Configuración de la alta disponibilidad de CMX

Contenido

Introducción

Este documento describe los fundamentos de Cisco Connected Mobile Experiences (CMX) y cómo configurarlo. Habla sobre cómo habilitar la alta disponibilidad, agregar el controlador de LAN inalámbrica (WLC) y realizar algunas pruebas que ayudan a verificar la configuración de alta disponibilidad (HA) con conmutación por fallo/recuperación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CMX
- WLC de Cisco

Nota: HA no tiene requisitos exclusivos para los controladores de LAN inalámbrica.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Arquitectura

El componente central de un sistema de HA es el monitor de salud. Configura, gestiona y monitorea la configuración de HA. El modo principal para mantener la vigilia es a través de latidos entre primaria y secundaria. El monitor de estado es responsable de configurar bases de datos (DB) y replicación de archivos y, a su vez, de supervisar la aplicación. CMX bajo el paradigma HA se puede definir como Primario o Secundario. La comunicación con el mundo exterior (protocolo de servicios de movilidad de red (NMSP) y llamadas API desde terminales de terceros y Prime Infrastructure (PI)) se produce a través de una dirección IP virtual. Por lo tanto, cuando el primario falla y el secundario toma el control, la IP virtual se conmuta de forma transparente.

El diseño proporciona una interfaz de usuario (IU) para configurar y supervisar los pares HA. Se generarán alarmas para CMX y fuera de CMX.

Las bases de datos se consideran el núcleo del sistema que siempre se debe replicar en tiempo real sin pérdida de datos. Los datos de la aplicación que se encuentran fuera de la base de datos son críticos pero no se necesitan sincronizarlos en tiempo real y no se traducirán en una pérdida de funcionalidad.

Infraestructura de red

El primario y el secundario deben ser accesibles entre cada sistema. Tanto el primario como el secundario deben estar en la misma subred. Esto es necesario para que la dirección IP virtual utilizada pueda conmutarse a cualquier sistema. Cualquier entidad, como los controladores de LAN inalámbrica accesibles desde el primario, también debe ser accesible desde el secundario. Para que la sincronización secundaria y la conmutación por fallas funcionen correctamente, la infraestructura de red debe permitir que el tráfico de estos puertos fluya entre el primario y el secundario. Los puertos se abrirán en CMX, pero los firewalls en CMX sólo permitirán que los otros sistemas de peer envíen tráfico en estos puertos.

Puertos	Descripción
6378, 6379, 6380, 6381, 6382, 6383, 6385, 16378, 16379, 16380, 16381, 16 382, 16383, 16385	Redis
7000, 7001, 9042	base de datos de Cassandra
5432	base de datos Postgres
4242	Servicio web y REST de alta disponibilidad
22	Puerto SSH y se utiliza para sincronizar archivos entre servidores

IP virtual

Con el sistema HA implementado, después de una conmutación por fallas, los usuarios deben ser redirigidos a la nueva instancia CMX que se ejecuta en el secundario. Para mantener la

conmutación por fallo transparente desde el punto de vista de la conectividad de red, se utilizará el concepto de IP virtual (VIP). Cuando tanto el primario como el secundario están en la misma subred, se utilizará una asignación de dirección VIP. En esta configuración, los sistemas externos están expuestos a un VIP. Este VIP se asigna a la IP real del CMX principal en ejecución. Cuando ocurre la conmutación por fallas, el VIP se reasigna a la dirección del CMX secundario. Todo esto ocurre automáticamente sin intervención humana.

No es obligatorio utilizar una IP virtual. De hecho, si está haciendo Alta Disponibilidad de Capa 3 de CMX (es decir, si tiene los dos servidores en subredes diferentes), no puede utilizar una IP virtual. La IP virtual proporciona una IP única para que el administrador de TI (o Prime Infrastructure/Cisco DNA Center) administre CMX independientemente de una recuperación tras fallos o fallos. Los WLC, sin embargo, tendrán un túnel NMSP solamente hacia la dirección IP física CMX actualmente activa.

Paso 1. Instalación de la interfaz web

Instalación principal:

Instale CMX normalmente con el login en https://cmx_ip_address:1984/. En el instalador web, seleccione el tipo de nodo Presencia o Ubicación. Este tipo de instalación no requiere especificar el tipo de nodo como primario. Esto se considera un servidor independiente que puede ejecutarse como primario, como se muestra en la imagen.

Instalación secundaria:

Instale CMX (https://cmx_ip_address:1984/) como normal hasta que el tipo de nodo deba seleccionarse en el instalador web. Se proporciona una tercera opción para el secundario. Si selecciona esta opción, el sistema se configurará como secundario y proporcionará un enlace a la interfaz de administración de alta disponibilidad de CMX.

La interfaz web de administración de alta disponibilidad de CMX se ejecuta en el puerto CMX 4242 y se puede acceder a ella: https://cmx_ip_address:4242/. Inicie sesión en la interfaz web HA con el uso de **userid cmxadmin** y la contraseña configurada **cmxadmin userid** en el momento de la instalación. Después de iniciar sesión, la interfaz de usuario tendrá información de estado y configuración. La función se mostrará como secundaria para el sistema.

Paso 2. Activar HA

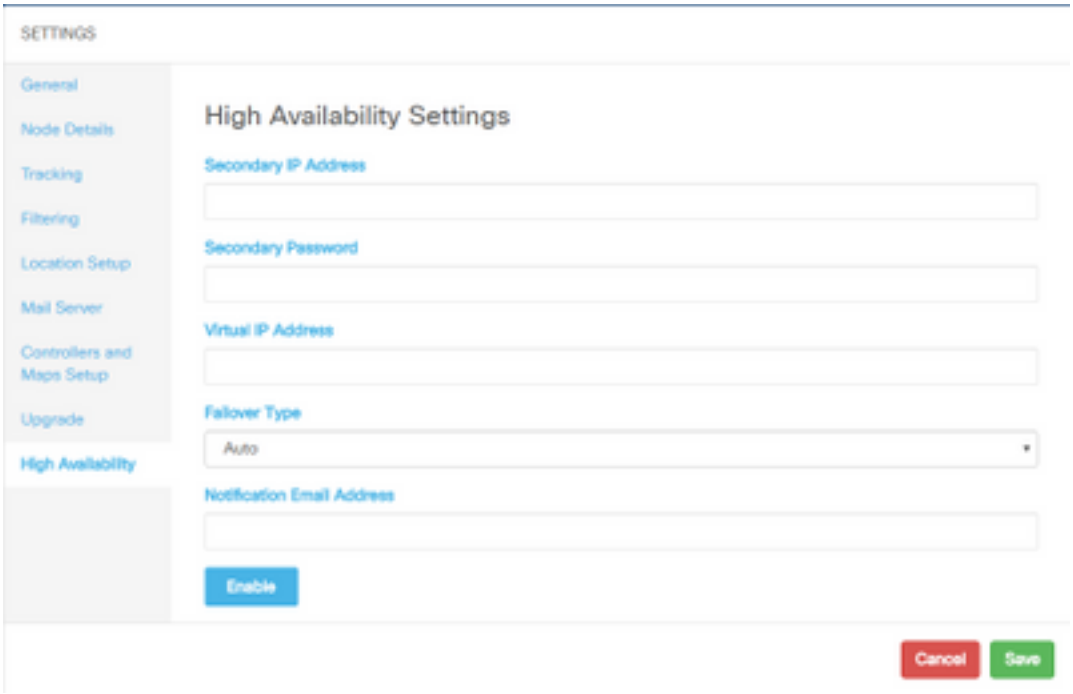
HA ahora se puede habilitar una vez que se hayan preparado los servidores primario y secundario. HA se puede habilitar en la interfaz web CMX o en la línea de comandos CMX. Estas son las opciones necesarias para configurar HA:

- Dirección de IP secundaria
- Contraseña secundaria: Contraseña para la cuenta **cmxadmin** en el servidor secundario
- Dirección VIP: Dirección VIP que utilizará el servidor activo
- Tipo de conmutación por fallo: La conmutación por fallas automática permitirá que CMX conmute automáticamente al servidor secundario cuando se detecte un problema grave. La conmutación por fallas manual requerirá que el usuario inicie la conmutación por fallas desde la interfaz web o la línea de comandos. La falla se notificará al usuario mediante notificaciones, pero no se realiza ninguna acción para la conmutación por fallas manual
- Dirección de correo electrónico de notificación: Dirección de correo electrónico para enviar notificaciones sobre información o problemas de HA. La configuración de correo electrónico utilizada para HA es la misma que para CMX. Este campo es obligatorio aunque no haya configurado un servidor de correo electrónico. No dude en introducir una dirección de correo electrónico falsa y haga clic en "activar" si no desea utilizar las notificaciones por correo electrónico.

Configuración de HA Web:

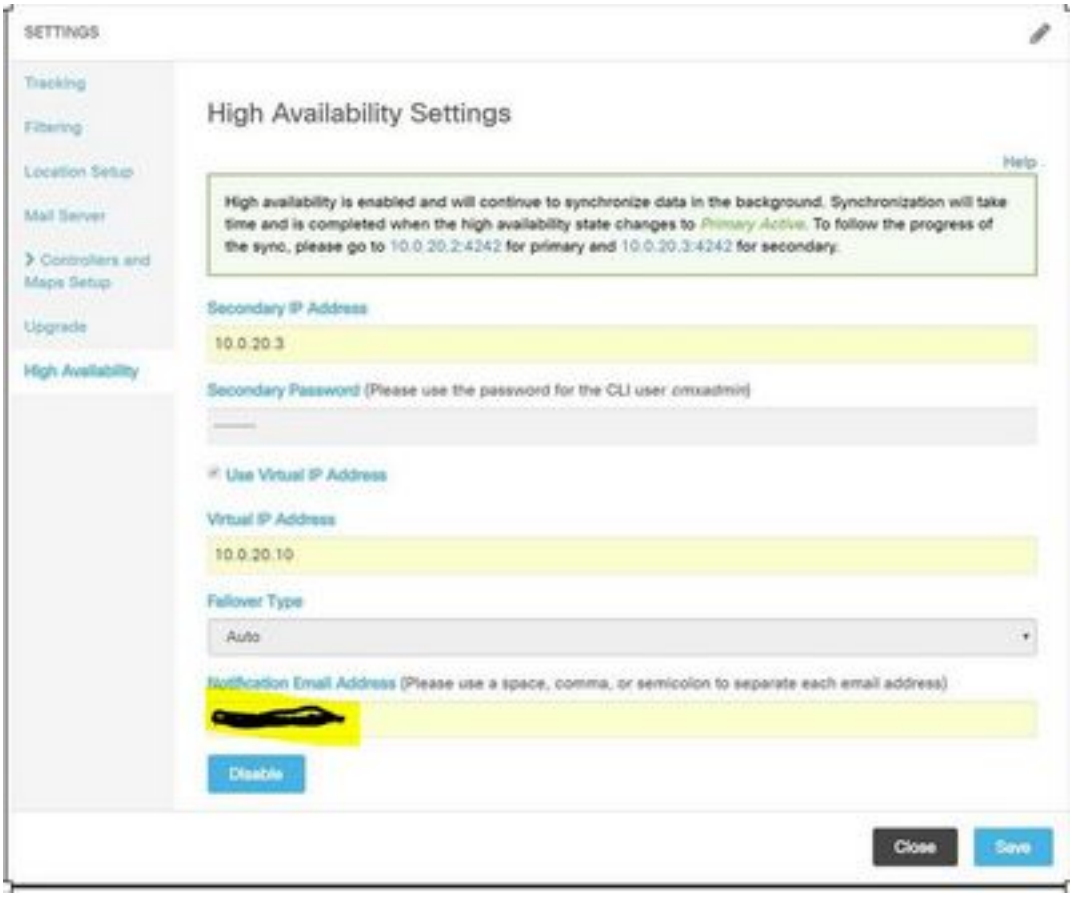
En CMX, desplácese a la **ficha Sistema** y haga clic en el **icono Configuración**. Esto mostrará un diálogo modal con una variedad de configuraciones en CMX. Seleccione la opción HA para mostrar las opciones necesarias para habilitar HA. Dirección de correo electrónico de notificación que puede proporcionar donde desea recibir las notificaciones.

Haga clic en el botón **Enable** cuando se proporcionen todas las opciones para comenzar a habilitar HA.



CMX verificará la configuración de HA y comenzará a habilitar HA entre Primario y Secundario. La interfaz de usuario web volverá cuando la configuración se haya iniciado correctamente.

Verifique que la configuración sea correcta y que la sincronización se esté realizando comprobando la presencia de una tabla de "Alta disponibilidad" en la página de configuración de CMX. Si no hay tal tabla y que, cuando vuelve a la sección de configuración de HA, todos los campos de configuración están vacíos, la información era incorrecta o incorrecta.



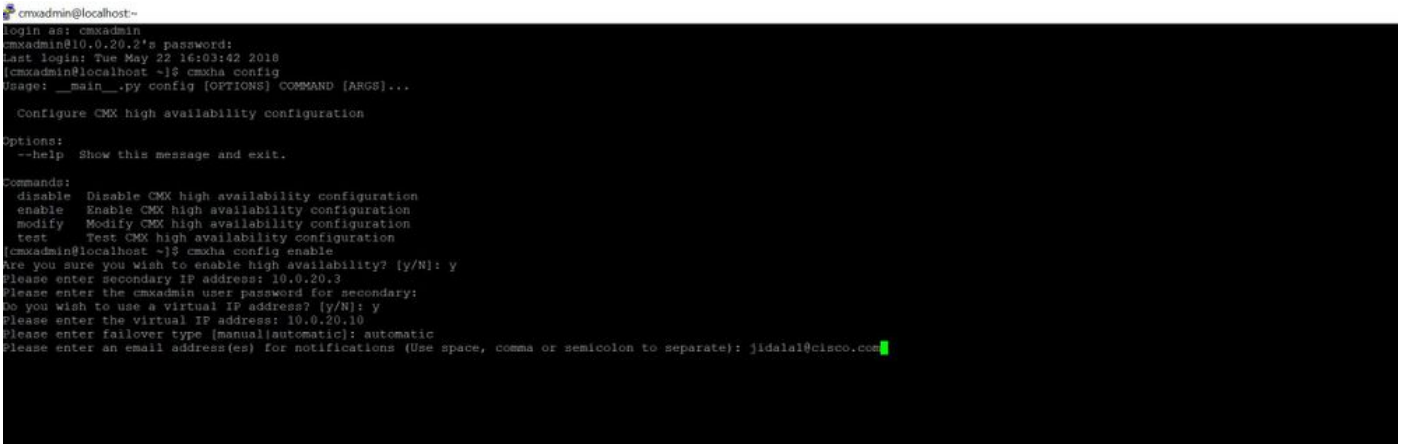
Sin embargo, HA no se ha completado al habilitarse. La sincronización inicial de todos los datos entre el servidor primario y el secundario puede tardar un tiempo considerable en completarse. La

interfaz de usuario indicará el estado como Sincronización principal mientras se realiza la sincronización.

Cuando la sincronización se haya completado correctamente, el servidor en el primario ingresará el estado Activo principal.

Cuando se complete, se generará una alerta de información en CMX. Además, se enviará una alerta por correo electrónico que indica que el sistema está activo y se sincroniza correctamente.

Habilitar CLI de alta disponibilidad (para referencia):

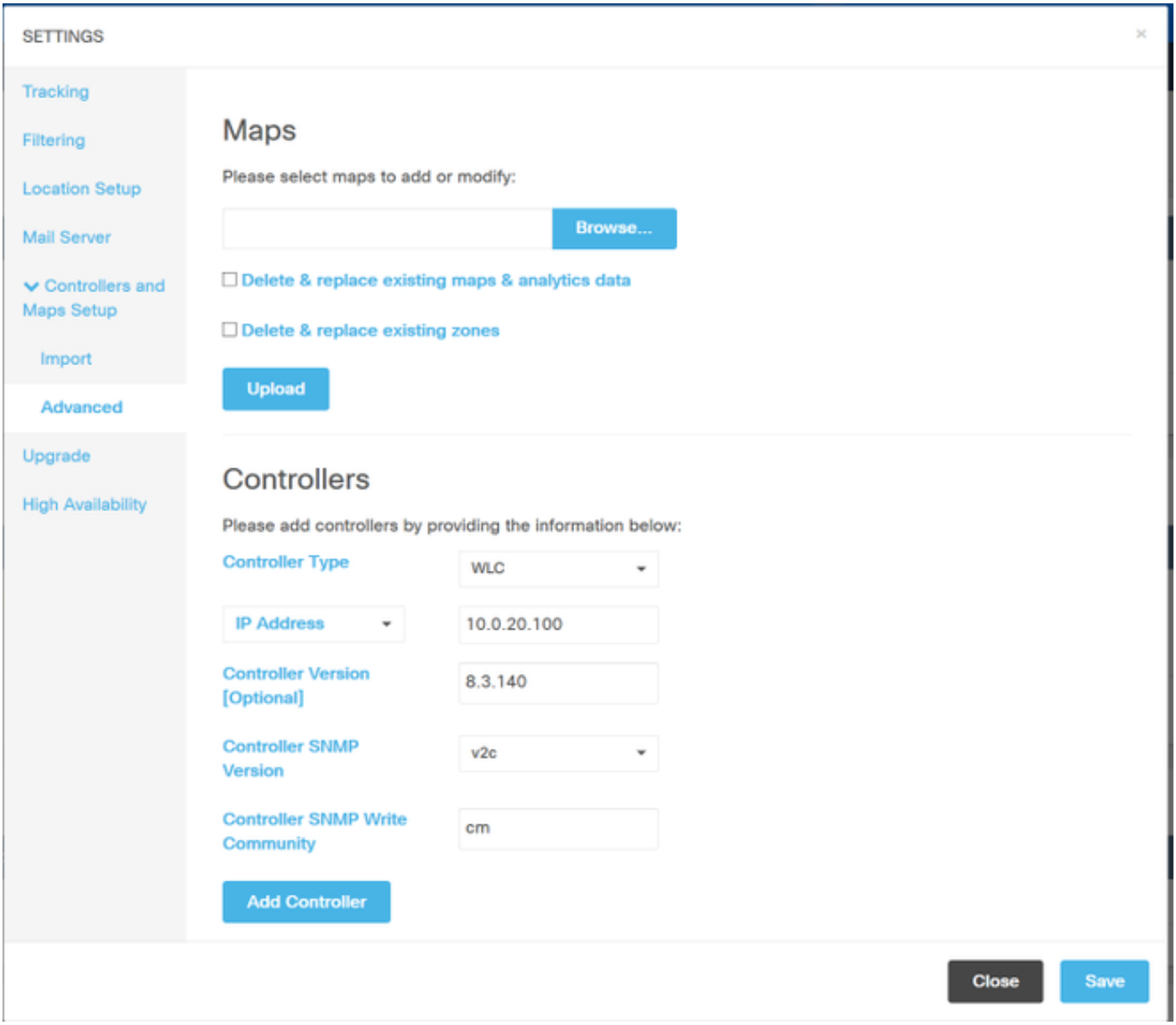


Paso 3. Agregar Cisco WLC a CMX

Puede agregar WLC de Cisco con el uso de la CLI o la interfaz de usuario CMX, o con el uso de la infraestructura Prime. Para este laboratorio, puede agregar directamente con el uso de CMX WebUI.

La configuración del controlador no funciona a menos que la conexión NMSP sea correcta. Sin embargo, aunque el controlador se pueda agregar correctamente, es posible que la conexión no funcione.

Navegue hasta el servidor CMX principal https://cmx_ip_address/. Haga clic en **Ficha Sistema > Icono Configuración > Menú izquierdo.**



Después de agregar los WLC de Cisco, debe verificar si el estado del controlador está activo y en ejecución.

Para validar el estado del controlador con el uso de la interfaz de usuario, debe navegar a la ficha Sistema. La lista del controlador se muestra en la pestaña y el nuevo controlador debe aparecer en **verde**.

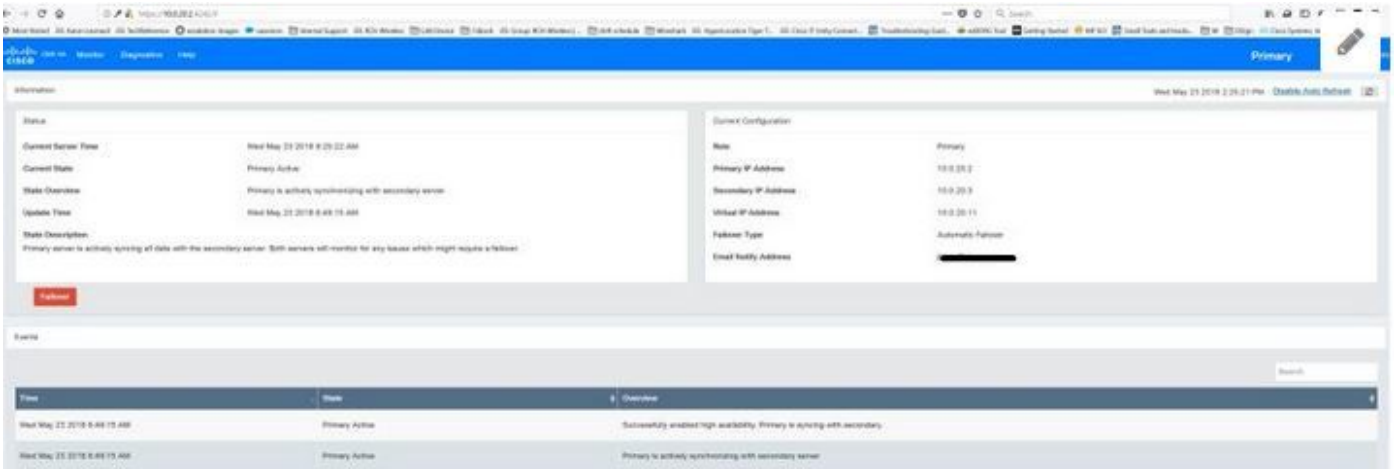
Paso 4. Failover

El proceso de failover implica la transferencia de operaciones al CMX secundario en caso de que el primario se desactive. Un failover puede ocurrir automáticamente cuando CMX detecta un problema con el servidor primario. Un usuario puede realizar un failover manualmente en la interfaz de usuario web o en la línea de comandos. El progreso de la conmutación por fallas se puede monitorear según el estado actual de cada sistema.

El proceso de failover puede ser iniciado manualmente por el usuario. La conmutación por fallas se puede realizar en la interfaz web de alta disponibilidad CMX o en la línea de comandos CMX.

Web de conmutación por fallo manual:

Inicie sesión en la interfaz web CMX HA en primaria o secundaria (**https://server_ip:4242**). La página de monitor tendrá un botón denominado Failover si los servidores se están sincronizando activamente. En la parte superior derecha, **active la actualización automática.**



Manual Failover CLI (para referencia):

```
[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 ~]$
```

Paso 5. Recuperación

Para ejecutar CMX en el secundario se debe considerar como una situación temporal hasta que se haya identificado la causa raíz de la falla primaria. Una vez restaurada la caja principal (o se proporciona una nueva caja), se debe iniciar el proceso de recuperación. La otra opción es convertir el sistema en un primario y reemplazar o convertir el otro sistema en un servidor secundario. En cualquier caso, un servidor debería estar disponible lo antes posible, ya que HA ya no se sincroniza con un servidor secundario.

El usuario debe realizar manualmente el proceso de recuperación de fallos. La conmutación por recuperación puede realizarse en la interfaz web CMX HA o en la línea de comandos CMX.

Web de recuperación manual:

Inicie sesión en la interfaz web CMX HA en primaria o secundaria (**https://server_ip:4242**). La página de monitor tendrá un botón denominado failback si ambos servidores indican que hay una conmutación por fallas activa.

GUI manual de recuperación de fallos:

Paso 6. Actualización / Desactivación de HA

En el formato actual de CMX, debe inhabilitar HA para realizar una actualización. Para inhabilitar HA de la línea de comandos, ejecute **cmxha config disable** del CMX primario

Si olvida interrumpir la HA antes de una actualización, el script de actualización le recordará. Tendrá que actualizar el servidor CMX secundario por separado antes de reformar HA.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

HA tiene ayuda en línea para la función. La ayuda se ha completado para y proporciona una descripción general y detalles adicionales sobre la función. Se puede acceder aquí: https://cmx_ip_address:4242/help

Referencia de Comandos para CMX HA: https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-3/cmx_command/cmxcli103/cmxcli10-3_chapter_010.pdf

Agrupar archivos para verificar desde el registro tar:

- cmx-hafile-sync

- cmx-haweb-service
- cmx-haserver