Configuración de SSO de alta disponibilidad en Catalyst 9800 | Guía de inicio rápido

Contenido

Introducción

Este documento describe cómo configurar High Availability stateful switchover (SSO) en un RP+RMI, en un Catalyst 9800 WLC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de

- Modelo de configuración de Catalyst Wireless 9800.
- Conceptos de alta disponibilidad según la guía de HA SSO.

Componentes Utilizados

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

- Catalyst 9800-CL (v. 17.12.3).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Aunque la configuración de HA SSO solo puede requerir 3 de ellas, aquí se han utilizado 4 direcciones IP de la misma red que la interfaz de administración inalámbrica (WMI) para facilitar el acceso a la GUI del controlador.

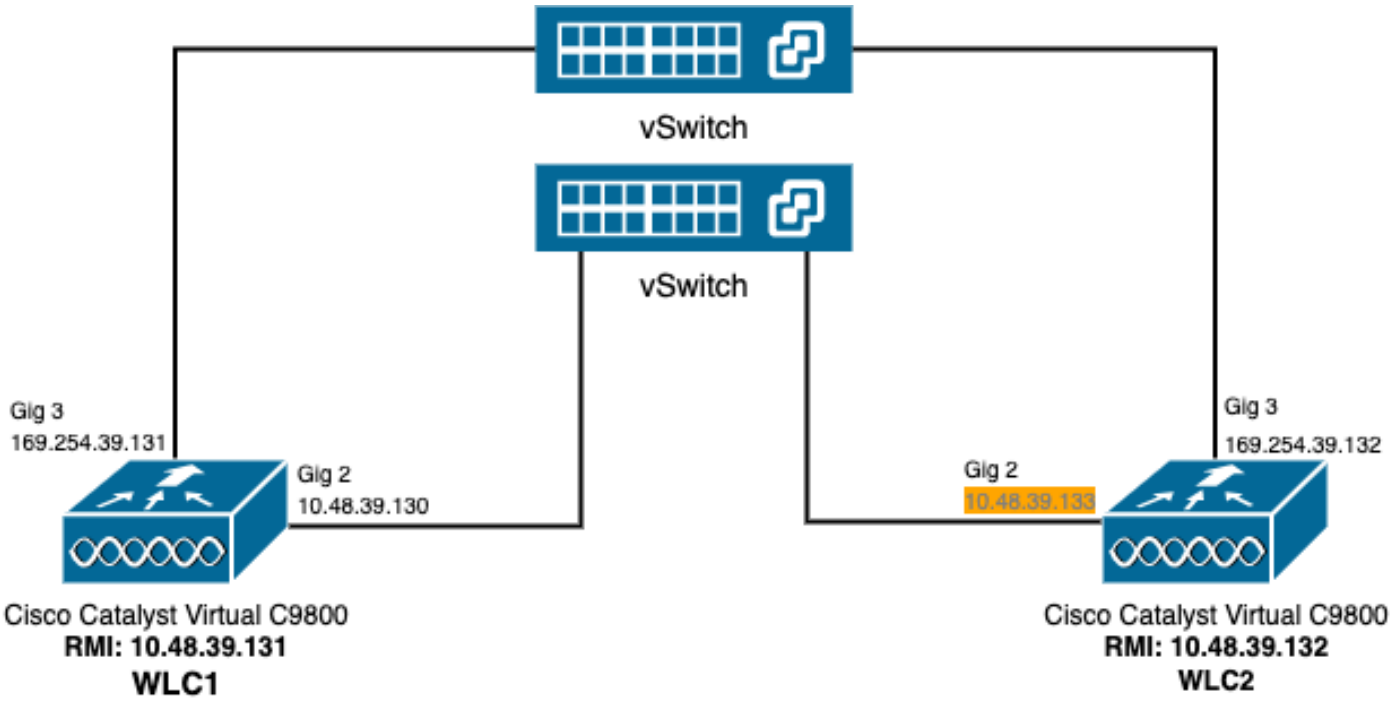
Antecedentes

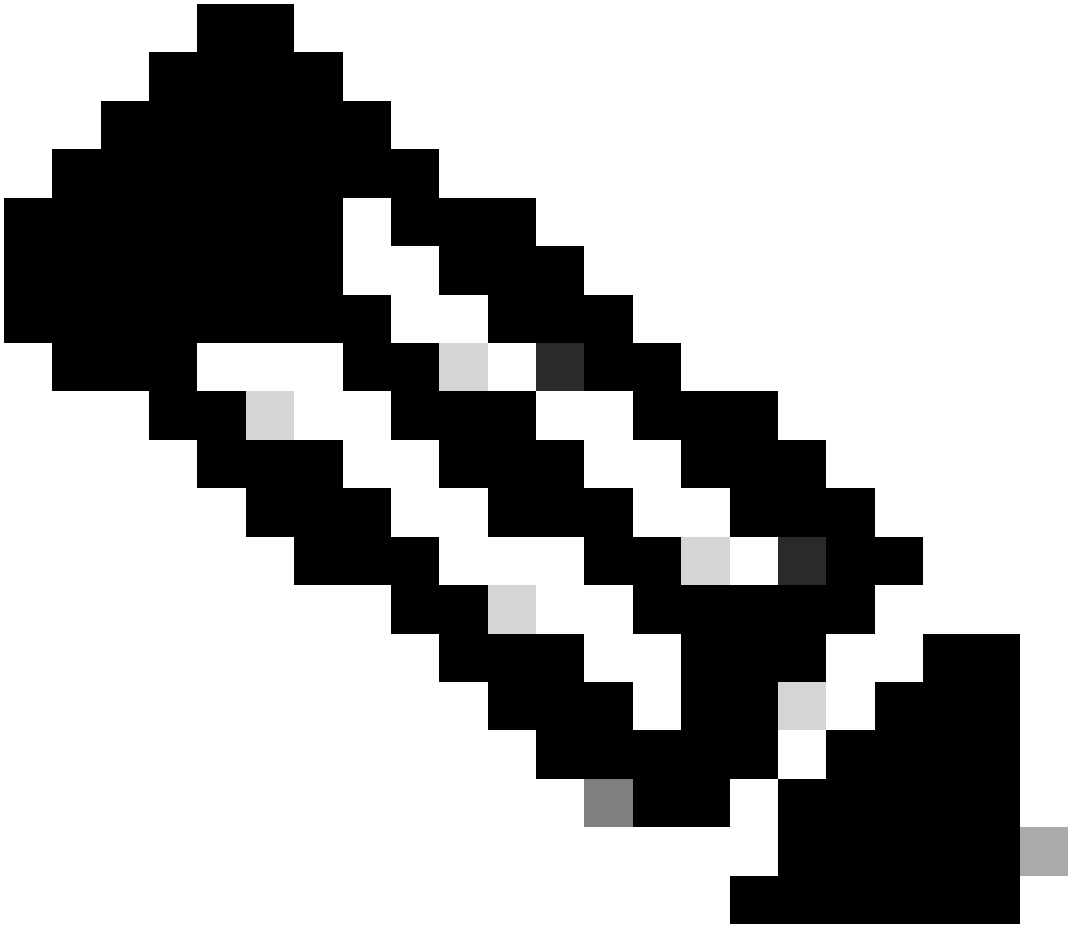
La capacidad SSO de alta disponibilidad en el controlador inalámbrico permite que el punto de acceso establezca un túnel CAPWAP con el controlador inalámbrico activo y el controlador inalámbrico activo para compartir una copia simétrica del AP y la base de datos del cliente con el controlador inalámbrico en espera. Cuando se producen los switchovers (es decir, el controlador activo falla y, por lo tanto, el Standby toma la mano), los AP unidos no entran en el estado de detección y los clientes no se desconectan. Solo hay un túnel CAPWAP mantenido a la vez entre los AP y el controlador inalámbrico que está en estado Activo.

Las dos unidades forman una conexión de peer a través de un puerto RP dedicado (o una interfaz virtual para VM) y ambos controladores comparten la misma dirección IP en la interfaz de administración. La interfaz RP se utiliza para sincronizar la configuración masiva e incremental en tiempo de ejecución y garantizar el estado operativo de ambos controladores del par HA. Además, cuando se utiliza RMI + RP, tanto los controladores en espera como los activos tienen una interfaz de administración de redundancia (RMI) a la que se asignan direcciones IP, es decir, que se utiliza para garantizar la accesibilidad del gateway. El estado CAPWAP de los puntos de acceso que están en estado de ejecución también se sincroniza desde el controlador inalámbrico activo al controlador inalámbrico Hot-Standby, que permite que los puntos de acceso se conmuten completamente por estado cuando falla el controlador inalámbrico activo. Los AP no pasan al estado de detección cuando falla el controlador inalámbrico activo, y el controlador inalámbrico en espera toma el control como el controlador inalámbrico activo para servir a la red.

Configurar

Diagrama de la red


vSwitch
vSwitch
Gig 3
169.254.39.131
Gig 2
10.48.39.130
Gig 3
169.254.39.132
Gig 2
10.48.39.133
Cisco Catalyst Virtual C9800
RMI: 10.48.39.131
WLC1
Cisco Catalyst Virtual C9800
RMI: 10.48.39.132
WLC2



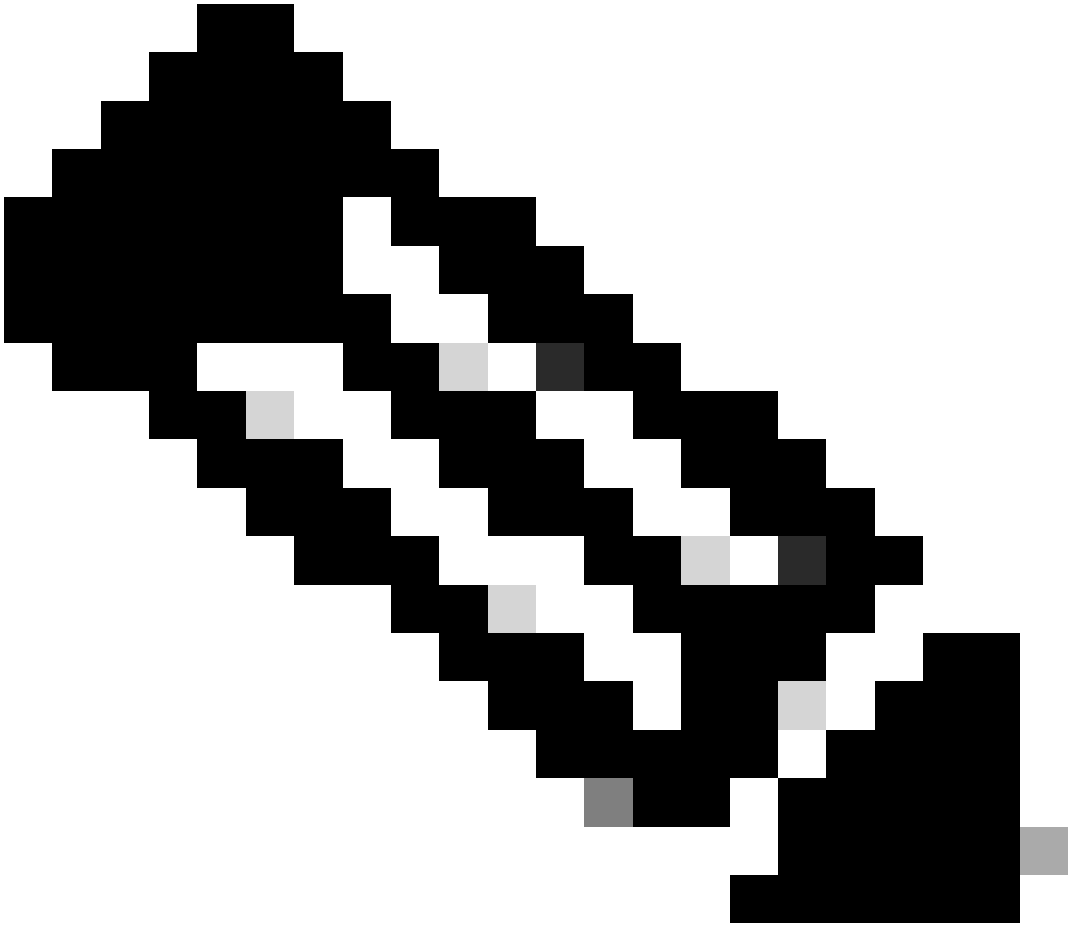
Nota: En naranja se resalta la dirección IP temporal asignada a la interfaz virtual GigabitEthernet 2 del controlador 9800-CL designado como WLC2. Esta dirección IP se define temporalmente como WMI para WLC2 y permite el acceso a la GUI de esta instancia para facilitar la configuración de HA SSO. Una vez configurado HA SSO, esta dirección se libera, ya que sólo se utiliza un único WMI para un par de controladores HA SSO.

Configuraciones

En este ejemplo, el stateful switchover (SSO) de alta disponibilidad (HA) se configura entre dos instancias de 9800-CL, que ejecutan la misma versión del software Cisco IOS, que se han configurado con WMI separados y con la GUI accesible en

- Dirección IP 10.48.39.130 para la primera, conocida como WLC1;
- Dirección IP 10.48.39.133 para la segunda, denominada WLC2.

Además de estas direcciones IP, se han utilizado 2 direcciones adicionales en la misma subred (y VLAN), a saber, 10.48.39.131 y 10.48.39.132. Éstas son las direcciones IP de la interfaz de administración de redundancia (RMI) para el chasis 1 (WLC1) y el chasis 2 (WLC2), respectivamente.



Nota: Una vez que se ha configurado HA entre los dos controladores, 10.48.39.133 se libera y 10.48.39.130 se convierte en el único WMI de mi configuración. Por lo tanto, después de la configuración, sólo se utilizan 3 direcciones IP, la de WMI y la de las RMI.

La configuración de las interfaces para ambos dispositivos antes incluso de iniciar la configuración de HA debe ser similar a las proporcionadas en este ejemplo.

```
WLC1#show running-config | s interface
interface GigabitEthernet1
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet2
 switchport trunk allowed vlan 39
 switchport mode trunk
 negotiation auto
 no mop enabled
 no mop sysid
```

```
interface GigabitEthernet3
 negotiation auto
 no mop enabled
 no mop sysid
interface Vlan1
 no ip address
 shutdown
 no mop enabled
 no mop sysid
interface Vlan39
 ip address 10.48.39.130 255.255.255.0
 no mop enabled
 no mop sysid
wireless management interface Vlan39
```

```
WLC2#show running-config | s interface
interface GigabitEthernet1
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet2
 switchport trunk allowed vlan 39
 switchport mode trunk
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet3
 negotiation auto
 no mop enabled
 no mop sysid
interface Vlan1
 no ip address
 shutdown
 no mop enabled
 no mop sysid
interface Vlan39
 ip address 10.48.39.133 255.255.255.0
 no mop enabled
 no mop sysid
wireless management interface Vlan39
```

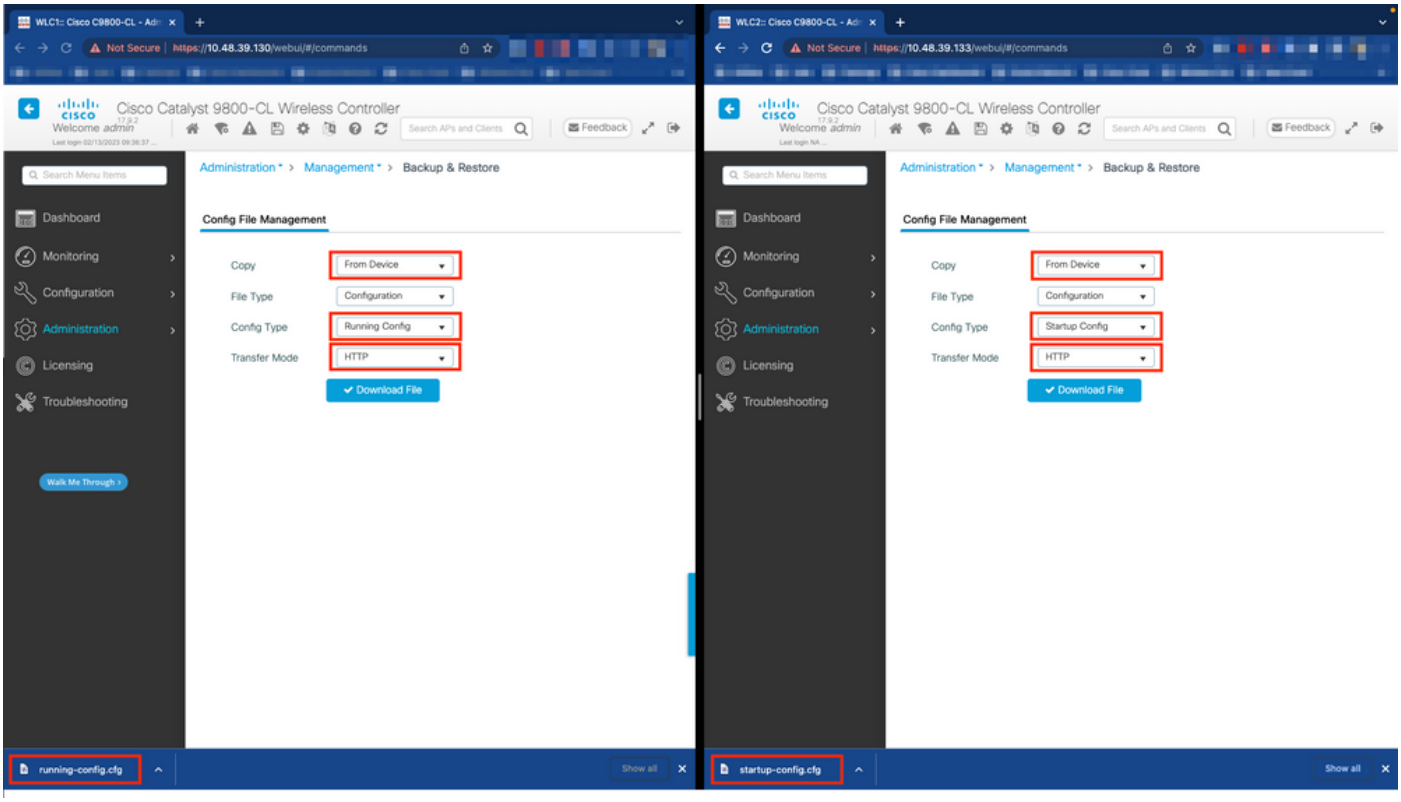
En este ejemplo, el WLC1 se designa como el controlador primario (que es el chasis 1) mientras que el WLC2 es el secundario (que es el chasis 2). Esto significa que el par de HA hecho de los 2 controladores utiliza la configuración de WLC1 y que el de WLC2 se pierde después del proceso.

Paso 1. (Opcional) Realice una copia de seguridad de los archivos de configuración de inicio y configuración en ejecución de los controladores.

Se puede producir un manejo incorrecto y la configuración se puede perder. Para evitar esto, se recomienda encarecidamente realizar una copia de seguridad de la configuración de inicio y ejecución desde ambos controladores utilizados en la configuración de HA. Esto se puede realizar fácilmente mediante la GUI del 9800 o la CLI.

Desde la GUI:

Desde la pestaña *Administration → Management → Backup & Restore* de la GUI del 9800 (consulte la captura de pantalla), se puede descargar la configuración de inicio y ejecución que actualmente utiliza el controlador.



En este ejemplo, tanto el inicio (lado izquierdo) como la configuración (lado derecho) se descargan directamente, a través de HTTP, en el dispositivo que aloja el navegador utilizado para acceder a la GUI del WLC. Uno puede ajustar fácilmente el modo de transferencia y el destino del archivo para hacer una copia de seguridad, con el campo Modo de transferencia.

Desde la CLI:

```
WLCx#copy running-config tftp://<SERVER-IP>/run-backup_x.cfg
Address or name of remote host [<SERVER-IP>]?
Destination filename [run-backup_x.cfg]?
!!
19826 bytes copied in 1.585 secs (12509 bytes/sec)
WLCx#copy startup-config tftp://<SERVER-IP>/start-backup_x.cfg
Address or name of remote host [<SERVER-IP>]?
Destination filename [start-backup_x.cfg]?
!!
20482 bytes copied in 0.084 secs (243833 bytes/sec)
```

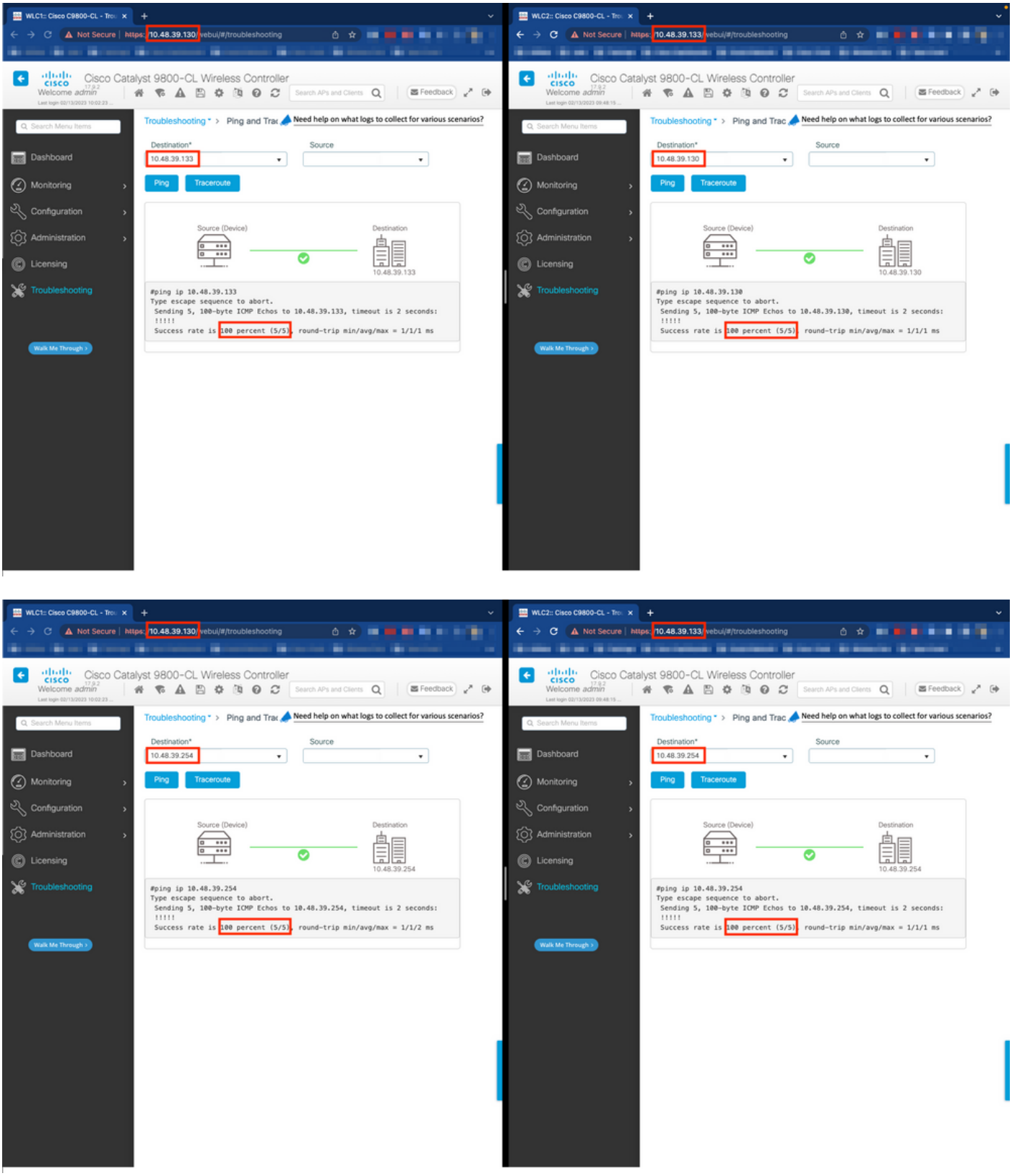
Reemplace el <SERVER-IP> por la IP del servidor TFTP en la que se copia el archivo de configuración de inicio/ejecución.

Paso 2. (Opcional) Garantizar la conectividad de red.

Tanto desde las GUI de WLC como desde las CLI, se pueden realizar sencillas pruebas de conectividad, es decir, hacer ping en la puerta de enlace desde ambos dispositivos y hacer ping entre los dispositivos. Esto garantiza que ambos controladores tengan la conectividad requerida para configurar HA.

Desde la GUI:

La herramienta *Ping and Traceroute* de la pestaña *Troubleshooting* de la GUI del 9800 se puede utilizar para probar la conectividad entre los controladores mismos y entre cada WLC y su gateway de red, como se muestra en estas figuras.



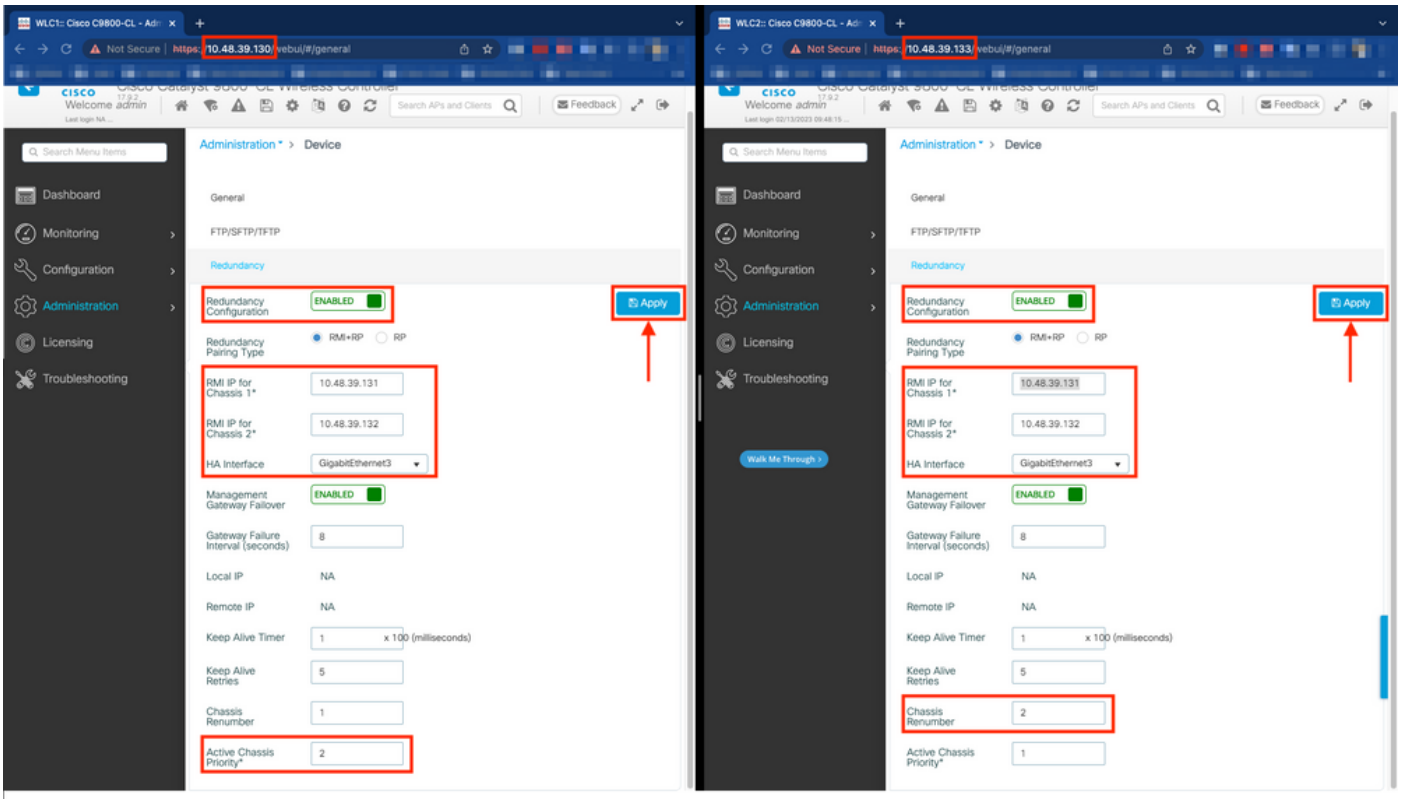
Desde la CLI:

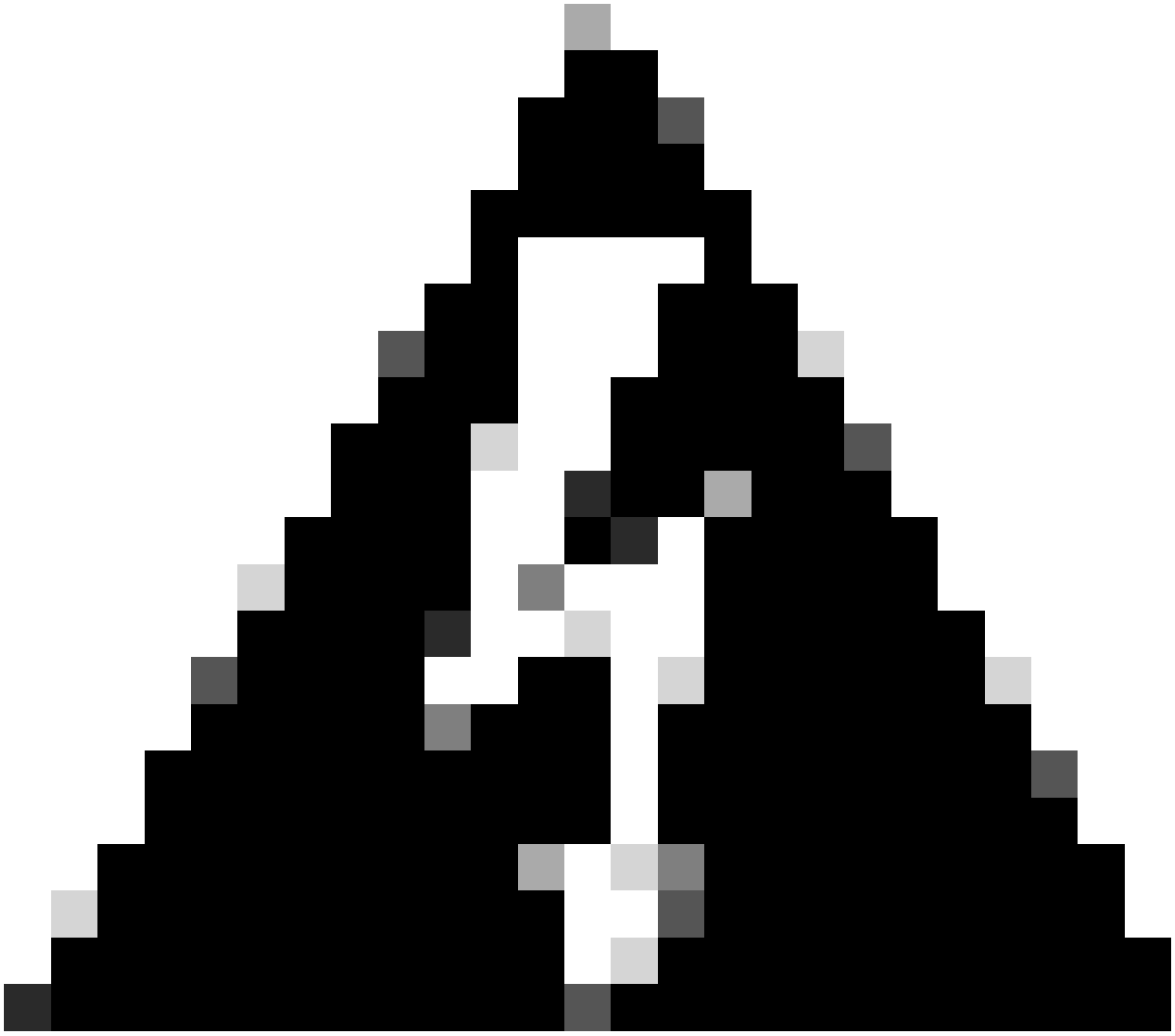
```
WLCx#ping 10.48.39.133 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.48.39.133, t
```

Paso 3. Configure la redundancia con el tipo de emparejamiento RMI + RP.

Con la conectividad asegurada entre cada dispositivo, se puede configurar la redundancia entre los controladores. Esta captura de pantalla

muestra cómo se realiza la configuración desde la pestaña *Redundancia* de la página *Administración→ Dispositivo* de la GUI del 9800.





Advertencia: Para este ejemplo, el WLC1 se ha designado como controlador primario, lo que significa que éste es el que cuya configuración se replica al otro controlador. Asegúrese de aplicar la prioridad/renumeración adecuada del chasis para utilizar la configuración adecuada con su par HA y no perder ninguna parte de él.

Vamos a revisar los campos configurados y su finalidad

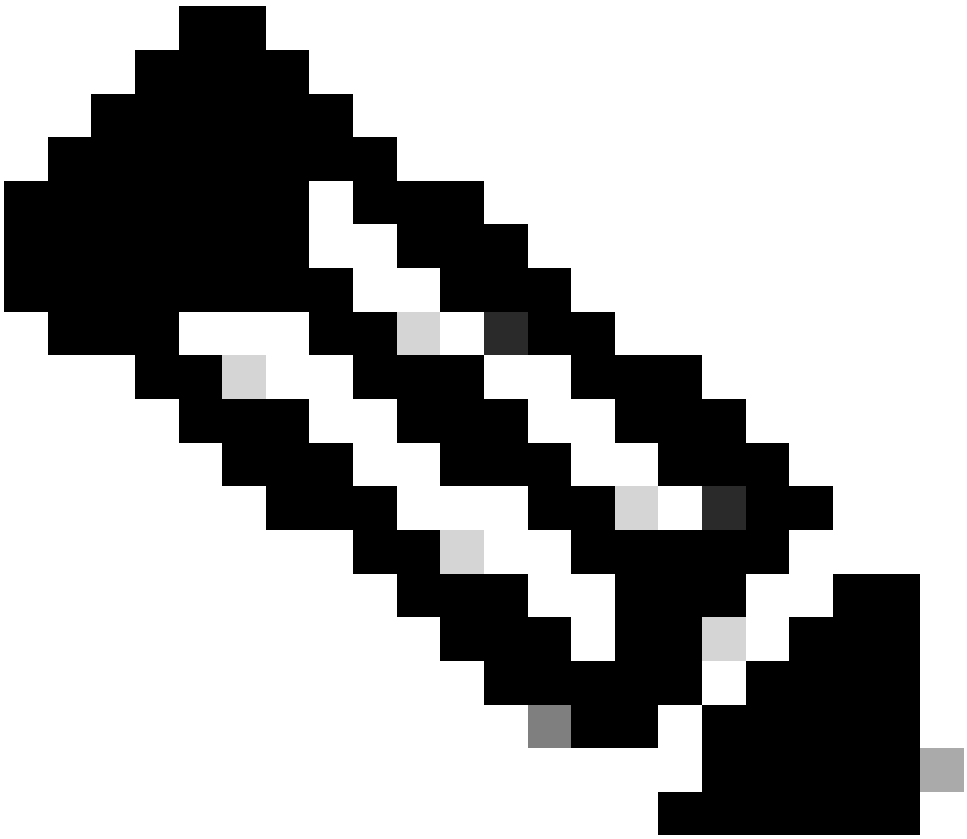
- **Configuración de Redundancia:** esto debe estar habilitado para utilizar redundancia entre los WLC.

- **Tipo de emparejamiento de redundancia:** dado que esta guía cubre HA SSO usando la configuración RMI, el tipo de emparejamiento configurado debe ser RMI + RP, usando tanto la interfaz de administración de redundancia como el puerto de

redundancia. También se puede optar por configurar la redundancia usando solamente el puerto de redundancia. Sin embargo, cuando se elige RP solamente, la accesibilidad del gateway no se verifica, solamente el estado WLC redundante es

- **IP RMI para chasis 1/2:** estos campos asignan las direcciones IP proporcionadas a la interfaz de redundancia designada para ambas instancias. En este ejemplo, las IP RMI para el chasis 1 y 2 se han configurado como 10.48.39.131 y 10.48.39.132 respectivamente, tal como se describió anteriormente y se muestra en el diagrama de red.

- **Interfaz HA:** cuando se utilizan appliances virtuales, la asignación entre las tarjetas de interfaces de red virtuales (vNIC) del hipervisor y las interfaces de red de la máquina virtual se puede configurar de diferentes formas. Por lo tanto, la interfaz utilizada para la redundancia es configurable para Cisco Catalyst 9800-CLs. Aquí se ha utilizado GigabitEthernet 3, tal y como se recomienda en la guía de implementación de 9800-CL.



Nota: al utilizar dispositivos físicos C9800, la interfaz utilizada en HA y RP es la predeterminada y no se puede configurar. De hecho, los WLC del hardware 9800 tienen una interfaz de redundancia dedicada que se separa de sus redes.

- **Failover de gateway de administración:** como se detalla en la guía de configuración de HA SSO, este método de redundancia implementa la comprobación de gateway predeterminada, que se realiza mediante el envío periódico de ping ICMP (Internet Control Message Protocol, Protocolo de mensajes de control de Internet) al gateway. Tanto los controladores activos como los de reserva utilizan la IP RMI como IP de origen para estas comprobaciones. Estos mensajes se envían en un intervalo de 1 segundo.

- **Intervalo de fallo de puerta de enlace:** representa la cantidad de tiempo durante el cual debe fallar consecutivamente una comprobación de puerta de enlace antes de que se declare que la puerta de enlace no es accesible. De forma predeterminada, esta opción está configurada como 8 segundos. Dado que las comprobaciones de la puerta de enlace se envían cada segundo, esto representa 8 fallos consecutivos para alcanzar la puerta de enlace.

- **IP local/remota:** IP de RP configurada para los chasis 1 y 2. Estas direcciones IP se generan automáticamente como 169.254.x.x, donde x.x se deriva de los últimos dos octetos de la interfaz de administración.

- **Keep Alive Timer:** como se detalla en la guía de configuración de HA SSO, el chasis activo y en espera se envían mensajes de señal de mantenimiento entre sí para asegurarse de que ambos aún estén disponibles. El temporizador de señal de mantenimiento es la cantidad de tiempo que se separa el envío de 2 mensajes de señal de mantenimiento entre cada chasis. De forma predeterminada, los mensajes keepalive se envían cada 100 ms. A menudo se recomienda aumentar este valor con 9800-CL para evitar los switchovers abusivos cada vez que la infraestructura de VM introduce pequeños retrasos (instantáneas, etc.)

- **Reintentos de Mantener Activo:** este campo configura el valor de reintento de keepalive del par antes de afirmar que el par está inactivo. Si se utilizan el temporizador de mantenimiento activo y el valor predeterminado de reintentos, se reclama un peer down si los 5 mensajes de mantenimiento activo enviados en el intervalo de tiempo de 100 ms quedan sin respuesta (es decir, si el link de redundancia está inactivo durante 500 ms).

- **Número de chasis:** el número de chasis que debe utilizar el dispositivo (1 o 2).

    - En el WLC2 (10.48.39.133), el chasis se renumera a 2. De forma predeterminada, el número de chasis es 1. Las direcciones IP de los puertos RP se derivan de RMI. Si el número de chasis es el mismo en ambos controladores, la derivación IP del puerto RP local es la misma y la detección falla. Renumérese el chasis para evitar este escenario denominado Activo-Activo.

- **Prioridad de chasis activo:** la prioridad utilizada para definir qué configuración debe utilizar el par HA. El dispositivo con la prioridad

más alta es el que se replica en el otro. Por lo tanto, se pierde la configuración del chasis con la prioridad más baja.

- En el WLC1 (10.48.39.130), la prioridad del chasis activo se ha configurado en 2. Esto es para asegurarse de que este chasis se elija como el activo (y por lo tanto, que se utilice su configuración) en el par HA creado.

Una vez realizadas estas configuraciones, utilice el botón *Apply* para aplicar la configuración a los controladores.

Desde la CLI

Primero, configure una dirección IP secundaria en la interfaz virtual utilizada para configurar la RMI en ambos dispositivos.

```
WLC1#configure terminal WLC1(config)#interface vlan 39 WLC1(config-if)# ip address 10.48.39.131 255.255
```

```
WLC2#configure terminal WLC2(config)#interface vlan 39 WLC2(config-if)# ip address 10.48.39.132 255.255
```

A continuación, habilite la redundancia en ambos dispositivos

```
WLC1#configure terminal WLC1(config)#redundancy WLC1(config-red)#mode sso WLC1(config-red)#end
```

```
WLC2#configure terminal WLC2(config)#redundancy WLC2(config-red)#mode sso WLC2(config-red)#end
```

Configure la prioridad del chasis, tal como el WLC1 se convierte en el controlador primario

```
WLC1#show chassis Chassis/Stack Mac Address : 0001.0202.aabb - Local Mac Address Mac persistency wait t
```

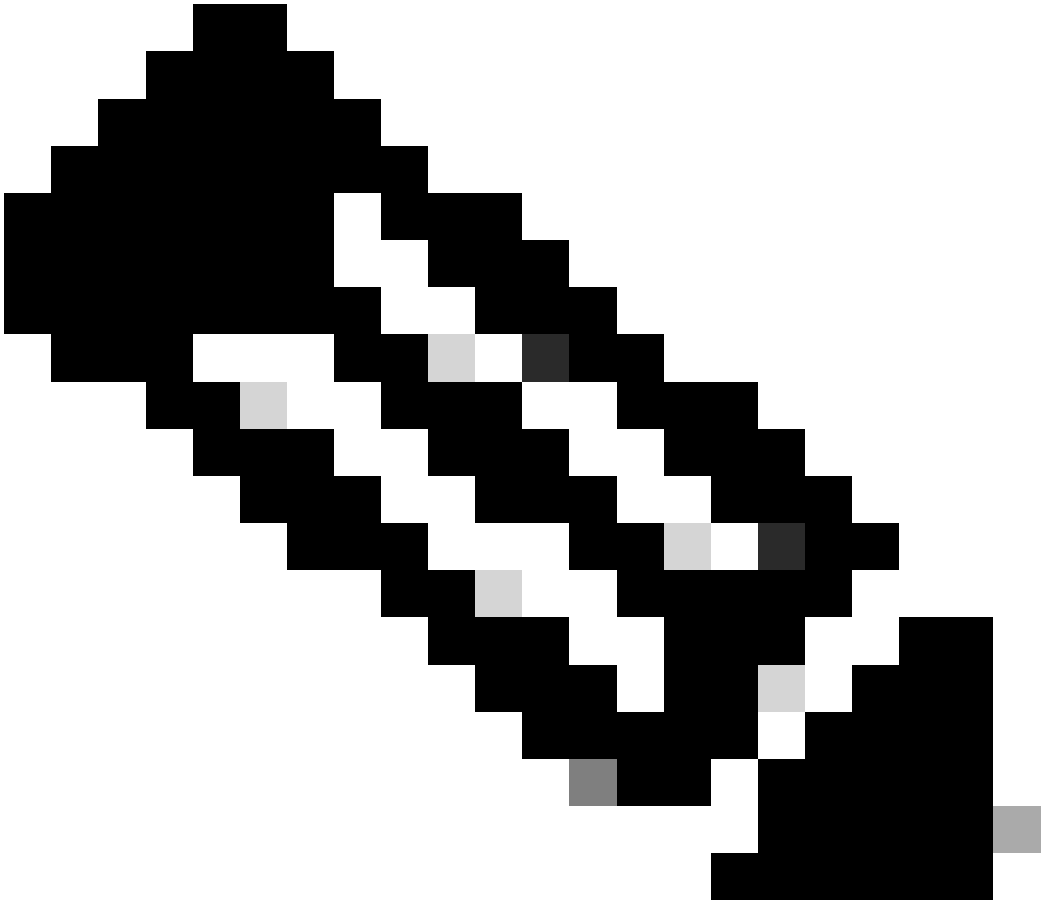
Renumérese el chasis para el WLC2 que se convierte en el controlador secundario

```
WLC2#show chassis Chassis/Stack Mac Address : 0001.0202.aabb - Local Mac Address Mac persistency wait t
```

Finalmente, configure RMI en ambos dispositivos

```
WLC1#chassis redundancy ha-interface GigabitEthernet 3 WLC1#configure terminal WLC1(config)#redun-manag
```

```
WLC2#chassis redundancy ha-interface GigabitEthernet 3 WLC2#configure terminal WLC2(config)#redun-manag
```



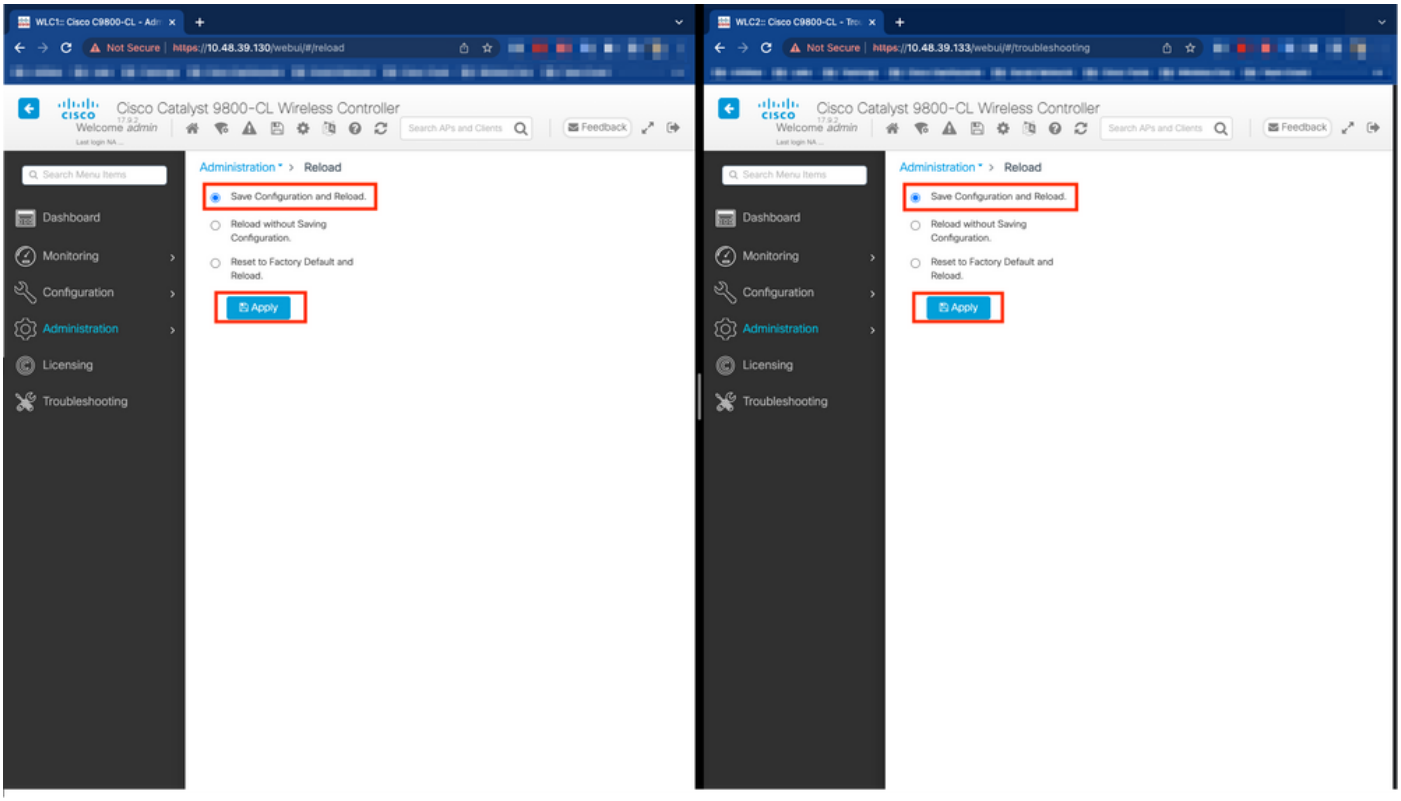
Nota: En cuanto a la configuración de la GUI, en el Catalyst 9800 virtual, la interfaz utilizada por el controlador debe seleccionarse entre las disponibles. Como se recomienda, GigabitEthernet 3 se utiliza aquí y se configura gracias al chassis redundancy ha-interface GigabitEthernet 3 comando. Este comando no forma parte de la configuración en ejecución, sin embargo, la interfaz utilizada por HA se puede ver en las variables de entorno ROMMON de instancia. Éstas se pueden ver usando el show romvar comando.

Paso 4. Recargue los controladores.

Para que se forme el par HA y la configuración sea efectiva, ambos controladores deben recargarse al mismo tiempo una vez que se haya guardado la configuración realizada en el paso 3.

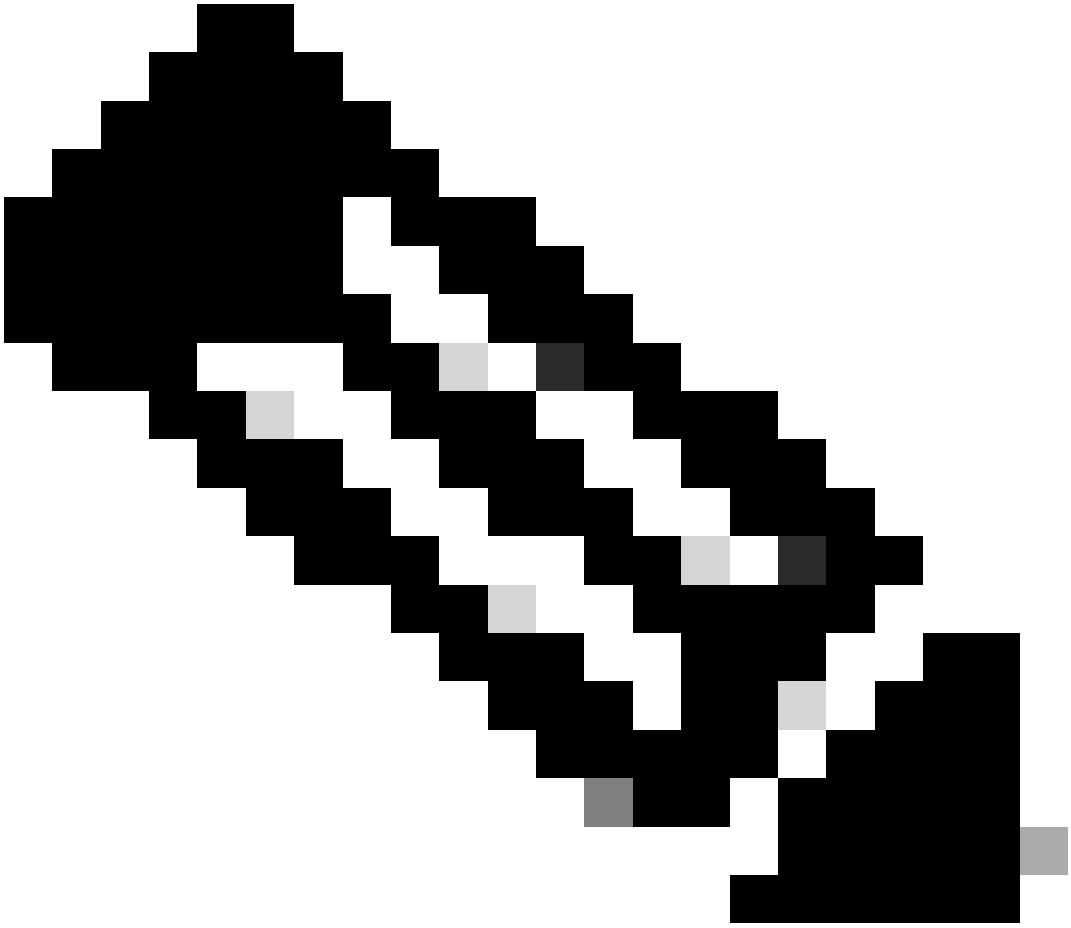
Desde la GUI:

Se puede utilizar la página Administration Reload (Recarga de administración) de ambas interfaces gráficas de usuario para reiniciar los controladores, como se muestra en esta captura de pantalla.



Desde CLI:

```
WLCx#reload Reload command is being issued on Active unit, this will reload the whole stack Proceed wit
```



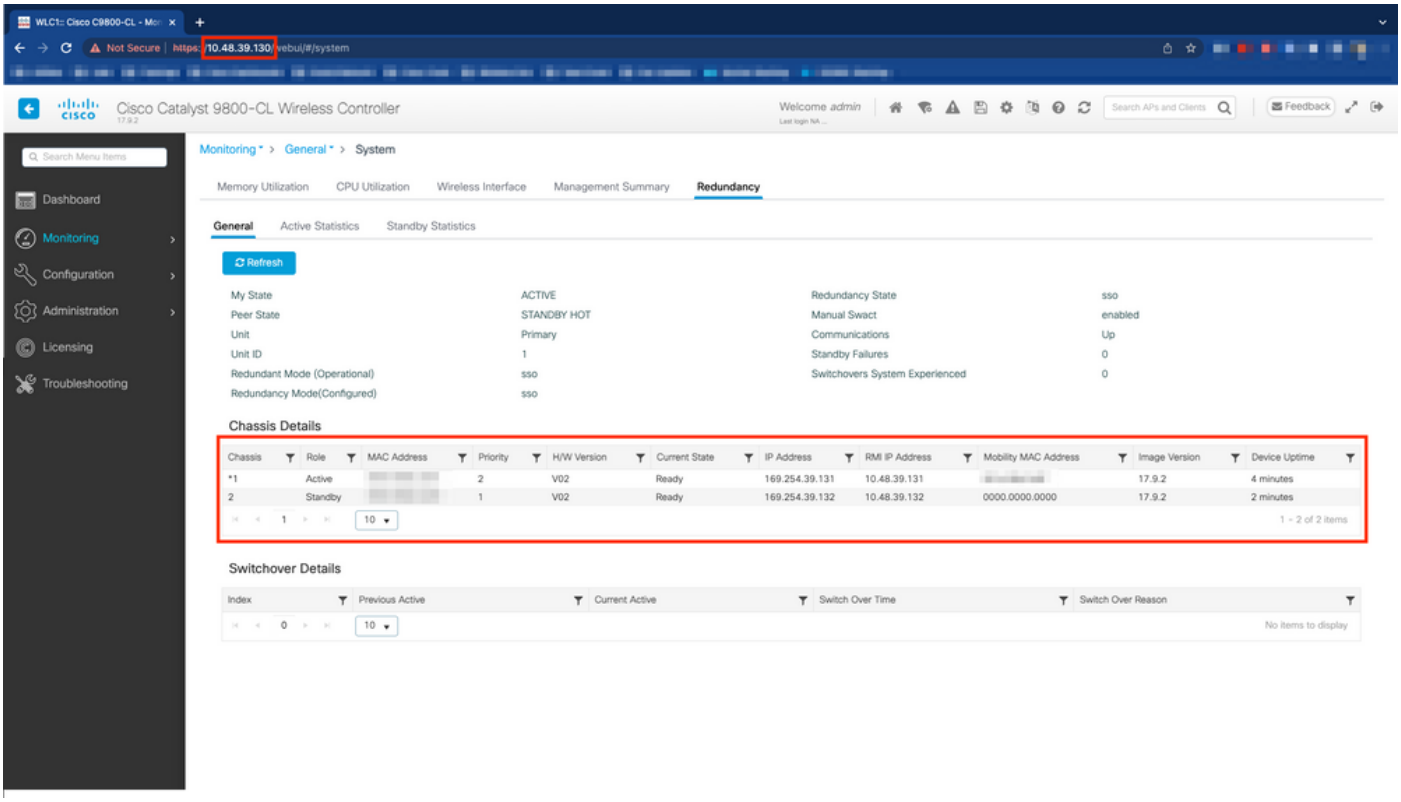
Nota: Si utiliza un servidor AAA, debe agregar la dirección IP de WMI y la dirección IP de RMI como clientes AAA en el servidor AAA. El WLC en espera siempre utiliza su IP RMI para autenticar las sesiones SSH. El WLC activo utiliza RMI y WMI para alcanzar al servidor AAA.

Verificación

Una vez que ambos controladores del par HA se descubren entre sí y crean el par HA deseado, un controlador (el principal) puede supervisar los dos chasis desde la GUI o CLI.

Desde la GUI:

Para supervisar la configuración de redundancia desde la GUI del 9800, navegue hasta la pestaña Redundancia desde la página Monitoring > General > System (Supervisión > General > Sistema), como se muestra en esta captura de pantalla.



Desde CLI:

```
WLC#show chassis rmi Chassis/Stack Mac Address : 0050.568d.cdf4 - Local Mac Address Mac persistency wai
```

```
WLC#show redundancy Redundant System Information : ------------------------------ Available system upti
```

Troubleshoot

Reflejo de ventanilla única

Lo habitual no show tech wireless incluye comandos que permitan comprender las fallas HA de un par HA ni su estado actual correctamente. Recopile este comando para tener la mayoría de los comandos relacionados con HA en una sola operación :

```
WLC#show tech wireless redundancy
```

Comandos show

Para el estado de los puertos de redundancia, se pueden utilizar estos comandos.

```
WLC#show chassis detail Chassis/Stack Mac Address : 0050.568d.2a93 - Local Mac Address Mac persistency
```

Este comando muestra el número de chasis y el estado del puerto redundante, útil como primer paso para solucionar problemas.

Para verificar los contadores de señal de mantenimiento en el puerto de señal de mantenimiento, se pueden utilizar estos comandos.

```
WLC#show platform software stack-mgr chassis active R0 sdp-counters Stack Discovery Protocol (SDP) Coun
```

Otros comandos

Es posible tomar una captura de paquetes en el puerto redundante del controlador con estos comandos

```
WLC#test wireless redundancy packetdump start Redundancy Port PacketDump Start Packet capture started o
```

Las capturas realizadas con estos comandos se guardan en el bootflash: del controlador, bajo el nombre haIntCaptureLo.pcap.

También se puede ejecutar una prueba de keepalive en el puerto redundante con este comando.

```
WLC#test wireless redundancy rping Redundancy Port ping PING 169.254.39.131 (169.254.39.131) 56(84) byt
```

Más detalles

Para ver la configuración de Variables ROMMON que nos muestra cómo se refleja la configuración real en las variables, puede utilizar este comando.

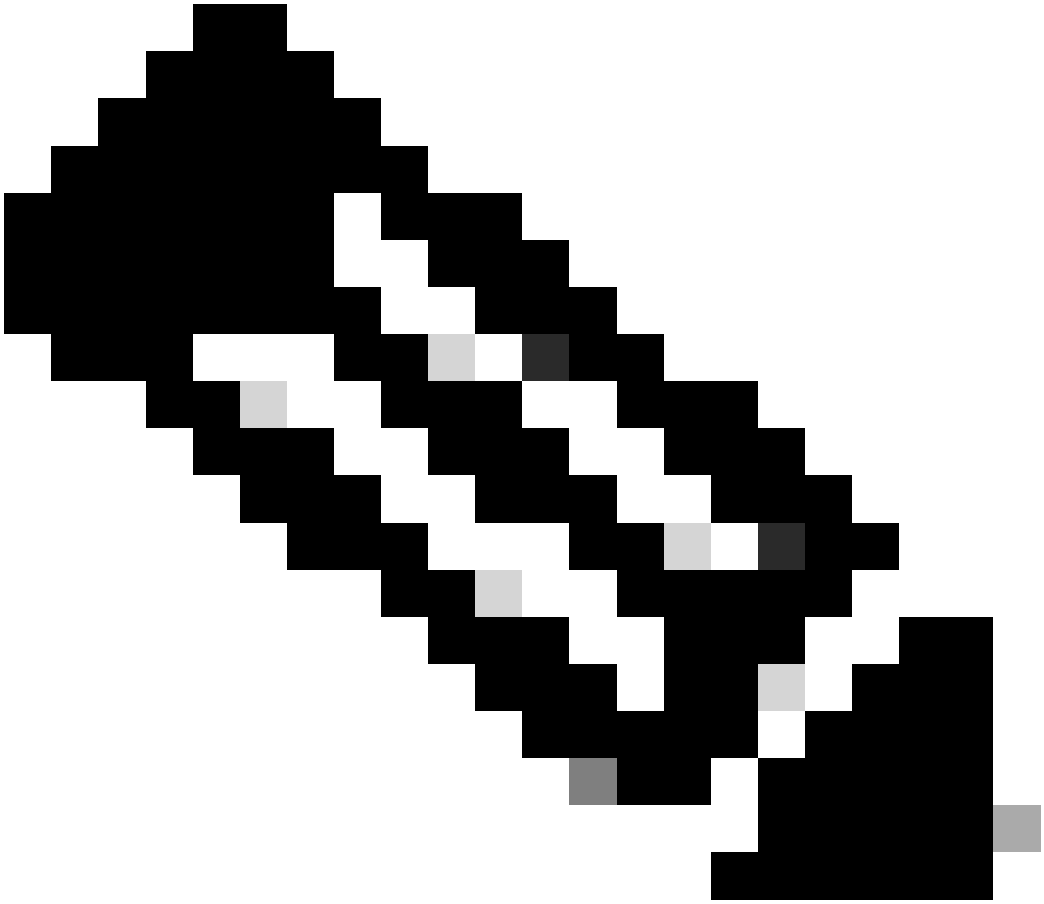
```
WLC#show romvar ROMMON variables: MCP_STARTUP_TRACEFLAGS = 00000000:00000000 SWITCH_NUMBER = 2 CONFIG_F
```

Este comando muestra la prioridad del chasis, tanto los detalles de RMI como RP, el tiempo de espera del par junto con detalles más útiles.

También podemos monitorear los procesos que ejecutan HA SSO en el WLC que son dos procesos, a saber, stack_mgr y rif_mgr.

Para hacer esto, recopile los seguimientos siempre activos a un archivo de texto usando el comando, el parámetro de tiempo aquí se puede ajustar para cubrir el marco de tiempo que queremos resolver.

```
show logging process stack_mgr start last 30 minutes to-file bootflash:stack_mgr_logs.txt show logging
```



Nota: Es importante tener en cuenta que el puerto de servicio del WLC en espera está desactivado e inalcanzable mientras el controlador actúa como en espera.

Escenarios típicos

Usuario forzado

Si observa el historial de switchover, puede ver "user forced" (el usuario forzado), que aparece cuando un usuario inició un switchover entre los controladores, usando el redundancy force-switchover comando.

```
WLC#show redundancy switchover history Index Previous Current Switchover Switchover active active reaso
```

Unidad activa quitada

Si observa el historial de switchover, puede ver "unidad activa eliminada" que apunta a una pérdida de comunicación en el puerto redundante entre los dos controladores.

```
WLC#show redundancy switchover history Index Previous Current Switchover Switchover active active reaso
```

Esto puede suceder si el link entre los dos controladores deja de funcionar, pero también puede suceder si una unidad WLC cae repentinamente (falla de energía) o se bloquea. Es interesante monitorear ambos WLCs para ver si tienen informes del sistema que indican caídas/reinicios inesperados.

GW perdido activo

Si observa el historial de switchover, puede ver "GW perdido activo" que apunta a una pérdida de comunicación con el gateway en el puerto RMI.

```
WLC#show redundancy switchover history Index Previous Current Switchover Switchover active active reaso
```

Esto sucede si el link entre el controlador activo y su gateway se desactiva.

Otras consideraciones

HA SSO para Catalyst 9800-CL

En entornos virtuales, debe aceptar que la latencia se introduce y que la latencia no es algo que HA tolere correctamente. Esto es legítimo, ya que HA SSO tiende a detectar rápida y eficientemente cualquier falla del chasis. Para lograr esto, cada chasis verifica el estado del otro mediante señales de mantenimiento en los links RP y RMI, así como pings hacia el gateway de sus RMI (y éste, el de su WMI que debe ser el mismo). Si se omite alguno de estos, la pila reacciona en función de los síntomas, como se detalla en "System and Network Fault Handling" (Gestión de fallos del sistema y la red) de la guía HA SSO.

Cuando se trabaja con pilas de HA SSO virtuales de Catalyst 9800, es común observar switchovers debido a keepalive perdido sobre el link RP. Esto puede deberse a la latencia introducida por el entorno virtualizado.

Para determinar si la pila HA SSO sufre de caídas de keepalive RP, puede utilizar los registros del administrador de stack/rif.

```
! Keepalives are missed 004457: Feb 4 02:15:50.959 Paris: %STACKMGR-6-KA_MISSED: Chassis 1 R0/0: stack_
```

Si ambos chasis están funcionando, el switchover crea una "detección activa dual" que es una consecuencia de las caídas en el RP.

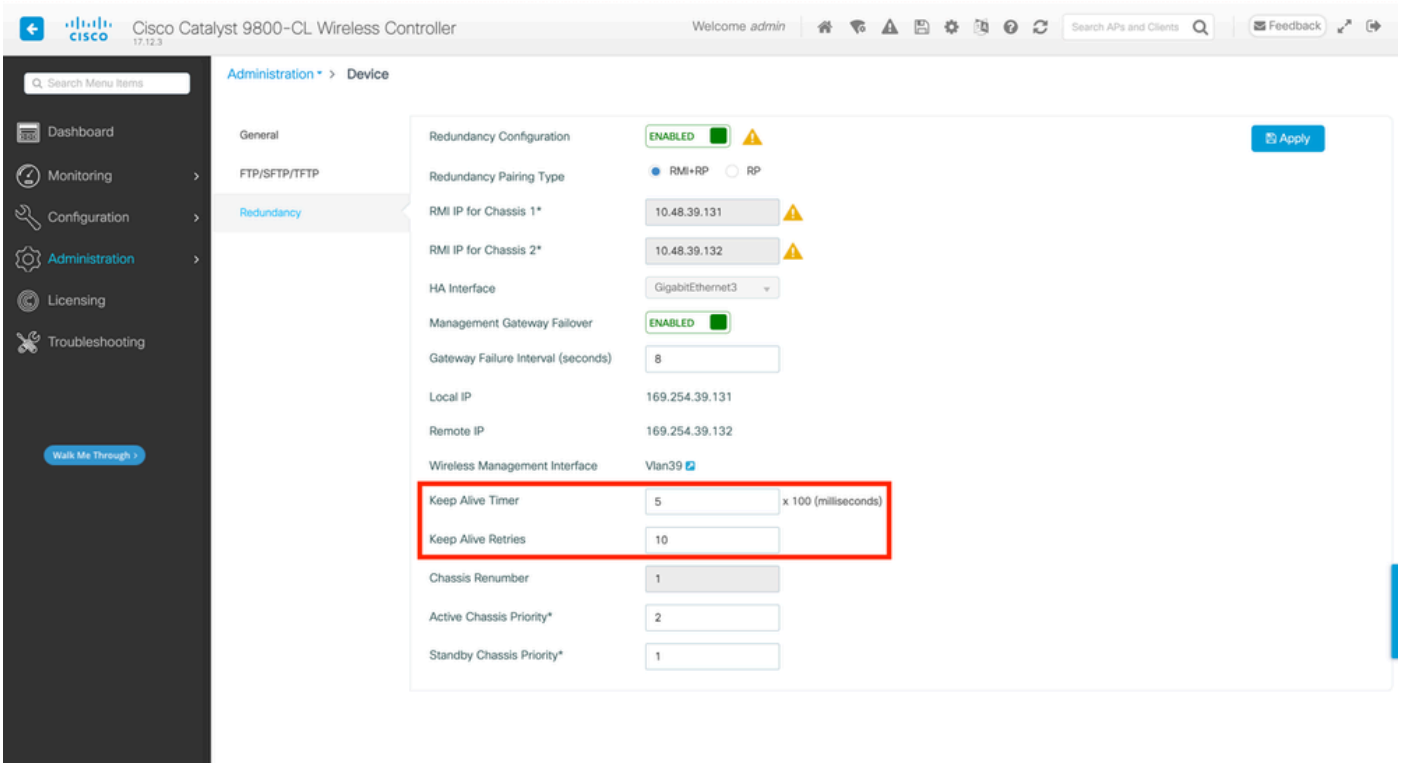
En tal situación, ajustar los parámetros de keepalive de HA para evitar estos switchovers innecesarios, puede ayudar. Se pueden configurar dos parámetros,

- **Temporizador de mantenimiento activo:** la cantidad de tiempo que separa el envío de 2 mensajes de keepalive entre cada chasis.
- **Reintentos de Mantener Activo:** el número de keepalive que debe perderse para declarar un par inactivo.

De forma predeterminada, el temporizador de mantenimiento activo se establece en 1ms y los reintentos en 5. Esto significa que después de que se pierdan 5ms de keepalive en el link RP, ocurre un switchover. Estos valores pueden ser demasiado bajos para implementaciones virtuales. Si está experimentando un switchover recurrente debido a que se pierden señales de mantenimiento RP, intente aumentar estos parámetros para estabilizar la pila.

Desde la GUI:

Para supervisar o modificar los parámetros de keepalive de HA SSO desde la GUI de 9800, navegue hasta la pestaña Redundancia desde la página *Administration > Device*, como se muestra en esta captura de pantalla.



Desde CLI:

```
WLC#chassis redundancy keep-alive retries <5-10> WLC#chassis redundancy keep-alive timer <1-10>
```

Junto con la configuración de estos parámetros, otra optimización puede ayudar con este comportamiento en la pila de HA SSO. En el caso de los dispositivos físicos, el hardware permite conectar un chasis a otro normalmente mediante un solo cable. En un entorno virtual, la interconexión del puerto RP para cada chasis debe realizarse mediante un switch virtual (vSwitch), que puede introducir de nuevo la latencia en comparación con las conexiones físicas. El uso de un vSwitch dedicado para crear el enlace RP es otra optimización que puede evitar la pérdida de keepalives de HA debido a la latencia. Esto también se documenta en la Guía de implementación del controlador inalámbrico Cisco Catalyst 9800-CL para la nube. Por lo tanto, lo mejor es utilizar un vSwitch dedicado para el link RP entre las VM 9800-CL y asegurarse de que ningún otro tráfico interfiera con él.

Implementaciones de Catalyst 9800 HA SSO Inside ACI

Cuando se produce un switchover en una pila HA SSO, el chasis recientemente activo utiliza el mecanismo ARP gratuito (GARP) para actualizar la asignación MAC a IP en la red y asegurarse de que recibe el tráfico dedicado al controlador. En particular, el chasis envía GARP para convertirse en el nuevo "propietario" de WMI y asegurarse de que el tráfico CAPWAP llegue al chasis adecuado.

El chasis que se activa en realidad no está enviando un solo GARP, sino una ráfaga de ellos para asegurarse de que cualquier dispositivo en la red actualice su asignación de IP a MAC. Esta ráfaga puede superar la función de aprendizaje ARP de ACI y, por lo tanto, cuando se utiliza ACI, se recomienda reducir esta ráfaga tanto como sea posible de la configuración de Catalyst 9800.

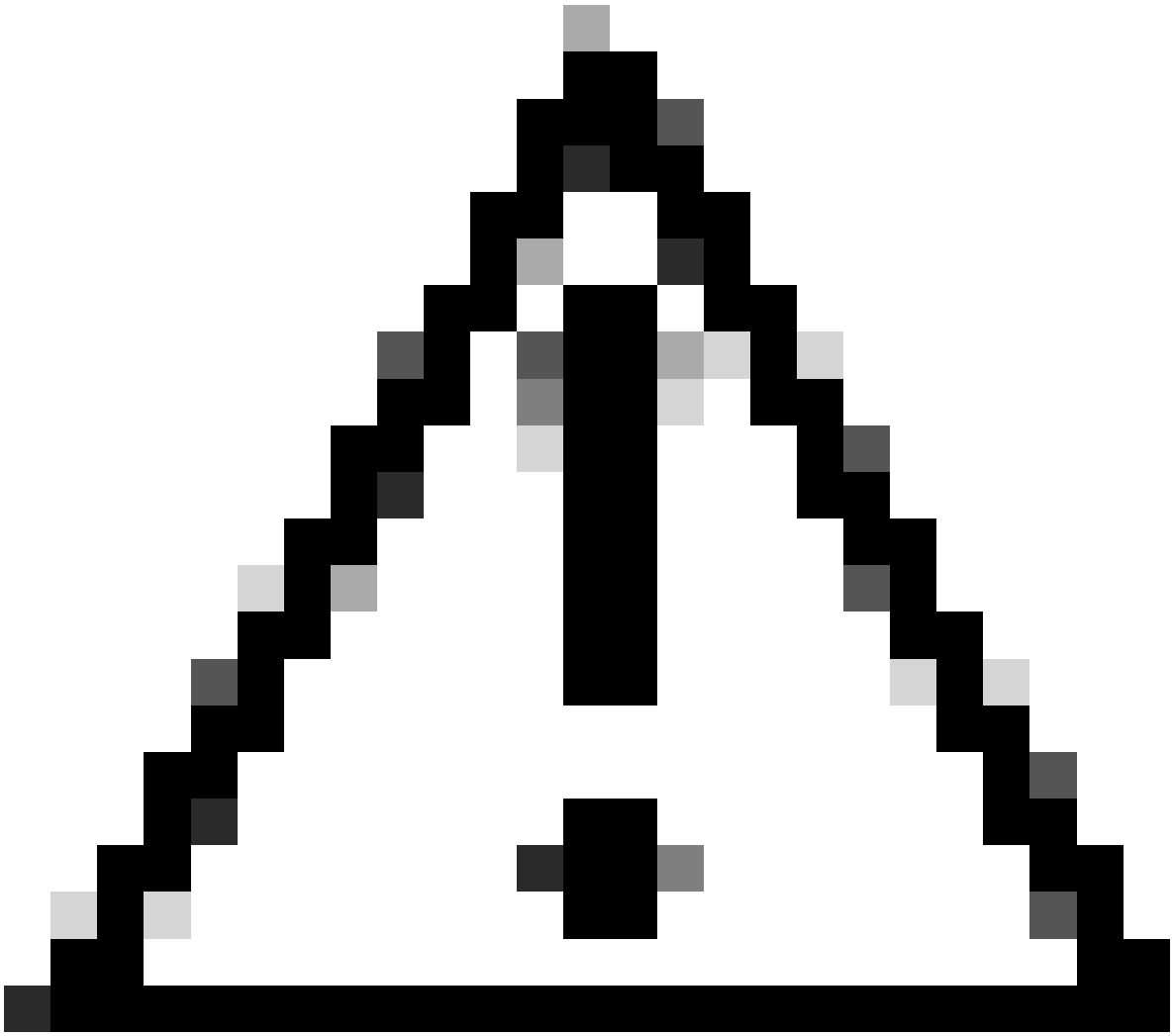
Desde CLI:

```
WLC# configure terminal WLC(config)# redun-management garp-retransmit burst 0 interval 0
```

Además de limitar la ráfaga GARP iniciada por el 9800 durante un switchover, también se recomienda inhabilitar la función fast switchover en esta plataforma. Cuando se configura el fast switchover, el controlador activo envía una notificación explícita al controlador en espera, indicando que se está apagando. Mientras se utiliza esto, el tráfico de entrelazado puede existir (AP y clientes que se descartan) entre ambos WLC que forman la pila de HA hasta que uno de ellos deja de funcionar. Por lo tanto, la desactivación de esta función ayuda a estabilizar la infraestructura inalámbrica mientras se trabaja con implementaciones de ACI.

Desde CLI:

```
WLC#configure terminal WLC(config)#no redun-management fast-switchover
```



Precaución: Tenga en cuenta que cuando se inhabilita el switchover rápido, el controlador en espera se basa únicamente en las fallas de tiempo de espera de keepalive para detectar cuando el controlador activo se desactivó. Por lo tanto, deben configurarse con sumo cuidado.

Los detalles sobre las consideraciones para las implementaciones de HA SSO para Catalyst 9800 dentro de la red ACI se pueden ver en la sección "Información sobre la implementación de la red ACI en el controlador" de la Guía de configuración del software del controlador inalámbrico Cisco Catalyst serie 9800.

Referencias

- Guía de SSO de 17.3 HA
- Guía de SSO de 17.6 HA

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).