CMXハイアベイラビリティの設定

内容

概要

このドキュメントでは、Cisco Connected Mobile Experiences(CMX)の基本とその設定方法について説明します。ハイアベイラビリティの有効化、ワイヤレスLANコントローラ(WLC)の追加、フェールオーバー/フェールバックによるハイアベイラビリティ(HA)設定の検証に役立つテストの実施方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CMX
- Cisco WLC

注：HAには、ワイヤレスLANコントローラに固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CMX 10.6
- WLC 8.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

アーキテクチャ

HAシステムの中心的なコンポーネントは、ヘルスモニタです。HAセットアップの設定、管理、監視を行います。監視を維持するための主モードは、プライマリとセカンダリの間のハートビートを通ります。ヘルスモニタは、データベース(DB)とファイルレプリケーションをセットアップし、次にアプリケーションをモニタします。HAパラダイム下のCMXは、プライマリまたはセカンダリとして定義できます。外部との通信(Network Mobility Services Protocol(NMSP)およびサードパーティのエンドポイントおよびPrime Infrastructure(PI)からのAPIコールは、仮想IPアドレスを介して行われます。そのため、プライマリに障害が発生してセカンダリが引き継ぐと、仮想IPが透過的に切り替わります。

この設計では、HAペアを設定およびモニタするために、ユーザインターフェイス(UI)が提供されます。CMXおよびCMX外部に対してアラームが生成されます。

DBは、データを失うことなく常にリアルタイムで複製する必要があるシステムのコアと見なされます。DB外のアプリケーションデータは重要ですが、リアルタイムで同期する必要はなく、機能が失われることもありません。

Network Infrastructure

プライマリとセカンダリは、各システム間で到達可能である必要があります。プライマリとセカンダリの両方が同じサブネット上にある必要があります。これは、使用する仮想IPアドレスをいずれかのシステムに切り替えるために必要です。プライマリから到達可能なワイヤレスLANコントローラなどのエンティティも、セカンダリから到達可能である必要があります。セカンダリ同期とフェールオーバーが正常に動作するには、ネットワークインフラストラクチャでこれらのポートのトラフィックがプライマリとセカンダリの間を流れるようにする必要があります。ポートはCMX上で開かれますが、CMX上のファイアウォールは、他のピアシステムがこれらのポート上でトラフィックを送信することのみを許可します。

ポート	説明
6378、6379、6380、6381、6382、6383、6385、16378、16379、16380、16381、16 382、16383、16385	レディス
7000、7001、9042	Cassandraデータベース
5432	Postgresデータベース
4242	高可用性RESTおよびWebサービス
22	サーバ間でファイルを同期するために使用されるSSHポート

仮想IP

HAシステムが確立されている状態で、フェールオーバーの後、ユーザをセカンダリで実行されている新しいCMXインスタンスにリダイレクトする必要があります。ネットワーク接続の観点から

透過的なフェールオーバーを維持するために、仮想IP(VIP)の概念が使用されます。プライマリとセカンダリの両方が同じサブネットにある場合、VIPアドレスマッピングが使用されます。この設定では、外部システムがVIPに公開されます。このVIPは、実行中のプライマリCMXの実際のIPにマッピングされます。フェールオーバーが発生すると、VIPはセカンダリCMXのアドレスに再マップされます。これらはすべて、人間の介入なしに自動的に行われます。

仮想IPを使用することは必須ではありません。実際、CMXレイヤ3ハイアベイラビリティ（つまり、異なるサブネットに2台のサーバがある）を実行している場合は、仮想IPを使用できません。仮想IPは、IT管理者（またはPrime Infrastructure/Cisco DNA Center）がフェールオーバーやフェールバックに関係なくCMXを管理するための一意のIPを提供します。ただし、WLCには、現在アクティブなCMX物理IPアドレスに対してのみNMSPトンネルがあります。

ステップ1:Webインターフェイスのインストール

プライマリインストール：

https://cmx_ip_address:1984/にログインしてCMXを通常インストール**します**。Webインストーラで、PresenceまたはLocationのノードタイプを選択します。このタイプのインストールでは、ノードタイプをプライマリとして指定する必要はありません。これは、図に示すように、プライマリとして実行できるスタンドアロンサーバと見なされます。

セカンダリインストール：

Webインストーラでノードタイプを選択する必要があるまで、CMX(https://cmx_ip_address:1984/)を通常どおりインストールします。セカンダリには3つ目のオプションがあります。このオプションを選択すると、システムはセカンダリとして設定され、CMX High Availability Adminインターフェイスへのリンクが提供されます。

CMX High Availability Admin WebインターフェイスはCMXポート4242で動作し、次のようにアクセスできます。https://cmx_ip_address:4242/ **にアクセスしてください。**userid cmxadminと、インストール時に設定したパスワードを使用してHA Webインターフェイスにログインします。ログインすると、ユーザインターフェイスのステータスと設定情報が表示されます。ロールは、システムのセカンダリとして表示されます。

ステップ2:HAの有効化

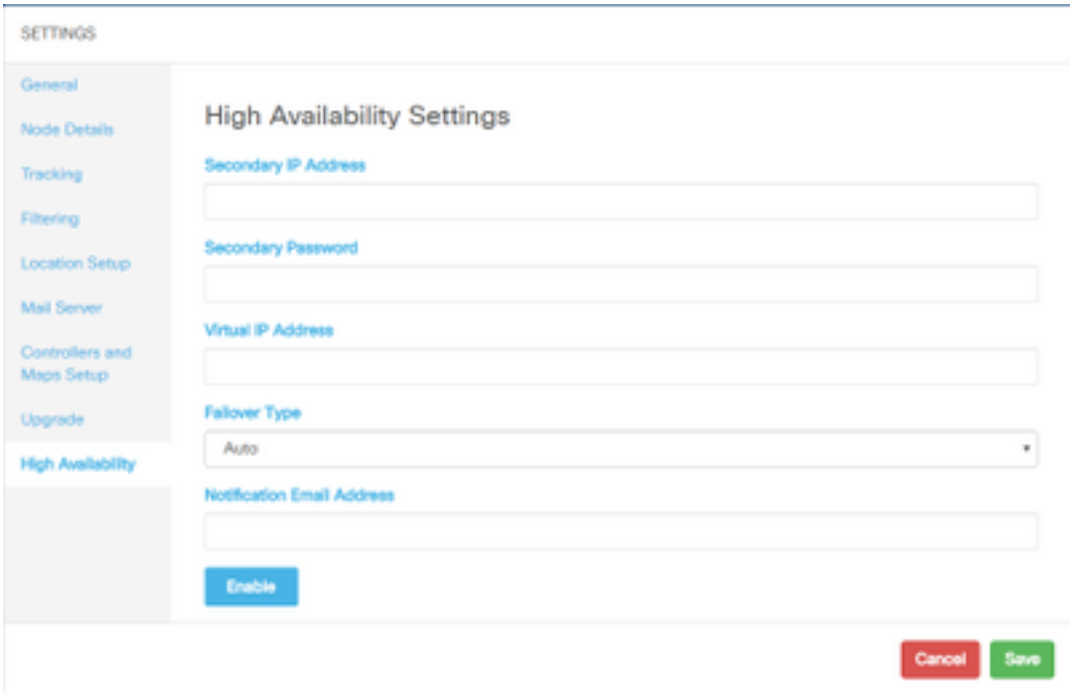
プライマリおよびセカンダリサーバが準備されると、HAを有効にできます。HAは、CMX Webインターフェイスまたは**CMX**コマンドラインで有効にできます。HAのセットアップに必要なオプションは次のとおりです。

- セカンダリIPアドレス
- セカンダリパスワード：セカンダリサーバの**cmxadmin**アカウントのパスワード
- VIP Address:アクティブサーバで使用されるVIPアドレス
- フェールオーバータイプ：自動フェールオーバーにより、重大な問題が検出されると、CMXはセカンダリサーバに自動的にフェールオーバーできます。手動フェールオーバーでは、Webインターフェイスまたはコマンドラインからフェールオーバーを開始する必要があります。この障害は通知によってユーザに報告されますが、手動フェールオーバーに対するアクションは実行されません
- 通知電子メールアドレス：HA情報または問題に関する通知を送信する電子メールアドレス。HAに使用される電子メール設定は、CMXと同じです。電子メールサーバが設定されていない場合でも、このフィールドは必須です。電子メール通知を使用しない場合は、ダミーの電子メールアドレスを自由に入力し、[enable]をクリックしてください。

HA Webの設定：

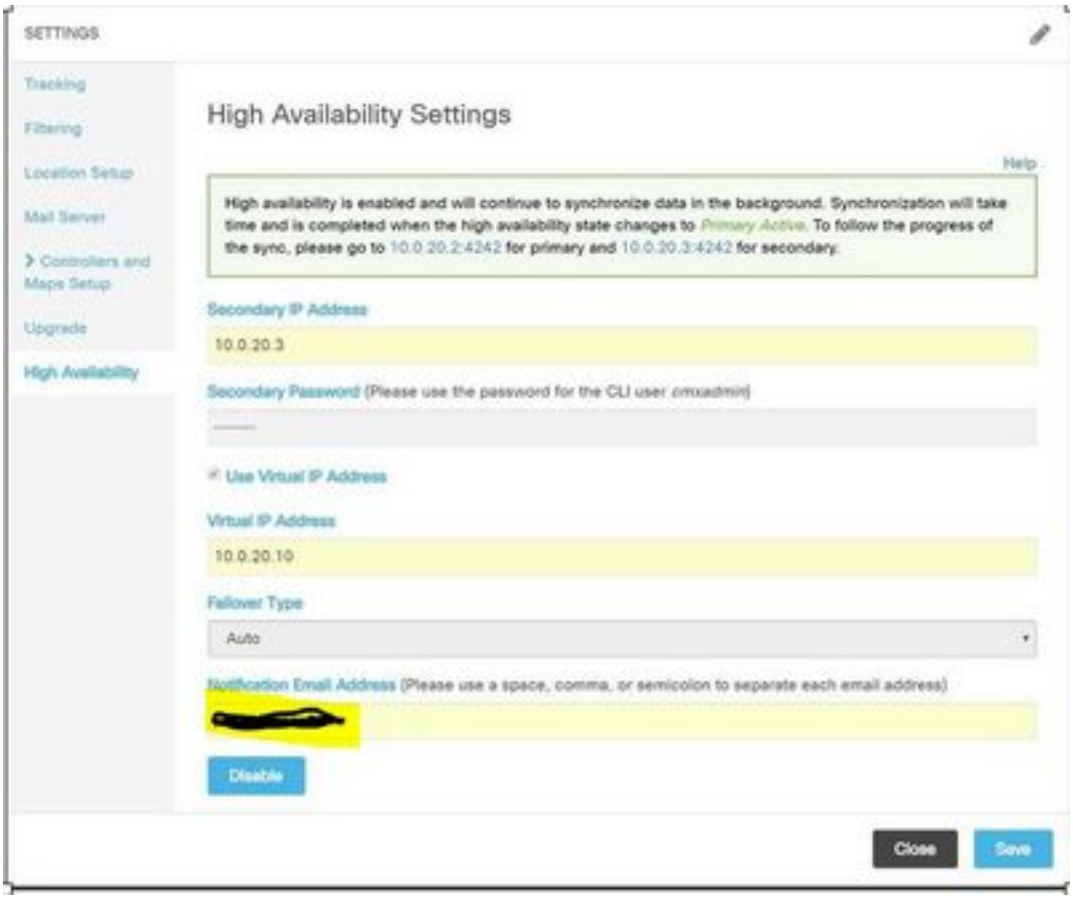
CMXで、[システム]タブに移動し、**[設**定]アイコンを**クリックします**。これにより、CMXのさまざまな設定を含むモーダルダイアログが表示されます。HAを有効にするために必要なオプションを表示するには、HAオプションを選択します。通知電子メールアドレス通知を受け取る場所を指定できます。

HAの有効化を開始するためにすべてのオプションが提供されたら、[**Enable**]ボタンをクリックします。



CMXはHA設定を確認し、プライマリとセカンダリの間のHAの有効化を開始します。設定が正常に開始されると、webUIが戻ります。

CMXの設定ページで「ハイアベイラビリティ」テーブルの存在をチェックして、設定が正しく、同期が行われていることを確認します。そのようなテーブルがなく、HA設定セクションに戻ると、すべての設定フィールドが空の場合、情報が間違っているか、正しくありません。

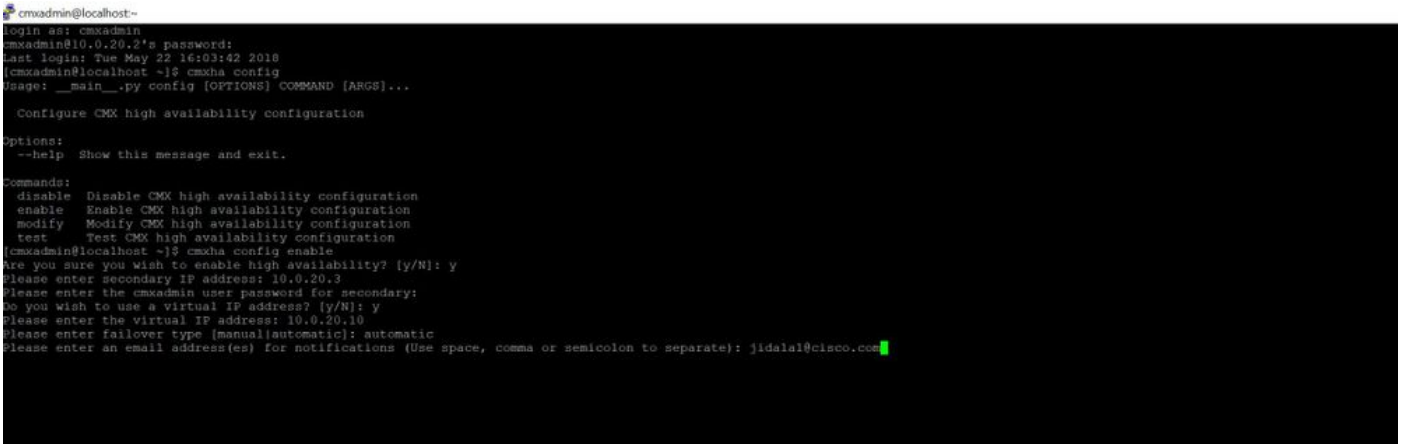


ただし、HAの有効化は完了していません。プライマリとセカンダリのサーバ間のすべてのデータの初期同期は、完了までに多大な時間がかかる場合があります。同期の実行中は、ユーザーインターフェイスに[プライマリ同期]と表示されます。

同期が正常に完了すると、プライマリ上のサーバはPrimary Active状態になります。

完了すると、情報アラートがCMXで生成されます。さらに、システムがアクティブで、同期が適切であることを示す電子メールアラートが送信されます。

ハイアベイラビリティCLIの有効化（参照用）:

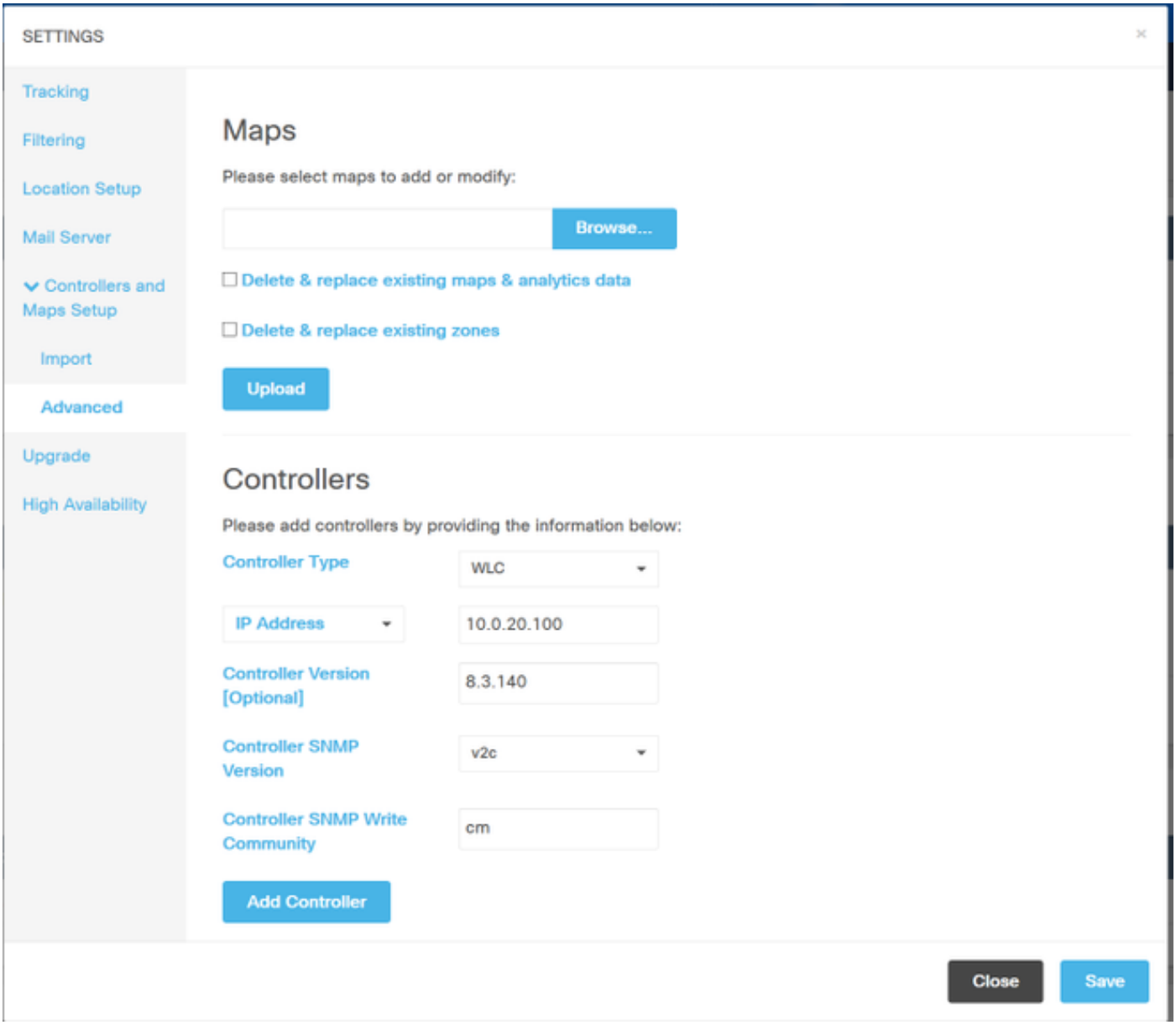


ステップ3:CMXへのCisco WLCの追加

Cisco WLCは、CLIまたはCMXユーザインターフェイス、またはPrime Infrastructureを使用して追加できます。この実習では、CMX WebUIを使用して直接追加できます。

コントローラの設定は、NMSP接続が正しくないと機能しません。ただし、コントローラが正常に追加されても、接続が機能しない場合があります。

プライマリCMXサーバhttps://cmx_ip_address/に**移動します**。[システム]タブ**> [設定]アイコン> [左メニュー]をクリックします。**



Cisco WLCを追加した後、コントローラのステータスがupで実行中であることを確認する必要があります。

ユーザインターフェイスを使用してコントローラのステータスを確認するには、[System]タブに移動する必要があります。コントローラのリストがタブに表示され、新しいコントローラが緑色で表示されます。

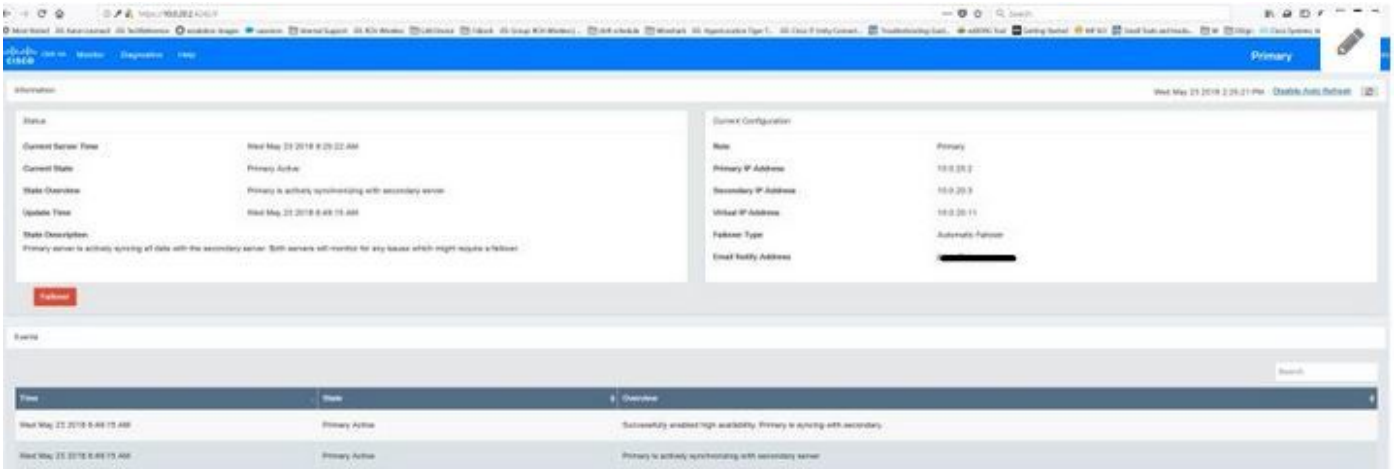
ステップ4：フェールオーバー

フェールオーバープロセスには、プライマリがダウンした場合のセカンダリCMXへのオペレーションの転送が含まれます。フェールオーバーは、CMXがプライマリサーバの問題を検出すると自動的に発生する可能性があります。フェールオーバーは、Webユーザインターフェイスまたはコマンドラインのユーザが手動で実行できます。フェールオーバーの進行状況は、各システムの現在の状態に基づいて監視できます。

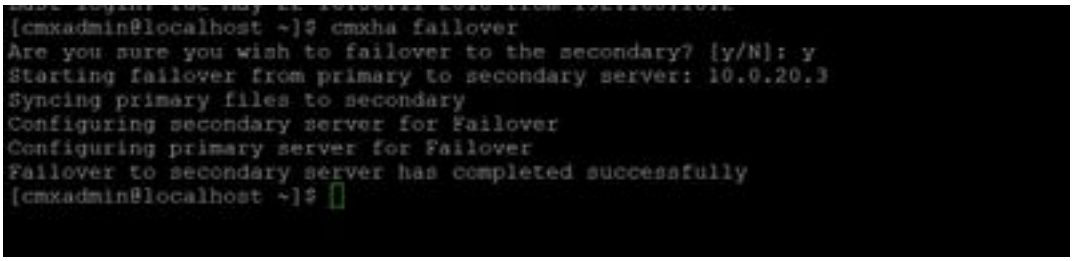
フェールオーバープロセスは、ユーザが手動で開始できます。フェールオーバーは、CMXハイアベイラビリティWebインターフェイスまたはCMXコマンドラインで実行できます。

手動フェールオーバーWeb:

プライマリまたはセカンダリ(https://server_ip:4242)のCMX HA Webインターフェイス**にログインします。** サーバーがアクティブに同期している場合は、モニターページに[フェールオーバー]というボタンが表示されます。右端で自動更新を**有効にします。**



手動フェイルオーバーCLI（参照用）:



ステップ5：フェールバック

セカンダリでCMXを実行するには、プライマリ障害の根本原因が特定されるまで、一時的な状況と見なす必要があります。プライマリボックスが復元された（または新しいボックスが提供された）後、フェールバックプロセスを開始する必要があります。もう1つのオプションは、システムをプライマリに変換し、もう一方のシステムをセカンダリサーバに置き換えるか、変換することです。いずれの場合も、HAがセカンダリサーバと同期しなくなるため、サーバをできるだけ早く使用可能にする必要があります。

フェールバックプロセスは、ユーザが手動で実行する必要があります。フェールバックは、CMX HA WebインターフェイスまたはCMXコマンドラインで実行できます。

手動フェールバックWeb:

プライマリまたはセカンダリ(https://server_ip:4242)のCMX HA Webインターフェイス**にログインします。** 両方のサーバがフェールオーバーがアクティブであることを示している場合は、モニタページに[フェールバック(Failback)]というボタンが表示されます。

手動フェールバックGUI:

ステップ6:HAのアップグレード/無効化

CMXの現在の形式では、アップグレードを実行するためにHAを無効にする必要があります。コマンドラインからHAを無効にするには、プライマリCMXから**cmxha config disable**を実行します

アップグレードの前にHAを中断することを忘れた場合は、アップグレードスクリプトによって通知されます。HAを改革する前に、セカンダリCMXサーバを別々にアップグレードする必要があります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

HAには、この機能のオンラインヘルプがあります。ヘルプは完全に表示され、機能の概要と詳細が表示されます。https://cmx_ip_address:4242/helpからアクセスできます。

CMX HAのコマンドリファレンス：https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-3/cmx_command/cmxcli103/cmxcli10-3_chapter_010.pdf

tarログから確認するバンドルファイル：

- cmx-hafile-sync
- cmx-haweb-service

- cmx-haserver