

# Configureer hoge beschikbaarheid SSO op Catalyst 9800 | Snelstartgids

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Reflex voor één stop-shop](#)

[Opdrachten weergeven](#)

[Andere opdrachten](#)

[Meer informatie](#)

[Typische scenario's](#)

[Gedwongen gebruiker](#)

[Actieve eenheid verwijderd](#)

[Active Lost GW](#)

[Verdere overwegingen](#)

[HA SSO voor Catalyst 9800-CL](#)

[Catalyst 9800 HA SSO binnen ACI-implementaties](#)

[Referenties](#)

---

## Inleiding

Dit document beschrijft hoe u de stateful switchover (SSO) met hoge beschikbaarheid op een RP+RMI-manier kunt configureren op een Catalyst 9800 WLC.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben van

- Catalyst draadloze 9800 configuratiemodel.
- Concepten van hoge beschikbaarheid zoals behandeld in de HA SSO gids.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C980-CL v17.9.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Terwijl de configuratie van HA SSO slechts 3 van hen kan vereisen, hier zijn 4 IP adressen van het zelfde netwerk zoals de draadloze beheersinterface (WMI) gebruikt om de toegang tot het controlemechanisme GUI te vergemakkelijken.

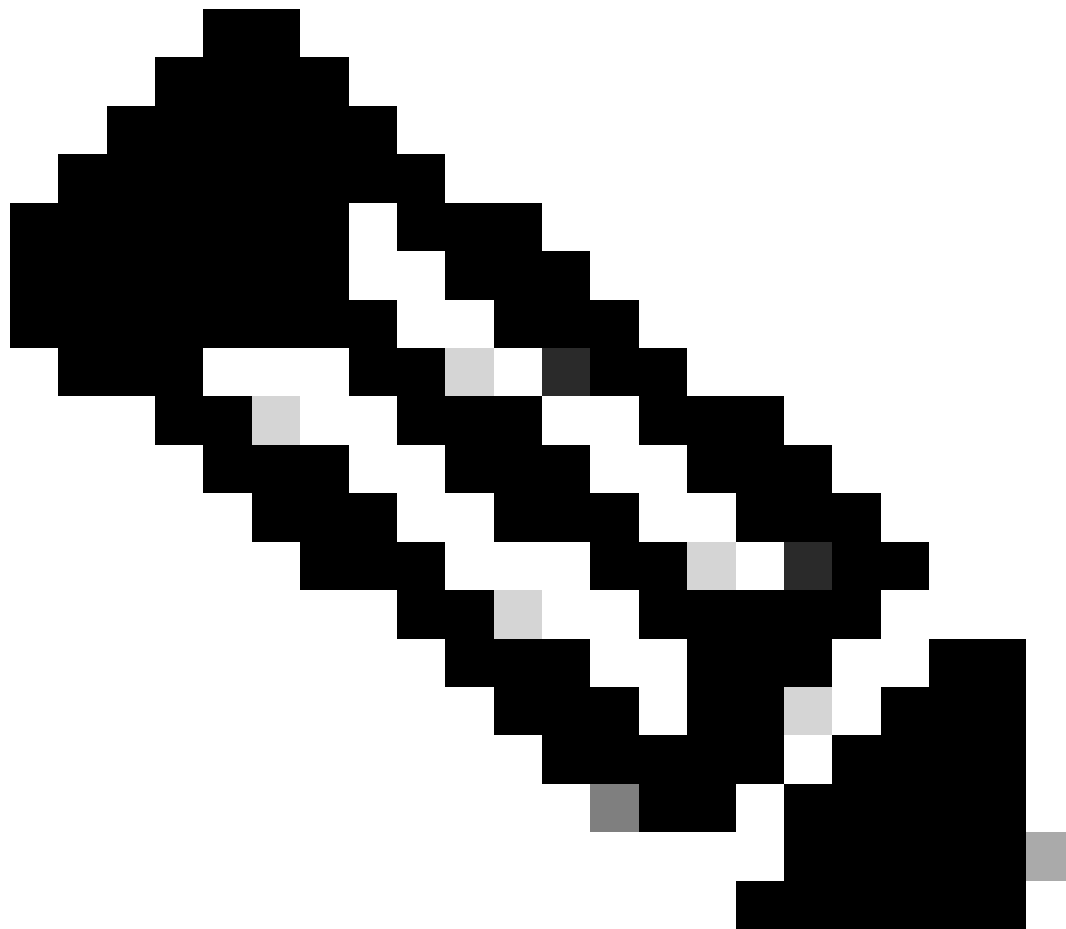
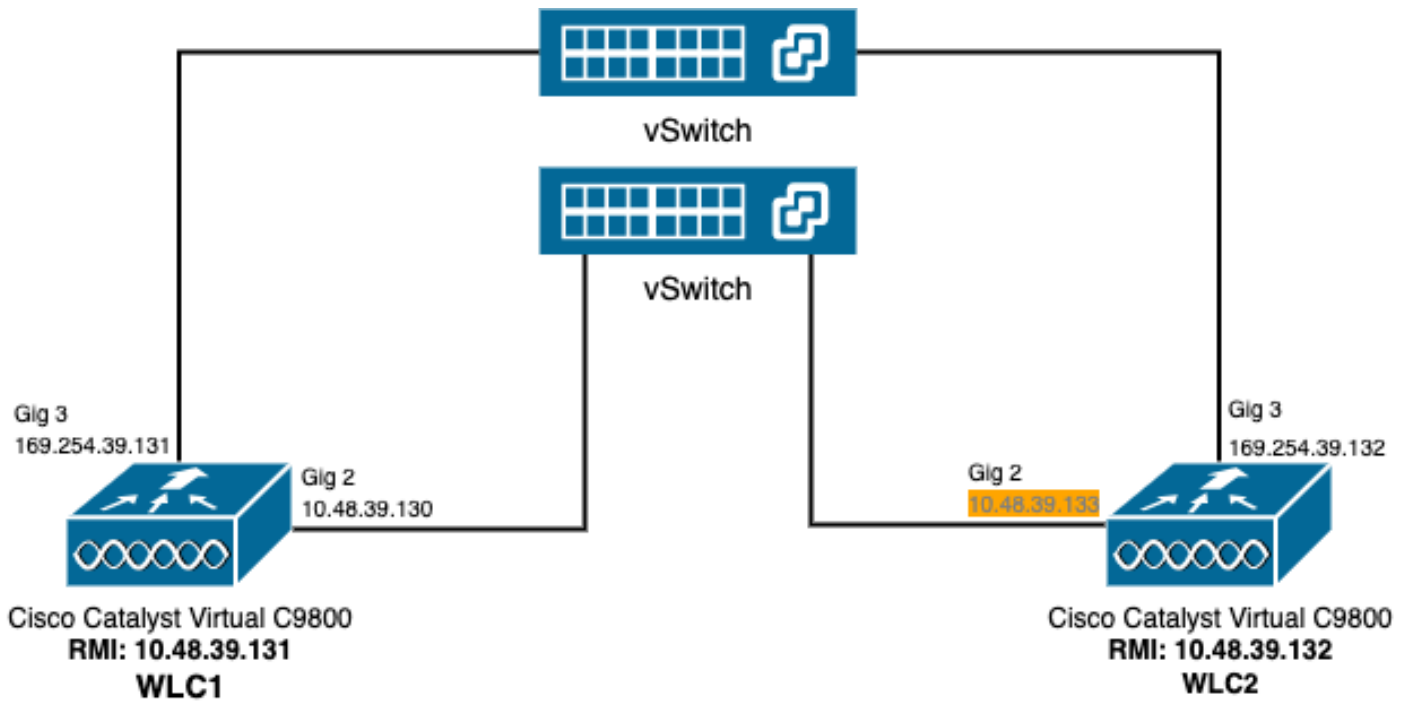
## Achtergrondinformatie

De hoge beschikbaarheid SSO-mogelijkheid op de draadloze controller stelt het toegangspunt in staat om een CAPWAP-tunnel te creëren met de actieve draadloze controller en de actieve draadloze controller om een kopie van de AP en client database te delen met de standby draadloze controller. Wanneer switchovers optreden (dat is de Active Controller mislukt en daarom de Standby neemt de hand), gaan aangesloten AP's niet naar de Discovery-status en clients maken geen verbinding. Er is slechts één CAPWAP-tunnel in een tijd onderhouden tussen de AP's en de draadloze controller die zich in een actieve staat bevindt.

De twee eenheden vormen een peer-verbinding via een speciale RP-poort (of een virtuele interface voor VM's) en beide controllers delen hetzelfde IP-adres op de beheerinterface. De RP-interface wordt gebruikt om bulk- en incrementele configuratie te synchroniseren bij uitvoering en de operationele status van beide controllers van het HA-paar te garanderen. Bovendien, wanneer RMI + RP wordt gebruikt, hebben zowel Standby als Actieve controllers een redundantie management interface (RMI) waaraan IP-adressen zijn toegewezen, namelijk gebruikt om gateway bereikbaarheid te garanderen. De CAPWAP-status van de access points die zich in de Run-status bevinden, wordt ook gesynchroniseerd van de actieve draadloze controller naar de Hot-Standby draadloze controller, waardoor de access points volledig kunnen worden overgeschakeld wanneer de actieve draadloze controller uitvalt. De AP's gaan niet naar de Discovery-status wanneer Active Wireless Controller mislukt, en Standby Wireless Controller neemt de rol over als Active Wireless Controller om het netwerk te bedienen.

## Configureren

### Netwerkdigram



---

Opmerking: in oranje wordt het tijdelijke IP-adres gemarkeerd dat is toegewezen aan de virtuele interface Gigabit Ethernet 2 van de 9800-CL controller die WLC2 heet. Dit IP-adres wordt tijdelijk gedefinieerd als de WMI voor WLC2 en biedt toegang tot de GUI van deze instantie om de HA SSO-configuratie te vergemakkelijken. Zodra HA SSO is geconfigureerd, wordt dit adres vrijgemaakt omdat slechts één WMI wordt gebruikt voor een HA SSO-paar controllers.

---

## Configuraties

In dit voorbeeld is de stateful switchover (SSO) met hoge beschikbaarheid (HA) geconfigureerd tussen twee 9800-CL-instanties, die dezelfde Cisco IOS-softwareversie uitvoeren, die geconfigureerd zijn met gescheiden WMI's en met GUI die toegankelijk is op

- IP-adres 10.48.39.130 voor de eerste, WLC1 genoemd;
- IP-adres 10.48.39.133 voor de tweede, WLC2 genoemd.

Naast deze IP-adressen zijn nog eens 2 adressen in hetzelfde subnetnummer (en VLAN) gebruikt, namelijk 10.48.39.131 en 10.48.39.132. Dit zijn de IP-adressen van de redundantie Management Interface (RMI) voor respectievelijk chassis 1 (WLC1) en chassis 2 (WLC2).



Opmerking: Zodra HA is geconfigureerd tussen de twee controllers, wordt 10.48.39.133 vrijgemaakt en 10.48.39.130 wordt de enige WMI van mijn configuratie. Daarom zijn na de configuratie slechts 3 IP-adressen in gebruik, de WMI en de RMI's.

---

De interfaceconfiguratie voor beide apparaten voordat ze zelfs de HA-configuratie starten moet gelijk zijn aan de interfaces die in dit voorbeeld worden geboden.

```
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
```

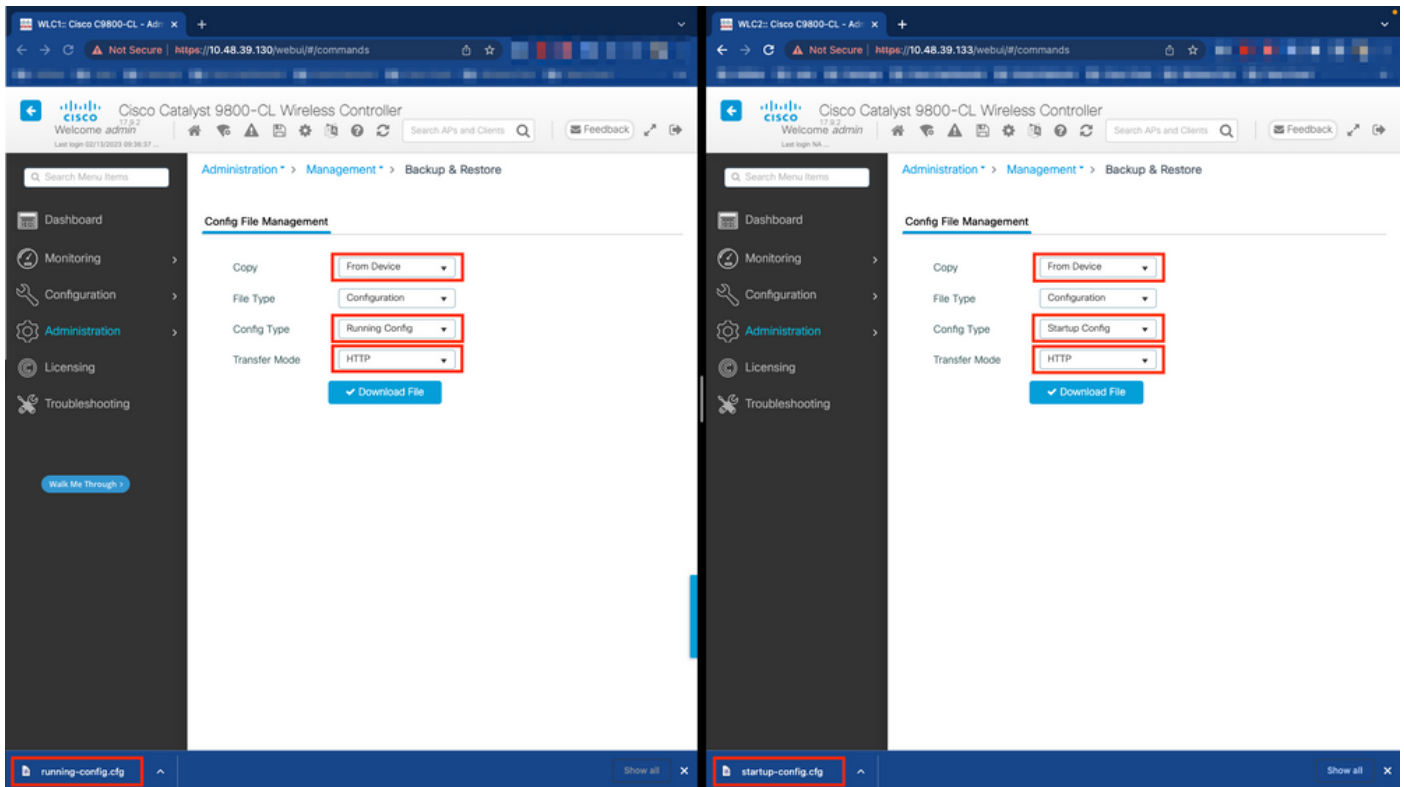
In dit voorbeeld wordt WLC1 aangeduid als de primaire controller (dat is chassis 1), terwijl WLC2 de secundaire controller is (dat is chassis 2). Dit betekent dat het HA-paar van de 2 controllers de configuratie van WLC1 gebruikt en dat de WLC2 na het proces verloren gaat.

**Stap 1.** (Optioneel) Back-up van de bestanden Startup Config en Running Config van de controllers.

Een foutieve verwerking kan leiden tot het verlies van de configuratie. Om dat te vermijden, wordt sterk aangeraden om zowel start- als loopconfiguratie van beide controllers die in de HA-configuratie worden gebruikt, te back-uppen. Dit kan eenvoudig worden gedaan met de 9800 GUI of CLI.

Via de GUI:

Van het tabblad *Beheer* → *Beheer* → *Back-up en herstel* van de 9800 GUI (zie de screenshot) kan men de opstart- en actieve configuratie downloaden die momenteel door de controller wordt gebruikt.



In dit voorbeeld worden zowel opstarten (linkerkant) en configuratie (rechterkant) direct gedownload, via HTTP, op het apparaat dat de browser host die wordt gebruikt om toegang te krijgen tot de GUI van de WLC. U kunt eenvoudig de overdrachtmodus en de bestemming van het bestand waarvan een back-up moet worden gemaakt, aanpassen met het veld Overdrachtmodus.

#### Van de 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)
```

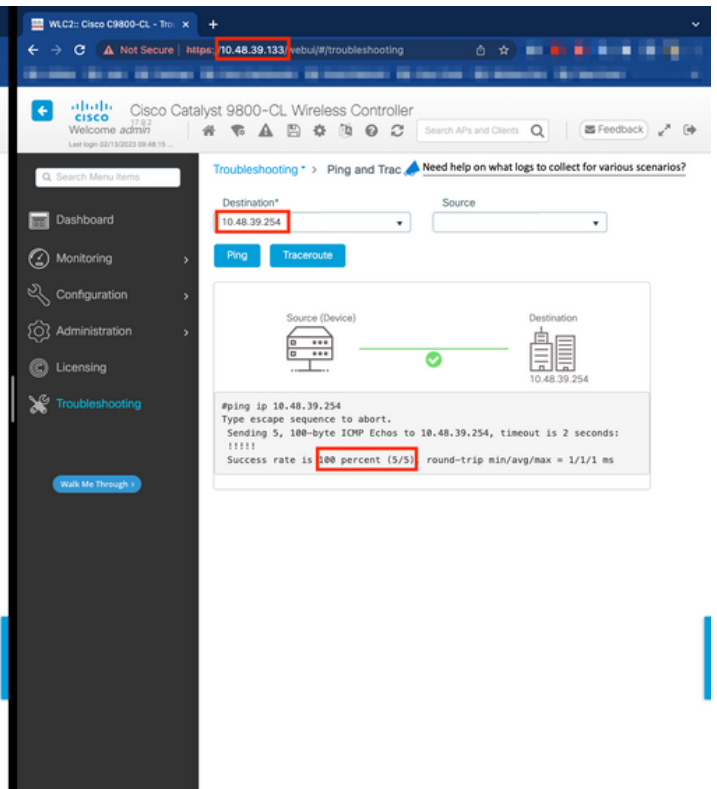
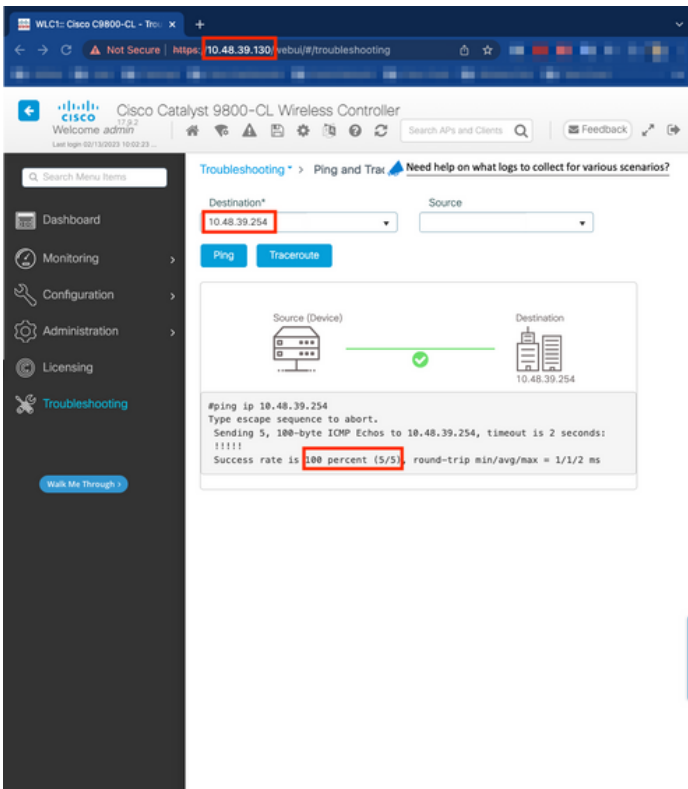
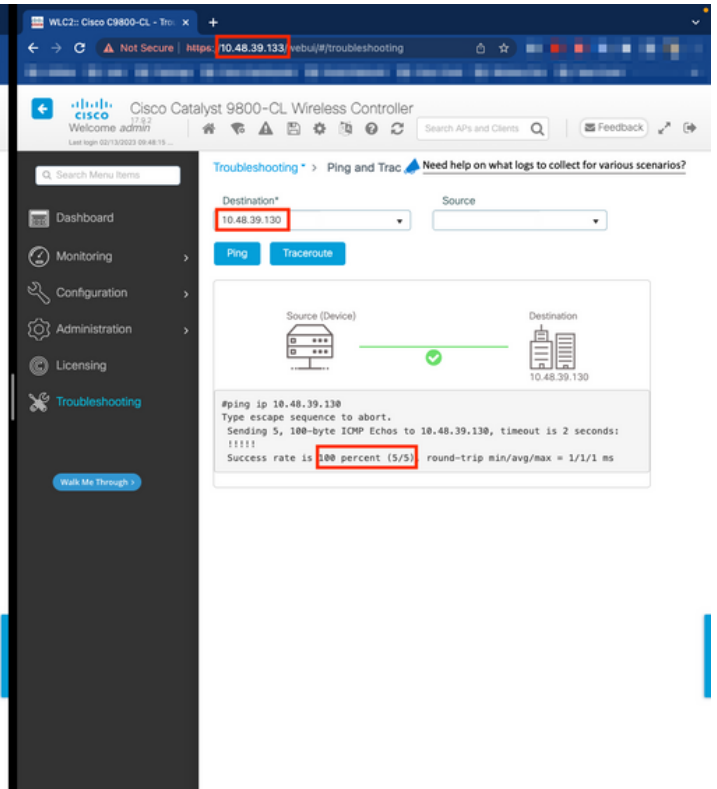
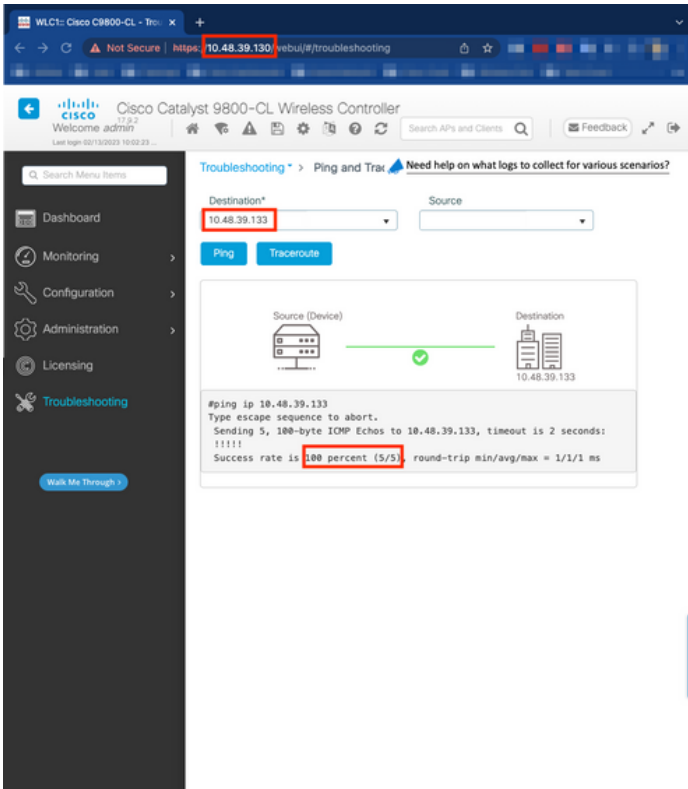
Vervang het bestand <SERVER-IP> door de TFTP-server IP waarnaar het opstart/actieve configuratiebestand wordt gekopieerd.

#### **Stap 2.** (optioneel) Zorg voor netwerkconnectiviteit.

Van zowel WLC GUIs als CLIs, kan men eenvoudige connectiviteitstests uitvoeren, namelijk pingelen de gateway van beide apparaten en pingelen de apparaten tussen elkaar. Dit zorgt ervoor dat beide controllers over de vereiste connectiviteit beschikken om HA te configureren.

#### Via de GUI:

De tool *Ping en Traceroute* van het tabblad *Problemen oplossen* van de 9800 GUI kan worden gebruikt om de connectiviteit tussen de controllers zelf en tussen elke WLC en zijn netwerkgateway te testen, zoals in deze cijfers wordt getoond.



Van de CLI:

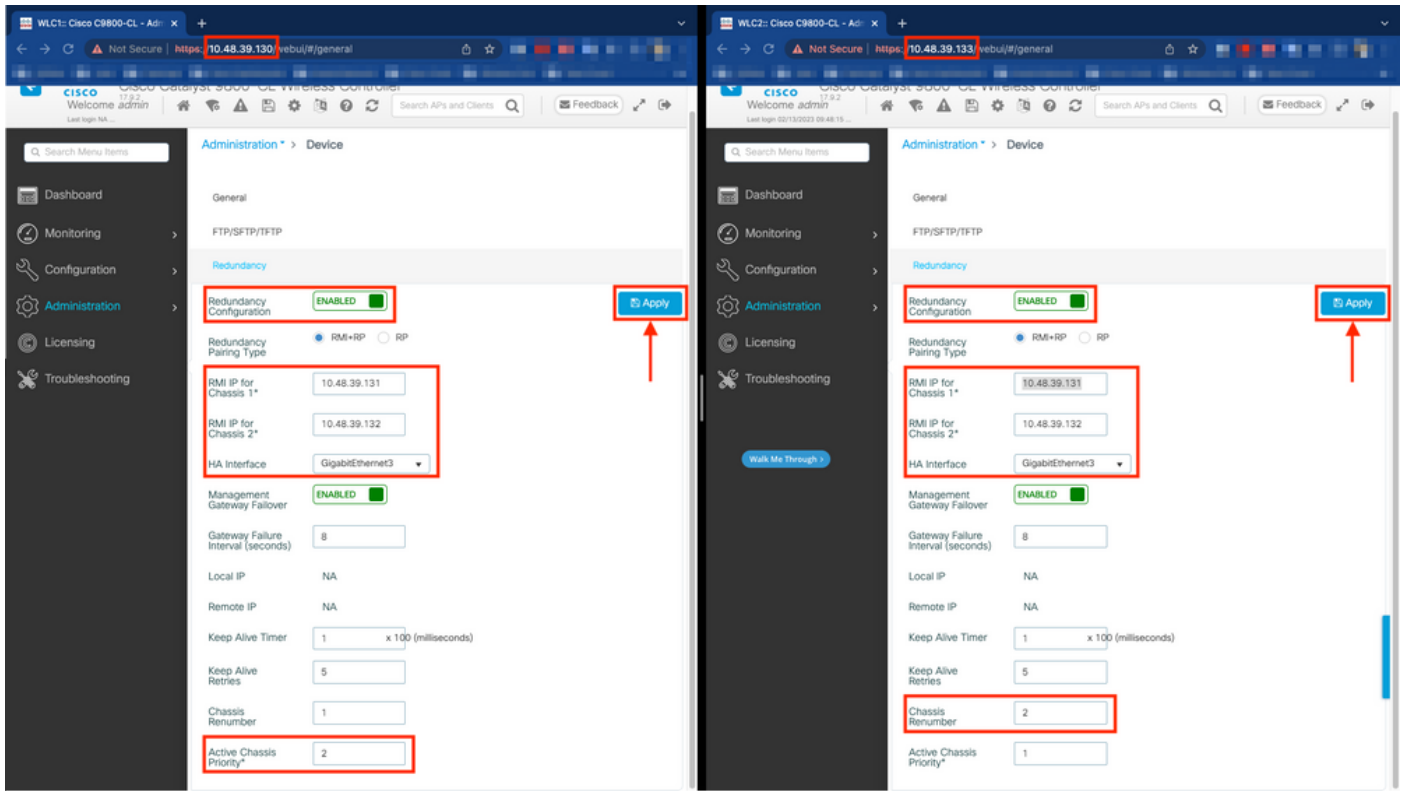
WLCx#ping 10.48.39.133 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.48.39.133, t

**Stap 3.** Configureer redundantie met RMI + RP-koppelingstype.

Als de verbinding tussen elk apparaat verzekerd is, kan redundantie worden geconfigureerd tussen de controllers. Deze screenshot laat zien hoe



de configuratie wordt gemaakt vanuit het tabblad *Redundantie* van de *pagina Beheer* → *Apparaat* van de 9800 GUI.





**Waarschuwing:** bij dit voorbeeld is WLC1 aangewezen als primaire controller, wat betekent dat dit degene is waarvan de configuratie wordt gerepliceerd naar de andere controller. Zorg ervoor dat u de juiste chassisprioriteit/hernummers toepast om de juiste configuratie met uw HA-paar te gebruiken en geen enkel deel ervan te verliezen.

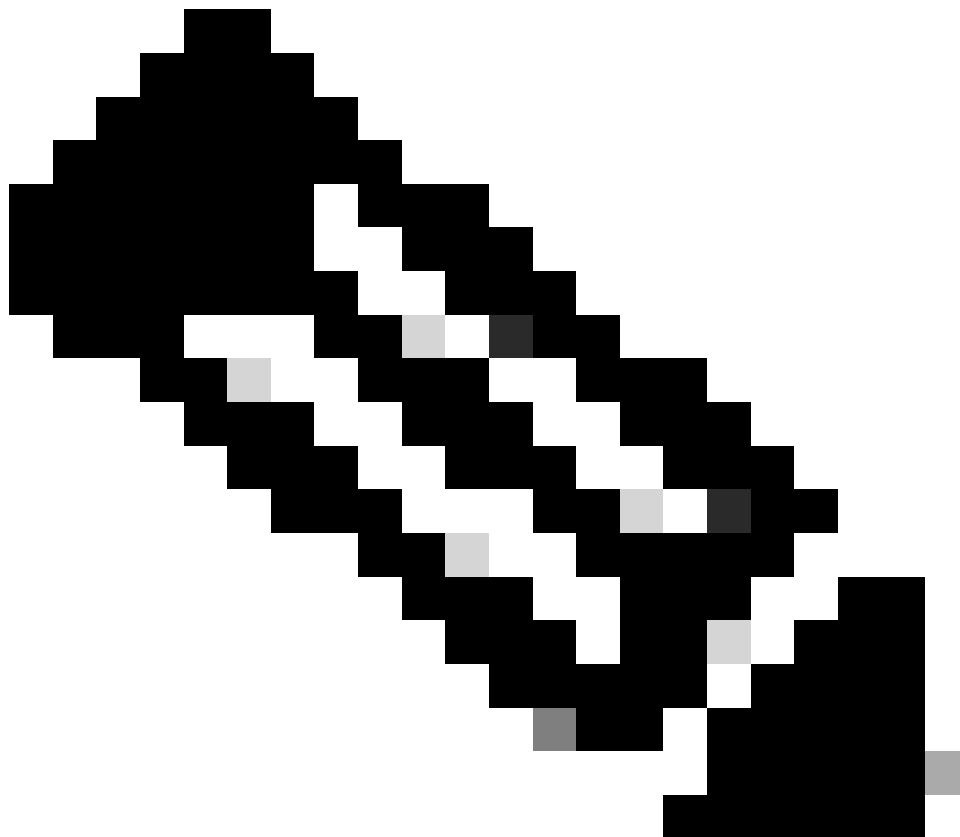
---

Laten we de geconfigureerde velden en hun doel bekijken

- **Redundantie Configuration:** dit moet zijn ingeschakeld om redundantie tussen WLC's te kunnen gebruiken.
- **Redundantie Pairing Type:** aangezien deze handleiding HA SSO omvat met behulp van RMI-configuratie, moet het geconfigureerde koppelingstype RMI + RP zijn, met behulp van zowel de redundantie management interface als de redundantie poort.

Men kan er ook voor kiezen om redundantie te configureren met alleen de redundantiepoort. Wanneer echter alleen RP wordt gekozen, wordt de bereikbaarheid van de gateway niet gecontroleerd, alleen de redundante WLC-status is

- **RMI IP voor chassis 1/2:** in deze velden worden de opgegeven IP-adressen toegewezen aan de aangewezen redundantie-interface voor beide instanties. In dit voorbeeld zijn beide RMI IP's voor chassis 1 en 2 geconfigureerd als respectievelijk 10.48.39.131 en 10.48.39.132, zoals eerder beschreven en in het [netwerkdigram](#) weergegeven.
- **HA-interface:** bij gebruik van virtuele apparaten kan de koppeling tussen de virtuele netwerkkinterfacekaarten (vNIC) van de hypervisor en de netwerkkinterfaces van de virtuele machine op verschillende manieren worden geconfigureerd. Daarom is de interface die wordt gebruikt voor redundantie configureerbaar voor Cisco Catalyst 9800-CL's. Hier is de Gigabit Ethernet 3 gebruikt, zoals aanbevolen in [de 9800-CL implementatiegids](#).



**Opmerking:** bij gebruik van fysieke C9800-toestellen is de interface die wordt gebruikt in HA en RP de standaardinterface en kan deze niet worden geconfigureerd. Inderdaad, hardware 9800 WLCs hebben een speciale redundantie interface die gescheiden is van hun netwerk degenen.

---

- **Management Gateway failover:** zoals gedetailleerd in de HA SSO-configuratiegids, implementeert deze redundantiemethode de standaard gateway-controle, uitgevoerd door periodiek het verzenden van Internet Control Message Protocol (ICMP) ping naar de gateway. Zowel de actieve als de standby controllers gebruiken de RMI IP als bron IP voor deze controles. Deze berichten worden verzonden met 1 tweede interval.

- **Het Interval van de mislukking van de gateway:** dit vertegenwoordigt de hoeveelheid tijd waarvoor een gatewaycontrole achtereenvolgens moet ontbreken alvorens de gateway als niet-bereikbaar wordt verklaard. Standaard is dit ingesteld op 8 seconden. Aangezien gatewaycontroles elke seconde worden verzonden, betekent dit 8 opeenvolgende mislukkingen om de gateway te bereiken.

- **Lokale/externe IP:** dit zijn de RP IP geconfigureerd voor chassis 1 en 2. Deze IP-adressen worden automatisch gegenereerd als 169.254.x.x, waarbij x.x is afgeleid van de laatste twee octetten van de beheerinterface.

- **Keep Alive Timer:** zoals beschreven in de HA SSO-configuratiehandleiding, versturen de Active- en stand-by-chassis onderhoudsberichten naar elkaar om ervoor te zorgen dat beide nog steeds beschikbaar zijn. De "keep alive"-timer is de hoeveelheid tijd die het verzenden van twee keeplive-berichten tussen elk chassis scheidt. Standaard worden elke 100 ms 's levensechte berichten verzonden. Het wordt vaak aanbevolen om deze waarde te verhogen met 9800-CL om misbruik van overschakelingen te voorkomen wanneer de VM-infrastructuur kleine vertragingen introduceert (snapshots, enzovoort ...)

- **Keep Alive Retries:** dit veld vormt de peer keeplive opnieuw proberen waarde voordat het beweert dat de peer is down. Als zowel de keep-alive timer als de opnieuw geprobeerd standaardwaarde worden gebruikt, wordt een peer neer geclaimd als 5 houden levende berichten die bij 100 ms tijdinterval worden verzonden onbeantwoord worden verlaten (namelijk als de overtolligheidsverbinding neer voor 500 ms is).

- **Chassis Hernummer:** het chassisnummer dat het apparaat moet gebruiken (1 of 2).

Op WLC2 (10.48.39.133), wordt het chassis hernummerd tot 2. Standaard is het chassisnummer 1. IP-adressen van RP-poorten zijn afgeleid van RMI. Als het chassisnummer hetzelfde is op beide controllers, is de lokale IP-afleiding van de RP-poort hetzelfde en is de ontdekking mislukt. Hernummer het chassis om dit zogenaamde Active-Active scenario te vermijden.

- **Prioriteit actief chassis:** de prioriteit die wordt gebruikt om te bepalen welke configuratie door het HA-paar moet worden gebruikt. Het

apparaat met de hoogste prioriteit is het apparaat dat naar de andere wordt gekopieerd. De configuratie van het chassis met de laagste prioriteit is daardoor verloren gegaan.

Op WLC1 (10.48.39.130), is de actieve chassisprioriteit ingesteld op 2. Dit is om ervoor te zorgen dat dit chassis wordt gekozen als de actieve (en daarom dat zijn configuratie wordt gebruikt) in het gemaakte HA-paar.

Zodra deze configuratie is gemaakt, gebruikt u de knop *Toepassen* om de configuratie op de controllers toe te passen.

#### Van de CLI

Configureer eerst een secundair IP-adres in de virtuele interface die wordt gebruikt om de RMI op beide apparaten te configureren.

```
WLC1#configure terminal WLC1(config)#interface vlan 39 WLC1(config-if)# ip address 10.48.39.131 255.255.255.0
```

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

Schakel vervolgens redundantie op beide apparaten in

```
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
```

Configureer de chassisprioriteit zoals WLC1 als de primaire controller

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

Hernumert chassis voor WLC2 dat de secundaire controller wordt

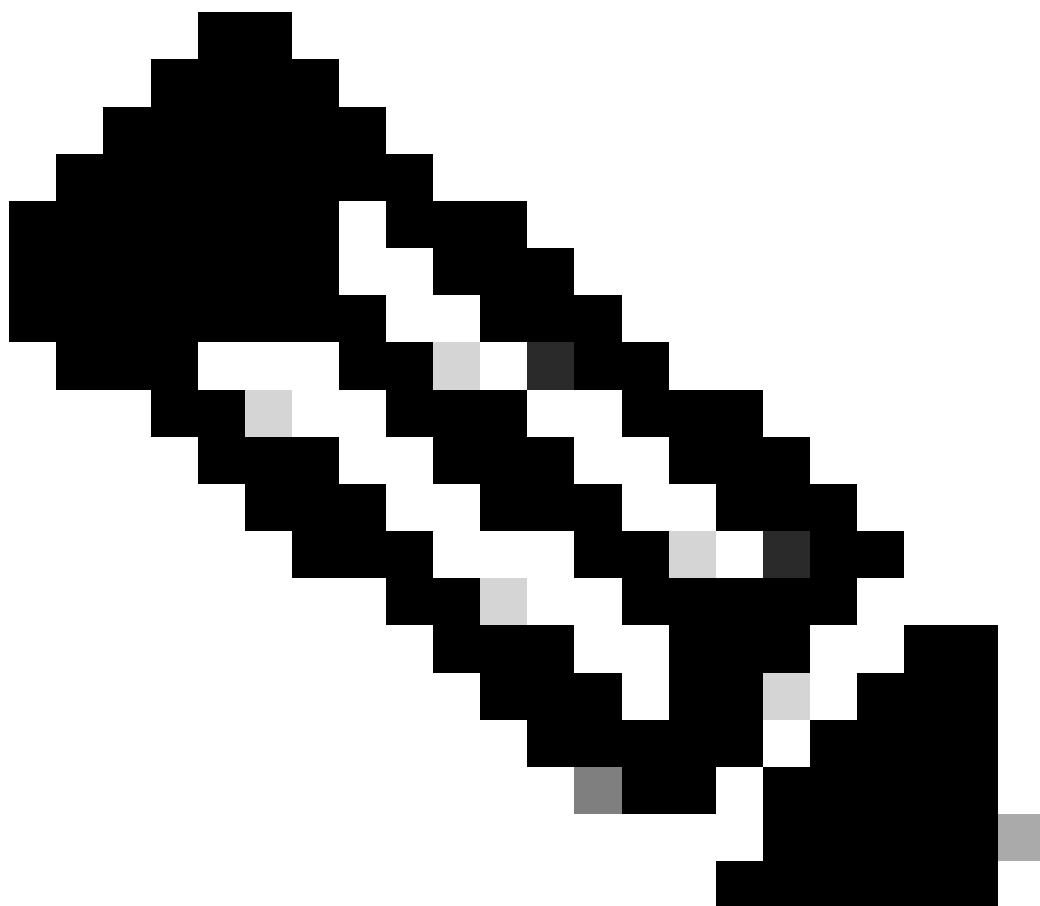
```
WLC2#show chassis Chassis/Stack Mac Address : 0001.0202.aabb - Local Mac Address Mac persistency wait t
```

Tenslotte moet u RMI op beide apparaten configureren

```
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
```

---



**Opmerking:** wat de GUI-configuratie betreft, moet op virtuele Catalyst 9800 de interface die door de controller wordt gebruikt tussen de beschikbare interfaces worden geselecteerd. Zoals aanbevolen wordt hier Gigabit Ethernet 3 gebruikt en dankzij de chassis redundancy ha-interface GigabitEthernet 3 opdracht geconfigureerd. Deze opdracht maakt geen deel uit van de actieve configuratie, maar de interface die wordt gebruikt door HA kan worden gezien in de instantie ROMMON-omgevingsvariabelen. Deze zijn te zien

---

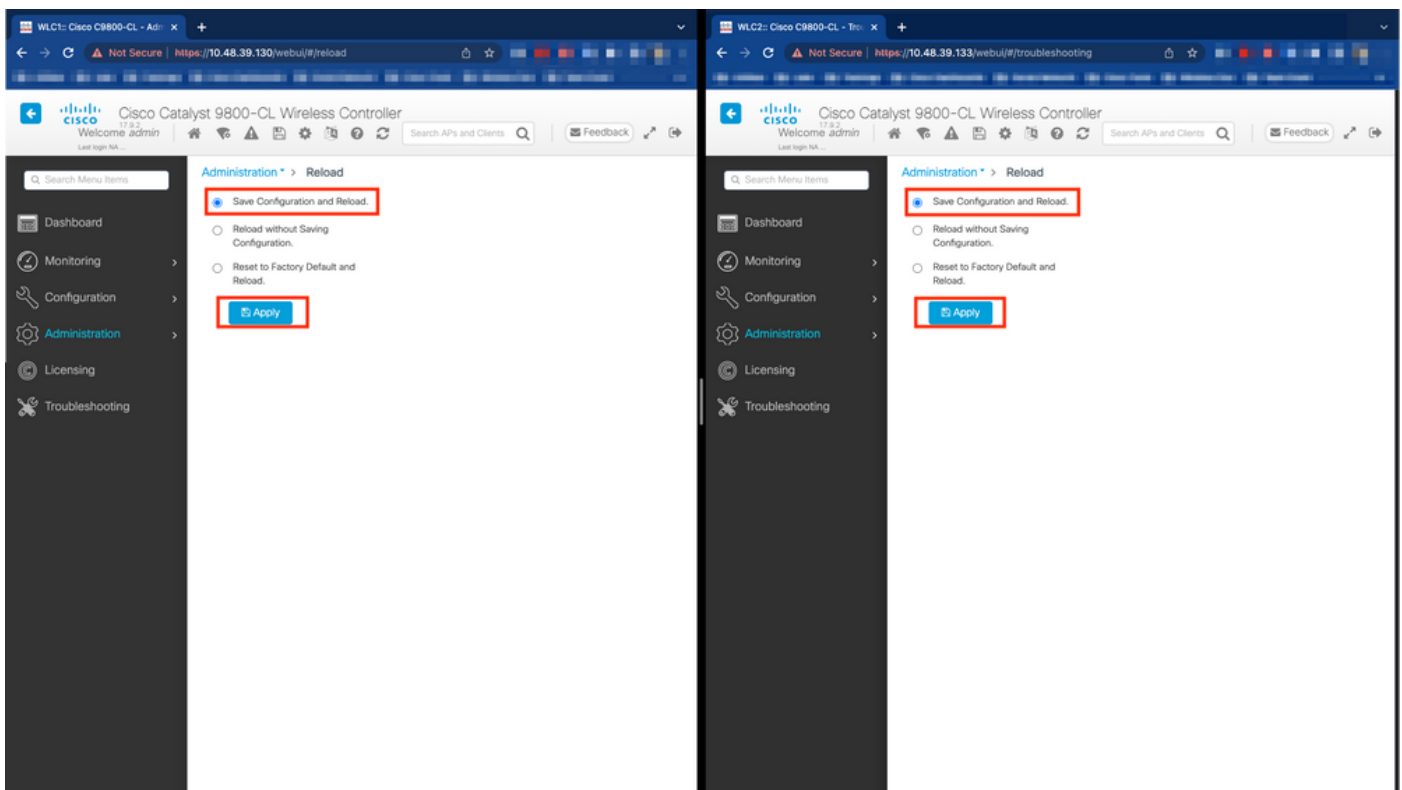
met de show romvar opdracht.

#### Stap 4. Opnieuw laden van controllers.

Om het HA-paar te kunnen vormen en de configuratie effectief te kunnen maken, moeten beide controllers tegelijkertijd opnieuw geladen worden zodra de configuratie gemaakt bij stap 3 is opgeslagen.

#### Van GUI:

Men kan de pagina van het Herladen van het Beleid van beide GUI gebruiken om de controlemechanismen opnieuw te beginnen, zoals die in dit screenshot worden getoond.



#### Van CLI:

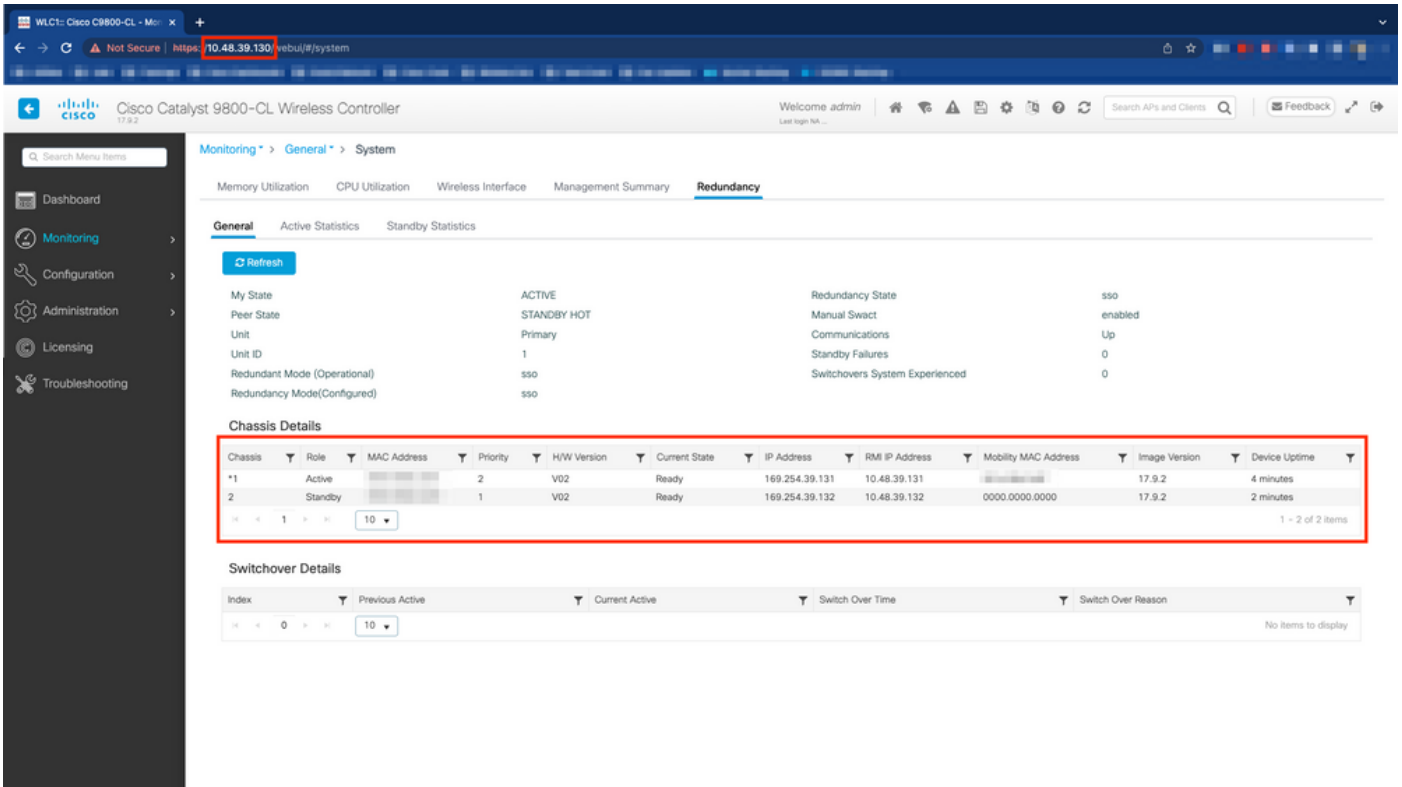
WLCx#reload Reload command is being issued on Active unit, this will reload the whole stack Proceed with

#### Verifiëren

Zodra beide controllers van het HA-paar elkaar ontdekken en het gewenste HA-paar creëren, kan één controller (de primaire) de twee chassis vanaf de GUI of CLI bewaken.

#### Van GUI:

Als u de redundantieconfiguratie vanaf de 9800 GUI wilt bewaken, navigeert u naar het tabblad Redundantie vanaf de pagina Monitoring > General > System, zoals in deze screenshot wordt weergegeven.



Van CLI:

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

WLC#show redundancy Redundant System Information : ----- Available system uptime

Problemen oplossen

Reflex voor één stop-shop

Het gebruikelijke show tech wireless omvat geen opdrachten die het mogelijk maken om de HA failover van een HA-paar te begrijpen, noch zijn huidige status naar behoren. Verzamel dit commando om de meeste HA-gerelateerde commando's in één operatie te hebben:

WLC#show tech wireless redundancy

Opdrachten weergeven

Voor de status van de redundantiepoorten kunnen deze opdrachten worden gebruikt.

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

Deze opdracht toont het chassisnummer en de poortstatus voor redundantie, en is nuttig als eerste stap voor probleemoplossing.



Om de keepalive tellers op de keepalive haven te verifiëren, kan men deze bevelen gebruiken.

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

Andere opdrachten

Het is mogelijk om met deze opdrachten een pakketopname op de redundantiepoort van de controller te maken

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

Opnamen die met deze opdrachten zijn gemaakt, worden in de vorm bootflash: van de controller opgeslagen onder de naam haIntCaptureLo.pcap.

Met deze opdracht kan ook een keepalive-test worden uitgevoerd op de redundantiepoort.

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

Meer informatie

Om de ROMMON Variables configuratie te bekijken, die ons laat zien hoe de eigenlijke configuratie wordt weerspiegeld op de variabelen, kunt u deze opdracht gebruiken.

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

Deze opdracht toont de prioriteit voor het chassis, zowel RMI- als RP-details, peer time-out samen met meer nuttige details.

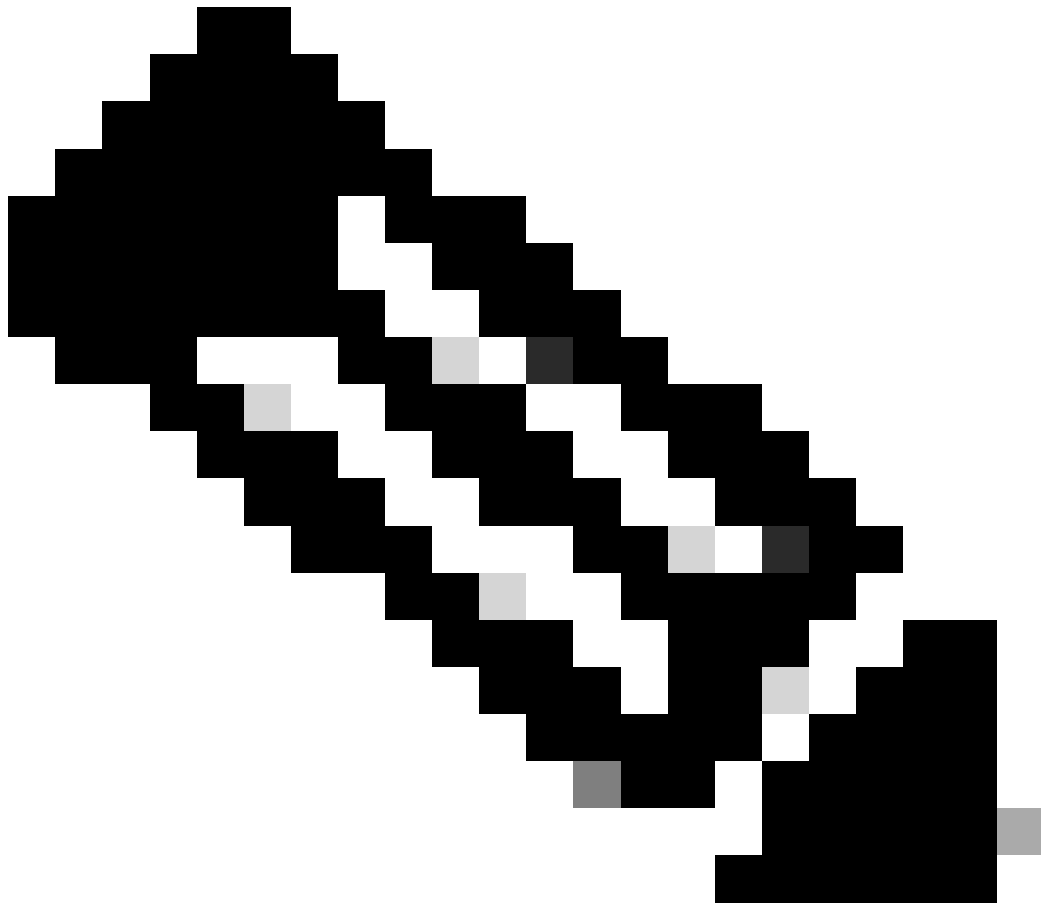
We kunnen ook de processen die HA SSO uitvoeren op de WLC die twee processen zijn, namelijk stack\_mgr en rif\_mgr.

Om dit te doen, verzamel altijd de sporen naar een tekstbestand met behulp van de opdracht, de tijdparameter hier kan worden aangepast om het tijdskader te bestrijken dat we willen oplossen.

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

---

---



**Opmerking:** het is belangrijk om op te merken dat de servicepoort van de standby WLC gedeactiveerd en onbereikbaar is terwijl de controller als standby fungeert.

---

Typische scenario's

Gedwongen gebruiker

Als u naar de overschakelgeschiedenis kijkt, kunt u zien "geforceerde gebruiker", verschijnen wanneer een gebruiker een overschakeling tussen de controllers initieerde, met behulp van de redundancy force-switchover opdracht.

WLC#show redundancy switchover history Index Previous Current Switchover Switchover active active reason

Actieve eenheid verwijderd

Als je kijkt naar de switchover geschiedenis, kun je zien "actieve unit verwijderd" wat wijst op een verlies van communicatie op de Redundantie poort tussen de twee controllers.

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

Dit kan gebeuren als de verbinding tussen de twee controllers uitvalt, maar het kan ook gebeuren als een WLC-unit plotseling uitvalt (stroomuitval) of crasht. Het is interessant om zowel WLCs te controleren om te zien of hebben zij systeemrapporten die op onverwachte crashes/reboots wijzen.

Active Lost GW

Als u naar de switchover-geschiedenis kijkt, kunt u "Active lost GW" zien, die wijst op een verlies van communicatie met de gateway op RMI-poort.

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

Dit gebeurt als de verbinding tussen de actieve controller en zijn gateway uitvalt.

Verdere overwegingen

HA SSO voor Catalyst 9800-CL

Wanneer in virtuele omgevingen, moet je accepteren dat latentie wordt geïntroduceerd, en latentie is niet iets dat HA goed tolereert. Dit is legitiem, aangezien HA SSO de neiging heeft om snel en efficiënt elke chassisfout te detecteren. Om dit te bereiken, controleert elk chassis de status van de andere door keepalives op zowel RP en RMI verbindingen te gebruiken evenals pings naar de gateway van hun RMI's (en dit, één van hun WMI die het zelfde moet zijn). Als een of meer van deze worden gemist, reageert de stack afhankelijk van de symptomen zoals beschreven in de "System and Network Fault Handling" uit de [HA SSO-handleiding](#).

Bij het werken met virtuele HA SSO stapels van Catalyst 9800, is het gebruikelijk om overschakelingen te observeren vanwege keepalive gemist over de RP-link. Dit kan het gevolg zijn van latentie die wordt geïntroduceerd door de gevirtualiseerde omgeving.

Om te bepalen of de HA SSO stack lijdt aan RP keepalive druppels, kunt u de stapel/rif manager logboeken gebruiken.

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

Als beide chassis in bedrijf zijn, dan creëert de overschakeling een "dubbele actieve detectie" die een gevolg is van de dalingen op RP.

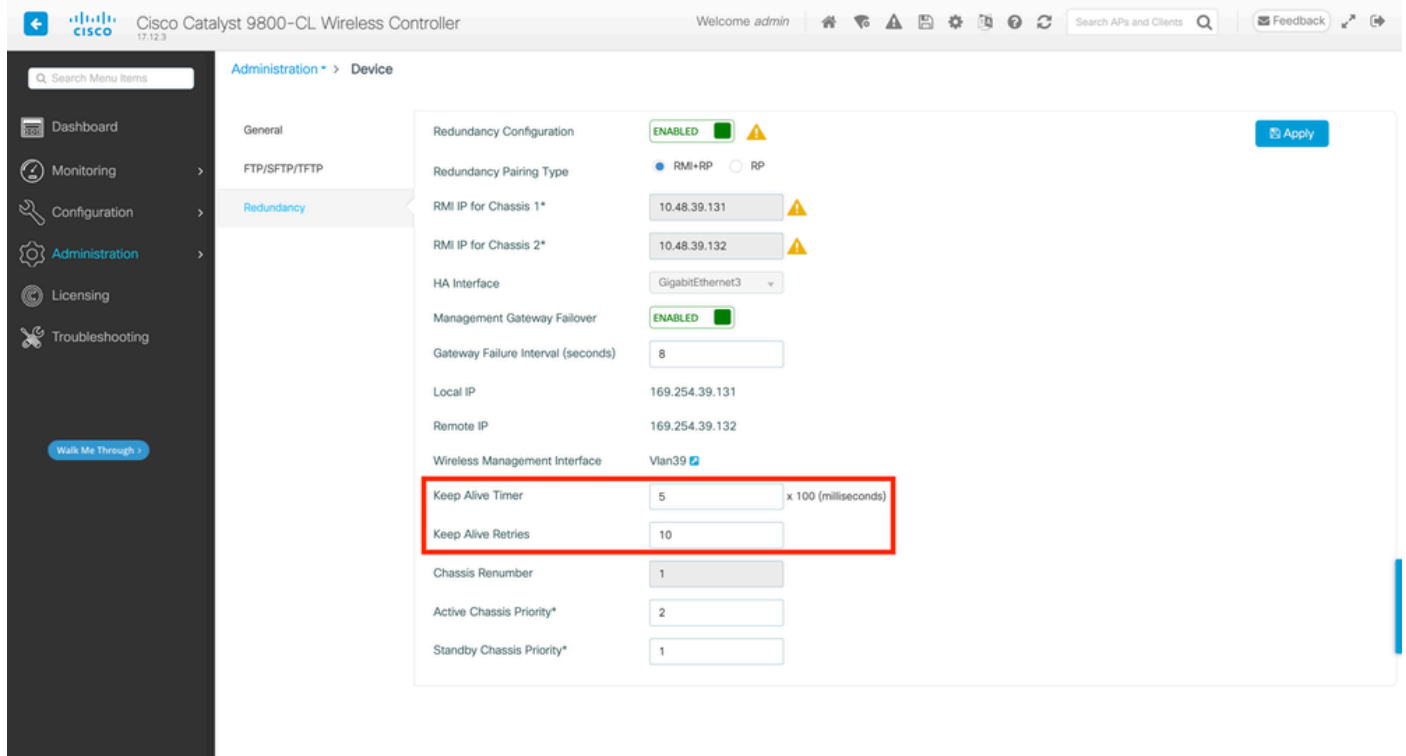
In zo'n situatie kan het aanpassen van HA keepalive parameters om deze onnodige overschakelingen te vermijden helpen. Er kunnen twee parameters worden geconfigureerd,

- **Keep Alive Timer:** de hoeveelheid tijd die het verzenden van twee keepalive-berichten tussen elk chassis scheidt.
- **Keep Alive Retries:** het aantal keepalive dat moet worden gemist om een peer down te verklaren.

Standaard is de timer voor levendig houden ingesteld op 1 ms en probeert deze opnieuw op 5. Dit betekent dat na 5ms van keepalive die op de verbinding van RP wordt gemist, een omschakeling voorkomt. Deze waarden zijn mogelijk te laag voor virtuele implementaties. Als u een terugkerende overschakeling ervaart doordat RP keepalives worden gemist, probeer dan deze parameters te verhogen om de stack te stabiliseren.

#### Van GUI:

Om de HA SSO keepalive parameters van de 9800 GUI te controleren of aan te passen, navigeer naar het tabblad Redundantie vanaf de pagina *Beheer > Apparaat*, zoals afgebeeld in deze screenshot.



#### Van CLI:

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

Samen met de configuratie van deze parameters kan een andere optimalisatie helpen met een dergelijk gedrag in de HA SSO stack. Voor fysieke apparaten is het met de hardware mogelijk een chassis met een andere te verbinden, meestal met behulp van één draad. In een virtuele omgeving moet de koppeling van de RP-poort voor elk chassis worden gemaakt door een Virtual switch (vSwitch), die weer latentie kan introduceren in vergelijking met de fysieke verbindingen. Een speciale vSwitch gebruiken om de RP-link te maken is een andere optimalisatie die HA keepalives kan voorkomen die verloren gaan door latentie. Dit is ook gedocumenteerd in de [Cisco Catalyst 9800-CL draadloze controller voor de cloudimplementatiegids](#). Daarom is het beste om een speciale vSwitch te gebruiken voor de RP-koppeling tussen de 9800-CL VM's en ervoor te zorgen dat er geen andere verkeersstoringen optreden.

#### Catalyst 9800 HA SSO binnen ACI-implementaties

Wanneer een overschakeling in een HA SSO-stack plaatsvindt, gebruikt het nieuw actieve chassis het gratuitous ARP (GARP) mechanisme om de MAC naar IP-mapping in het netwerk bij te werken en ervoor te zorgen dat het verkeer ontvangt dat gewijd is aan de controller. In het bijzonder, het chassis verzenden GARP om de nieuwe "eigenaar" van WMI te worden en ervoor te zorgen CAPWAP het verkeer de juiste chassis bereikt.

Het chassis dat actief wordt, verstuurt niet één GARP, maar een burst van hen om ervoor te zorgen dat elk apparaat in het netwerk zijn IP naar MAC-toewijzing bijwerkt. Deze burst kan de ARP-leerfunctie van ACI overweldigen en daarom wordt aanbevolen, wanneer ACI wordt gebruikt, deze burst zo veel mogelijk te beperken vanaf de Catalyst 9800-configuratie.

#### Van CLI:

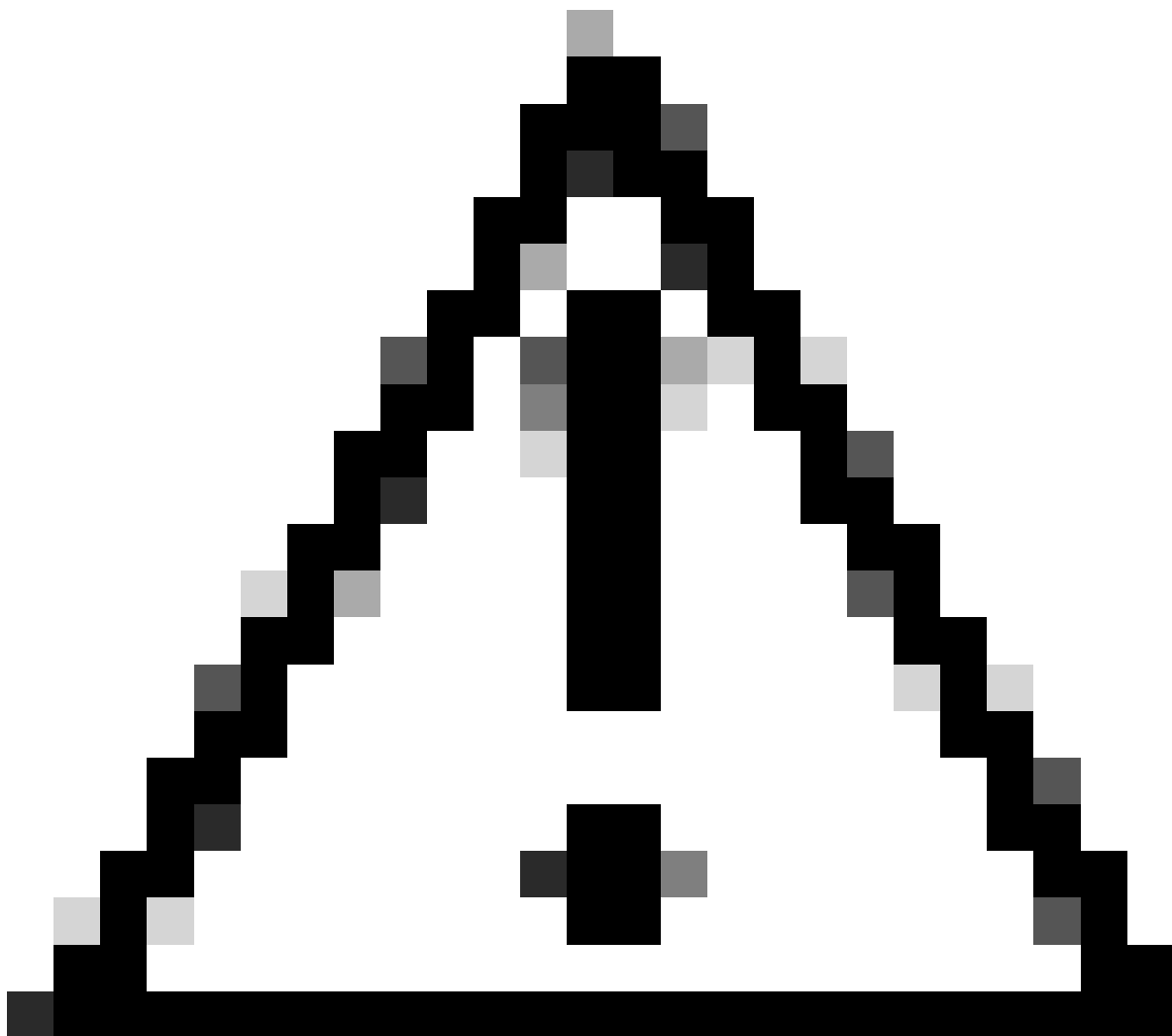
```
WLC# configure terminal WLC(config)# redun-management garp-retransmit burst 0 interval 0
```

Naast het beperken van de GARP burst geïnitieerd door de 9800 tijdens een switchover, wordt het ook aanbevolen om de snelle switchover optie op dit platform uit te schakelen. Wanneer de snelle overschakeling wordt geconfigureerd, stuurt de actieve controller een expliciete melding naar de stand-by controller, die zegt dat het naar beneden gaat. Tijdens het gebruik van dit, kan interleaving verkeer bestaan (AP's en clients worden gedropt) tussen beide WLC's die de HA-stack vormen totdat een van hen naar beneden gaat. Door deze functie uit te schakelen, stabiliseert u uw draadloze infrastructuur terwijl u met ACI-implementaties werkt.

Van CLI:

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

---



---

**Waarschuwing:** Houd in gedachten dat wanneer snelle switchover is uitgeschakeld, de stand-by controller alleen vertrouwt op de keepalive time-out-fouten om te detecteren wanneer de actieve controller is uitgeschakeld. Deze moeten daarom met de grootst mogelijke zorgvuldigheid worden opgesteld.

---

De details over overwegingen voor de plaatsingen van HSSD voor Catalyst 9800 binnen netwerk ACI kunnen in de sectie "Informatie over het Opstellen van ACI Netwerk in Controlemechanisme" van de [Gids](#) van de [Software van de](#) Controllerconfiguratie van [Cisco Catalyst 9800 Series draadloze controller](#) worden gezien.

#### Referenties

- [17.3 HA SSO gids](#)
- [17.6 HA SSO gids](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.