Guide de démarrage rapide de configuration de HA SSO sur Catalyst 9800

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Configurations
- Vérifier
- Dépannage
  - réflexes guichets uniques
  - Commandes show
  - Autres commandes
  - En savoir plus
  - Scénarios types
    - Utilisateur forcé
    - Unité active supprimée
    - GW perdue active
- Autres considérations
  - Activation de l'accès console pour le 9800 de secours
  - SSO HA pour Catalyst 9800-CL
  - Catalyst 9800 HA SSO Déploiements ACI internes
- Références

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 de connaître les points suivants :

- Modèle de configuration sans fil Catalyst 9800
- Les concepts de haute disponibilité sont décrits dans le guide de l'offre SSO de haute disponibilité (HA).

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).

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.

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.

Informations générales

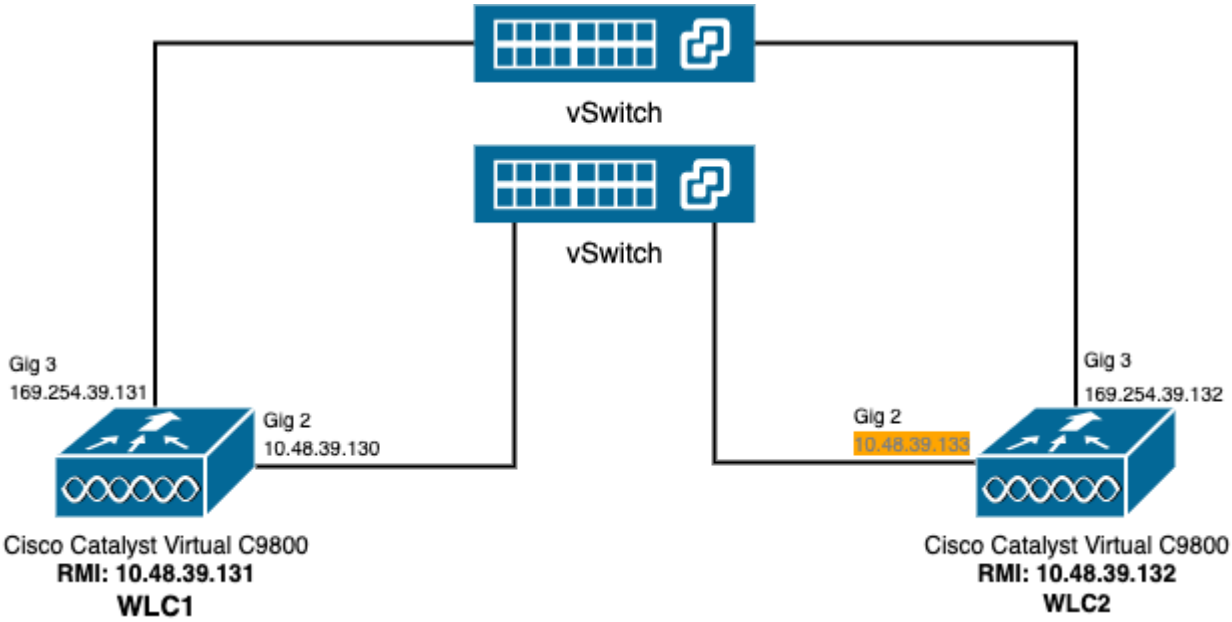
La capacité SSO haute disponibilité sur le contrôleur sans fil permet au point d'accès d'établir un tunnel CAPWAP avec le contrôleur sans fil actif et le contrôleur sans fil actif pour partager une copie miroir du point d'accès et de la base de données client avec le contrôleur sans fil de secours. Lorsque 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



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 HA SSO. 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
```

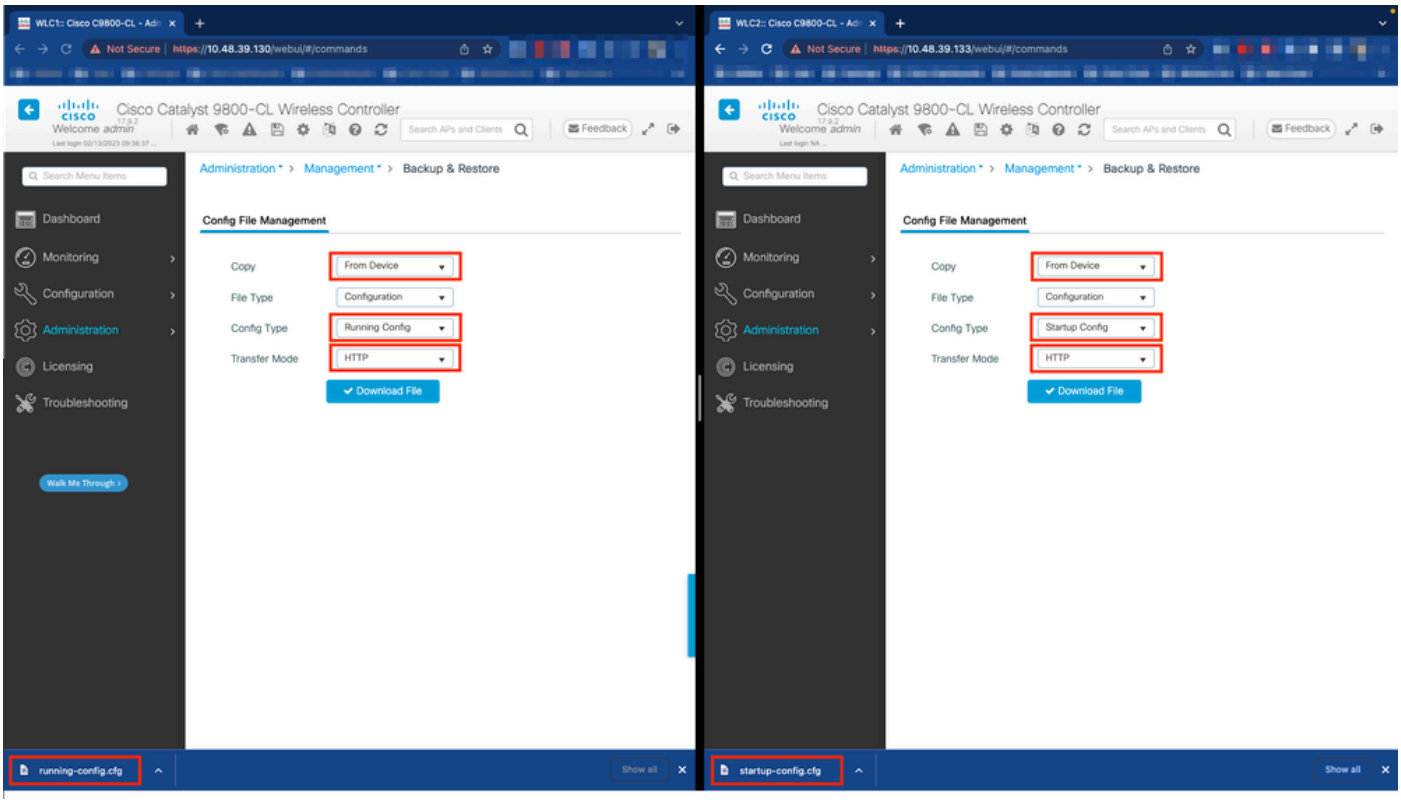
Dans cet exemple, WLC1 est désigné comme contrôleur principal (c'est-à-dire le châssis 1) tandis que WLC2 est le contrôleur secondaire (c'est-à-dire le châssis 2). Cela signifie que la paire HA composée des 2 contrôleurs utilise la configuration du WLC1 et que celui du WLC2 est perdu après le processus.

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 l'interface utilisateur :

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. Vous pouvez facilement modifier le mode de transfert et la destination du fichier à sauvegarder, à l'aide du champ Mode de transfert.

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)
```

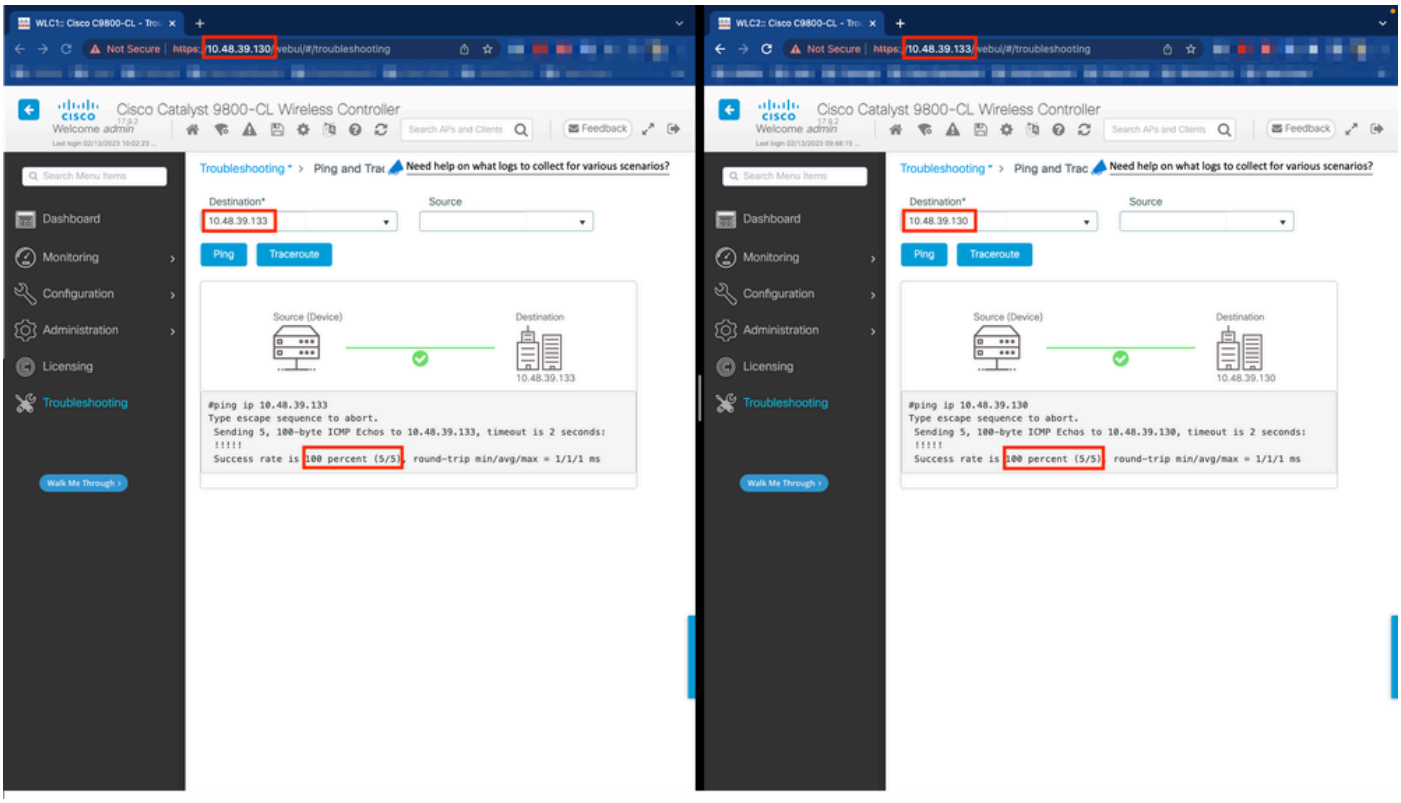
Remplacez le
par l'adresse IP du serveur TFTP vers lequel le fichier de configuration de démarrage/en cours est copié.

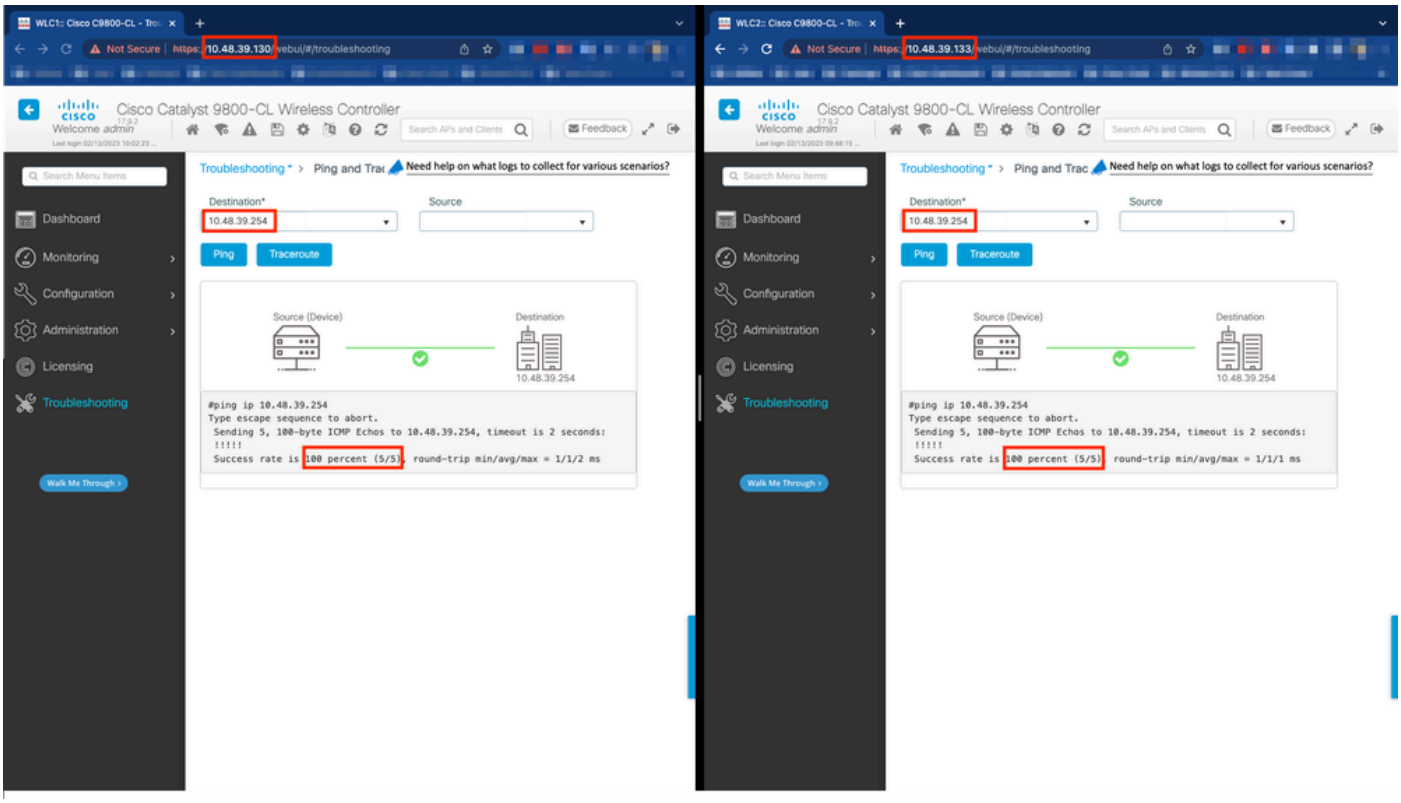
Étape 2. (Facultatif) Vérifiez la connectivité réseau.

À partir des interfaces utilisateur graphiques WLC ou des interfaces de ligne de commande, vous pouvez effectuer des tests de connectivité simples, notamment 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 l'interface utilisateur :

L'outil Ping et Traceroute de l'onglet Dépannage de l'interface graphique du 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.



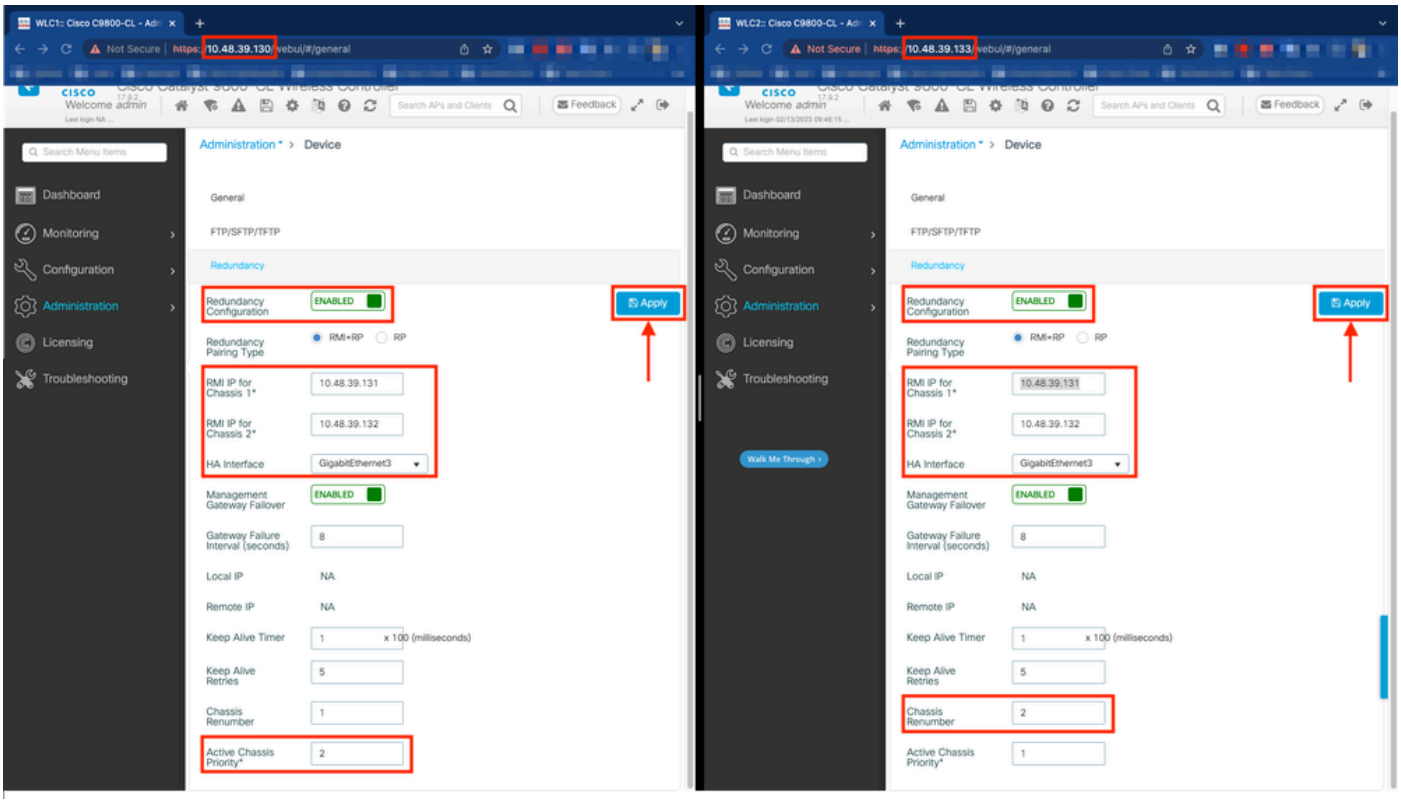


À partir de la CLI :

```
WLCx#ping 10.48.39.133
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.48.39.133, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
WLCx#ping 10.48.39.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.48.39.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Étape 3 : configuration de la redondance avec le type d'appariement 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 Redundancy de la page Administration > Device de l'interface graphique utilisateur 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.

Vérifiez les champs configurés et leur objectif :

- Priorité du châssis actif : la priorité utilisée pour définir la configuration qui doit être utilisée 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 le WLC1 (10.48.39.130), la priorité de châssis active a été définie sur 2. Ceci 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 10.48.39.131 255.255.255.0 secondary
WLC1(config-if)# end
```

```
WLC2#configure terminal
WLC2(config)#interface vlan 39
WLC2(config-if)# ip address 10.48.39.132 255.255.255.0 secondary
WLC2(config-if)# end
```

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
```

La configuration de 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 time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
--------------------------------------------------------------------------------
*1       Active   0001.0202.aabb     1      V02     Ready               169.254.39.131
WLC1#chassis 1 priority 2
WLC1#show chassis
Chassis/Stack Mac Address : 0001.0202.aabb - Local Mac Address
Mac persistency wait time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
--------------------------------------------------------------------------------
*1       Active   0001.0202.aabb     2      V02     Ready               169.254.39.131
```

Renumérotez 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 time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
--------------------------------------------------------------------------------
*1       Active   0001.0202.aabb     1      V02     Ready               169.254.39.132
WLC2#chassis 1 renumber 2
WLC2#show chassis
Chassis/Stack Mac Address : 0001.0202.aabb - Local Mac Address
Mac persistency wait time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
--------------------------------------------------------------------------------
*2       Active   0001.0202.aabb     1      V02     Ready               169.254.39.132
```

Enfin, configurez RMI sur les deux périphériques.

```
WLC1#chassis redundancy ha-interface GigabitEthernet 3
WLC1#configure terminal
WLC1(config)#redun-management interface Vlan39 chassis 1 address 10.48.39.131 chassis 2 address 10.48.3
WLC1(config)#end
```

```
WLC2#chassis redundancy ha-interface GigabitEthernet 3
WLC2#configure terminal
WLC2(config)#redun-management interface Vlan39 chassis 1 address 10.48.39.131 chassis 2 address 10.48.3
WLC2(config)#end
```



Remarque : En ce qui concerne la configuration de l'interface graphique utilisateur, 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 commande chassis redundancy ha-interface GigabitEthernet 3. 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 voir à l'aide de la show romvarcommande.

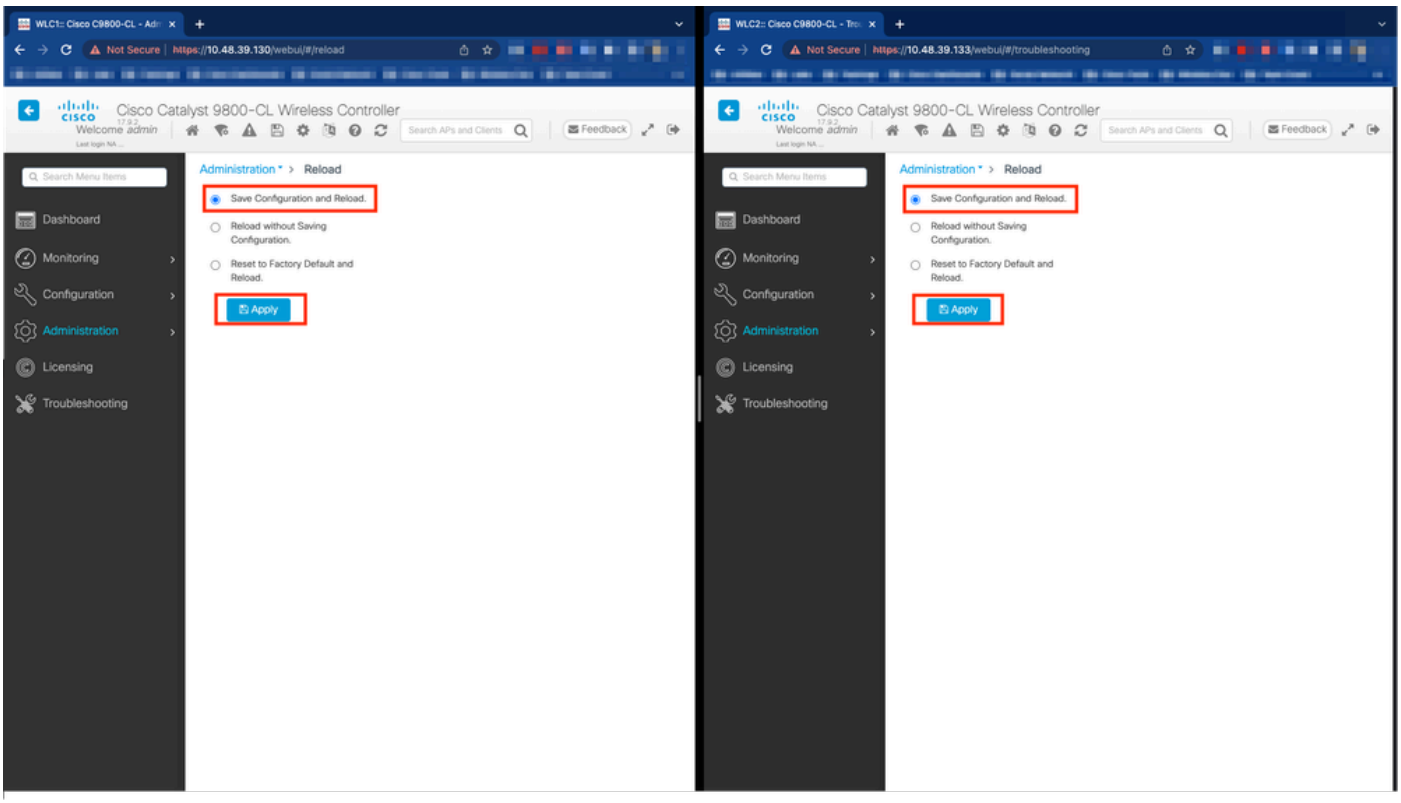
Étape 4. Rechargez les contrôleurs.

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 with reload? [confirm]
```

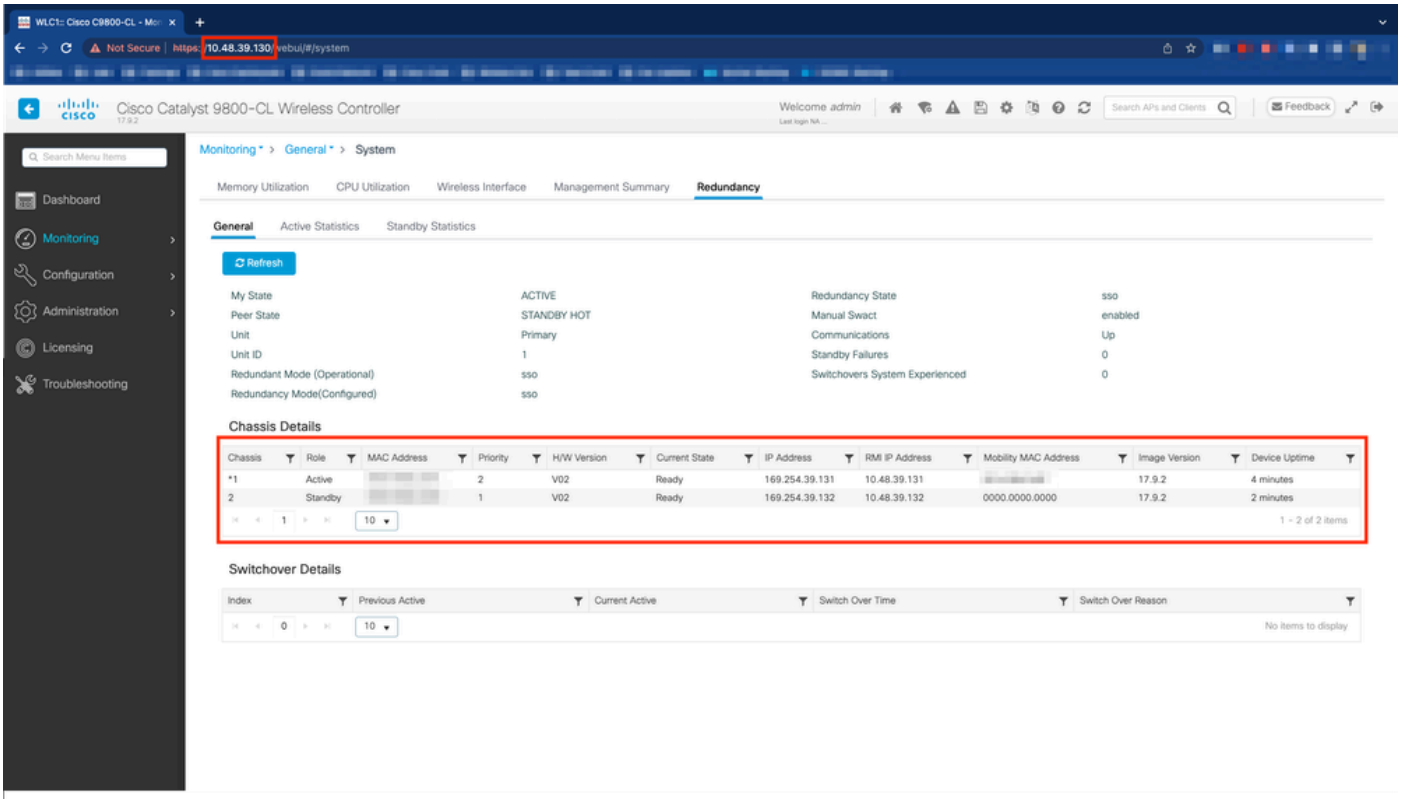
Remarque : Si vous utilisez un serveur AAA, vous devez ajouter l'adresse IP WMI ainsi que l'adresse IP RMI en tant que clients AAA sur votre serveur AAA. Le WLC en veille utilise toujours son IP RMI pour authentifier les sessions SSH. Le WLC actif utilise à la fois RMI et WMI pour atteindre le serveur 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 redondance à partir de l'interface graphique utilisateur du 9800, accédez à l'onglet Redundancy de la page Monitoring > General > System, 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 wait time: Indefinite
                                                     H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP                RMI-IP
-----------------------------------------------------------------------------------------------------
*1       Active   0050.568d.cdf4     2      V02     Ready               169.254.39.131     10.48.39.13
 2       Standby  0050.568d.2a93     1      V02     Ready               169.254.39.132     10.48.39.13
```

```
WLC#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 22 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 22 minutes
                 Image Version = Cisco IOS Software [Cupertino], C9800-CL Software (C9800-CL-K9_IOSXE),
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed 02-Nov-22 15:12 by mcpre
                          BOOT = bootflash:packages.conf,12;
                   CONFIG_FILE =
        Configuration register = 0x102
               Recovery mode   = Not Applicable
             Fast Switchover   = Enabled
                Initial Garp   = Enabled

Peer Processor Information :
----------------------------
              Standby Location = slot 2
        Current Software state = STANDBY HOT
       Uptime in current state = 20 minutes
                 Image Version = Cisco IOS Software [Cupertino], C9800-CL Software (C9800-CL-K9_IOSXE),
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed 02-Nov-22 15:12 by mcpre
                          BOOT = bootflash:packages.conf,12;
                   CONFIG_FILE =
        Configuration register = 0x102
```

Dépannage

réflexes guichets uniques

La commande habituelle `show tech wireless` n'inclut 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 wait time: Indefinite
                                            H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
-----------------------------------------------------------------------------
 1       Standby  aaaa.aaaa.aaaa     2      V02     Ready               169.254.39.131
*2       Active   bbbb.bbbb.bbbb     1      V02     Ready               169.254.39.132


         Stack Port Status             Neighbors
Chassis#  Port 1     Port 2           Port 1   Port 2
---------------------------------------------------------
  1         OK          OK               2        2
  2         OK          OK               1        1
WLC#show chassis rmi
Chassis/Stack Mac Address : 0050.568d.2a93 - Local Mac Address
Mac persistency wait time: Indefinite
                                            H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP                RMI-IP
-------------------------------------------------------------------------------------------------------
 1       Standby  aaaa.aaaa.aaaa     2      V02     Ready               169.254.39.131     10.48.39.13
*2       Active   bbbb.bbbb.bbbb     1      V02     Ready               169.254.39.132     10.48.39.13
```

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 de keepalive sur le port keepalive, vous pouvez utiliser ces commandes.

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

---------------------------------------

Message                 Tx Success    Tx Fail       Rx Success    Rx Fail
------------------------------------------------------------------------
Discovery               162054        2             28            0
Neighbor                23            3             12            0
Keepalive               189856        1665          187970        0
SEPPUKU                 0             0             0             0
```

```
Standby Elect Req       2             0             0             0
Standby Elect Ack       0             0             2             0
Standby IOS State       0             0             4             0
Reload Req              0             0             0             0
Reload Ack              0             0             0             0
SESA Mesg               0             0             0             0
RTU Msg                 0             0             0             0
Disc Timer Stop         1             0             2             0

---------------------------------------

WLC#show platform software stack-mgr chassis standby R0 sdp-counters
Stack Discovery Protocol (SDP) Counters

---------------------------------------

Message                 Tx Success    Tx Fail       Rx Success    Rx Fail
------------------------------------------------------------------------------
Discovery               14            2             19            0
Neighbor                6             2             5             0
Keepalive               175905        0             176196        0
SEPPUKU                 0             0             0             0
Standby Elect Req       0             0             1             0
Standby Elect Ack       1             0             0             0
Standby IOS State       2             0             0             0
Reload Req              0             0             0             0
Reload Ack              0             0             0             0
SESA Mesg               0             0             0             0
RTU Msg                 0             0             0             0
Disc Timer Stop         1             0             0             0

---------------------------------------

WLC#show platform software stack-mgr chassis standby R0 peer-timeout
Peer Chassis    Peer-timeout (ms)   50% Mark            75% Mark
------------------------------------------------------------------------
2               500                 0                   0
```

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 on RP port.

WLC#test wireless redundancy packetdump stop
Redundancy Port PacketDump Stop

Packet capture stopped on RP port.
```

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) bytes of data.
64 bytes from 169.254.39.131: icmp_seq=1 ttl=64 time=0.316 ms
64 bytes from 169.254.39.131: icmp_seq=2 ttl=64 time=0.324 ms
64 bytes from 169.254.39.131: icmp_seq=3 ttl=64 time=0.407 ms

--- 169.254.39.131 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.316/0.349/0.407/0.041 ms
```

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_FILE =
 BOOTLDR =
 STACK_1_1 = 0_0
 BOOT = bootflash:packages.conf,12;
 LICENSE_SUITE =
 CHASSIS_HA_IFNAME = GigabitEthernet3
 CHASSIS_HA_IFMAC = 00:50:56:8D:2A:93
 SWITCH_PRIORITY = 1
 RMI_INTERFACE_NAME = Vlan39
 RMI_CHASSIS_LOCAL_IP = 10.48.39.132
 RMI_CHASSIS_REMOTE_IP = 10.48.39.131
 CHASSIS_HA_LOCAL_IP = 169.254.39.132
 CHASSIS_HA_REMOTE_IP = 169.254.39.131
 CHASSIS_HA_LOCAL_MASK = 255.255.255.0
 RET_2_RTS =
 LICENSE_BOOT_LEVEL = ,csr1000v:csr1000v;
 BSI = 0
 RET_2_RCALTS =
 RANDOM_NUM = 193112462
```

Cette commande affiche la priorité du châssis, les détails RMI et RP, le délai d'attente des

homologues ainsi que des détails plus utiles.

Vous pouvez 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 vous souhaitez dépanner.

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



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 l'utilisateur forcé, qui apparaît lorsqu'un utilisateur a initié un basculement entre les contrôleurs, à l'aide de la commande redundancy force-switchover.

```
WLC#show redundancy switchover history
Index  Previous  Current  Switchover            Switchover
       active    active   reason                time
-----  --------  -------  ----------            ----------
   1       1        2     user forced           11:38:23 Central Fri Mar 10 2023
```

Unité active supprimée

Si vous regardez l'historique de commutation, vous pouvez voir l'unité active retirée, ce 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   reason                time
```

```
-----  --------  -------  ----------             ----------
   2       2        1     active unit removed    11:55:36 Central Fri Mar 10 2023
```

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   reason                 time
-----  --------  -------  ----------             ----------
   3       1        2     Active lost GW         12:00:26 Central Fri Mar 10 2023
```

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

Autres considérations

Activation de l'accès console pour le 9800 de secours

Connectez-vous à l'interface de ligne de commande du WLC actif et exécutez cette commande pour activer l'accès à la console pour le 9800 de secours. Sinon, l'accès à la console est verrouillé sur le WLC de secours :

```
WLC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
WLC(config)#redundancy
WLC(config-red)#main-cpu
WLC(config-r-mc)#standby console enable
```

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 décrits 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_mgr: Keepalive missed f
! Chassis is removed
%STACKMGR-6-CHASSIS_REMOVED_KA: Chassis 1 R0/0: stack_mgr: Chassis 2 has been removed from the stack du
! RP link is down
004469: Feb  4 02:17:28.707 Paris: %RIF_MGR_FSM-6-RP_LINK_DOWN: Chassis 1 R0/0: rif_mgr: Setting RP lin
! Dual active detection
004470: Feb  4 02:17:28.707 Paris: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Chassis 1 R0/0: stack_mgr: Dual Act
```

Si les deux châssis fonctionnent, la commutation crée une détection active Dual qui est une conséquence des pertes sur le RP.

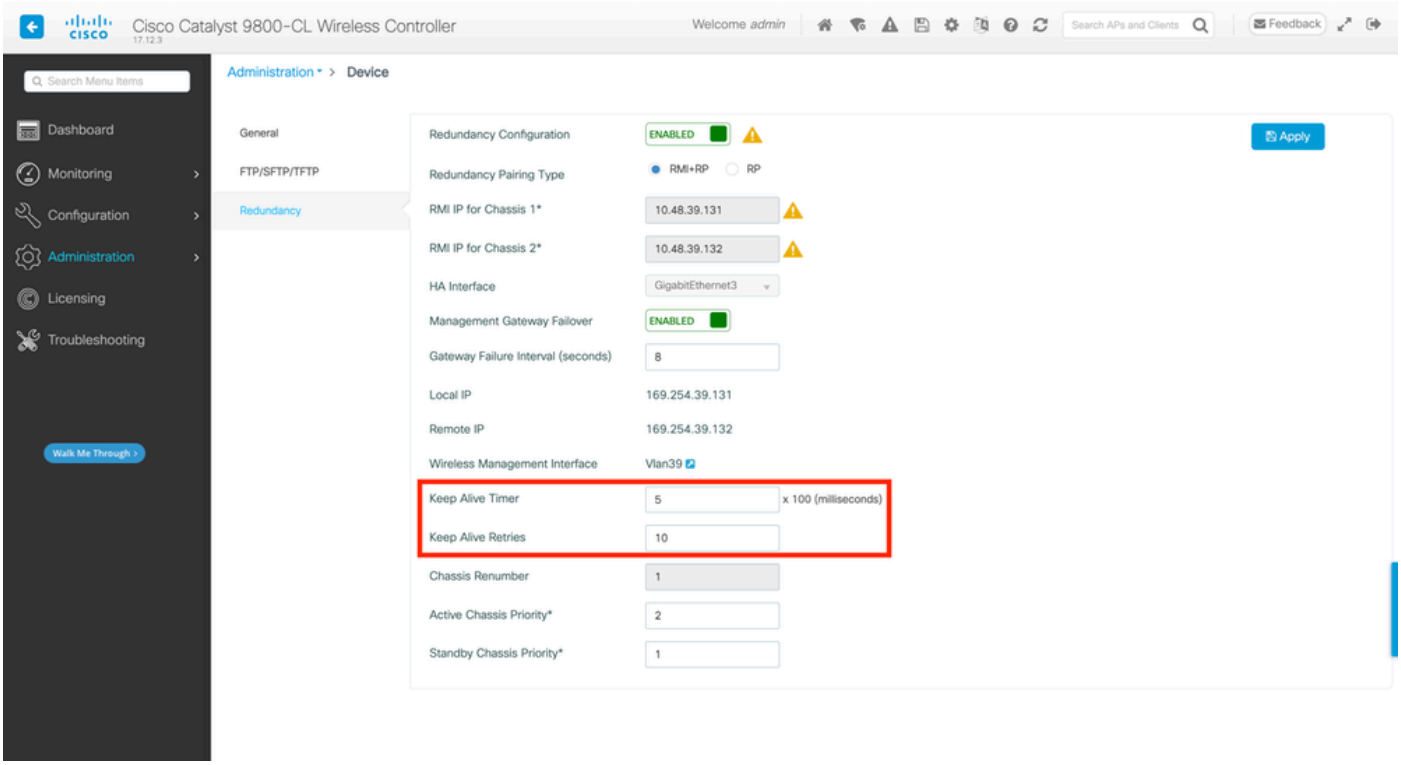
Dans ce cas, il peut être utile de modifier les paramètres de test d'activité haute disponibilité pour éviter ces basculements inutiles. Deux paramètres peuvent être configurés,

1. Minuteur de maintien de la connexion : durée séparant l'envoi de 2 messages de maintien de la connexion entre chaque châssis.
2. 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 retente sur 5. Cela signifie qu'après 5ms de maintien de la connexion 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 test d'activité de l'authentification unique haute disponibilité à partir de l'interface utilisateur graphique 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 de l'interface 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
```

⚠ Mise en garde : Gardez à l'esprit que lorsque la commutation rapide est désactivée, le contrôleur de secours s'appuie 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 de HA SSO pour le Catalyst 9800 au sein du réseau ACI, reportez-vous à la section Informations sur le déploiement du réseau ACI dans le contrôleur du Guide de configuration du logiciel du contrôleur sans fil Cisco Catalyst 9800.

Références

- 17.3 Guide HA SSO
- 17.6 Guide HA SSO

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.