Configurar a alta disponibilidade do CMX

Contents

Introdução

Este documento descreve os conceitos básicos do Cisco Connected Mobile Experiences (CMX) e como configurá-lo.

Pré-requisitos

Este documento fala sobre como habilitar a alta disponibilidade, adicionar o Wireless LAN Controller (WLC) e executar alguns testes que ajudam a verificar a configuração de Alta Disponibilidade (HA) com failover/failback.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CMX
- WLC Cisco

Observação: o HA não tem requisitos exclusivos para os controladores de LAN sem fio.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CMX 10.6
- WLC 8.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Arquitetura

O componente central de um sistema HA é o monitor de saúde. Ele configura, gerencia e monitora a configuração de HA. O modo principal para manter a vigília é através de batimentos cardíacos entre o primário e secundário. O monitor de integridade é responsável por configurar bancos de dados (DBs) e replicação de arquivos e, por sua vez, monitorar o aplicativo. O CMX no paradigma HA pode ser definido como primário ou secundário. A comunicação com o mundo externo (Network Mobility Services Protocol (NMSP)) e chamadas de API de endpoints de terceiros e Prime Infrastructure (PI)) acontece através de um endereço IP virtual. Assim, quando o primário falha e o secundário assume, o IP virtual é comutado de forma transparente.

O design fornece uma interface de usuário (UI) para configurar e monitorar os pares de HA. Os alarmes são gerados para o CMX e fora do CMX.

Os DBs são considerados o núcleo do sistema que deve sempre ser replicado em tempo real sem perda de dados. Os dados de aplicativos que estão fora do banco de dados são críticos, mas não precisam ser sincronizados em tempo real e não resultarão em perda de funcionalidade.

Infraestrutura de Rede

O primário e o secundário devem estar acessíveis entre cada sistema. Tanto o primário como o secundário devem estar na mesma sub-rede. Isso é necessário para que o endereço IP virtual usado possa ser comutado para qualquer um dos sistemas. Qualquer entidade, como controladores de LAN sem fio, acessível a partir do principal também deve estar acessível a partir do secundário. Para que a sincronização secundária e o failover funcionem corretamente, a infraestrutura de rede deve permitir que esse tráfego de porta flua entre o primário e o secundário. O CMX usa o VRRP para verificar a manutenção de atividade de ambas as unidades CMX em alta disponibilidade, garantindo que não haja restrições entre as duas no par de alta disponibilidade, já que o Gateway deve estar acessível para estabelecer a acessibilidade do CMX.

As portas serão abertas no CMX, mas os firewalls no CMX permitirão apenas que os outros sistemas pares enviem tráfego nessas portas.

Portas	Descrição

6378, 6379, 6380, 6381, 6382, 6383, 6385, 16378, 16379, 16380, 16381, 16382, 16383, 16385	Redis
7000, 7001, 9042	banco de dados Cassandra
5432	banco de dados Postgres
4242	Alta disponibilidade de REST e serviço da Web
22	Porta SSH e usada para sincronizar arquivos entre servidores

IP virtual

Com o sistema HA implantado, após um failover, os usuários devem ser redirecionados para a nova instância do CMX que é executada no secundário. Para manter o failover transparente do ponto de vista da conectividade de rede, o conceito de VIP (IP Virtual) será usado. Quando o primário e o secundário estiverem na mesma sub-rede, será usado um mapeamento de endereço VIP. Nessa configuração, os sistemas externos são expostos a um VIP. Esse VIP é mapeado para o IP real do CMX primário em execução. Quando ocorre failover, o VIP é remapeado para o endereço do CMX secundário. Tudo isso acontece automaticamente, sem qualquer intervenção humana.

Não é obrigatório usar um IP virtual. Na verdade, se você estiver fazendo a Alta Disponibilidade da Camada 3 do CMX (ou seja, tendo os dois servidores em sub-redes diferentes), não poderá usar um IP virtual. O IP virtual fornece um IP exclusivo para o administrador de TI (ou Prime Infrastructure/ Cisco DNA center) gerenciar o CMX, independentemente de um failover ou failback. As WLCs, no entanto, têm um túnel NMSP apenas para o endereço IP físico CMX ativo atualmente.

Etapa 1. Instalação da interface da Web

Instalação primária:

Instale o CMX normalmente com login em https://cmx_ip_address:1984/. No instalador da Web, selecione o tipo de nó Presença ou Localização. Esse tipo de instalação não requer a especificação do tipo de nó como primário. Ele é considerado um servidor autônomo que pode ser executado como primário, como mostrado na imagem.

Instalação secundária:

Instale o CMX (https://cmx_ip_address:1984/) normalmente até que o tipo de nó precise ser selecionado no instalador da Web. Uma terceira opção é fornecida para secundário. Se você selecionar essa opção, o sistema será configurado como secundário e fornecerá um link para a interface CMX High Availability Admin.

A interface da Web do CMX High Availability Admin é executada na porta 4242 do CMX e pode ser acessada: https://cmx_ip_address:4242/. Faça login na interface da Web do HA com o uso do userid cmxadmin e da senha configurada como cmxadmin userid no momento da instalação. Após o login, a interface de usuário tem informações de status e configuração. A função é mostrada como secundária para o sistema.

Etapa 2. Ativar HA

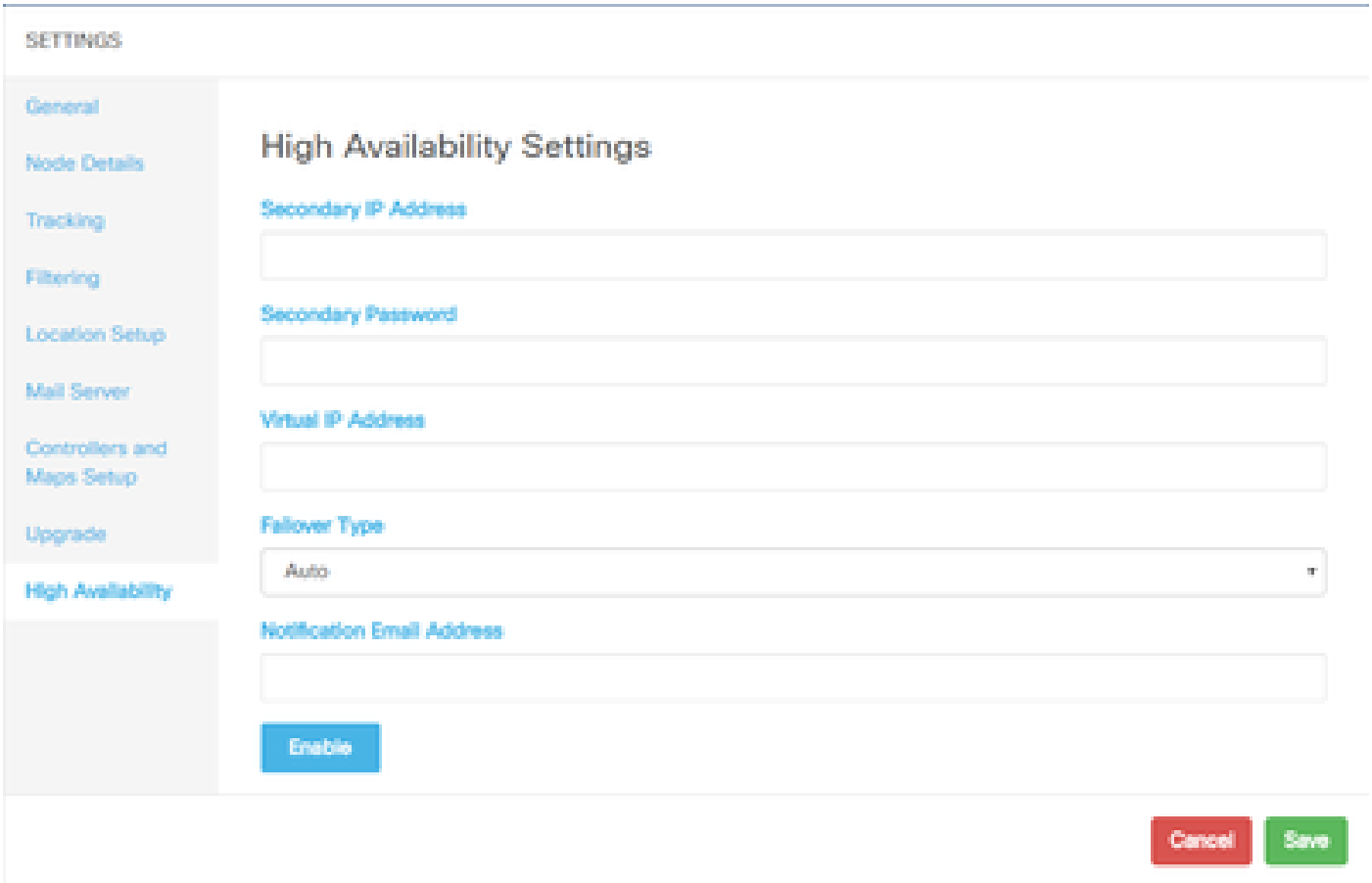
O HA agora pode ser habilitado depois que os servidores primário e secundário estiverem preparados. O HA pode ser ativado na interface da Web do CMX ou na linha de comando do CMX. Estas são as opções necessárias para configurar o HA:

- Endereço IP secundário
- Senha secundária: senha da conta cmxadmin no servidor secundário
- Endereço VIP: endereço VIP a ser usado pelo servidor ativo
- Tipo de failover: o failover automático permitirá que o CMX faça o failover automaticamente para o servidor secundário quando um problema grave for detectado. O failover manual exigirá que o usuário inicie o failover na interface da Web ou na linha de comando. A falha será relatada ao usuário por meio de notificações, mas nenhuma ação será tomada para failover manual
- Endereço de e-mail para notificação: endereço de e-mail para enviar notificações sobre informações ou problemas de alta disponibilidade. As configurações de e-mail usadas para HA são as mesmas do CMX. Este campo é obrigatório mesmo que você não tenha um servidor de e-mail configurado. Sinta-se à vontade para inserir um endereço de e-mail fictício e clique em "habilitar" se não quiser usar notificações por e-mail.

Configurar Web HA:

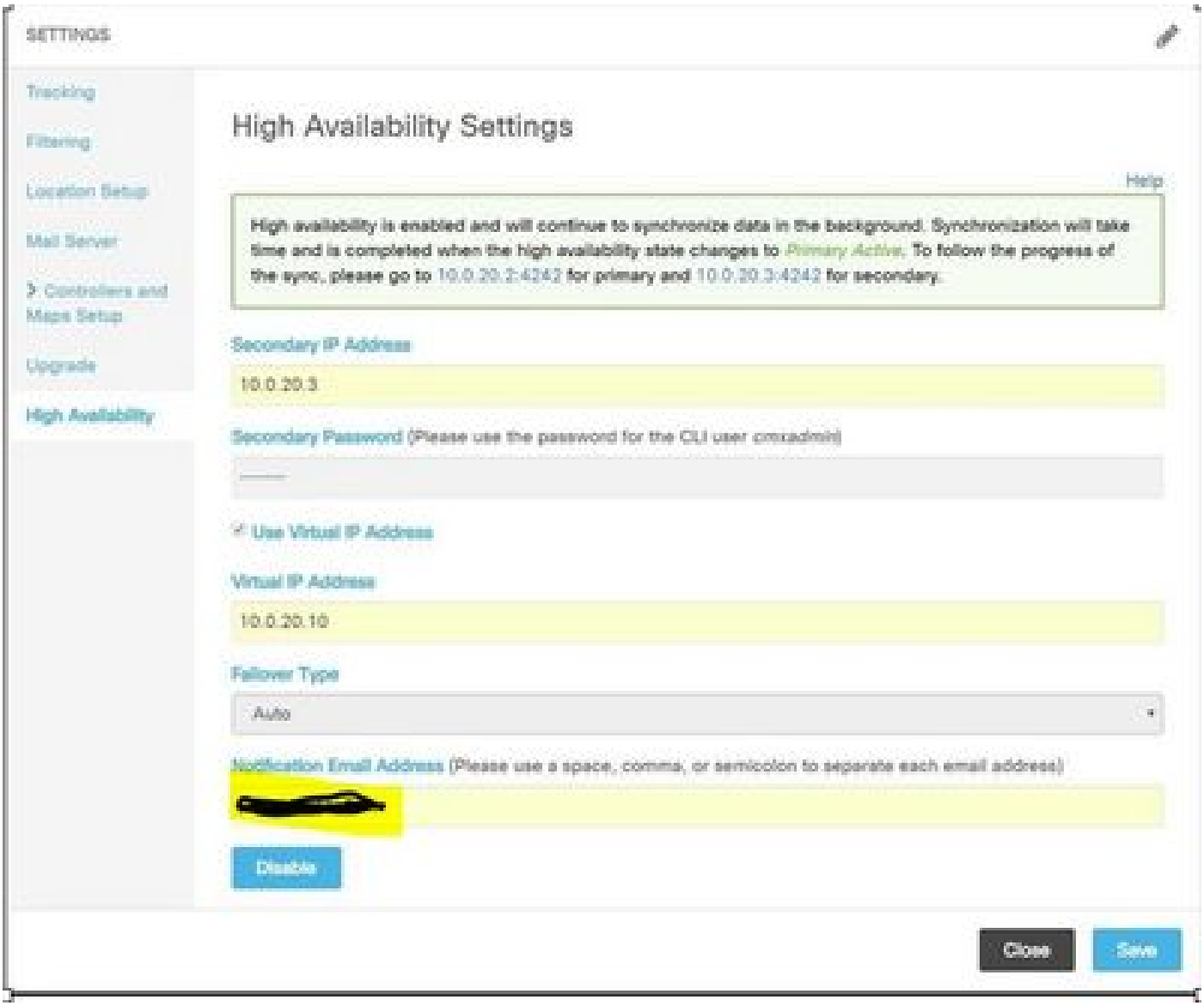
No CMX, navegue até a guia Sistema e clique no ícone Configurações. Isso exibirá um diálogo modal com uma variedade de configurações no CMX. Selecione a opção HA para exibir as opções necessárias para habilitar o HA. Endereço de e-mail de notificação que você pode fornecer onde deseja receber notificações.

Clique no botão Enable quando todas as opções forem fornecidas para iniciar a ativação do HA.



O CMX verificará as configurações de HA e começará a ativar a HA entre o primário e o secundário. A webUI retornará quando a configuração for iniciada com êxito.

Verifique se as configurações estavam corretas e se a sincronização está ocorrendo verificando a presença de uma tabela de "Alta disponibilidade" na página de configurações do CMX. Se não houver essa tabela e quando você voltar para a seção de configurações de HA, todos os campos de configuração estarão vazios, pois as informações estavam incorretas ou incorretas.

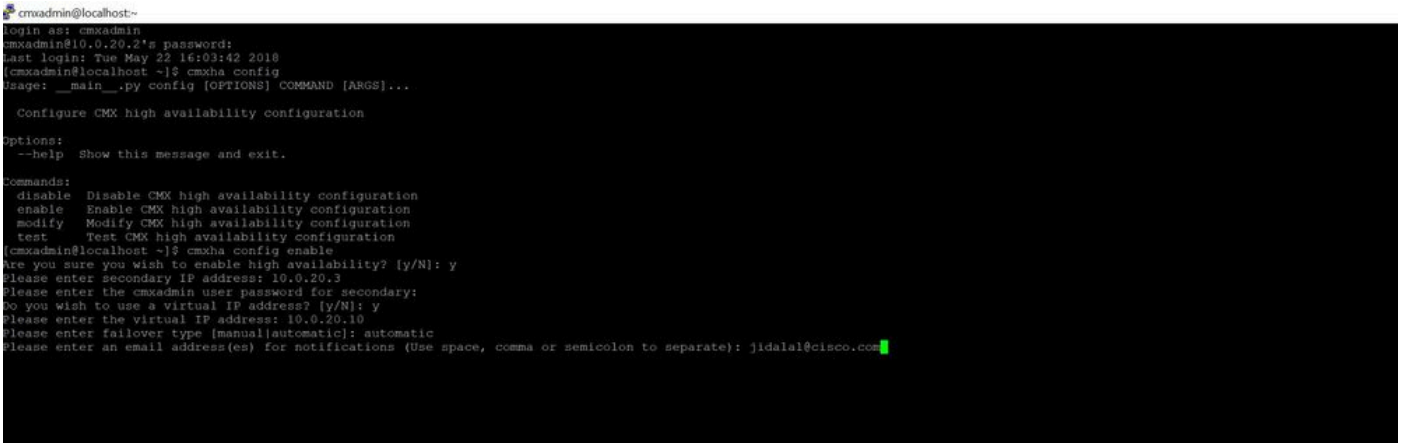


No entanto, o HA não concluiu a ativação. A sincronização inicial de todos os dados entre o servidor primário e o secundário pode levar um tempo significativo para ser concluída. A interface de usuário indicará o estado como Sincronização primária enquanto a sincronização estiver sendo feita.

Quando a sincronização for concluída com êxito, o servidor no principal entrará no estado Ativo primário.

Quando concluído, um alerta informativo será gerado no CMX. Além disso, será enviado um alerta por e-mail indicando que o sistema está ativo e sincronizando corretamente.

Habilitar CLI de alta disponibilidade (para referência):

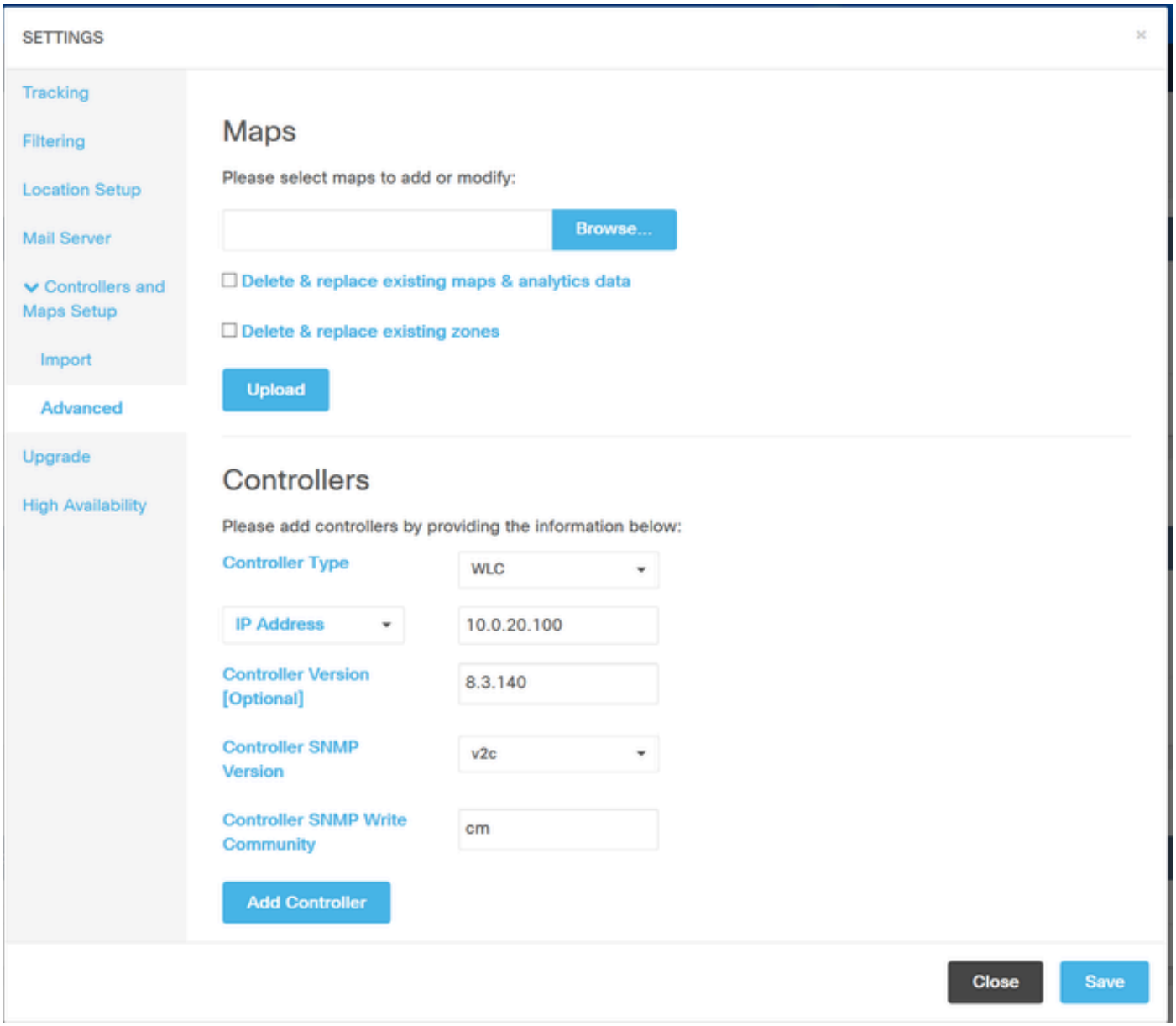


Etapa 3. Adicionar Cisco WLC ao CMX

Você pode adicionar Cisco WLCs com o uso da CLI ou da interface de usuário CMX, ou com o uso da Prime Infrastructure. Para este laboratório, você pode adicionar diretamente com o uso do CMX WebUI.

A configuração do controlador não funciona a menos que a conexão NMSP esteja correta. No entanto, mesmo que o controlador possa ser adicionado com êxito, mas a conexão talvez não funcione.

Navegue até Servidor CMX primário https://cmx_ip_address/. Clique na guia System > Settings Icon > Left Menu.



Depois de adicionar Cisco WLCs, você deve verificar se o status do controlador está ativo e em execução.

Para validar o status do controlador com o uso da interface de usuário, você precisa navegar até a guia Sistema. A lista de controladores é exibida na guia e o novo controlador deve aparecer em verde.

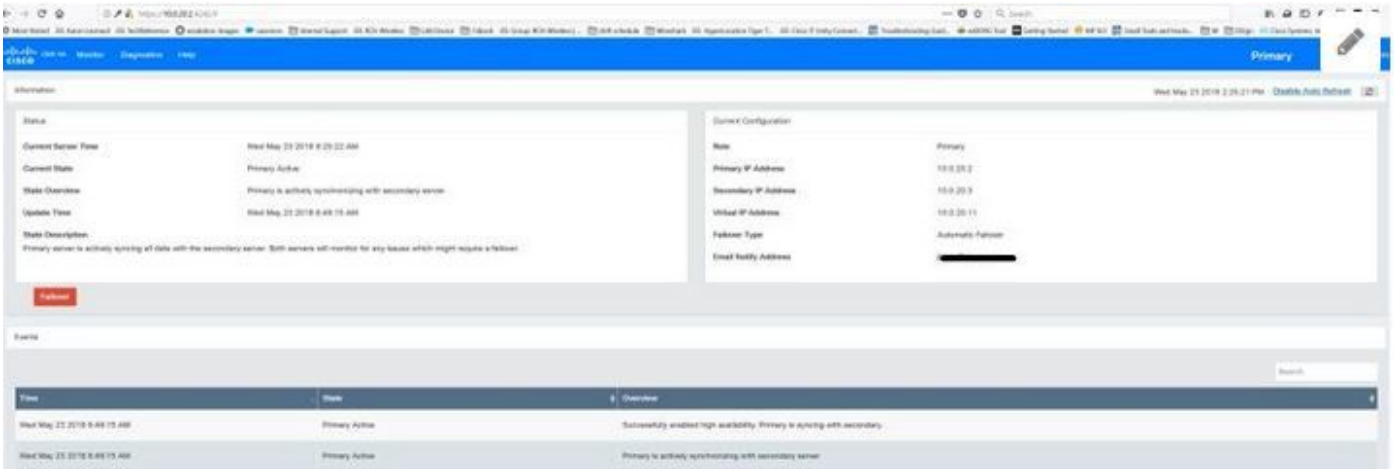
Etapa 4. Failover

O processo de failover envolve a transferência de operações para o CMX secundário, caso o principal fique inativo. Um failover pode ocorrer automaticamente quando o CMX detecta um problema no servidor primário. Um failover pode ser feito manualmente por um usuário na interface de usuário da Web ou na linha de comando. O progresso do failover pode ser monitorado com base no estado atual de cada sistema.

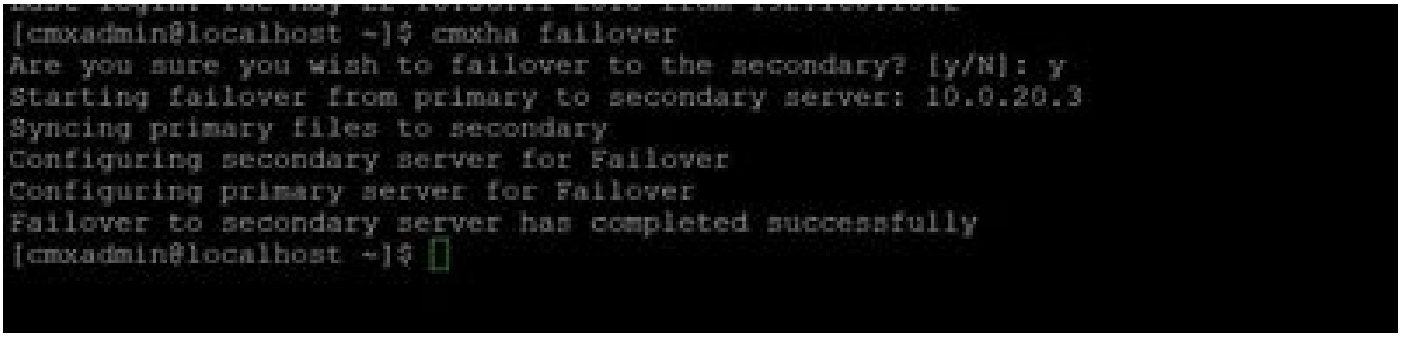
O processo de failover pode ser iniciado manualmente pelo usuário. O failover pode ser feito na interface da Web de alta disponibilidade do CMX ou na linha de comando do CMX.

Web de failover manual:

Faça login na interface da Web do CMX HA no primário ou secundário (https://server_ip:4242). A página do monitor terá um botão chamado Failover se os servidores estiverem sincronizando ativamente. Na parte superior direita, habilite a atualização automática.



CLI de failover manual (para referência):



Etapa 5. Failback

Para executar o CMX no secundário deve ser considerado como uma situação temporária até que a causa raiz da falha primária seja identificada. Quando a caixa principal for restaurada (ou uma nova caixa for fornecida), o processo de failback deverá ser iniciado. A outra opção é converter o sistema em um primário e substituir ou converter o outro sistema em um servidor secundário. Em ambos os casos, um servidor deve ser disponibilizado o mais rápido possível, já que o HA não está mais sendo sincronizado com um servidor secundário.

O processo de failback deve ser feito manualmente pelo usuário. O failback pode ser feito na interface da Web do CMX HA ou na linha de comando do CMX.

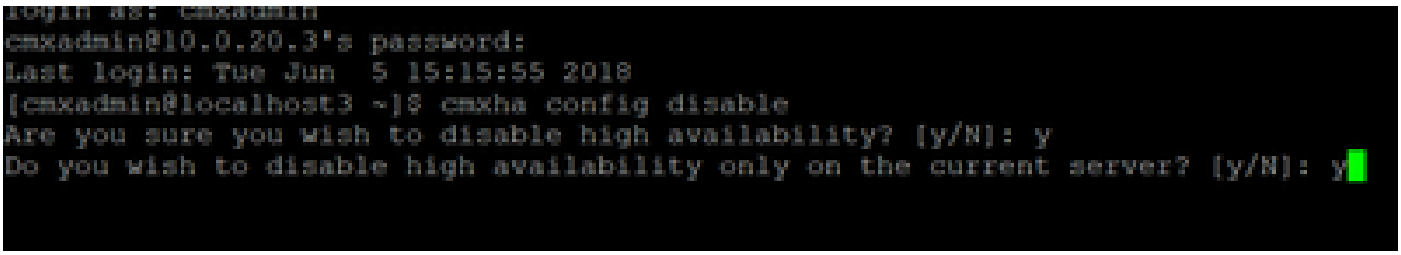
Web de failback manual:

Faça login na interface da Web do CMX HA no primário ou secundário (https://server_ip:4242). A página do monitor terá um botão chamado Failback se ambos os servidores indicarem que um failover está ativo.

GUI de failback manual:

Etapa 6. Atualizar/Desabilitar HA

No formato atual do CMX, é necessário desabilitar o HA para executar uma atualização. Para desabilitar o HA na linha de comando, execute cmxha config disable no CMX principal



Se você se esquecer de interromper o HA antes de uma atualização, o script de atualização o lembrará. Você terá que atualizar o servidor CMX secundário separadamente antes de reformar o HA.

Como recarregar com segurança o par HA CMX

Execute as próximas etapas para recarregar o par HA do CMX:

- Desligar CMX secundário
- Reinicializar CMX primário
- Verifique se o CMX principal está ativo e em execução
- Ligar o CMX secundário
- Verificar status de HA: informações de cmxha

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

O HA tem ajuda on-line para o recurso. A ajuda está completa para e fornece uma visão geral e mais detalhes sobre o recurso. Ele pode ser acessado aqui: https://cmx_ip_address:4242/help

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

Arquivos de pacote a serem verificados a partir do log tar:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.