Configuration de la haute disponibilité CMX

Table des matières

Introduction

Ce document décrit les bases de Cisco Connected Mobile Experiences (CMX) et comment le configurer.

Conditions préalables

Ce document explique comment activer la haute disponibilité, ajouter un contrôleur LAN sans fil (WLC) et effectuer certains tests qui aident à vérifier la configuration de la haute disponibilité (HA) avec basculement/re-basculement.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CMX
- WLC Cisco

Remarque : la haute disponibilité n'a pas de configuration requise unique pour les contrôleurs LAN sans fil.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMX 10,6
- WLC 8.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Architecture

La composante centrale d'un système haute disponibilité est le moniteur de santé. Il configure, gère et surveille la configuration de la haute disponibilité. Le mode principal pour maintenir la vigilance est par des battements de coeur entre le primaire et secondaire. Le moniteur d'intégrité est chargé de configurer les bases de données (DB) et la réplication de fichiers, puis de surveiller l'application. CMX sous le paradigme HA peut être défini comme primaire ou secondaire. La communication avec le monde extérieur (protocole NMSP (Network Mobility Services Protocol) et appels API provenant de terminaux tiers et de l'infrastructure Prime (IP)) s'effectue via une adresse IP virtuelle. Ainsi, lorsque le primaire tombe en panne et que le secondaire prend le relais, l'IP virtuel est commuté de manière transparente.

La conception prévoit une interface utilisateur (UI) afin de configurer et de surveiller les paires haute disponibilité. Des alarmes sont générées pour CMX et en dehors de CMX.

Les bases de données sont considérées comme le coeur du système qui doit toujours être répliqué en temps réel sans perte de données. Les données d'application qui se trouvent en dehors de la base de données sont critiques, mais ne doivent pas être synchronisées en temps réel et n'entraînent pas de perte de fonctionnalité.

Infrastructure réseau

Le principal et le secondaire doivent être accessibles entre chaque système. Le réseau principal et le réseau secondaire doivent se trouver sur le même sous-réseau. Cette opération est nécessaire pour que l'adresse IP virtuelle utilisée puisse être commutée vers l'un ou l'autre système. Toute entité, telle que les contrôleurs LAN sans fil, accessible depuis le routeur principal doit également être accessible depuis le routeur secondaire. Pour que la synchronisation secondaire et le basculement fonctionnent correctement, l'infrastructure réseau doit permettre à ce trafic de port de circuler entre le port principal et le port secondaire. Le CMX utilise le protocole VRRP pour vérifier le keepalive des deux unités CMX en haute disponibilité, en s'assurant qu'aucune restriction n'existe entre les deux unités de la paire haute disponibilité, car la passerelle doit être accessible pour établir l'accessibilité CMX.

Les ports seront ouverts sur CMX, mais les pare-feu sur CMX permettront uniquement aux autres

systèmes homologues d'envoyer du trafic sur ces ports.

Ports	Description
6378, 6379, 6380, 6381, 6382, 6383, 6385, 16378, 16379, 16380, 16381, 16382, 16383, 16385	Redis
7000, 7001, 9042	base de données Cassandra
5432	base de données Postgres
4242	Service REST et Web haute disponibilité
22	Port SSH et utilisé pour synchroniser les fichiers entre les serveurs

IP virtuelle

Une fois le système haute disponibilité en place, après un basculement, les utilisateurs doivent être redirigés vers la nouvelle instance CMX qui s'exécute sur le serveur secondaire. Afin de maintenir la transparence du basculement du point de vue de la connectivité réseau, le concept d'IP virtuelle (VIP) sera utilisé. Lorsque le principal et le secondaire se trouvent dans le même sous-réseau, un mappage d'adresse VIP est utilisé. Dans cette configuration, les systèmes externes sont exposés à un VIP. Ce VIP est mappé à l'IP réelle du CMX principal en cours d'exécution. Lorsque le basculement se produit, VIP est remappé à l'adresse du CMX secondaire. Tout cela se passe automatiquement sans aucune intervention humaine.

L'utilisation d'une adresse IP virtuelle n'est pas obligatoire. En fait, si vous utilisez la haute disponibilité de couche 3 CMX (c'est-à-dire que les deux serveurs se trouvent dans des sous-réseaux différents), vous ne pouvez pas utiliser une adresse IP virtuelle. L'adresse IP virtuelle fournit une adresse IP unique à l'administrateur informatique (ou Prime Infrastructure/Cisco DNA center) pour gérer le CMX, indépendamment du basculement ou du re-basculement. Les WLC, cependant, ont un tunnel NMSP seulement vers l'adresse IP physique CMX actuellement active.

Étape 1. Installation de l'interface Web

Installation principale :

Installez CMX normalement avec login dans https://cmx_ip_address:1984/. Dans le programme d'installation Web, sélectionnez le type de noeud Présence ou Emplacement. Ce type d'installation ne nécessite pas de spécifier le type de noeud comme principal. Il s'agit d'un serveur autonome pouvant être exécuté en tant que serveur principal, comme illustré dans l'image.

Installation secondaire :

Installez CMX (https://cmx_ip_address:1984/) normalement jusqu'à ce que le type de noeud doive être sélectionné dans le programme d'installation Web. Une troisième option est proposée pour le secondaire. Si vous sélectionnez cette option, le système est configuré en tant que secondaire et fournit un lien vers l'interface d'administration de la haute disponibilité CMX.

L'interface Web d'administration de la haute disponibilité CMX s'exécute sur le port CMX 4242 et est accessible à l'adresse suivante : https://cmx_ip_address:4242/. Connectez-vous à l'interface Web HA avec l'ID d'utilisateur cmxadmin et le mot de passe configuré avec l'ID d'utilisateur cmxadmin au moment de l'installation. Une fois que vous êtes connecté, l'interface utilisateur dispose d'informations d'état et de configuration. Le rôle est affiché comme secondaire pour le système.

Étape 2. Activer HA

La haute disponibilité peut maintenant être activée une fois que les serveurs principal et secondaire ont été préparés. La haute disponibilité peut être activée dans l'interface Web CMX ou sur la ligne de commande CMX. Voici les options requises pour configurer la haute disponibilité :

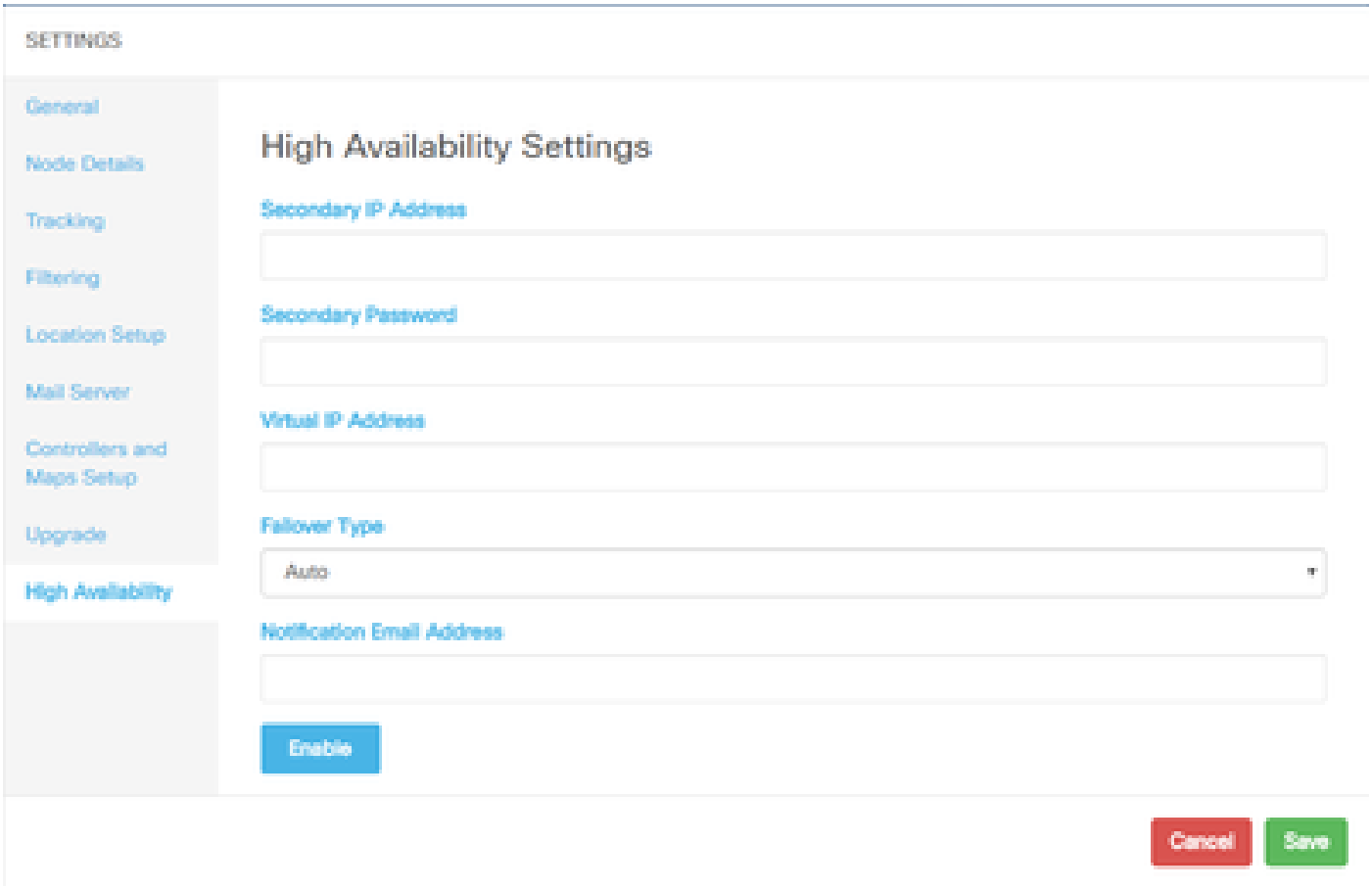
- Adresse IP secondaire
- Secondary Password : mot de passe du compte cmxadmin sur le serveur secondaire
- Adresse VIP : adresse VIP à utiliser par le serveur actif
- Type de basculement : le basculement automatique permet à CMX de basculer automatiquement sur le serveur secondaire lorsqu'un problème grave est détecté. Le basculement manuel nécessite que l'utilisateur lance le basculement à partir de l'interface Web ou de la ligne de commande. La défaillance sera signalée à l'utilisateur via des notifications, mais aucune action n'est entreprise pour le basculement manuel
- Adresse e-mail de notification : adresse e-mail pour envoyer des notifications sur les informations ou les problèmes de haute disponibilité. Les paramètres de messagerie utilisés pour la haute disponibilité sont identiques à ceux de CMX. Ce champ est obligatoire même si aucun serveur de messagerie n'est configuré. N'hésitez pas à saisir une adresse e-mail factice et cliquez sur « activer » si vous n'avez pas l'intention d'utiliser les notifications par e-mail.

Configurer le Web haute disponibilité :

Dans CMX, accédez à l'onglet Système et cliquez sur l'icône Paramètres. Une boîte de dialogue modale s'affiche avec divers paramètres dans CMX. Sélectionnez l'option HA afin d'afficher les options requises pour activer la haute disponibilité. Adresse e-mail de notification que vous pouvez indiquer à l'endroit où vous souhaitez recevoir les notifications.

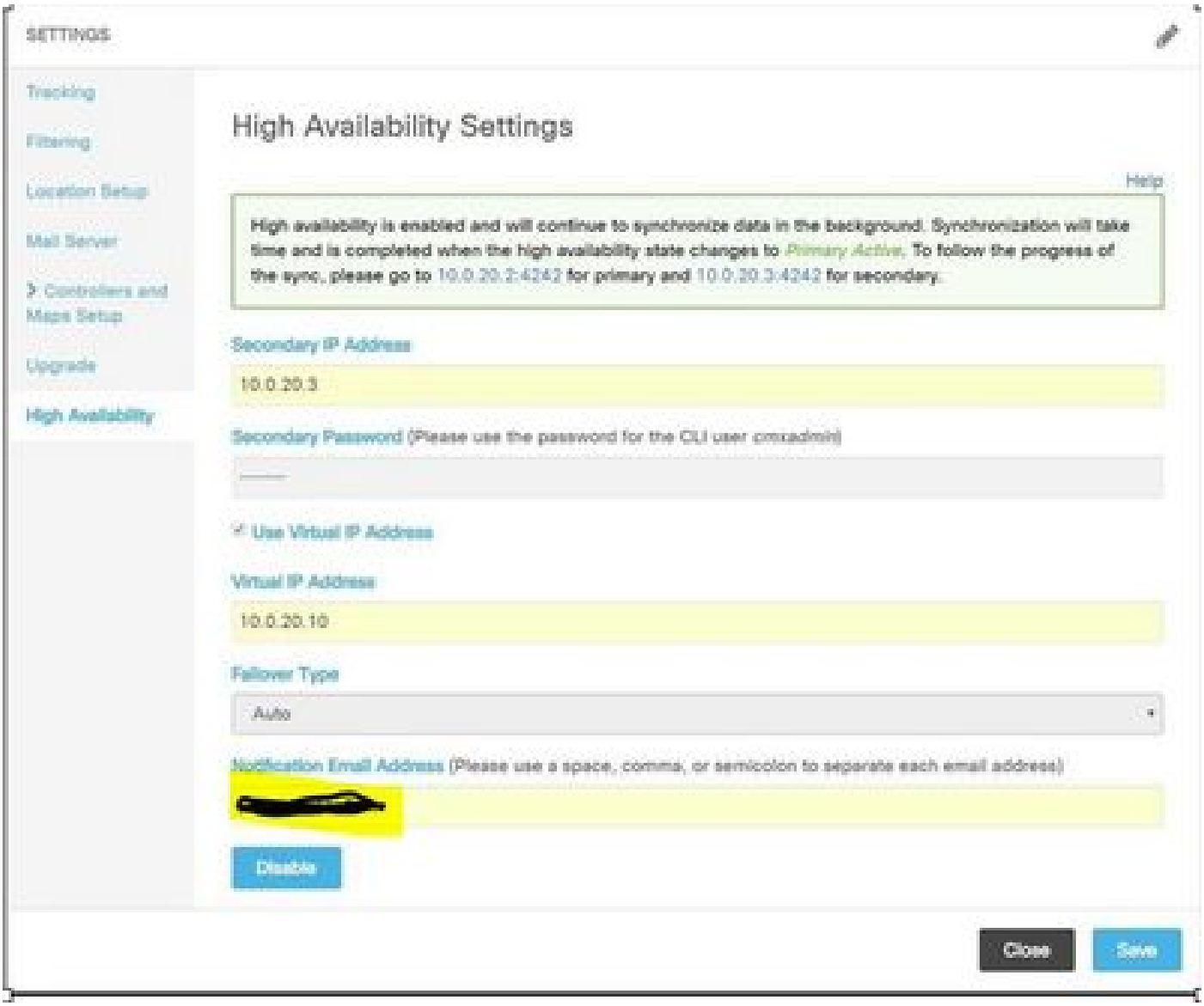
Cliquez sur le bouton Enable lorsque toutes les options sont fournies pour commencer à activer

HA.



CMX vérifiera les paramètres de haute disponibilité et commencera à activer la haute disponibilité entre le principal et le secondaire. L'interface WebUI reviendra lorsque la configuration aura démarré correctement.

Vérifiez que les paramètres sont corrects et que la synchronisation est en cours en vérifiant la présence d'une table « Haute disponibilité » dans la page des paramètres de CMX. S'il n'y a pas de tableau de ce type et que, lorsque vous revenez à la section des paramètres de haute disponibilité, tous les champs de configuration sont vides, les informations étaient erronées ou incorrectes.

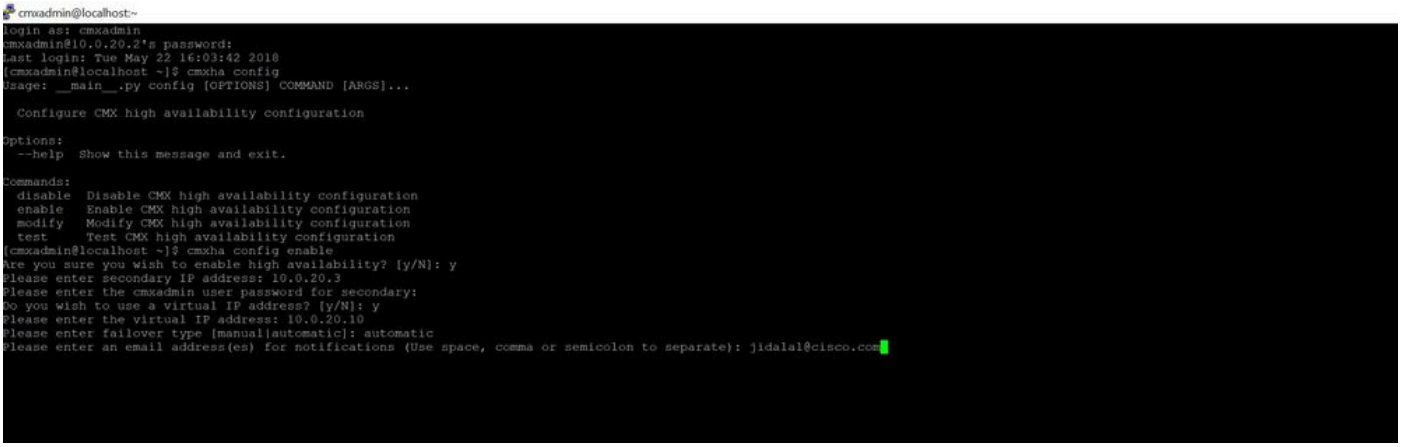


Cependant, la haute disponibilité n'a pas encore été activée. La synchronisation initiale de toutes les données entre le serveur principal et le serveur secondaire peut prendre un temps considérable. L'interface utilisateur indique l'état Synchronisation primaire pendant la synchronisation.

Une fois la synchronisation terminée, le serveur sur le serveur principal passe à l'état Principal actif.

Lorsque vous avez terminé, une alerte d'informations est générée dans CMX. En outre, une alerte par e-mail sera envoyée pour indiquer que le système est actif et qu'il se synchronise correctement.

Activer la CLI haute disponibilité (pour référence) :

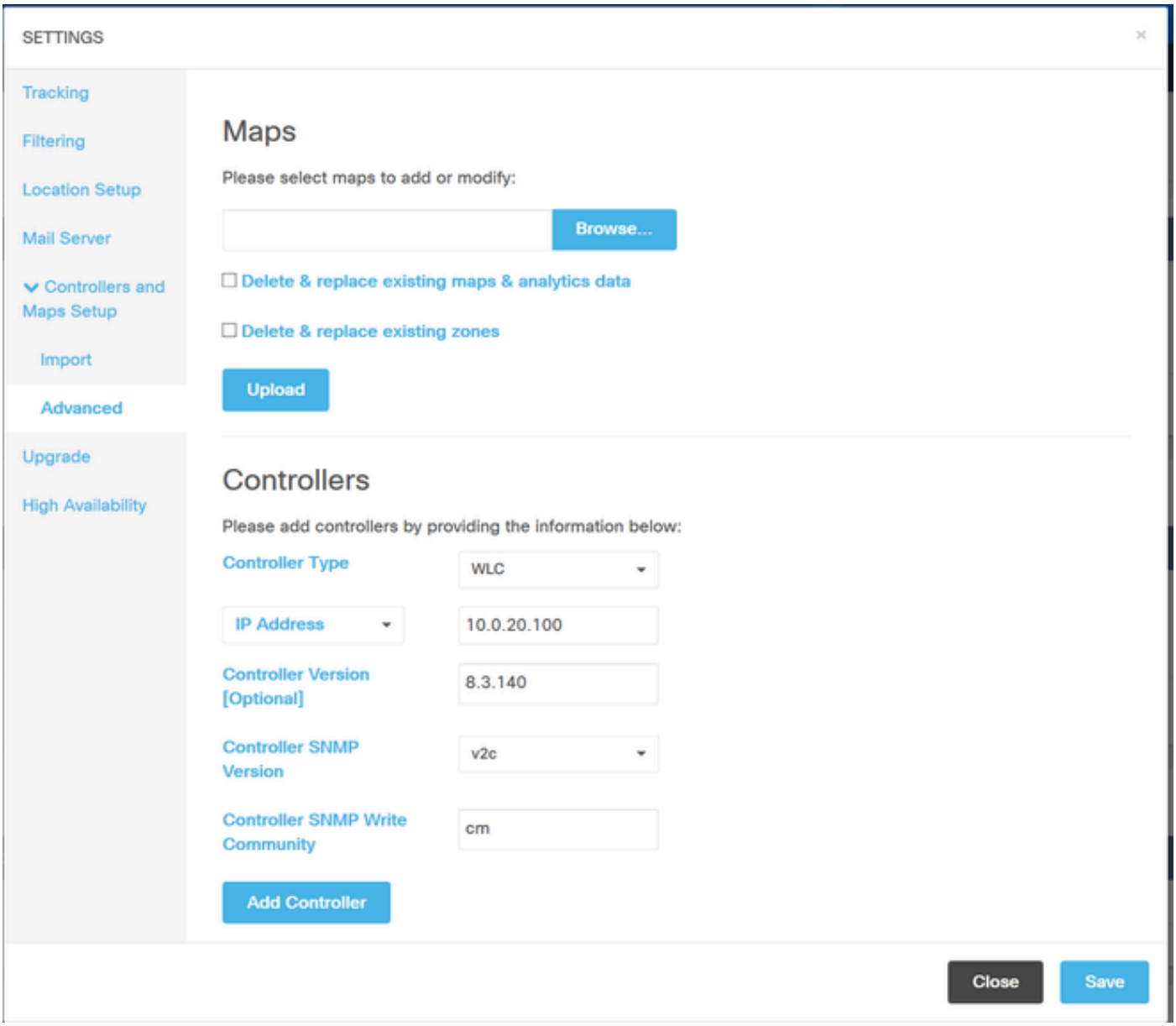


Étape 3. Ajouter Cisco WLC à CMX

Vous pouvez ajouter des WLC Cisco en utilisant l'interface de ligne de commande ou l'interface utilisateur CMX, ou en utilisant l'infrastructure Prime. Pour ces travaux pratiques, vous pouvez ajouter directement à l'aide de CMX WebUI.

La configuration du contrôleur ne fonctionne que si la connexion NMSP est correcte. Cependant, même si le contrôleur peut être ajouté avec succès, mais la connexion ne fonctionne peut-être pas.

Accédez au serveur CMX principal https://cmx_ip_address/. Cliquez sur l'onglet Système > Icône Paramètres > Menu Gauche.



Après avoir ajouté des WLC Cisco, vous devez vérifier si l'état du contrôleur est opérationnel.

Afin de valider l'état du contrôleur avec l'utilisation de l'interface utilisateur, vous devez naviguer jusqu'à l'onglet Système. La liste des contrôleurs s'affiche dans l'onglet et le nouveau contrôleur doit apparaître en vert.

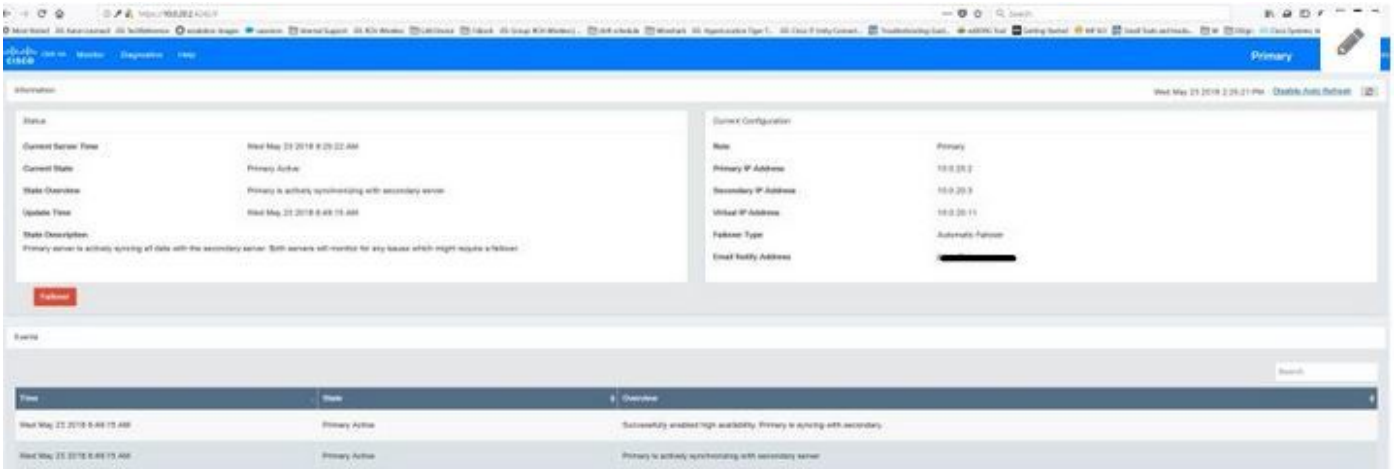
Étape 4. Basculement

Le processus de basculement implique le transfert des opérations vers le CMX secondaire en cas de panne du serveur principal. Un basculement peut se produire automatiquement lorsque CMX détecte un problème avec le serveur principal. Un basculement peut être effectué manuellement par un utilisateur dans l'interface utilisateur Web ou sur la ligne de commande. La progression du basculement peut être surveillée en fonction de l'état actuel de chaque système.

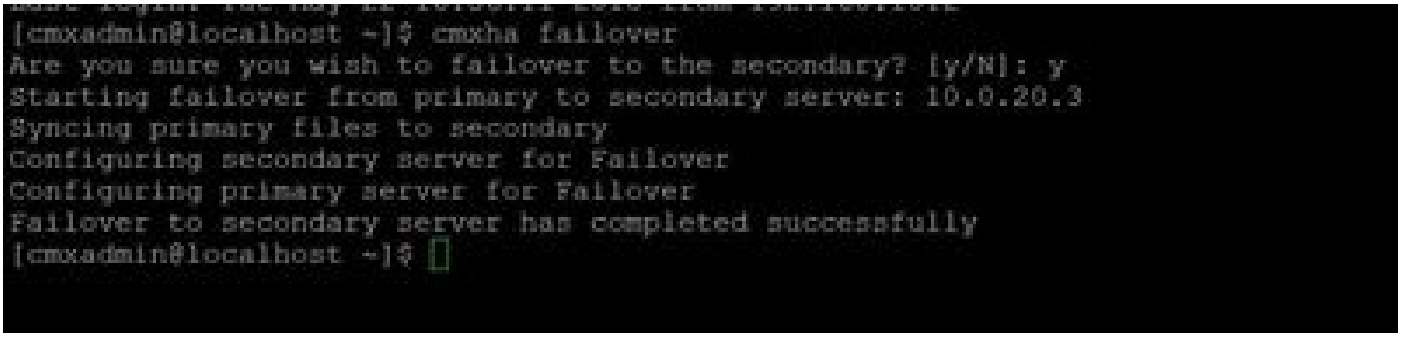
Le processus de basculement peut être lancé manuellement par l'utilisateur. Le basculement peut être effectué dans l'interface Web CMX High Availability ou sur la ligne de commande CMX.

Web de basculement manuel :

Connectez-vous à l'interface Web CMX HA sur le routeur principal ou secondaire (https://server_ip:4242). La page de surveillance comporte un bouton intitulé Basculement si les serveurs sont en cours de synchronisation. En haut à droite, activez l'actualisation automatique.



CLI de basculement manuel (pour référence) :



Étape 5. Restauration

Pour exécuter CMX sur le secondaire doit être considéré comme une situation temporaire jusqu'à ce que la cause première de la panne ait été identifiée. Une fois le boîtier principal restauré (ou un nouveau boîtier fourni), le processus de restauration doit être lancé. L'autre option consiste à convertir le système en serveur principal et à remplacer ou convertir l'autre système en serveur secondaire. Dans les deux cas, un serveur doit être mis à disposition le plus rapidement possible, car la haute disponibilité n'est plus synchronisée avec un serveur secondaire.

Le processus de restauration doit être effectué manuellement par l'utilisateur. Le re-basculement peut être effectué dans l'interface Web de CMX HA ou sur la ligne de commande CMX.

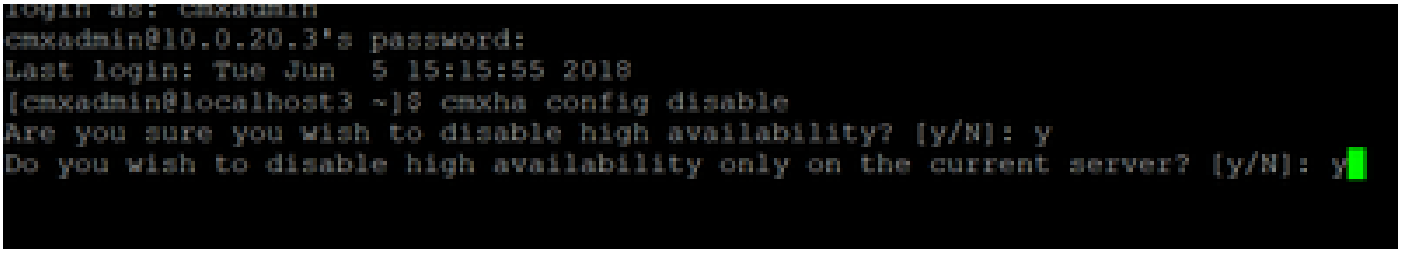
Restauration manuelle Web :

Connectez-vous à l'interface Web CMX HA sur le routeur principal ou secondaire (https://server_ip:4242). La page de surveillance comporte un bouton intitulé Failback si les deux serveurs indiquent qu'un basculement est actif.

GUI de restauration manuelle :

Étape 6. Mise à niveau/désactivation de HA

Dans le format actuel de CMX, vous devez désactiver la haute disponibilité pour effectuer une mise à niveau. Afin de désactiver la haute disponibilité depuis la ligne de commande, exécutez cmxha config disable depuis le CMX principal



Si vous oubliez d'interrompre la haute disponibilité avant une mise à niveau, le script de mise à niveau vous le rappellera. Vous devrez mettre à niveau le serveur CMX secondaire séparément avant de reformer la haute disponibilité.

Comment recharger en toute sécurité la paire CMX HA

Exécutez les étapes suivantes pour recharger la paire CMX HA :

- Désactiver le CMX secondaire
- Redémarrer le CMX principal
- Vérifier que le CMX principal est opérationnel
- Mise sous tension du CMX secondaire
- Vérifier l'état de haute disponibilité : cmxha info

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

HA dispose d'une aide en ligne pour cette fonctionnalité. L'aide est complète pour et fournit une vue d'ensemble et des détails supplémentaires sur la fonctionnalité. Il est accessible ici : https://cmx_ip_address:4242/help

Référence des commandes pour CMX HA : https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-3/cmx_command/cmxcli103/cmxcli10-3_chapter_010.pdf

Bundle de fichiers à vérifier à partir du journal tar :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.