

# CMXハイアベイラビリティの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[アーキテクチャ](#)

[Network Infrastructure](#)

[仮想IP](#)

[ステップ1:Webインターフェイスのインストール](#)

[ステップ2:HAの有効化](#)

[ステップ 3 : CMXへのCisco WLCの追加](#)

[ステップ 4 : フェールオーバー](#)

[ステップ 5 : フェールバック](#)

[手順 6 : HAのアップグレード/無効化](#)

[CMX HAペアを安全にリロードする方法](#)

[確認](#)

[トラブルシューティング](#)

---

## はじめに

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。

## 前提条件

このドキュメントでは、ハイアベイラビリティ(HA)をイネーブルにし、ワイヤレスLANコントローラ(WLC)を追加し、フェールオーバー/フェールバックを使用してハイアベイラビリティ(HA)設定を確認するのに役立つテストを実行する方法について説明します。

## 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コントローラに関する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、クリアな（デフォルト）設定で作業を開始しています。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システムの主要コンポーネントはヘルスマニタです。HAセットアップを設定、管理、およびモニタします。ビジルを維持するための主要なモードは、プライマリとセカンダリの間のハートビートを通じて行われます。ヘルスマニタは、データベース(DB)とファイルレプリケーションを設定し、次にアプリケーションをモニタします。HAパラダイムの下の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エンドポイントと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いだ場合、仮想IPはトランスペアレントにスイッチングされます。

この設計では、HAペアを設定および監視するためのユーザインターフェイス(UI)が提供されます。アラームはCMXおよびCMX外で生成されます。

DBはシステムのコアと見なされ、データを損失することなく常にリアルタイムで複製する必要があります。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、使用されている仮想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。セカンダリの同期とフェールオーバーが正しく機能するには、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。CMXはハイアベイラビリティの両方のCMXユニットからのキープアライブをVRRPを使用してチェックし、ハイアベイラビリティペアの間に制限がないようにします。これは、CMXの到達可能性を確立するためにゲートウェイが到達可能である必要があるためです。

ポートはCMXで開かれますが、CMX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、16382、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	SSHポート。サーバ間でファイルを同期するために使用されます。

## 仮想IP

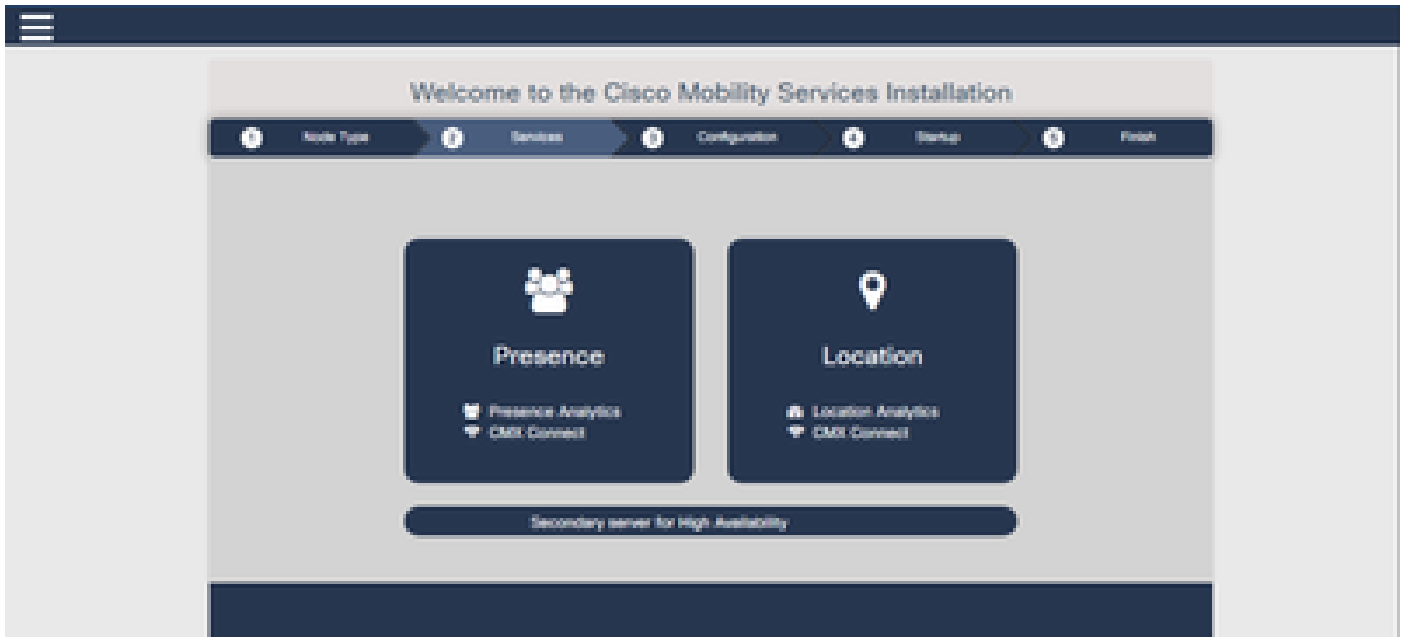
HAシステムが有効な場合、フェールオーバー後に、ユーザはセカンダリ上で稼働する新しいCMXインスタンスにリダイレクトされる必要があります。ネットワーク接続の観点からフェールオーバーを透過的に維持するために、仮想IP(VIP)の概念が使用されます。プライマリとセカンダリの両方が同じサブネットにある場合は、VIPアドレスマッピングが使用されます。この設定では、外部システムはVIPに公開されます。このVIPは、稼働中のプライマリCMXの実際のIPにマッピングされます。フェールオーバーが発生すると、VIPはセカンダリCMXのアドレスに再マッピングされます。これらはすべて、人間の介入なしに自動的に行われます。

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センター)に対して固有のIPを提供し、フェールオーバーやフェールバックに関係なくCMXを管理します。ただし、WLCには、現在アクティブなCMXの物理IPアドレスに向かうNMSPトンネルしかありません。

## 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/](https://cmx_ip_address:1984/)にログインして、CMXを通常どおりインストールします。Webインストーラで、ノードの種類としてプレゼンスまたはロケーションを選択します。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/](https://cmx_ip_address:1984/))を通常どおりインストールします。3番目のオプションは、セカンダリ用に提供されます。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で稼働し、[https://cmx\\_ip\\_address:4242/](https://cmx_ip_address:4242/)からアクセスできます。ユーザID cmxadminを使用してHA Webインターフェイスにログインし、インストール時にパスワードcmxadmin useridを設定します。ログインすると、ユーザインターフェイスに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

プライマリサーバとセカンダリサーバの準備が完了したら、HAを有効にすることができます。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をセットアップするため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：アクティブサーバが使用する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では、重大な問題が検出された場合にCMXがセカンダリサーバに自動的にフェールオーバーします。手動フェールオーバーでは、ユーザは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。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ための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入力して[有効]をクリックしてください。

HA Webの設定：

CMXで、Systemタブに移動し、Settings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。通知メール・アドレス通知を受け取る場所を指定できます。

すべてのオプションが表示されたらEnableボタンをクリックして、HAを有効にします。

SETTINGS

General  
Node Details  
Tracking  
Filtering  
Location Setup  
Mail Server  
Controllers and Maps Setup  
Upgrade  
High Availability

## High Availability Settings

Secondary IP Address

Secondary Password

Virtual IP Address

Fallover Type

Notification Email Address

CMXはHA設定を確認し、プライマリとセカンダリ間のHAを有効にします。webUIは、設定が正常に開始されると戻ります。

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きに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。

SETTINGS

Tracking

Filtering

Location Setup

Mail Server

> Controllers and Maps Setup

Upgrade

High Availability

## High Availability Settings

Help

High availability is enabled and will continue to synchronize data in the background. Synchronization will take time and is completed when the high availability state changes to *Primary Active*. To follow the progress of the sync, please go to 10.0.20.3:4242 for primary and 10.0.20.3:4242 for secondary.

Secondary IP Address

10.0.20.3

Secondary Password (Please use the password for the CLI user cmxadmin)

\_\_\_\_\_

Use Virtual IP Address

Virtual IP Address

10.0.20.10

Falover Type

Auto

Notification Email Address (Please use a space, comma, or semicolon to separate each email address)

\_\_\_\_\_

Disable

Close Save

ただし、HAの有効化は完了していません。プライマリ・サーバとセカンダリ・サーバ間のすべてのデータの初期同期は、完了するまでに非常に長い時間がかかる場合があります。同期が実行されている間、ユーザインターフェイスでは状態がPrimary Syncingと表示されます。

同期が正常に完了すると、プライマリのサーバの状態はPrimary Activeになります。

完了すると、CMXで情報アラートが生成されます。さらに、システムがアクティブで正常に同期してい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) :

```
cmxadmin@localhost:~$
login as: cmxadmin
cmxadmin@10.0.20.2's password:
Last login: Tue May 22 16:03:42 2018
cmxadmin@localhost ~]$ cmxha config
Usage: __main__.py config [OPTIONS] COMMAND [ARGS]...

Configure CMX high availability configuration

Options:
  --help  Show this message and exit.

Commands:
  disable  Disable CMX high availability configuration
  enable   Enable CMX high availability configuration
  modify   Modify CMX high availability configuration
  test     Test CMX high availability configuration
cmxadmin@localhost ~]$ cmxha config enable
Are you sure you wish to enable high availability? [y/N]: y
Please enter secondary IP address: 10.0.20.3
Please enter the cmxadmin user password for secondary:
Do you wish to use a virtual IP address? [y/N]: y
Please enter the virtual IP address: 10.0.20.10
Please enter failover type [manual|automatic]: automatic
Please enter an email address(es) for notifications (Use space, comma or semicolon to separate): jidalal@cisco.com
```

## ステップ 3 : CMXへのCisco WLCの追加

CLIまたはCMXユーザインターフェイスを使用するか、Prime Infrastructureを使用して、Cisco WLCを追加できます。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、コントローラを正常に追加できても、接続が機能しない可能性があります。

プライマリCMXサーバ[https://cmx\\_ip\\_address/](https://cmx_ip_address/)に移動します。Systemタブ> Settings Icon > Left Menuの順にクリックします。



SETTINGS ×

- Tracking
- Filtering
- Location Setup
- Mail Server
- ▼ Controllers and Maps Setup
- Import
- Advanced
- Upgrade
- High Availability

## Maps

Please select maps to add or modify:

- Delete & replace existing maps & analytics data
- Delete & replace existing zones

---

## Controllers

Please add controllers by providing the information below:

Controller Type	WLC
IP Address	10.0.20.100
Controller Version [Optional]	8.3.140
Controller SNMP Version	v2c
Controller SNMP Write Community	cm

Cisco WLCを追加したら、コントローラの状態が稼働しているかどうか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状態を検証するには、Systemタブに移動する必要があります。タブにコントローラリストが表示され、新しいコントローラが緑色で表示されます。

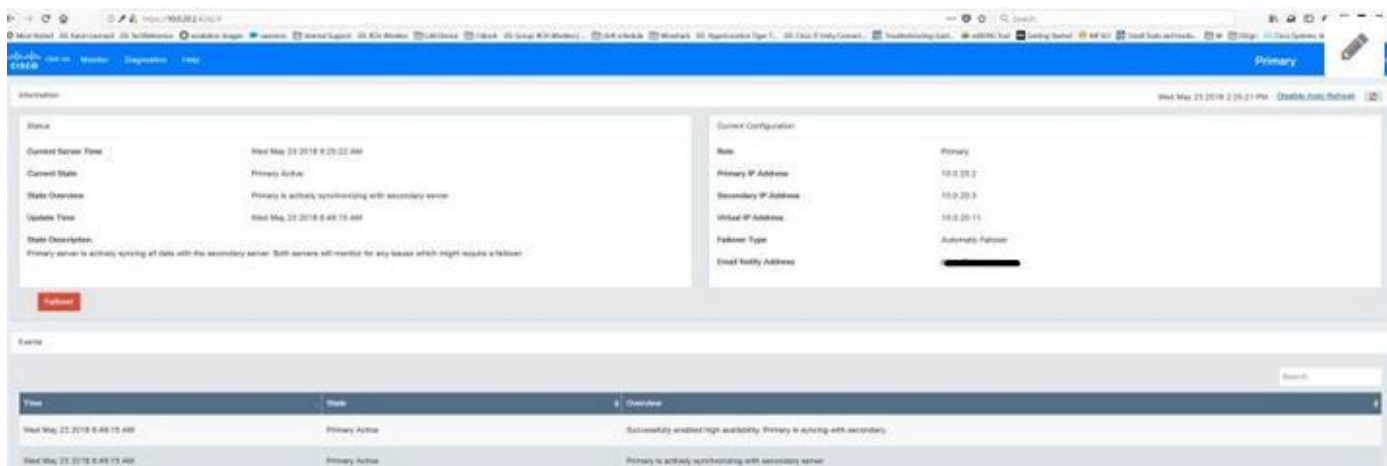
## ステップ 4：フェールオーバー

フェールオーバープロセスでは、プライマリがダウンした場合にセカンダリCMXにオペレーションを転送します。CMXがプライマリサーバの問題を検出すると、フェールオーバーが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で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](https://server_ip:4242))でCMX HA Webインターフェイスにログインします。サーバがアクティブに同期している場合、モニターページには「Failover」というラベルのボタンがあります。右端で、自動更新を有効にします。



手動フェールオーバーCLI ( 参照用 ):

```
[cmxadmin@localhost ~]$ cmxha failover
Are you sure you wish to failover to the secondary? [y/N]: y
Starting failover from primary to secondary server: 10.0.20.3
Syncing primary files to secondary
Configuring secondary server for Failover
Configuring primary server for Failover
Failover to secondary server has completed successfully
[cmxadmin@localhost ~]$
```

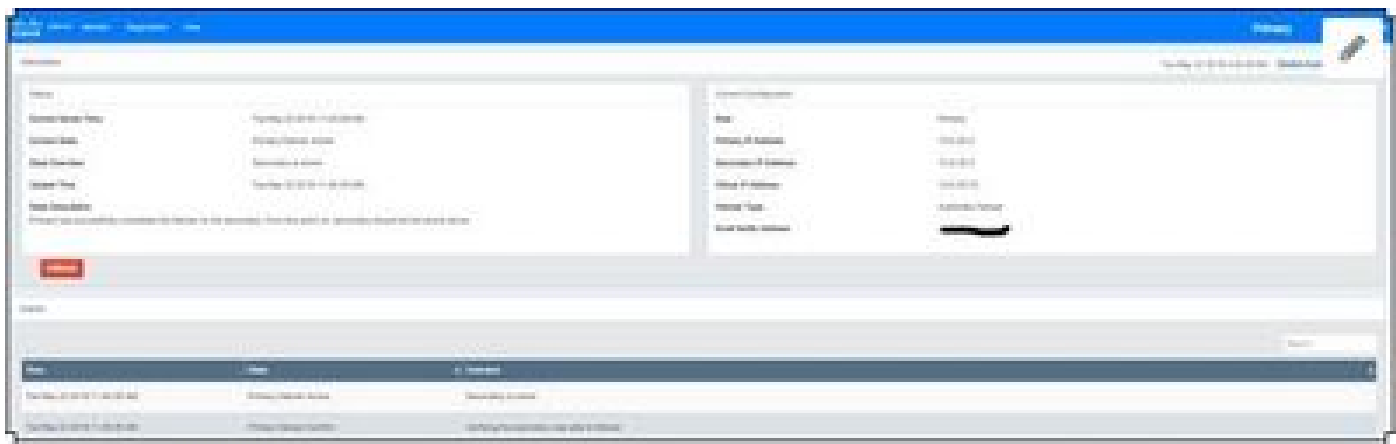
## ステップ 5 : フェールバック

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・ボックスがリストアされた後 ( 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、他のシステムをセカンダリサーバに交換または変換することです。いずれの場合も、HAはセカンダリサーバと同期していないため、サーバはできるだけ早く使用可能にする必要があります。

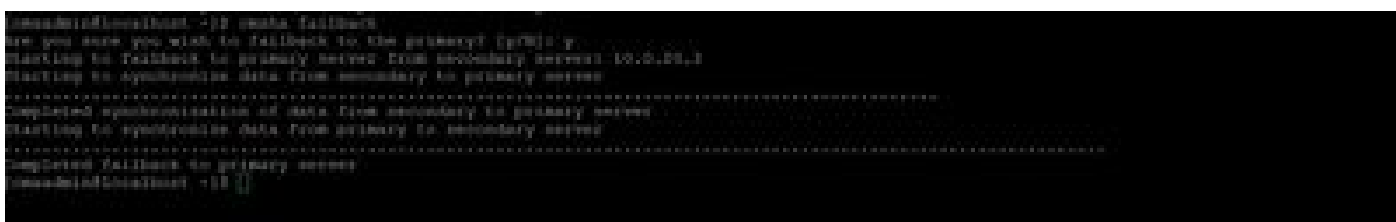
フェールバックプロセスは、ユーザが手動で実行する必要があります。フェールバックは、CMX HA WebインターフェイスまたはCMXコマンドラインで実行できます。

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](https://server_ip:4242))でCMX HA Webインターフェイスにログインします。両方のサーバでフェールオーバーがアクティブであると示されている場合、モニターページには「Failback」というラベルの付いたボタンがあります。

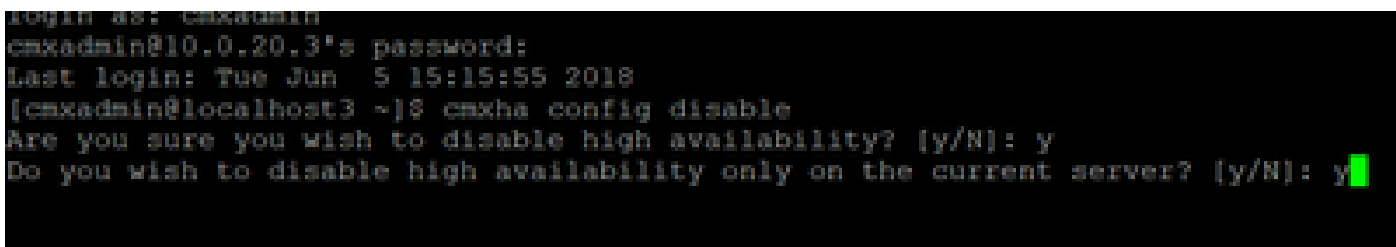


手動フェールバックGUI:



## 手順 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をディセーブルにする必要があります。コマンドラインからHAをディセーブルにするには、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を中断し忘れた場合は、アップグレードスクリプトによって通知されます。HAを変更する前に、セカンダリCMXサーバを個別にアップグレードする必要があります。

## CMX HAペアを安全にリロードする方法

次の手順を実行して、CMX HAペアをリロードします。

- セカンダリCMXの電源をオフにする
- プライマリCMXのリブート
- プライマリCMXが稼働していることを確認します。
- セカンダリCMXの電源投入
- HAステータスの確認 : `cmxha info`

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシューティング

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、機能のオンラインヘルプがあります。のヘルプでは、の機能の概要と詳細について説明しています。[https://cmx\\_ip\\_address:4242/help](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](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 ( 非同期 )
- CMX-HAWEBサービス
- CMXサーバ

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。