Configura alta disponibilità CMX

Sommario

Introduzione

Questo documento descrive i concetti fondamentali di Cisco Connected Mobile Experience (CMX) e come configurarlo. Viene descritto come abilitare l'alta disponibilità, aggiungere il controller WLC (Wireless LAN Controller) ed eseguire alcuni test che consentono di verificare la configurazione ad alta disponibilità (HA, High Availability) con failover/failback.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CMX
- Cisco WLC

Nota: HA non ha requisiti specifici per i controller LAN wireless.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CMX 10.6
- WLC 8,3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Architettura

La componente centrale di un sistema HA è il monitoraggio dello stato. Consente di configurare, gestire e monitorare l'impostazione HA. La modalità principale per mantenere la veglia è attraverso heartbeat tra primario e secondario. Il monitoraggio dello stato è responsabile dell'impostazione dei database (DB) e della replica dei file e, di conseguenza, del monitoraggio dell'applicazione. CMX sotto il paradigma HA può essere definito come Primario o Secondario. La comunicazione con il mondo esterno (chiamate NMSP (Network Mobility Services Protocol) e API da endpoint di terze parti e Prime Infrastructure (PI)) avviene tramite un indirizzo IP virtuale. In questo modo, quando il server principale subentra al server secondario, l'IP virtuale viene commutato in modo trasparente.

La progettazione prevede un'interfaccia utente (UI) per la configurazione e il monitoraggio delle coppie HA. Gli allarmi verranno generati per CMX e all'esterno di CMX.

I database sono considerati il nucleo del sistema che deve essere sempre replicato in tempo reale senza perdita di dati. I dati delle applicazioni che si trovano all'esterno del database sono critici, ma non devono essere sincronizzati in tempo reale e non comportano una perdita di funzionalità.

Infrastruttura di rete

Il sistema primario e quello secondario devono essere raggiungibili tra ogni sistema. Sia il database primario che quello secondario devono trovarsi nella stessa subnet. Questa operazione è necessaria in modo che l'indirizzo IP virtuale utilizzato possa essere commutato in entrambi i sistemi. Qualsiasi entità, ad esempio i controller LAN wireless, raggiungibile dal server primario deve essere raggiungibile anche dal server secondario. Affinché la sincronizzazione e il failover secondari funzionino correttamente, l'infrastruttura di rete deve consentire il flusso del traffico di queste porte tra la porta primaria e quella secondaria. Le porte verranno aperte su CMX, ma i firewall su CMX consentiranno solo agli altri sistemi peer di inviare il traffico su queste porte.

Porte	Descrizione
6378, 6379, 6380, 6381, 6382, 6383, 6385, 16378, 16379, 16380, 16381, 16382, 16383, 16385	Redis
7000, 7001, 9042	database Cassandra
5432	database Postgres
4242	Servizio Web e REST ad alta disponibilità
22	Porta SSH e utilizzata per sincronizzare i file tra i server

IP virtuale

Con il sistema HA installato, dopo un failover gli utenti devono essere reindirizzati alla nuova

istanza CMX in esecuzione sul sistema secondario. Per mantenere il failover trasparente dal punto di vista della connettività di rete, verrà utilizzato il concetto di IP virtuale (VIP). Quando nella stessa subnet si trovano sia il sito principale che quello secondario, verrà utilizzato un mapping di indirizzi VIP. In questa configurazione, i sistemi esterni sono esposti a un VIP. Questo VIP è mappato all'IP reale del CMX primario in esecuzione. Quando si verifica il failover, viene eseguito un nuovo mapping dell'indirizzo VIP all'indirizzo del CMX secondario. Tutto questo avviene automaticamente senza alcun intervento umano.

Non è obbligatorio utilizzare un IP virtuale. Infatti, se si sta eseguendo CMX Layer 3 High Availability (ossia disponendo i due server in subnet diverse), non è possibile utilizzare un IP virtuale. L'IP virtuale fornisce un IP univoco per l'amministratore IT (o Prime Infrastructure/ Cisco DNA Center) per gestire CMX indipendentemente da failover o failback. I WLC, tuttavia, avranno un tunnel NMSP solo verso l'indirizzo IP fisico CMX attualmente attivo.

Passaggio 1. Installazione dell'interfaccia Web

Installazione primaria:

Installare CMX normalmente con il login in https://cmx_ip_address:1984/. Nel programma di installazione Web, selezionare il tipo di nodo Presenza o Posizione. Per questo tipo di installazione non è necessario specificare il tipo di nodo come primario. Si tratta di un server autonomo che può essere eseguito come server primario, come mostrato nell'immagine.

Installazione secondaria:

Installare CMX (https://cmx_ip_address:1984/) normalmente finché non è necessario selezionare il tipo di nodo nel programma di installazione Web. Una terza opzione è prevista per le licenze secondarie. Se si seleziona questa opzione, il sistema verrà configurato come secondario e fornirà un collegamento all'interfaccia CMX High Availability Admin.

L'interfaccia Web CMX High Availability Admin è in esecuzione sulla porta CMX 4242 ed è accessibile: https://cmx_ip_address:4242/. Accedere all'interfaccia Web HA utilizzando l'ID utente **cmxadmin** e la password configurata per l'**ID utente cmxadmin** al momento dell'installazione. Dopo aver eseguito l'accesso, l'interfaccia utente disporrà di informazioni di stato e configurazione. Il ruolo verrà visualizzato come secondario per il sistema.

Passaggio 2. Abilitare HA

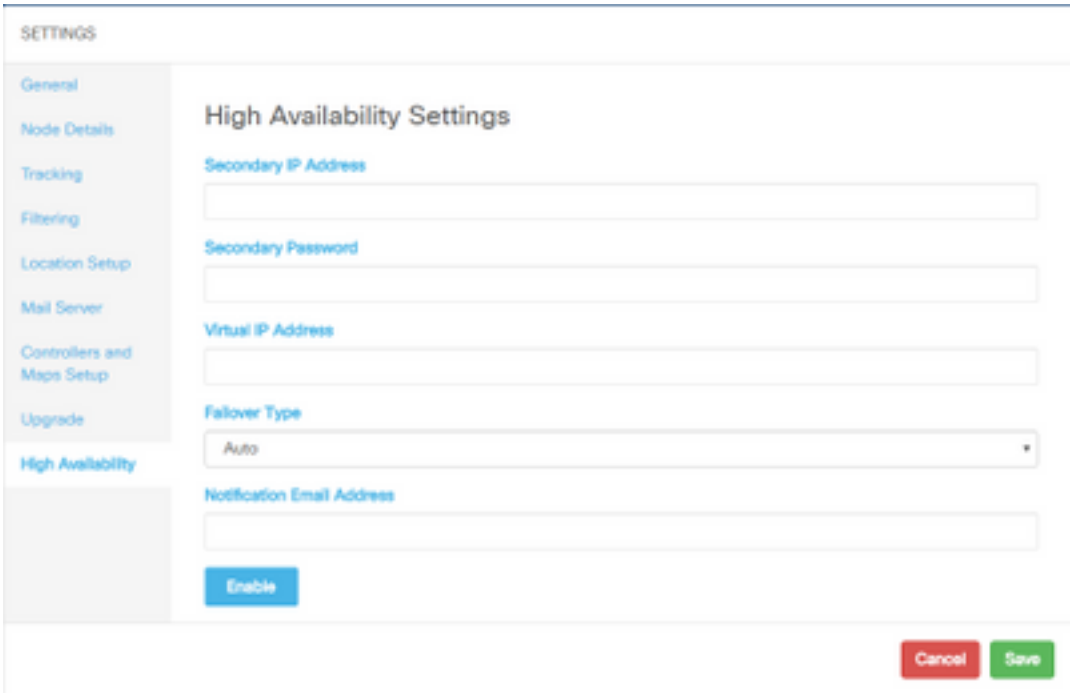
Èora possibile abilitare HA una volta preparati i server primario e secondario. È possibile abilitare HA nell'interfaccia Web CMX o nella riga di comando CMX. Di seguito sono riportate le opzioni necessarie per impostare HA:

- Indirizzo IP secondario
- Password secondaria: Password per l'account **cmxadmin** sul server secondario
- Indirizzo VIP: Indirizzo VIP da utilizzare per il server attivo
- Tipo di failover: Il failover automatico consente il failover automatico di CMX sul server secondario quando viene rilevato un problema grave. Il failover manuale richiederà l'avvio del failover dall'interfaccia Web o dalla riga di comando. L'errore verrà segnalato all'utente tramite notifiche ma non verrà intrapresa alcuna azione per il failover manuale
- Indirizzo di posta elettronica notifica: Indirizzo e-mail per inviare notifiche su problemi o informazioni HA. Le impostazioni e-mail utilizzate per HA sono le stesse di CMX. Questo campo è obbligatorio anche se non hai un server e-mail configurato. Immetti liberamente un indirizzo e-mail fittizio e fai clic su "abilita" se non intendi utilizzare le notifiche e-mail.

Configurare il Web HA:

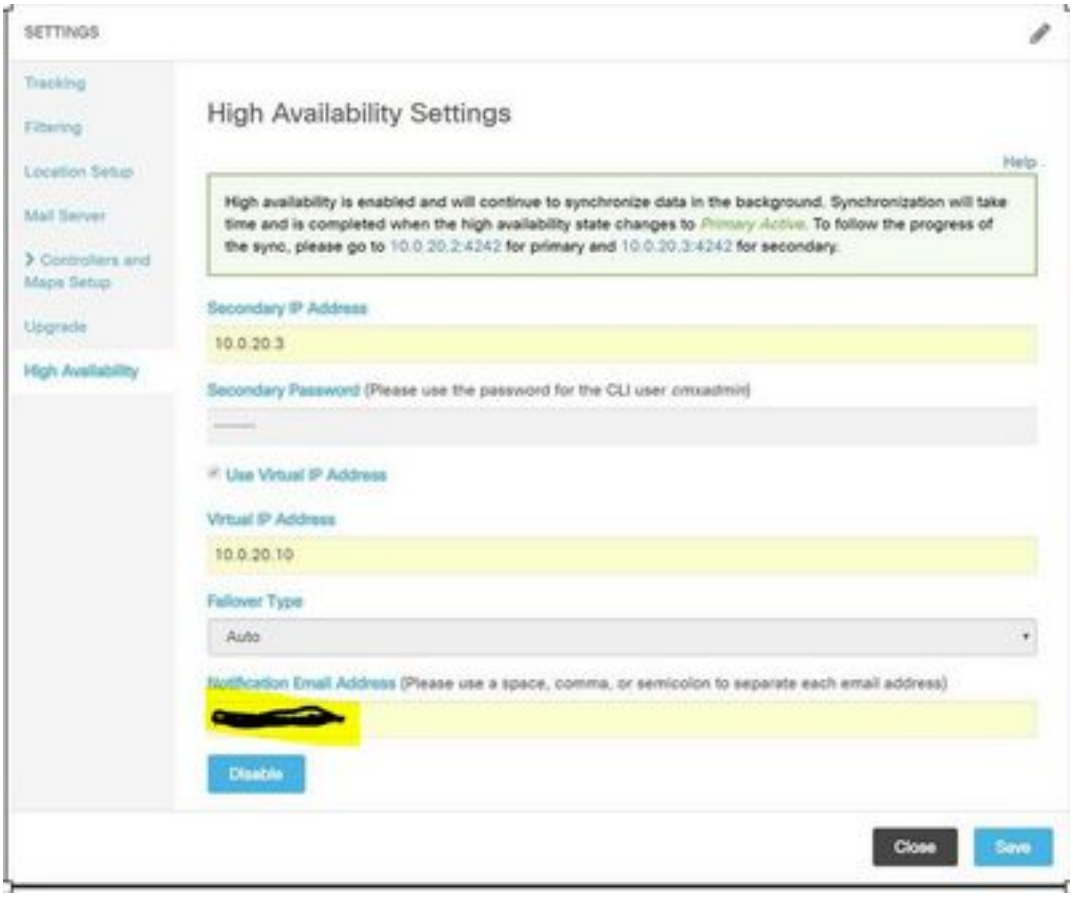
In CMX, passare alla **scheda Sistema** e fare clic sull'**icona Impostazioni**. Verrà visualizzata una finestra di dialogo modale con diverse impostazioni in CMX. Selezionare l'opzione HA per visualizzare le opzioni necessarie per abilitare HA. Indirizzo di posta elettronica di notifica è possibile specificare dove si desidera ricevere le notifiche.

Fare clic sul pulsante **Abilita** quando sono disponibili tutte le opzioni per avviare l'abilitazione di HA.



CMX verificherà le impostazioni HA e inizierà ad abilitare HA tra primario e secondario. WebUI restituirà una volta avviata la configurazione.

Verificare che le impostazioni siano corrette e che la sincronizzazione sia in corso verificando la presenza di una tabella "Alta disponibilità" nella pagina delle impostazioni di CMX. Se tale tabella non è presente e, quando si torna alla sezione delle impostazioni HA, tutti i campi di configurazione sono vuoti, le informazioni sono errate o errate.



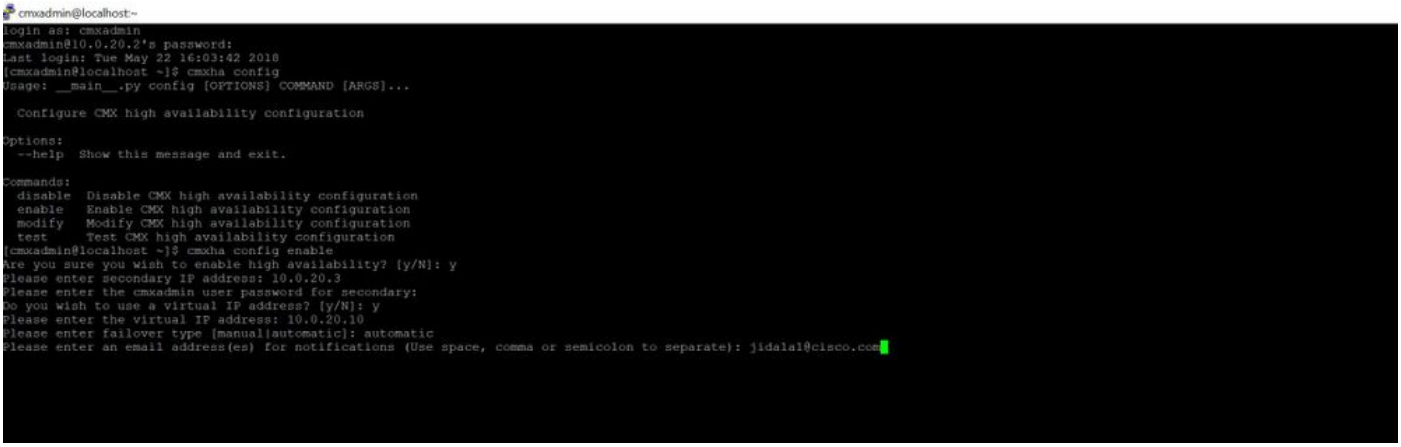
L'abilitazione di HA non è stata completata. La sincronizzazione iniziale di tutti i dati tra il server principale e quello secondario può richiedere molto tempo. L'interfaccia utente indicherà lo stato

come Sincronizzazione primaria durante l'esecuzione della sincronizzazione.

Al termine della sincronizzazione, il server sul server primario passerà allo stato Primario attivo.

Una volta completato, verrà generato un avviso relativo alle informazioni in CMX. Inoltre, verrà inviato un avviso tramite e-mail che indica che il sistema è attivo e in fase di sincronizzazione.

Abilitare High Availability CLI (per riferimento):

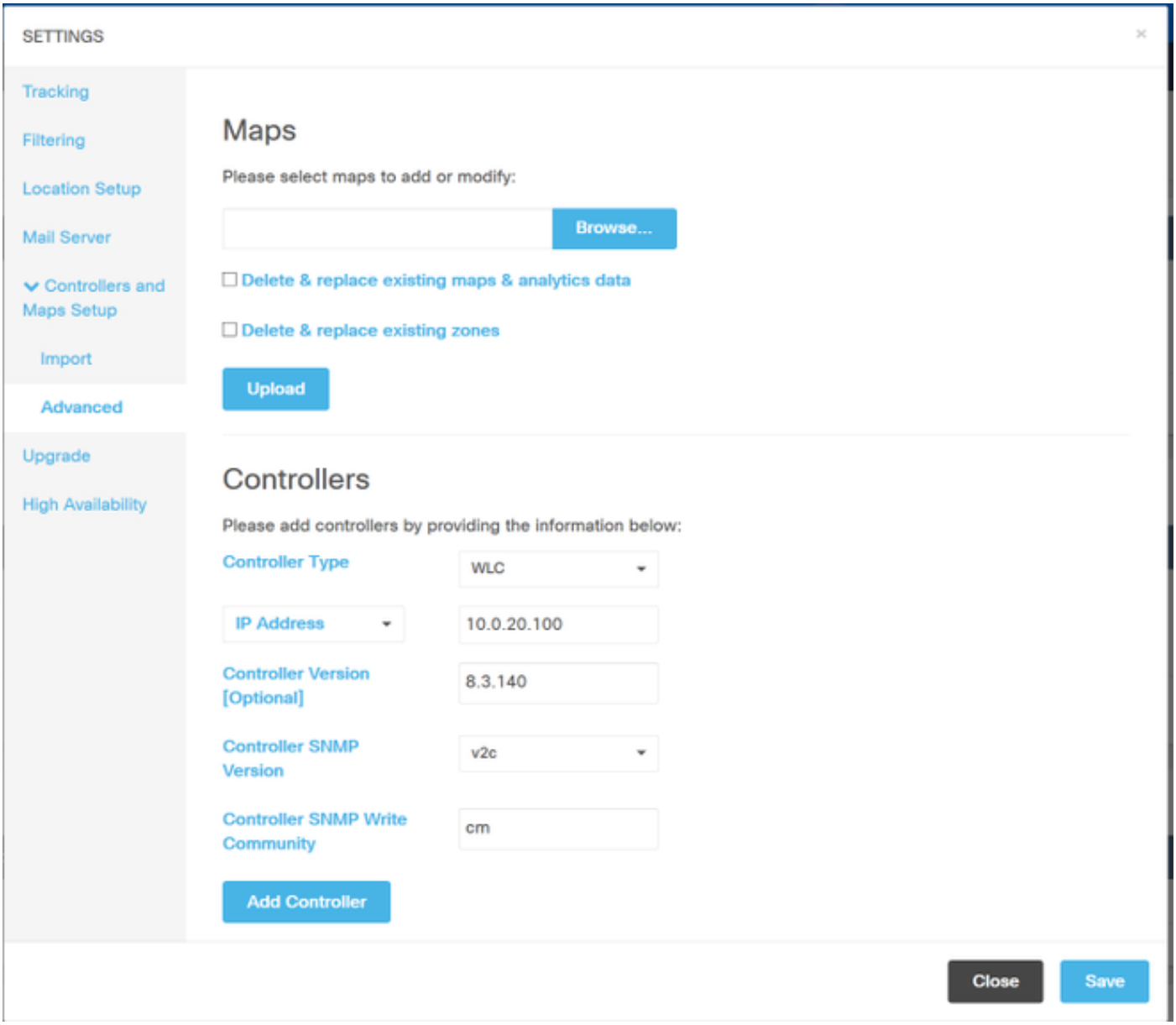


Passaggio 3. Aggiungere Cisco WLC a CMX

Èpossibile aggiungere i WLC Cisco usando la CLI o l'interfaccia utente CMX, o usando Prime Infrastructure. Per questa esercitazione, è possibile aggiungere elementi direttamente utilizzando CMX WebUI.

La configurazione del controller funziona solo se la connessione NMSP è corretta. Tuttavia, anche se il controller può essere stato aggiunto correttamente, ma la connessione potrebbe non funzionare.

Passare al server CMX primario https://cmx_ip_address/. Fare clic sulla **scheda Sistema > Icona Impostazioni > Menu a sinistra.**



Dopo aver aggiunto i WLC Cisco, è necessario verificare se lo stato del controller è attivo e in esecuzione.

Per convalidare lo stato del controller tramite l'interfaccia utente, è necessario selezionare la scheda Sistema. L'elenco del controller viene visualizzato nella scheda e il nuovo controller viene visualizzato in **verde**.

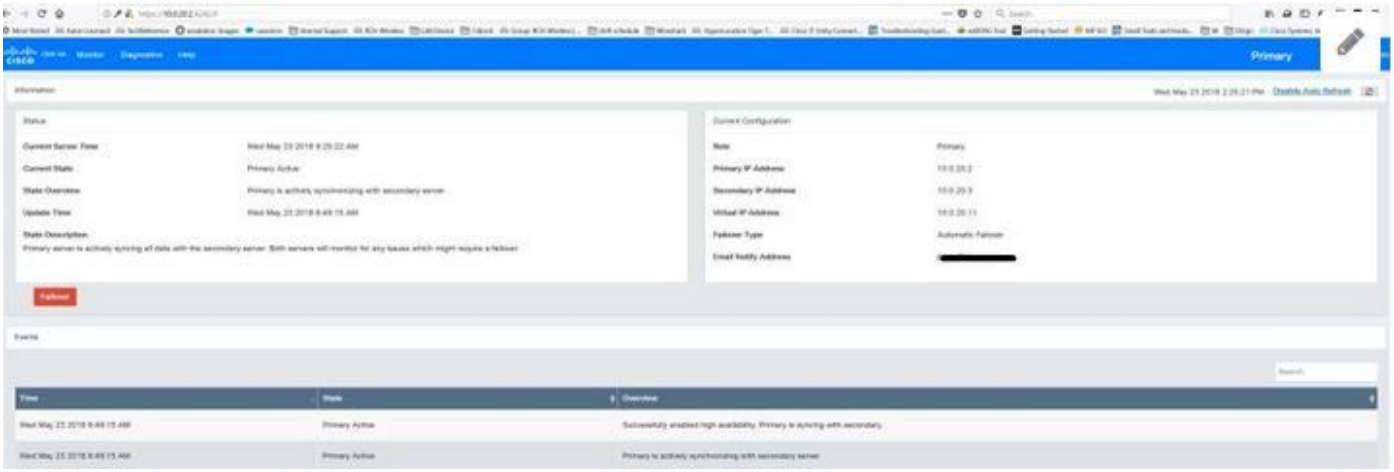
Passaggio 4. Failover

Il processo di failover comporta il trasferimento delle operazioni al CMX secondario in caso di inattività del sistema principale. Il failover può avvenire automaticamente quando CMX rileva un problema con il server principale. Il failover può essere eseguito manualmente da un utente tramite l'interfaccia utente Web o la riga di comando. L'avanzamento del failover può essere monitorato in base allo stato corrente di ciascun sistema.

Il processo di failover può essere avviato manualmente dall'utente. Il failover può essere eseguito tramite l'interfaccia Web CMX High Availability o la riga di comando CMX.

Failover manuale Web:

Accedere all'interfaccia Web CMX HA sul sito principale o secondario (https://server_ip:4242). Se i server stanno eseguendo la sincronizzazione attiva, nella pagina di monitoraggio sarà presente un pulsante denominato Failover. In alto a destra **abilitare l'aggiornamento automatico.**



CLI failover manuale (per riferimento):

```
[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 ~]$
```

Passaggio 5. Failback

L'esecuzione di CMX sul database secondario deve essere considerata una situazione temporanea fino a quando non viene identificata la causa principale dell'errore primario. Una volta ripristinata la casella principale (o fornita una nuova casella), deve essere avviato il processo di failback. L'altra opzione consiste nel convertire il sistema in un server primario e sostituire o convertire l'altro sistema in un server secondario. In entrambi i casi, un server deve essere reso disponibile il prima possibile poiché HA non è più sincronizzato con un server secondario.

Il processo di failback deve essere eseguito manualmente dall'utente. Il failback può essere eseguito tramite l'interfaccia Web CMX HA o la riga di comando CMX.

Failback manuale Web:

Accedere all'interfaccia Web CMX HA sul sito principale o secondario (https://server_ip:4242). Se entrambi i server indicano che è attivo un failover, nella pagina del monitor sarà presente un pulsante con l'etichetta Failback.

Interfaccia grafica di failback manuale:

Passaggio 6. Aggiornare/Disabilitare HA

Nel formato corrente di CMX è necessario disattivare HA per eseguire un aggiornamento. Per disabilitare HA dalla riga di comando, eseguire **cmxha config disable** dal CMX primario

Se si dimentica di interrompere HA prima di un aggiornamento, lo script di aggiornamento lo ricorda. Prima di riformare HA, sarà necessario aggiornare separatamente il server CMX secondario.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

HA dispone della Guida in linea per la funzione. La Guida è completa per e fornisce una panoramica e ulteriori dettagli su questa funzione. È possibile accedervi al seguente indirizzo: https://cmx_ip_address:4242/help

Guida di riferimento ai comandi per CMX HA: https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-3/cmx_command/cmxcli103/cmxcli10-3_chapter_010.pdf

Pacchetto di file da controllare dal registro TAR:

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