Configuration de l'authentification SSO haute disponibilité sur Catalyst 9800 | Guide de démarrage rapide

Table des matières

Introduction

Ce document décrit comment configurer la commutation à état haute disponibilité (SSO) d'une manière RP+RMI, sur un WLC Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance de

- Modèle de configuration Catalyst Wireless 9800.

- Les concepts de haute disponibilité sont décrits dans le guide HA SSO.

Composants utilisés

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

- Catalyst 9800-CL (v. 17.12.3).

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.

Alors que la configuration de HA SSO ne peut en nécessiter que 3, ici, 4 adresses IP du même réseau que l'interface de gestion sans fil (WMI) ont été utilisées pour faciliter l'accès à l'interface graphique utilisateur du contrôleur.

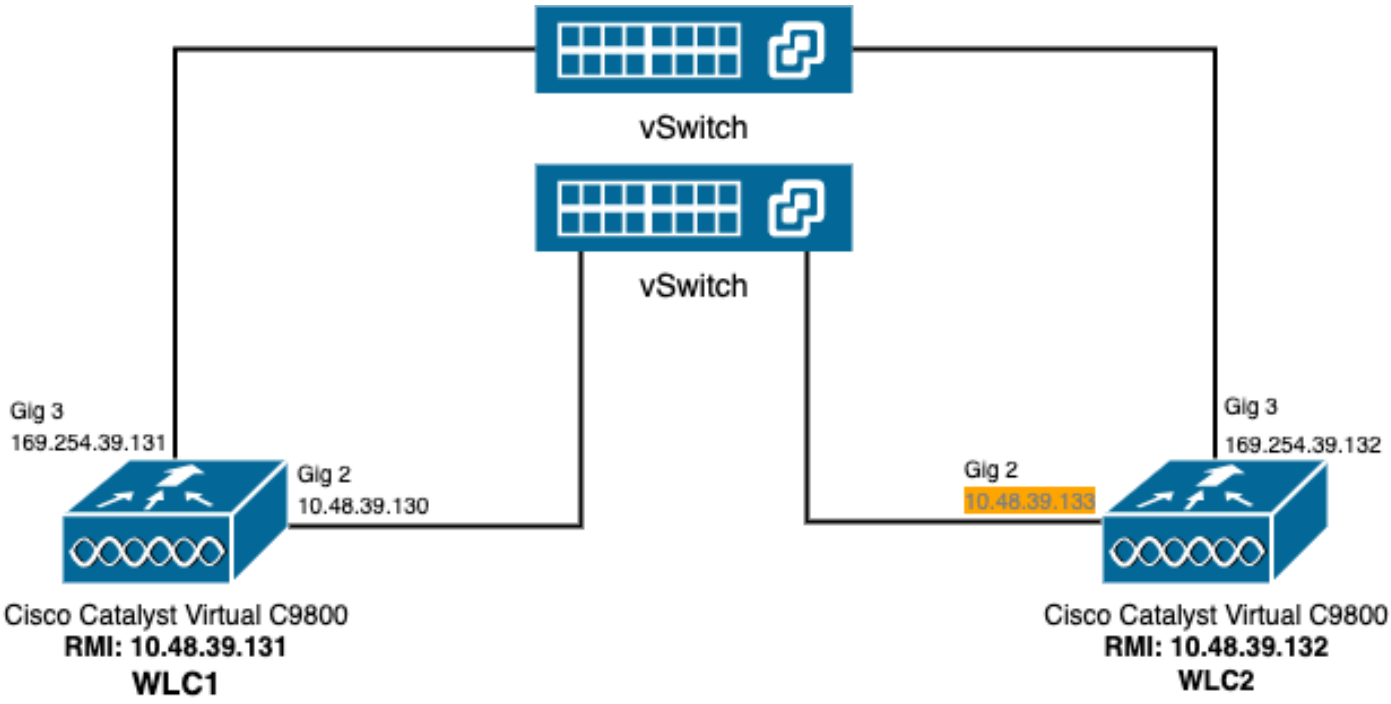
Informations générales

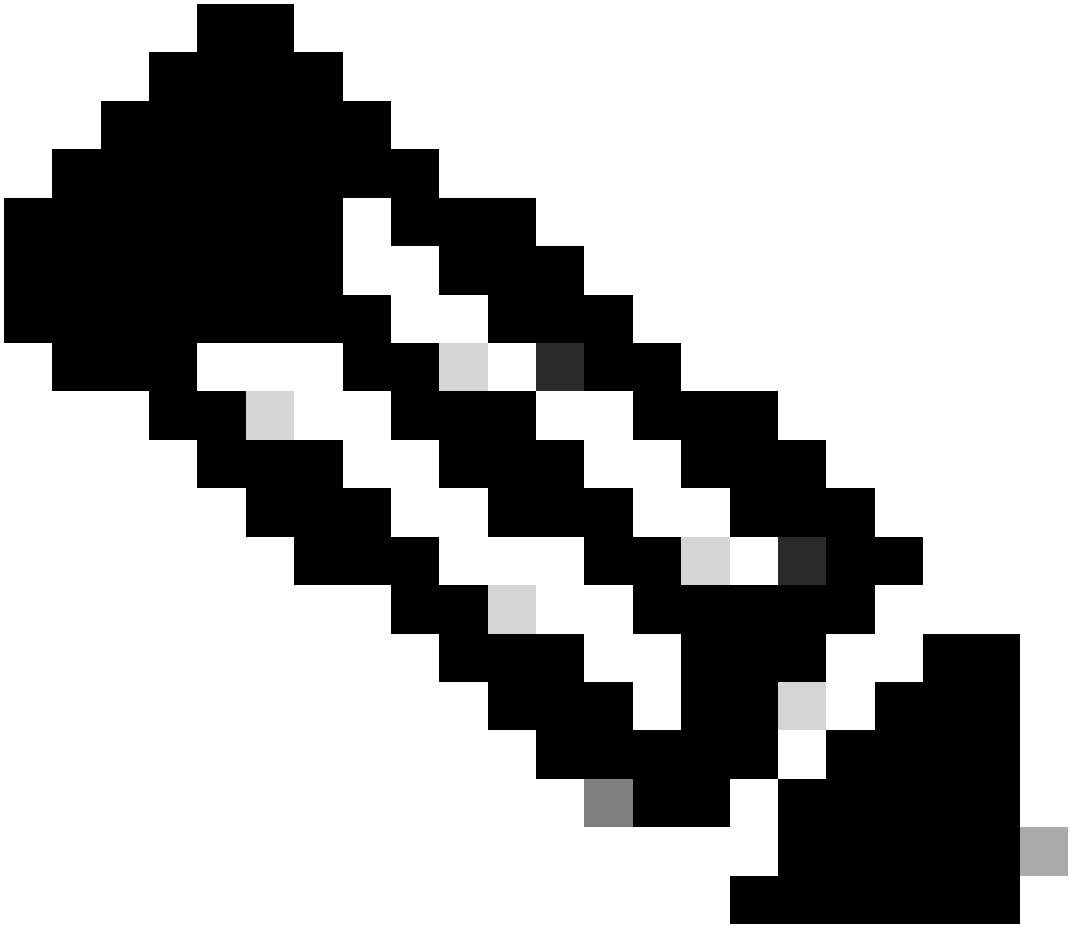
La capacité SSO haute disponibilité sur le contrôleur sans fil permet au point d'accès d'établir un tunnel CAPWAP avec le contrôleur sans fil actif et le contrôleur sans fil actif pour partager une copie miroir du point d'accès et de la base de données client avec le contrôleur sans fil de secours. Lorsque des commutations se produisent (c'est-à-dire que le contrôleur actif tombe en panne et que le mode veille prend la main), les points d'accès joints ne passent pas à l'état de détection et les clients ne se déconnectent pas. Il n'y a qu'un seul tunnel CAPWAP maintenu à la fois entre les AP et le contrôleur sans fil qui est dans un état actif.

Les deux unités forment une connexion homologue via un port RP dédié (ou une interface virtuelle pour les machines virtuelles) et les deux contrôleurs partagent la même adresse IP sur l'interface de gestion. L'interface RP est utilisée pour synchroniser la configuration en masse et incrémentielle au moment de l'exécution et garantir l'état opérationnel des deux contrôleurs de la paire haute disponibilité. En outre, lorsque RMI + RP est utilisé, les contrôleurs en veille et actifs disposent d'une interface de gestion de redondance (RMI) à laquelle sont attribuées des adresses IP, notamment pour assurer l'accessibilité de la passerelle. L'état CAPWAP des points d'accès qui sont à l'état d'exécution est également synchronisé du contrôleur sans fil actif au contrôleur sans fil de secours automatique, ce qui permet aux points d'accès d'être complètement commutés lorsque le contrôleur sans fil actif tombe en panne. Les points d'accès ne passent pas à l'état de détection lorsque le contrôleur sans fil actif tombe en panne et que le contrôleur sans fil en veille prend le relais en tant que contrôleur sans fil actif pour servir le réseau.

Configurer

Diagramme du réseau


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



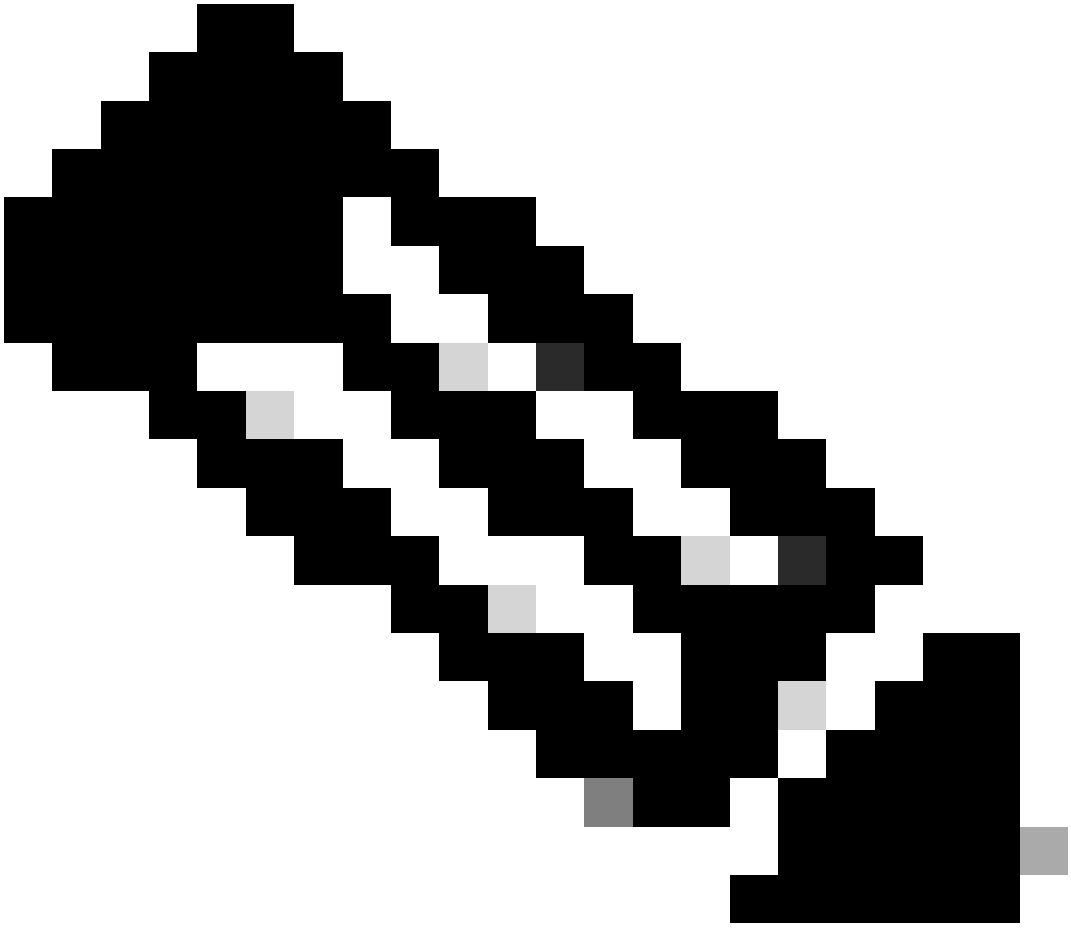
Remarque : en orange est mise en surbrillance l'adresse IP temporaire attribuée à l'interface virtuelle GigabitEthernet 2 du contrôleur 9800-CL désigné comme WLC2. Cette adresse IP est temporairement définie comme WMI pour WLC2 et permet l'accès à l'interface utilisateur graphique de cette instance pour faciliter la configuration de l'authentification unique haute disponibilité. Une fois HA SSO configurée, cette adresse est libérée car une seule WMI est utilisée pour une paire de contrôleurs HA SSO.

Configurations

Dans cet exemple, la commutation avec état (SSO) haute disponibilité (HA) est configurée entre deux instances 9800-CL, qui exécutent la même version du logiciel Cisco IOS, qui ont été configurées avec des WMI séparés et avec une interface utilisateur graphique accessible à l'adresse

- l’adresse IP 10.48.39.130 pour le premier, appelé WLC1 ;
- L'adresse IP 10.48.39.133 pour le deuxième, appelé WLC2.

En plus de ces adresses IP, deux adresses supplémentaires dans le même sous-réseau (et VLAN) ont été utilisées, à savoir 10.48.39.131 et 10.48.39.132. Il s'agit des adresses IP de l'interface de gestion de redondance (RMI), respectivement pour le châssis 1 (WLC1) et le châssis 2 (WLC2).



Remarque : une fois que la haute disponibilité est configurée entre les deux contrôleurs, 10.48.39.133 est libéré et 10.48.39.130 devient le seul WMI de ma configuration. Par conséquent, après la configuration, seules 3 adresses IP sont utilisées, celle de l'interface WMI et celles des interfaces RMI.

La configuration des interfaces pour les deux périphériques avant même de lancer la configuration de haute disponibilité doit être similaire à celles fournies dans cet exemple.

```
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
```

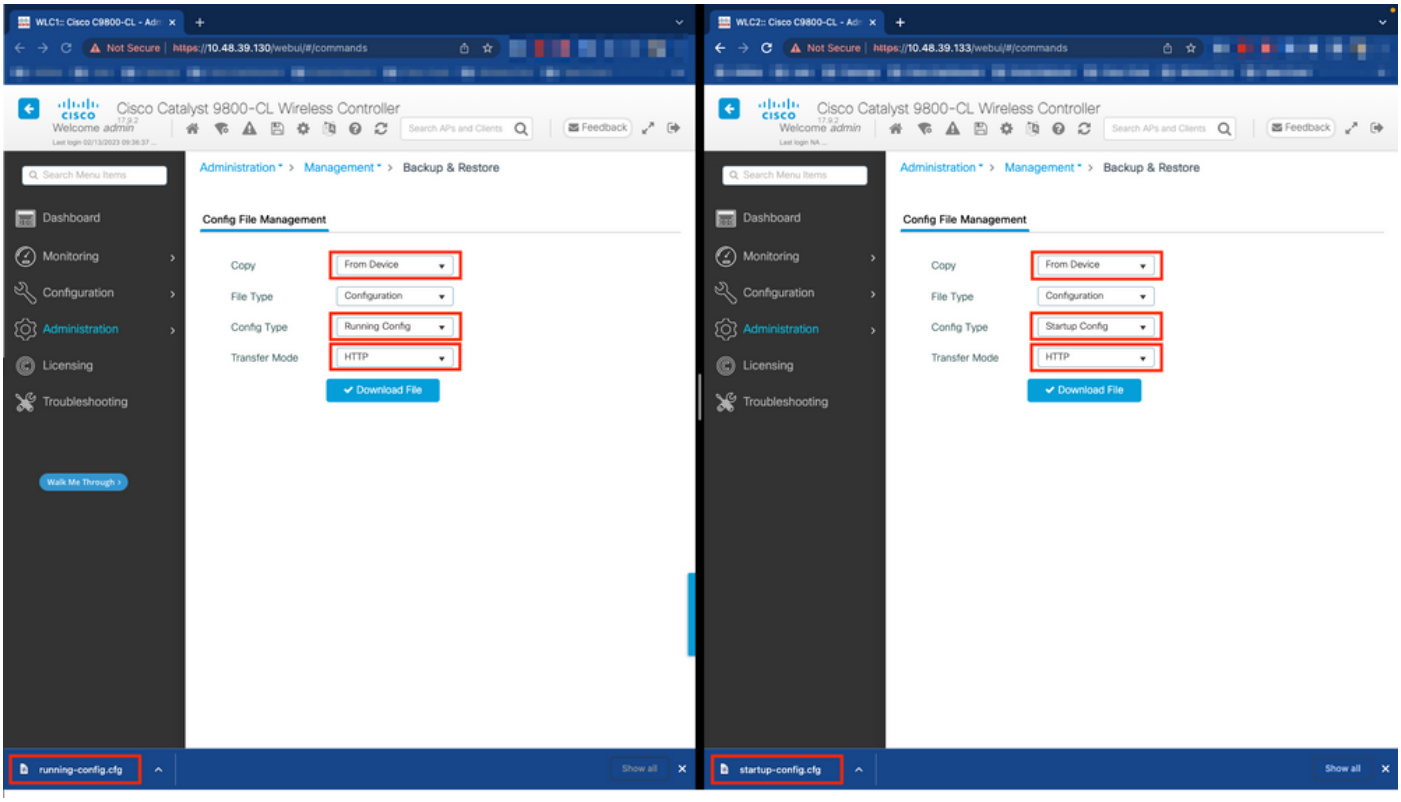
Dans cet exemple, WLC1 est désigné comme contrôleur principal (c'est-à-dire le châssis 1) tandis que WLC2 est le contrôleur secondaire (c'est-à-dire le châssis 2). Cela signifie que la paire HA composée des 2 contrôleurs utilise la configuration du WLC1 et que celui du WLC2 est perdu après le processus.

Étape 1. (Facultatif) Sauvegardez les fichiers de configuration de démarrage et de configuration en cours des contrôleurs.

Une mauvaise manipulation peut se produire et entraîner une perte de configuration. Pour éviter cela, il est vivement recommandé de sauvegarder la configuration initiale et la configuration en cours à partir des deux contrôleurs utilisés dans la configuration haute disponibilité. Vous pouvez facilement le faire à l'aide de l'interface graphique utilisateur ou de la CLI du 9800.

À partir de la GUI :

Dans l'onglet *Administration → Management → Backup & Restore* de l'interface graphique utilisateur du 9800 (reportez-vous à la capture d'écran), vous pouvez télécharger la configuration de démarrage et en cours actuellement utilisée par le contrôleur.



Dans cet exemple, le démarrage (côté gauche) et la configuration (côté droit) sont directement téléchargés, via HTTP, sur le périphérique qui héberge le navigateur utilisé pour accéder à l'interface graphique utilisateur du WLC. Le champ Mode de transfert permet de modifier facilement le mode de transfert et la destination du fichier à sauvegarder.

À partir de 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)
```

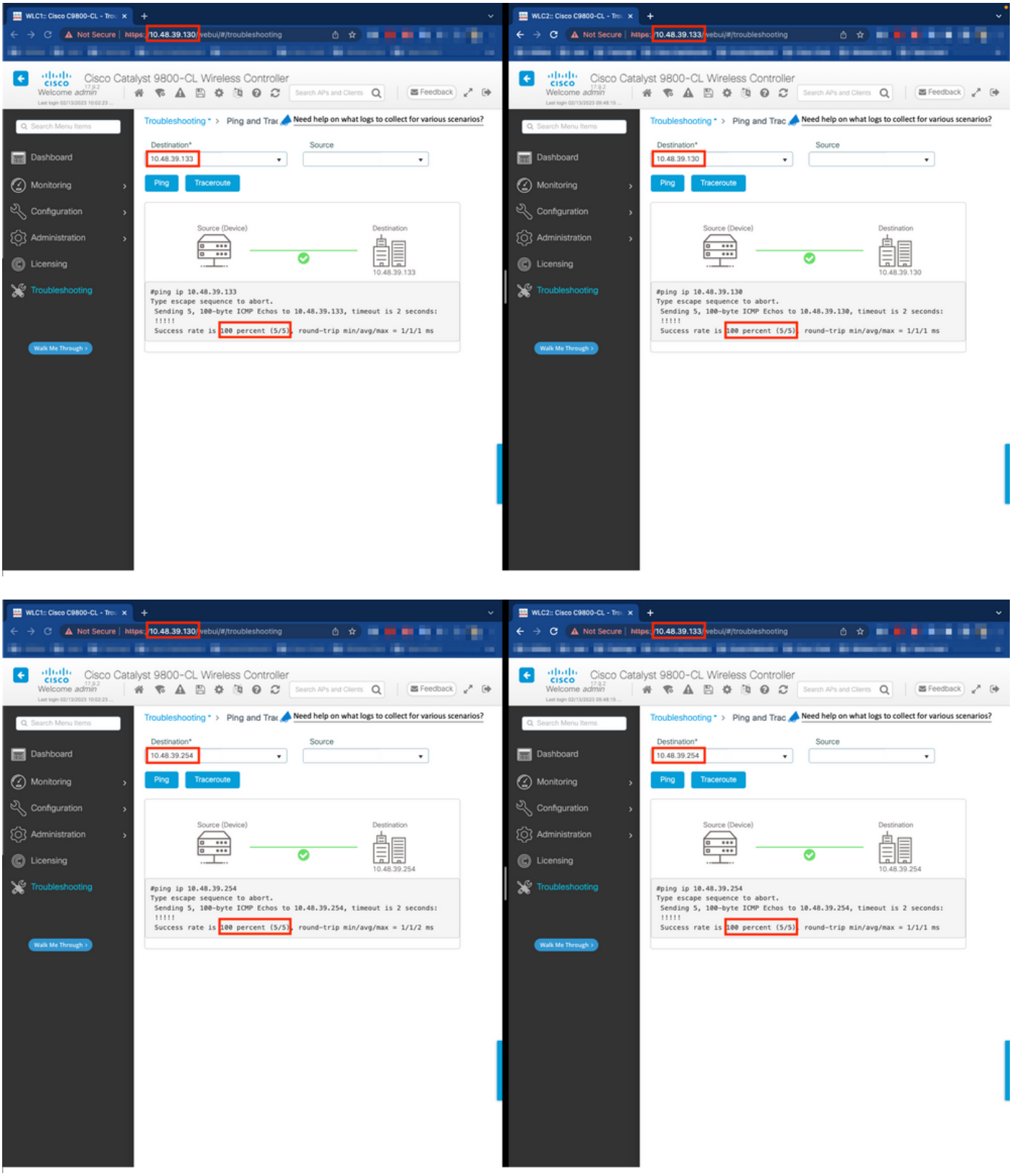
Remplacez le <SERVER-IP> par l'adresse IP du serveur TFTP vers lequel le fichier de configuration initiale/en cours est copié.

Étape 2. (Facultatif) Vérifiez la connectivité réseau.

À partir des interfaces utilisateur graphiques WLC ou des interfaces de ligne de commande, on peut effectuer des tests de connectivité simples, à savoir envoyer une requête ping à la passerelle à partir des deux périphériques et envoyer une requête ping aux périphériques entre eux. Cela garantit que les deux contrôleurs disposent de la connectivité requise pour configurer la haute disponibilité.

À partir de la GUI :

L'outil *Ping and Traceroute* de l'onglet *Troubleshooting* de l'interface graphique 9800 peut être utilisé afin de tester la connectivité entre les contrôleurs eux-mêmes et entre chaque WLC et sa passerelle réseau, comme illustré dans ces figures.



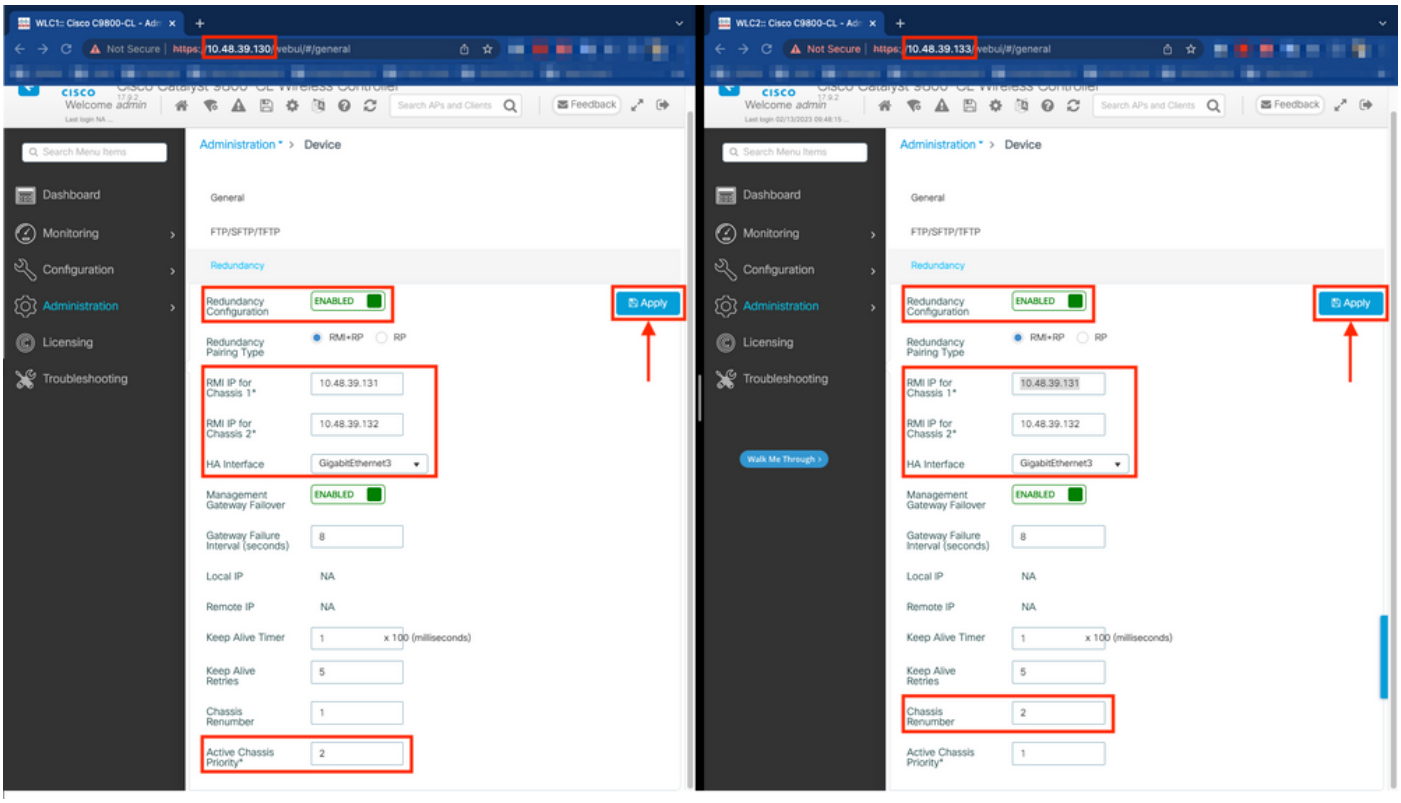
À partir de la CLI :

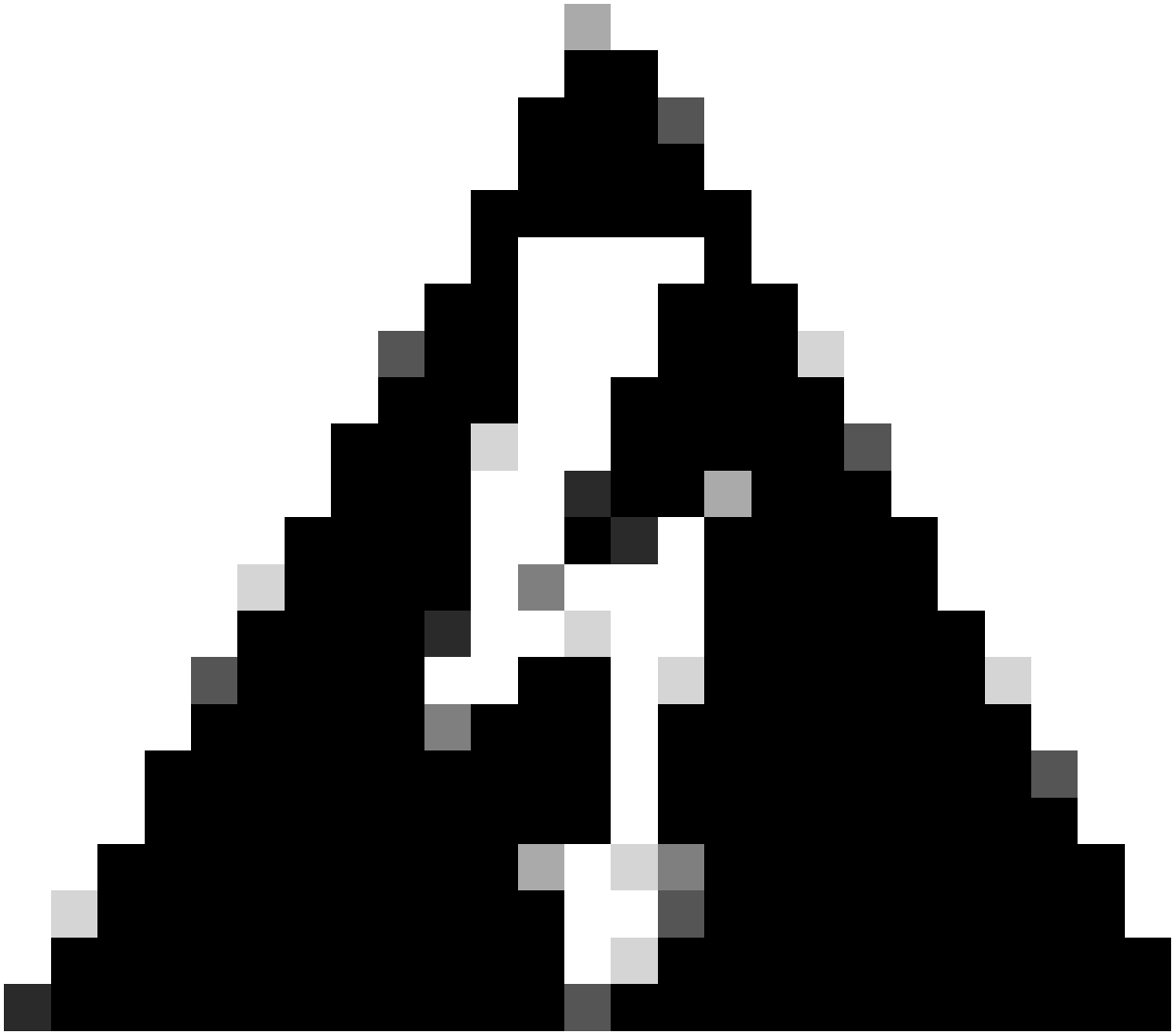
```
WLCx#ping 10.48.39.133 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.48.39.133, t
```

Étape 3. Configurez la redondance avec le type de couplage RMI + RP.

Une fois la connectivité entre chaque périphérique assurée, la redondance peut être configurée entre les contrôleurs. Cette capture d'écran montre

comment la configuration est effectuée à partir de l'onglet *Redondance* de la page *Administration→ Device* de l'interface utilisateur graphique du 9800.





Avertissement : pour cet exemple, WLC1 a été désigné comme contrôleur principal, ce qui signifie que c'est celui dont la configuration est répliquée sur l'autre contrôleur. Assurez-vous d'appliquer la priorité/renumérotation de châssis appropriée afin d'utiliser la configuration appropriée avec votre paire haute disponibilité et de ne pas en perdre une partie.

Passons en revue les champs configurés et leur objectif

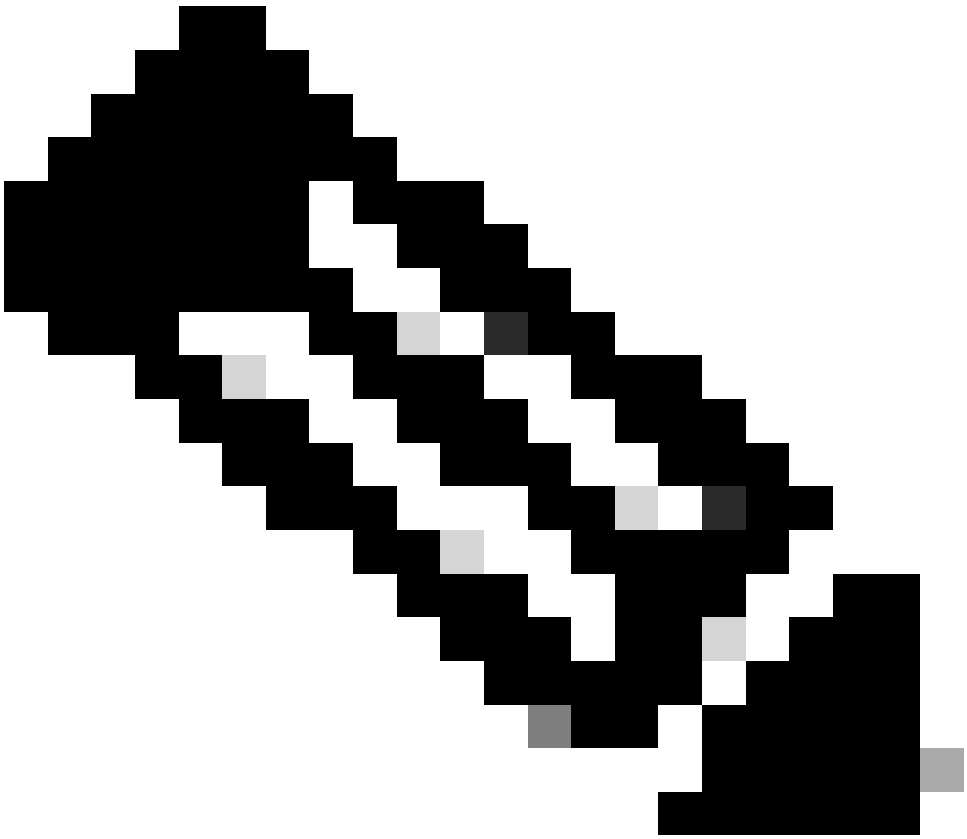
- **Configuration de la redondance :** cette option doit être activée afin d'utiliser la redondance entre les WLC.

- **Type d'appariement de redondance :** étant donné que ce guide couvre l'authentification unique haute disponibilité à l'aide de la configuration RMI, le type d'appariement configuré doit être RMI + RP, à l'aide de l'interface de gestion de redondance et du port de

redondance. On peut également choisir de configurer la redondance en utilisant uniquement le port de redondance. Cependant, lorsque RP seulement est choisi, l'accessibilité de la passerelle n'est pas vérifiée, seul l'état du WLC redondant est

- **RMI IP for Chassis 1/2 :** ces champs attribuent les adresses IP fournies à l'interface de redondance désignée pour les deux instances. Dans cet exemple, les deux adresses IP RMI pour les châssis 1 et 2 ont été configurées comme étant respectivement 10.48.39.131 et 10.48.39.132, comme décrit précédemment et illustré dans le schéma du réseau.

- **Interface haute disponibilité :** lors de l'utilisation d'appareils virtuels, le mappage entre les cartes d'interface réseau virtuelles (vNIC) de l'hyperviseur et les interfaces réseau de la machine virtuelle peut être configuré de différentes manières. Par conséquent, l'interface utilisée pour la redondance peut être configurée pour les commutateurs Cisco Catalyst 9800-CL. Ici, le GigabitEthernet 3 a été utilisé, comme recommandé par le guide de déploiement du 9800-CL.



Remarque : lorsque vous utilisez des appliances C9800 physiques, les interfaces utilisées dans HA et RP sont les interfaces par défaut et ne sont pas configurables. En effet, les WLC 9800 matériels ont une interface de redondance dédiée qui est séparée de leurs interfaces réseau.

- **Basculement de la passerelle de gestion :** comme détaillé dans le guide de configuration de HA SSO, cette méthode de redondance implémente la vérification de la passerelle par défaut, effectuée en envoyant régulièrement une requête ping ICMP (Internet Control Message Protocol) à la passerelle. Les contrôleurs actif et en veille utilisent l'adresse IP RMI comme adresse IP source pour ces vérifications. Ces messages sont envoyés à un intervalle d'une seconde.

- **Intervalle de défaillance de la passerelle :** indique la durée pendant laquelle une vérification de la passerelle doit échouer consécutivement avant que la passerelle ne soit déclarée inaccessible. Par défaut, cette valeur est configurée sur 8 secondes. Comme les vérifications de passerelle sont envoyées toutes les secondes, cela représente 8 échecs consécutifs pour atteindre la passerelle.

- **Local/Remote IP :** il s'agit de l'adresse IP RP configurée pour les châssis 1 et 2. Ces adresses IP sont générées automatiquement sous la forme 169.254.x.x, où x.x est dérivé des deux derniers octets de l’interface de gestion.

- **Minuteur de maintien de la connexion :** comme indiqué dans le guide de configuration de l'authentification unique haute disponibilité, les châssis actif et de secours s'envoient mutuellement des messages de maintien de la connexion pour s'assurer que les deux sont toujours disponibles. Le compteur de test d'activité correspond au temps séparant l'envoi de 2 messages de test d'activité entre chaque châssis. Par défaut, les messages keep-alive sont envoyés toutes les 100 ms. Il est souvent recommandé d'augmenter cette valeur avec le 9800-CL pour éviter les basculements abusifs à chaque fois que l'infrastructure de VM introduit de petits retards (instantanés, etc.)

- **Keep Alive Retries :** ce champ configure la valeur keepalive retry de l'homologue avant de prétendre que l'homologue est hors service. Si le minuteur de maintien de la connexion et la valeur par défaut réessayée sont utilisés, un homologue est désactivé si les 5 messages de maintien de la connexion envoyés à un intervalle de 100 ms restent sans réponse (c'est-à-dire si la liaison de redondance est désactivée pendant 500 ms).

- **Renumérotation du châssis :** numéro de châssis que le matériel doit utiliser (1 ou 2).

    - Sur WLC2 (10.48.39.133), le châssis est renuméroté 2. Par défaut, le numéro de châssis est 1. Les adresses IP des ports RP sont dérivées de RMI. Si le numéro de châssis est le même sur les deux contrôleurs, la dérivation IP du port RP local est la même et la détection échoue. Renumérotez le châssis pour éviter ce scénario dit « actif-actif ».

- **Priorité active du châssis :** priorité utilisée pour définir la configuration à utiliser par la paire haute disponibilité. L'appliance dont la

priorité est la plus élevée est celle qui est répliquée sur l'autre. La configuration du châssis avec la priorité la plus basse est donc perdue.

Sur WLC1 (10.48.39.130), la priorité de châssis active a été définie sur 2. Cela permet de s'assurer que ce châssis est choisi comme châssis actif (et donc que sa configuration est utilisée) dans la paire haute disponibilité créée.

Une fois ces configurations effectuées, utilisez le bouton *Apply* pour appliquer la configuration aux contrôleurs.

À partir de la CLI

Configurez d'abord une adresse IP secondaire dans l'interface virtuelle utilisée pour configurer l'interface RMI sur les deux périphériques.

```
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
```

Activez ensuite la redondance sur les deux périphériques

```
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
```

Configurez la priorité du châssis telle que WLC1 devient le contrôleur principal

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

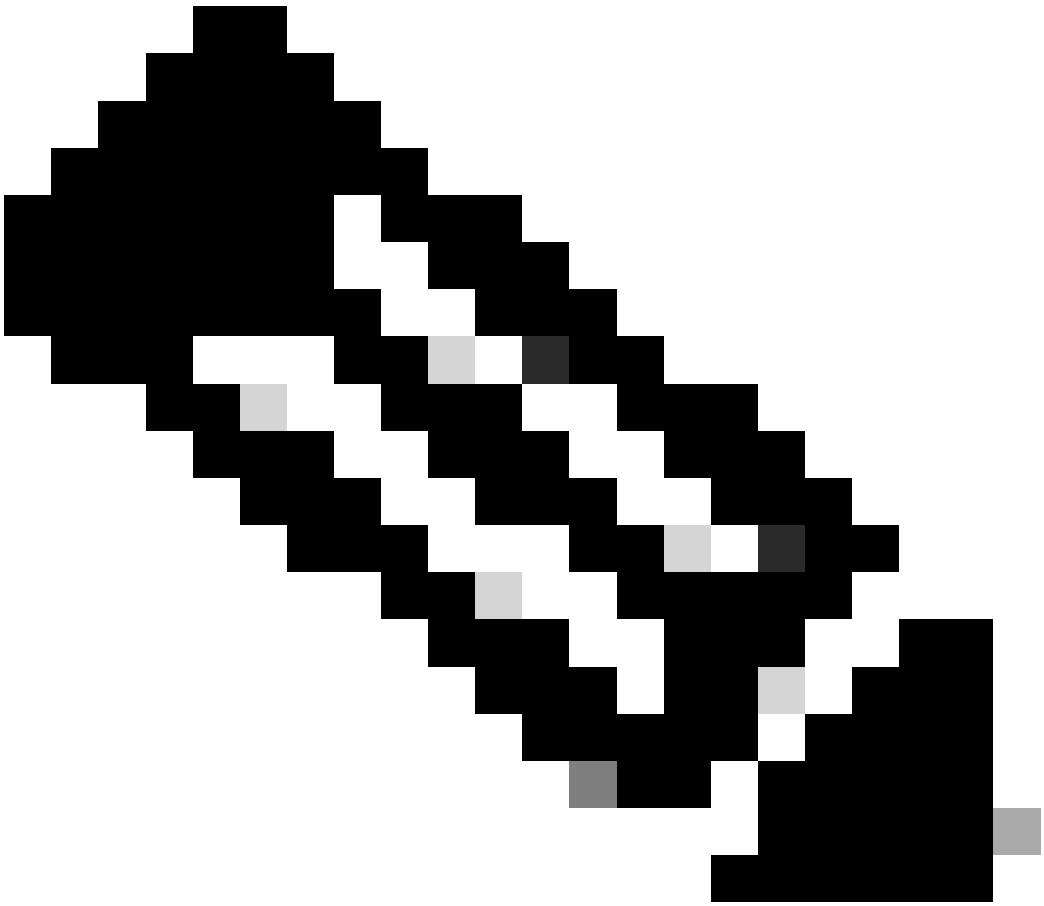
Renuméroter le châssis pour WLC2 qui devient le contrôleur secondaire

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

Enfin, configurez RMI sur les deux périphériques

```
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
```



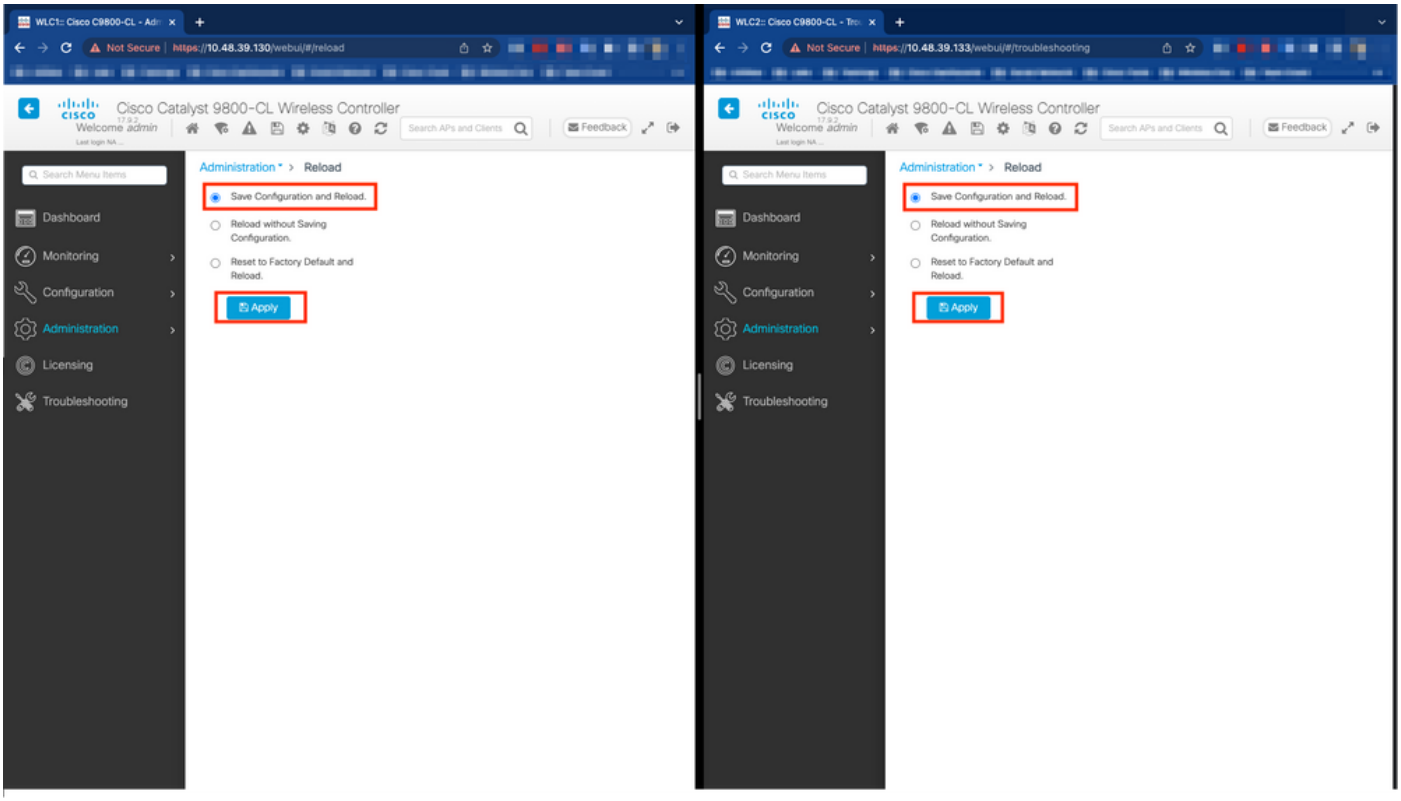
Remarque : comme pour la configuration de l'interface graphique, sur le Catalyst 9800 virtuel, l'interface utilisée par le contrôleur doit être sélectionnée parmi celles disponibles. Comme recommandé, GigabitEthernet 3 est utilisé ici et configuré grâce à la chassis redundancy ha-interface GigabitEthernet 3 commande. Cette commande ne fait pas partie de la configuration en cours, mais l'interface utilisée par HA peut être vue dans les variables d'environnement ROMMON de l'instance. Vous pouvez les afficher à l'aide de la show romvar commande.

Étape 4. Rechargez les contrôleurs.

Pour que la paire haute disponibilité se forme et que la configuration soit efficace, les deux contrôleurs doivent être rechargés en même temps une fois que la configuration effectuée à l'étape 3 a été enregistrée.

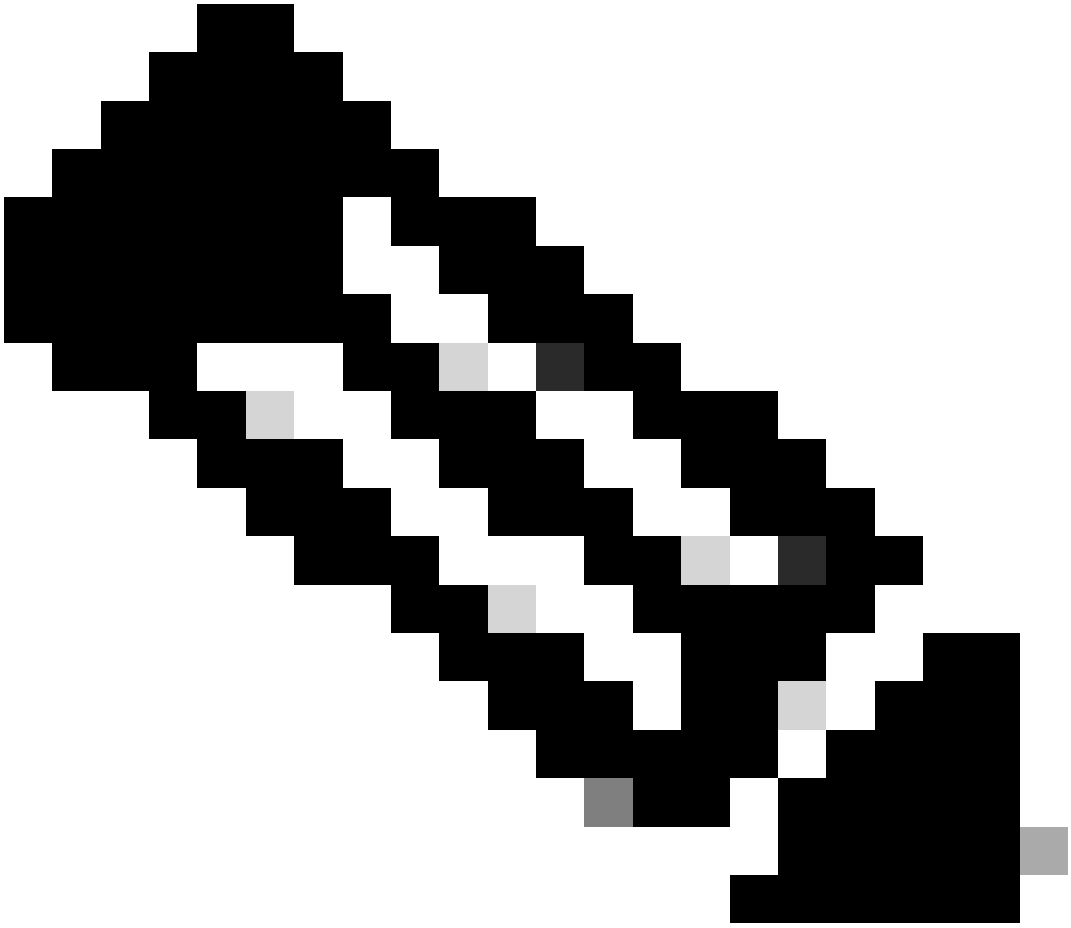
À partir de la GUI :

Vous pouvez utiliser la page Administration Reload des deux interfaces utilisateur graphiques pour redémarrer les contrôleurs, comme illustré dans cette capture d'écran.



À partir de CLI :

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



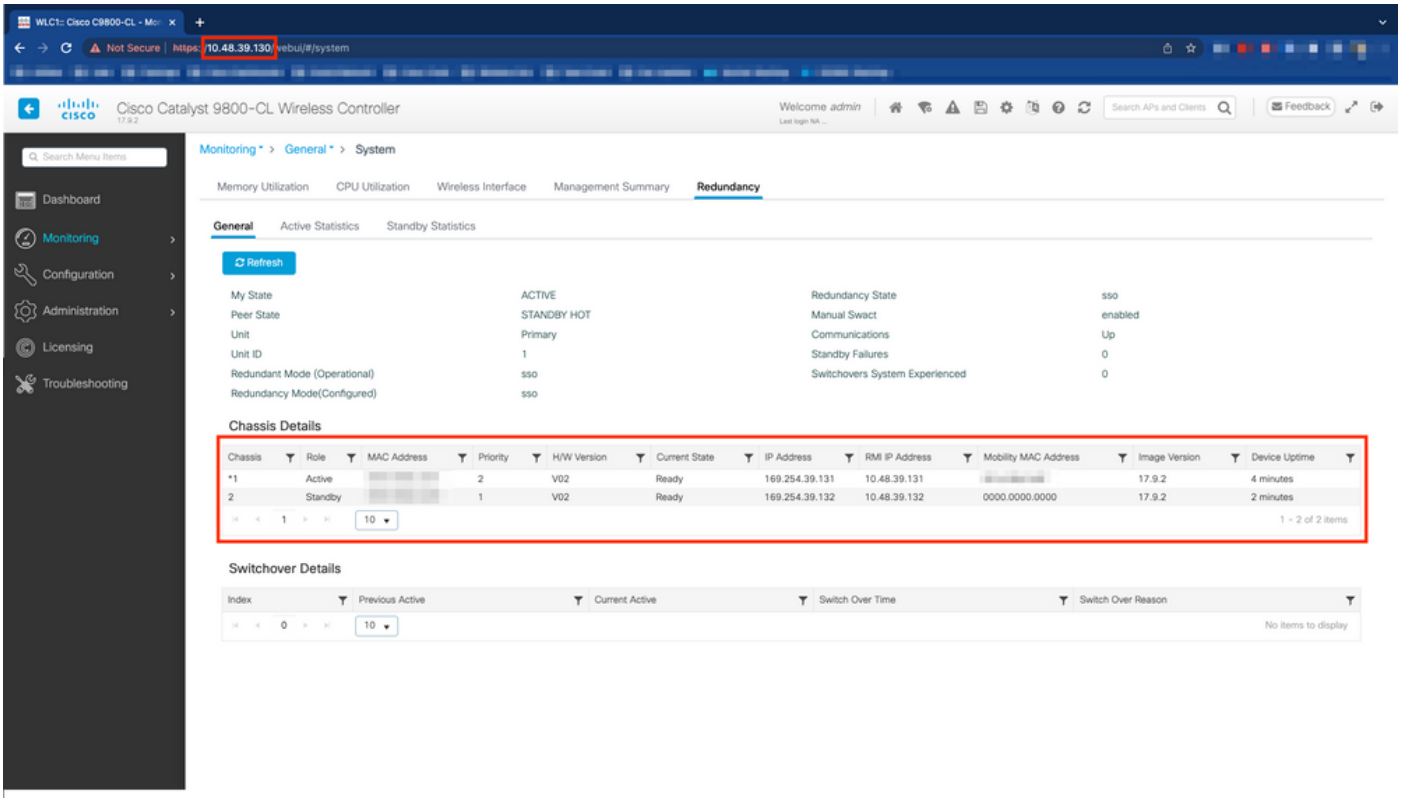
Remarque : si vous utilisez un serveur AAA, vous devez ajouter l'adresse IP WMI ainsi que l'adresse IP RMI en tant que clients AAA sur votre serveur AAA. Le WLC en veille utilise toujours son IP RMI pour authentifier les sessions SSH. Le WLC actif utilise à la fois RMI et WMI pour atteindre le serveur AAA.

Vérifier

Une fois que les deux contrôleurs de la paire haute disponibilité se découvrent et créent la paire haute disponibilité souhaitée, un contrôleur (le contrôleur principal) peut surveiller les deux châssis à partir de l'interface graphique utilisateur ou de l'interface de ligne de commande.

À partir de la GUI :

Pour surveiller la configuration de la redondance à partir de l'interface graphique utilisateur du 9800, accédez à l'onglet Redondance à partir de la page Surveillance > Général > Système, comme illustré dans cette capture d'écran.



À partir de 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
```

Dépannage

réflexes guichets uniques

La commande habituelle n'inclut show tech wireless pas de commandes permettant de comprendre correctement les basculements haute disponibilité d'une paire haute disponibilité ni son état actuel. Collectez cette commande afin d'avoir la plupart des commandes relatives à la haute disponibilité en une seule opération :

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

Commandes show

Pour connaître l'état des ports de redondance, ces commandes peuvent être utilisées.

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

Cette commande indique le numéro de châssis et l'état du port de redondance, ce qui est utile dans une première étape de dépannage.

Afin de vérifier les compteurs keepalive sur le port keepalive, on peut utiliser ces commandes.

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

Autres commandes

Il est possible de prendre une capture de paquet sur le port de redondance du contrôleur avec ces commandes

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

Les captures effectuées à l'aide de ces commandes sont enregistrées dans le bootflash: du contrôleur, sous le nom haIntCaptureLo.pcap.

Vous pouvez également exécuter un test keepalive sur le port de redondance avec cette commande.

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

En savoir plus

Pour afficher la configuration des variables ROMMON qui nous montre comment la configuration réelle est reflétée sur les variables, vous pouvez utiliser cette commande.

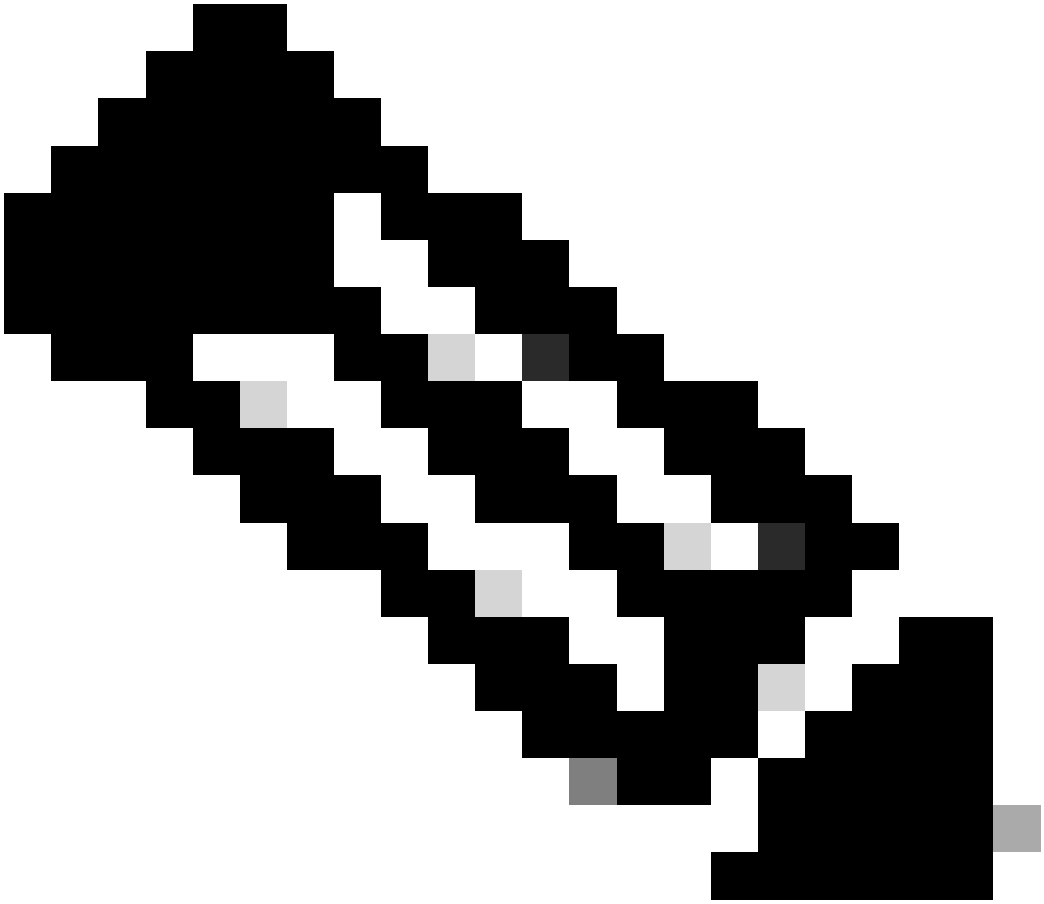
```
WLC#show romvar ROMMON variables: MCP_STARTUP_TRACEFLAGS = 00000000:00000000 SWITCH_NUMBER = 2 CONFIG_F
```

Cette commande affiche la priorité du châssis, les détails RMI et RP, le délai d'attente des homologues ainsi que des détails plus utiles.

Nous pouvons également surveiller les processus qui exécutent HA SSO sur le WLC qui sont deux processus, à savoir stack_mgr et rif_mgr.

Pour ce faire, collectez les traces toujours actives dans un fichier texte à l'aide de la commande, le paramètre de temps ici peut être ajusté pour couvrir la période que nous voulons dépanner.

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



Remarque : il est important de noter que le port de service du WLC en veille est désactivé et inaccessible pendant que le contrôleur agit en tant que standby.

Scénarios types

Utilisateur forcé

Si vous regardez l'historique de basculement, vous pouvez voir "user forced", qui apparaît quand un utilisateur a initié un basculement entre les contrôleurs, en utilisant la redundancy force-switchover commande.

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

Unité active supprimée

Si vous regardez l'historique de commutation, vous pouvez voir « unité active retirée » qui indique une perte de communication sur le port de redondance entre les deux contrôleurs.

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

Cela peut se produire si la liaison entre les deux contrôleurs tombe en panne, mais cela peut également se produire si une unité WLC tombe soudainement en panne (panne de courant) ou tombe en panne. Il est intéressant de surveiller les deux WLC pour voir s'ils ont des rapports système qui indiquent des pannes/redémarrages inattendus.

GW perdue active

Si vous regardez l'historique de commutation, vous pouvez voir « Active lost GW » qui indique une perte de communication avec la passerelle sur le port RMI.

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

Cela se produit si la liaison entre le contrôleur actif et sa passerelle tombe en panne.

Autres considérations

SSO HA pour Catalyst 9800-CL

Lorsque vous travaillez dans des environnements virtuels, vous devez accepter que la latence est introduite et que la latence n'est pas tolérée correctement par la haute disponibilité. Ceci est légitime, car HA SSO a tendance à détecter rapidement et efficacement toute défaillance du châssis. Pour ce faire, chaque châssis vérifie l'état de l'autre en utilisant des keepalives sur les liaisons RP et RMI ainsi que des pings vers la passerelle de leurs RMI (et ceci, celui de leur WMI qui doit être le même). Si l'un de ces problèmes n'est pas détecté, la pile réagit en fonction des symptômes, comme indiqué dans la section « Gestion des pannes du système et du réseau » du guide de l'authentification unique haute disponibilité.

Lors de l'utilisation de piles SSO HA virtuelles de Catalyst 9800, il est courant d'observer des commutations en raison d'une absence de keepalive sur la liaison RP. Cela peut être dû à la latence introduite par l'environnement virtualisé.

Pour déterminer si la pile HA SSO souffre de pertes de keepalive RP, vous pouvez utiliser les journaux du gestionnaire de pile/rif.

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

Si les deux châssis fonctionnent, le basculement crée une « double détection active » qui est une conséquence des pertes sur le RP.

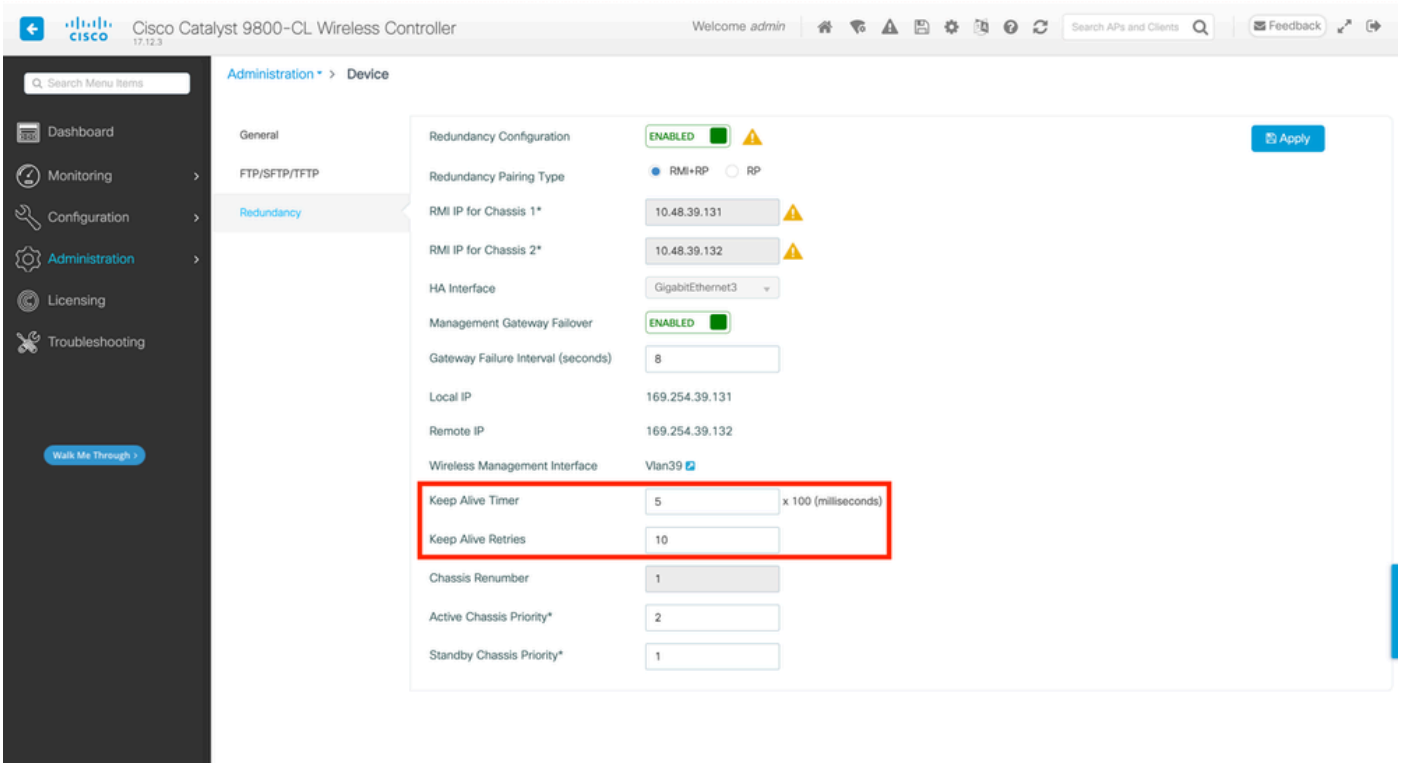
Dans ce cas, il peut être utile de modifier les paramètres de test d'activité haute disponibilité pour éviter ces basculements inutiles. Deux paramètres peuvent être configurés,

- **Minuteur de maintien de** la connexion **:** durée séparant l'envoi de 2 messages de maintien de la connexion entre chaque châssis.
- **Tentatives de maintien de la connexion :** nombre de tentatives de maintien de la connexion qui doivent être manquées pour déclarer un homologue inactif.

Par défaut, le minuteur de maintien de la connexion est défini sur 1ms et le système réessaie sur 5. Cela signifie qu'après 5 ms de keepalive manqués sur la liaison RP, une commutation se produit. Ces valeurs peuvent être trop faibles pour les déploiements virtuels. Si vous rencontrez une commutation récurrente en raison de messages de test d'activité RP manqués, essayez d'augmenter ces paramètres pour stabiliser la pile.

À partir de la GUI :

Pour surveiller ou modifier les paramètres de keepalive de HA SSO à partir de l'interface graphique utilisateur du 9800, accédez à l'onglet Redundancy de la page *Administration* > *Device*, comme illustré dans cette capture d'écran.



À partir de CLI :

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

En plus de la configuration de ces paramètres, une autre optimisation peut aider avec un tel comportement dans la pile HA SSO. Pour un appareil physique, le matériel permet de connecter un châssis à un autre, généralement à l'aide d'un seul câble. Dans un environnement virtuel, l'interconnexion du port RP pour chaque châssis doit être effectuée par un commutateur virtuel (vSwitch), qui peut à nouveau introduire une latence par rapport aux connexions physiques. L'utilisation d'un commutateur virtuel dédié pour créer la liaison RP est une autre optimisation qui peut empêcher la perte de messages de veille haute disponibilité en raison de la latence. Ceci est également décrit dans le Guide de déploiement du contrôleur sans fil Cisco Catalyst 9800-CL pour le cloud. Par conséquent, le mieux est d'utiliser un commutateur virtuel dédié pour la liaison RP entre les machines virtuelles 9800-CL et de s'assurer qu'aucun autre trafic ne l'interfère.

Catalyst 9800 HA SSO Déploiements ACI internes

Lorsqu'une commutation se produit dans une pile HA SSO, le châssis nouvellement actif utilise le mécanisme ARP gratuit (GARP) pour mettre à jour le mappage MAC vers IP dans le réseau et s'assurer qu'il reçoit le trafic dédié au contrôleur. En particulier, le châssis envoie GARP pour devenir le nouveau « propriétaire » du WMI et s'assurer que le trafic CAPWAP atteint le châssis approprié.

En fait, le châssis qui devient actif n'envoie pas un seul GARP, mais une rafale d'entre eux afin de s'assurer que n'importe quel périphérique du réseau met à jour son mappage IP/MAC. Cette rafale peut submerger la fonction d'apprentissage ARP de l'ACI et, par conséquent, lorsque l'ACI est utilisée, il est recommandé de réduire cette rafale autant que possible à partir de la configuration du Catalyst 9800.

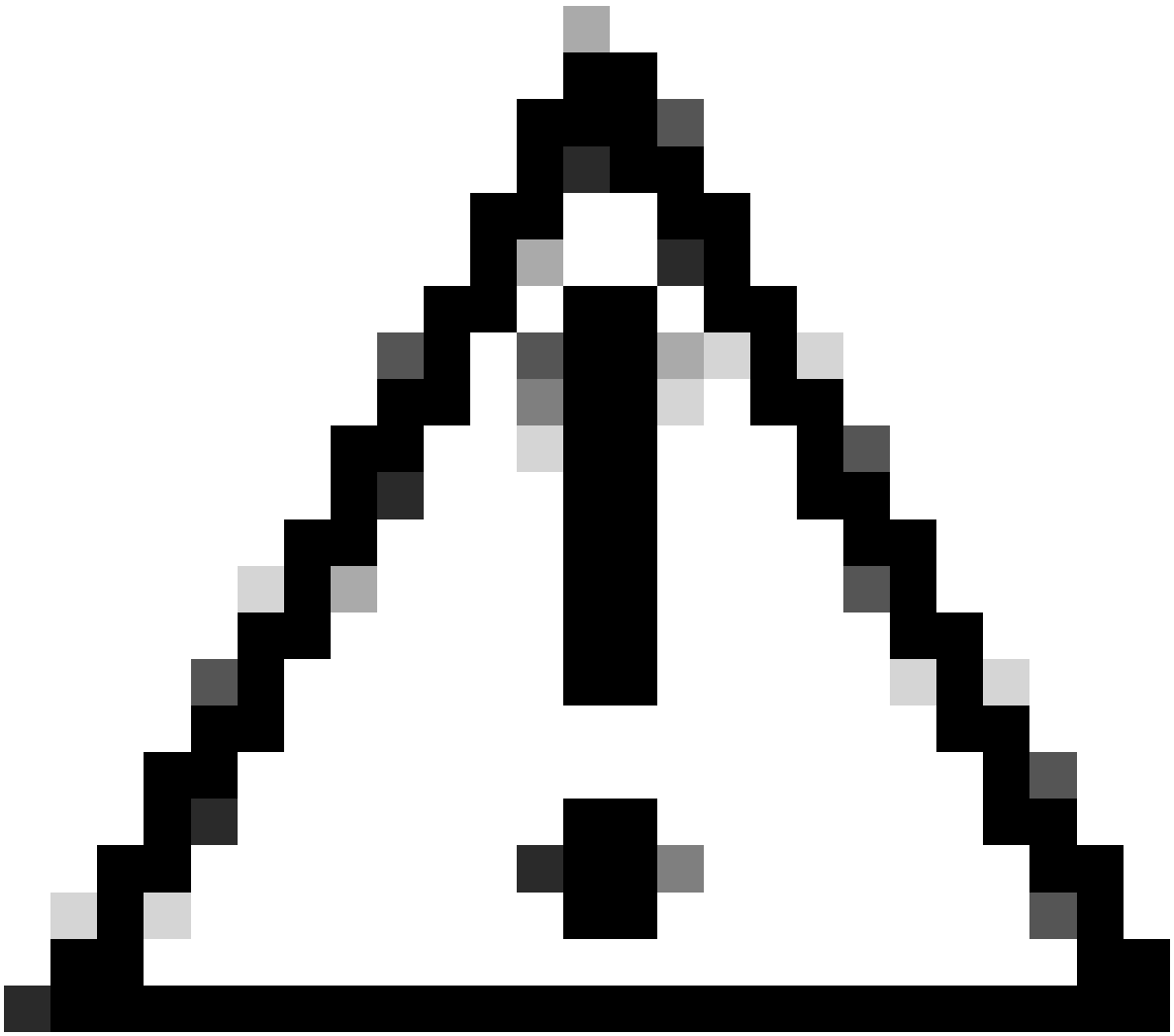
À partir de CLI :

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

Outre la limitation de la rafale GARP initiée par le 9800 lors d'une commutation, il est également recommandé de désactiver la fonctionnalité de commutation rapide sur cette plate-forme. Lorsque la commutation rapide est configurée, le contrôleur actif envoie une notification explicite au contrôleur en veille, indiquant qu'il est en panne. Lors de l'utilisation de ceci, le trafic entrelacé peut exister (AP et clients abandonnés) entre les deux WLC formant la pile HA jusqu'à ce que l'un d'eux tombe en panne. Ainsi, la désactivation de cette fonctionnalité permet de stabiliser votre infrastructure sans fil tout en travaillant avec les déploiements ACI.

À partir de CLI :

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



Attention : Gardez à l'esprit que lorsque la commutation rapide est désactivée, le contrôleur en veille se base uniquement sur les échecs de temporisation keepalive pour détecter quand le contrôleur actif est tombé en panne. Il faut donc les configurer avec le plus grand soin.

Pour plus d'informations sur les considérations relatives aux déploiements SSO HA pour le Catalyst 9800 au sein du réseau ACI, reportez-vous à la section « Information About Deploying ACI Network in Controller » du Guide de configuration du logiciel du contrôleur sans fil de la gamme Cisco Catalyst 9800.

Références

- 17.3 Guide HA SSO
- Guide SSO 17,6 HA

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.