You	r VPCs (1/4) Info							C	Actions VPC
VPC Dashboard		Q	Filter VPCs								< 1 > @
EC2 Global View	4	•	Name	Ŧ	VPC ID	v	State	V IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP opti
Q. Select a VPC			Default-VPC-MAIN		vpc-07416219	8b20dfc64	O Available	172.31.0.0/16	-		dopt-d954
UNDITIAL DODIATE	÷.,		capic-bastion-vpc		vpc-09c4da805	17c83dcf6	⊘ Available	10.10.5.0/24	-	-	dopt-d954
CLOUD			context-[overlay-1]-add	dr-[10.10.1.0/25]	vpc-0a101492	2dce8c381	 Available 	10.10.1.0/25	-	-	dopt-d954
Your VPCs			case-infra-vpc		vpc-005358d8	dd0e6ece7	O Available	172.35.0.0/16	-	-	dopt-d954
Subnets											
Route Tables New											
internet Gateways											
Egress Only Internet Sateways											
DHCP Options Sets											
DHCP Options Sets Bastic IPs											
DHCP Options Sets Elastic IPs Services New VPC Experience Indua what you firek.		Sub	mets (5) info	Q. Search for sen	ices, features, mar	ialplace products,	and docs	(Option+5)		 administrationation 8 87 0 C 	COL70-1750 ♥ N: Castorna ♥ Support Actions ♥ Create subnet
DHCP Options Sets Eastic IPs Services V New VPC Experience Tel us what you then: VPC Dashboard		Sub	nets (5) anto Filter subsets	(Q. Search for serv	rces, Peatures, mar	selplace products,	and docs	(Option+5)		 	Actions ▼ K California ▼ Support Actions ▼ Create subnet < 1 > ©
DHCP Options Sets Eastic IPs Services * New VPC Experience Net as what you free. VPC Dashboard EC2 Global View two		Sub	nets (5) into Filter subrets	Q Search for serv	ices, features, mar	segolace products,	and docs	[Option+5]			Collective & Castorna & Dapport Actions ¥ Create subnet < 1 > @
DHCP Options Sets Eastic IPs New VPC Experience New VPC Experience New uPC Experience EC2 Global View new Timer by VPC:	4	Sub Q	nets (5) toto Filter subnets Name V	Q. Search for serv Subnet ID	ices. features, man	secplace products,	end docs	[Spton+5]	v IPv4 CIDR	AlterNetworksbook.com 0 to 10 C	Actions Create subsect Available IPv4 addresses
DHCP Options Sets Eastic IPs Services V D New VPC Experience Net as what you fire: VPC Dashboard EC2 Global View rear- Timer by VPC: Q Select a VPC	4	Sub Q	nets (5) toto Filter subnets Name ♥ -	Q Search for serv Subnet ID subnet-06449;	ices, feitures, men v sab05711b32c	selphace products. State Ø Available	end docs v V	[005600+60] PC pc-09c4da8097c83dcf6 [ca	♥ IPv4 CIDR pl 10.10.5.0/25	2 2	Actions V Crasts submet Actions V Crasts submet (1) (V Arailable IPv4 addresses 123
HCP Options Sets lastic IPs Services V New VPC Experience he is and you may VPC Dashboard EC2 Global View may littler by VPC: Q Select a VPC	4	Sub Q	nets (5) todo Filter subvets Name ♥ -	Q. Search for som Subnet ID subnet-06449, subnet-0672ba	van fastures men v sab05711b32c bd29c0f6d03	stentice products State @ Available @ Available	and docs V V V V V	Ucclum+0) PC pc-09c4da8097c83dcf6 ca pc-074162198620dfc64 D	 ✓ IPv4 CIDR pl 10.10.5.0/25 ef 172.31.0.0/20 		Actions V Creatone V Report Actions V Create subset (1) (V Arailable IPv4 addresses 123 4091
HCP Options Sets lastic IPs MCC Experience New VPC Experience VPC Dashboard EC2 Global View New Ret by VPC: Q Belect a VPC VINTUAL PPI/VATE CLOUD	4	Sub	nets (5) tote Filter subvets Name V - -	Q Search for sen Subnet ID subnet-06489 subnet-06489	aabo5711b32c bd29c0f6d03 8b21f1c1d83	State	and doos V V V V V V V	(0)5001+0] PC pc-09c4da8097c83dcf5 [caj pc-074162198b20dfc64 [D pc-074162198b20dfc64 [D	 ✓ IPv4 CIDR pl 10.10.5.0/25 ef 172.31.16.0/20 	Extension control and a local Torrest of the local Torrest	Actions Constrained Constrai
HCP Options Sets Isatic Pis Service: Viol Experience bit a viol po this VPC Dashboard EC2 Slobal View New Het by VPC: Q Select a VPC VIIITUAL PRIVATE CLOUD Thus VPCs	•	Sub (4) (5) (5) (5) (5) (5) (5) (5) (5	nets (5) toto Filter subsets Name V - - subset-{10.10.1.16	Q Search for ten Subnet ID subnet-06489 subnet-072ba subnet-0abchd subnet-056b9	v aab05711b32c bd29c0f6d03 8b21f1c1d83 s57c905d0c32	State Available Available Available Available	and doos	COSISCIPACIÓN COSISCIPACIÓN PC PC PC-09C46480097c83dcf6 ca pc-074152198b20dcf64 D pc-041014922dc8638 cc	 ♥ IPv4 CIDR pk 10.10.5.0/25 ef 172.31.0.0/20 ef 172.31.16.0/20 m 10.10.1.16/28 	abrevieweeksbookson 0 to 10 0	Actions Create subsect Create subsect Actions Actions
DHCP Options Sets Eartic Pile D New YOC Experiment Into a role run man Ver C Experiment EC2 Global View run Clobal Ver C Experiment CLOBA Ver VPCs Setters CLOBA Ver VPCs Setters CLOBA Ver VPCs Setters Clobal Setters Clobal Ver VPCs Setters Clobal Seters Clobal Setters Clobal Setters Clobal Setters	•	Sub (4) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4	nets (5) take Filter salvets Name $@$ - - - - - - - - - - - - -	Subnet ID subnet-06c49, subnet-0ac649, subnet-03c699 subnet-03c699	vda felikova red aabo5711b32c bd29c0f6d03 bd29c0f6d03 b57c905d0c32 v0c69ef58af7	State Available Available Available Available Available	and does ज V भ भ भ भ भ भ	PC pc-0944a8097c83dcf6 ca pc-074162198b20dr64 Da pc-074162198b20dr64 Da pc-074162198b20dr64 Da pc-041014922def6431 ca	 ✓ IPv4 CIDR pl 10.10.5.0/25 ef 172.31.0.0/20 ef 10.10.16/28 e 10.10.1/28 	Extension Extension The CODE	Actions V Creatonie V Record Actions V Create subsect (1) (V Arealiable IPv4 addresses 123 4091 10 10
DHCP Options Sets Bastic IPs Deve VPC Experience Market options Deve VPC Experience Deve	4	Sub	nets (5) into Filter subsets - - subset-{10.10.1.16 subset-{10.10.1.16	G. Saaroh Korsan Subnet ID subnet-06449; subnet-06449; subnet-0abcfd subnet-0abcfd subnet-0a18af	0001 0011000 (voi aab005711b32c bd29c0f6d03 ab21f1c1d83 s57c905d0c32 00c69ef58ar7	State Available Available Available Available	জন্ব বিহুৱা জন্ম ম ম ম ম ম ম ম ম ম ম ম ম ম ম ম ম ম ম	PC pc-09-64a8097c83dcf6 [ca pc-09-64a8097c83dcf6] ca pc-074162198b20dr6d4 [D pc-074162198b20dr6d4] D pc-074162198b20dr6d4] D pc-074162198b20dr6d8] [ca	 ✓ IPv4 CIDR pl 10.10.5.0/25 ef 172.31.16.0/20 ef 10.10.1.16/28 ef 10.10.1.0/28 	♦ Extension control to the total of total o	Actions V Create subset Actions V Create subset (1) (Arailable IP4 addresset 123 4091 4091 10 10

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

> [CloudFormation] エリアに移動し、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller スタックの横にある丸をクリックし、[更新(Update)]をクリックします。

CloudFormation > Stacks					
Stacks (1)				C Delete Update Stack action	ns 🔻 Create stack 🔻
Q, Filter by stack name			Active	View nested	< 1 > @
Stack name	Status	Created time	Ψ.	Description	
O capic-1	CREATE_COMPLETE	2021-09-08 18:36:10 UTC-0700		This template creates the environment to launch a cloud environment.	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 R	ie that contains configuration information at	bout the AWS resources you want to include in the stack.
Configure stack options	O Use current template	Replace current template	Edit template in designer
Step 4	•		

[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、#unique_68 unique_68_Connect_42_step_ayv_tsz_yrb 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 dacs.	[Option+S]	م admin/vemovva@v
		pExtNw	0.0.0.0/0	
		pFabricName	Cloud-APIC	
		pInfraVPCPool	10.10.1.0/24	
		pinstanceType	m5.2xlarge	
		pKeyName	case-ssh-key-2	
		pPassword	Use existing value	
		Tags (1)		
		Tags (1)		
		Q Search togs		
		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。

Services V	Q. Search for services, featu	res, marketplace products, and docs [Option+5]	مل admin/vemovv	ağıcısco.com (8 9210-0878-1758 🔻 N. California 🔻 Support 👻		
CloudFormation \times	CloudFormation > Stacks > capic-1					
Stacks Stack details	🖸 Stacks (1)	capic-1	Delete	Update Stack actions V Create stack V		
Drifts	Q Filter by stack name	Stack info Events Resources Outputs Parameters Template Change sets				
StackSets Exports	Active v View nested	Fvents (82)				
Designer	Capic-1 2021-09-08 18:56:10 UTC-0700 ⊘ UPOATE_COMPLETE	Q. Search events		©		
		Timestamp V Logical ID	Status	Status reason		
Registry Dublic 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	O DELETE_IN_PROGRESS			
		2021-09-08 19:03:20 UTC-0700 capic-1	UPDATE_COMPLETE_CLE ANUP_IN_PROGRESS			
Fredhade		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 Cisco Cloud Network Controller VM を作成します。
- •スタック更新の一環として、古い Cisco Cloud Network Controller VM の削除が試みられます。ただし、これは手動ですでに削除されています。
- Cisco Cloud Network Controller はスタックにポストされます。
- 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。
 - Cisco Cloud Network Controller インスタンスは新しいインスタンス ID を取得し、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。
 - Cisco Cloud Network Controller の管理 IP アドレスも同じです。
- ステップ12 約5~10分経過したら、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller にログインします。
 リリース 25.0(3) 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** 古い Cisco Cloud Services Router 1000v への CCR ダウングレードをトリガーします。

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

ダウングレードが完了すると、システムは CCR と Cisco Cloud Network Controller との互換性がなくなったことを認識します。CCR と Cisco Cloud Network Controller に互換性がなく、Cisco Cloud Network Controller

用に構成された新しいポリシーは、CCRをダウングレードするまでCCRに適用されないことを示すメッ セージが表示されます。

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

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

[オペレーション(Operations)] > [ファームウェア管理]

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

- **ステップ14** 既存設定のバックアップ (7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 Network Controller GUIで、[インフラストラクチャ(Infrastructure)] > [システム設定 (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(7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15** リリース25.0(3)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構成をインポートし、以前の構成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 CCR の作成が自動的に開始されます。

ステップ16 サイトが ACI マルチサイト オーケストレータ/Nexus Dashboard Orchestrator によって管理されている場合 は、新しい Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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(11ページ)を参照 してください。

CCRのアップグレードのトリガー

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

CCRのアップグレードのトリガー

Cisco Cloud Network Controller のアップグレードとは関係なく、CCR のアップグレードをトリ ガーし、それら CCR のアップグレードをモニタできます。これにより、管理プレーン(Cisco Cloud APIC)とデータプレーン(CCR)のアップグレードを分離できるため、トラフィック不 足を抑えるのに役立ちます。 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 Network Controller へのアップグレードをトリガーした後に CCR へのアップグレードをトリガーするこ とです。この機能を有効にすると、無効にすることはできません。

この機能を有効にすると、Cisco Cloud Network Controller と CCR の固有アップグレードシーケンスは次のようになります。

- (注) 次に、CCRへのアップグレードをトリガーするための全体的なプロセスを説明する上位レベルの手順を示します。具体的な手順については、を参照してください。Cisco Cloud Network Controller GUI を使用した CCR のアップグレードのトリガー
 - 1. この章の手順に従って Cisco Cloud Network Controller をアップグレードします。
 - Cisco Cloud Network Controller のアップグレード手順が完了するまで待ちます。アップグレードが完了すると、システムは CCR と Cisco Cloud Network Controller との互換性がなくなったことを認識します。CCR と Cisco Cloud Network Controller に互換性がなく、Cisco Cloud Network Controller 用に構成された新しいポリシーは、CCR をアップグレードするまで CCR に適用されないことを示すメッセージが表示されます。
 - 3. AWS ポータルで CCR の利用規約を確認し、同意します。
 - CSR のアップグレードをトリガーして、Cisco Cloud Network Controller との互換性のある バージョンになるようにします。

次の2つの方法のいずれかを使用して、CCR アップグレードのトリガー プロセスを開始 できます。

- ・画面上部のバナーで、[CCRのアップグレード(Upgrade CCRs)]リンクをクリックします。
- •[ファームウェアの管理(Firmware Management)]ページの[CCR] 領域を使用しま す。次の順に選択:

[オペレーション(Operations)] > [ファームウェア管理]

また、REST APIを使用して CCR のアップグレードをトリガーすることもできます。手順については、REST APIを使用した CCR のアップグレードのトリガー (37 ページ) を参照してください。

ガイドラインと制約事項

 Cisco Cloud Network Controller をアップグレードした後も、CCR と Cisco Cloud Network Controller に互換性がないというメッセージが表示されない場合は、そのメッセージを表示するためにブラウザを更新する必要があるでしょう。

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

- Cisco Cloud Network Controller をアップグレードした後で、CCR へのアップグレードをトリガーします。Cisco Cloud Network Controller をアップグレードする前に、CCR へのアップグレードをトリガーしないでください。
- CCR へのアップグレードをトリガーすると、停止することはできません。
- CCRへのアップグレードをトリガーした後にエラーが表示された場合は、それらのエラー を確認して解決します。これらの CCR アップグレードエラーが解決されると、CCR アッ プグレードが自動的に続行されます。

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、「CCR のアップグレードのト リガー (34 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 CCR のアップグレードのトリガー

このセクションでは、REST APIを使用した CCR へのアップグレードをトリガーする方法を示します。詳細については、CCR のアップグレードのトリガー (34 ページ)を参照してください。

クラウドテンプレートで routerUpgrade フィールドの値を「true」に設定し、REST APIを介して CCR への アップグレードをトリガーします (routerUpgrade = "true")。

```
<polUni>
<fvTenant name="infra">
   <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
       <cloudtemplateProfile name="defaultxyz" routerUsername="SomeFirstName"
routerPassword="SomePass" routerUpgrade="true">
        </cloudtemplateProfile>
        <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
        <cloudtemplateIntNetwork name="default">
            <cloudRegionName provider="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>
```

I

REST API を使用した CCR のアップグレードのトリガー

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。