Konfigurieren von Hochverfügbarkeit SSO auf Catalyst 9800 | Kurzanleitung

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Konfigurieren
  - Netzwerkdiagramm
  - Konfigurationen
- Überprüfung
- Fehlerbehebung
  - Ein Stopp-Shop-Reflex
  - Befehle anzeigen
  - Andere Befehle
  - Mehr Details
  - Typische Szenarien
    - Vom Benutzer erzwungen
    - Aktive Einheit entfernt
    - Aktiv Verloren GW
- Weitere Überlegungen
  - HA SSO für Catalyst 9800-CL
  - Catalyst 9800 HA SSO in ACI-Bereitstellungen
- Referenzen

Einleitung

In diesem Dokument wird beschrieben, wie Sie auf einem Catalyst 9800 WLC ein Stateful Switchover (SSO) mit hoher Verfügbarkeit auf RP+RMI-Basis konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse

- Catalyst Wireless 9800-Konfigurationsmodell
- Hochverfügbarkeitskonzepte, wie sie im HA SSO-Leitfaden behandelt werden.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C9800-CL v17.9.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Während die HA SSO-Konfiguration nur drei davon erfordern kann, wurden hier vier IP-Adressen aus demselben Netzwerk wie die Wireless Management Interface (WMI) verwendet, um den Zugriff auf die Controller-GUI zu vereinfachen.

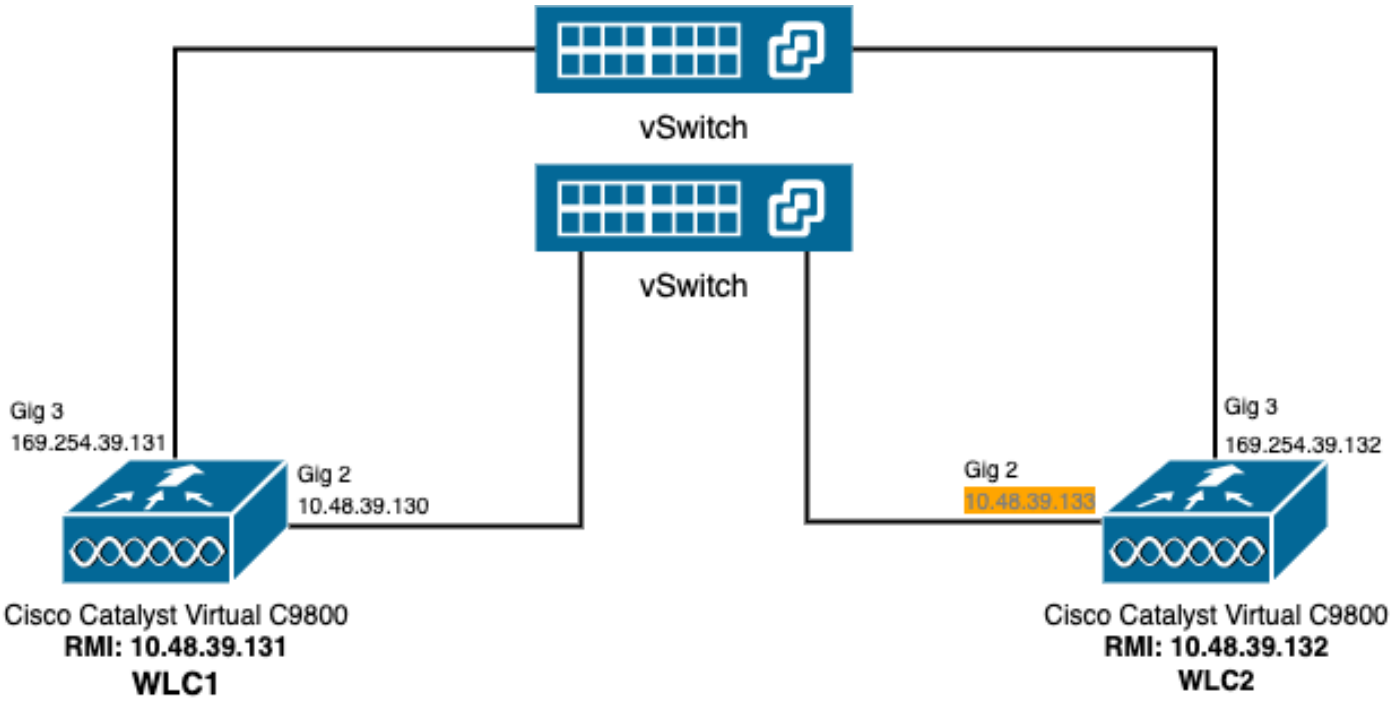
Hintergrundinformationen

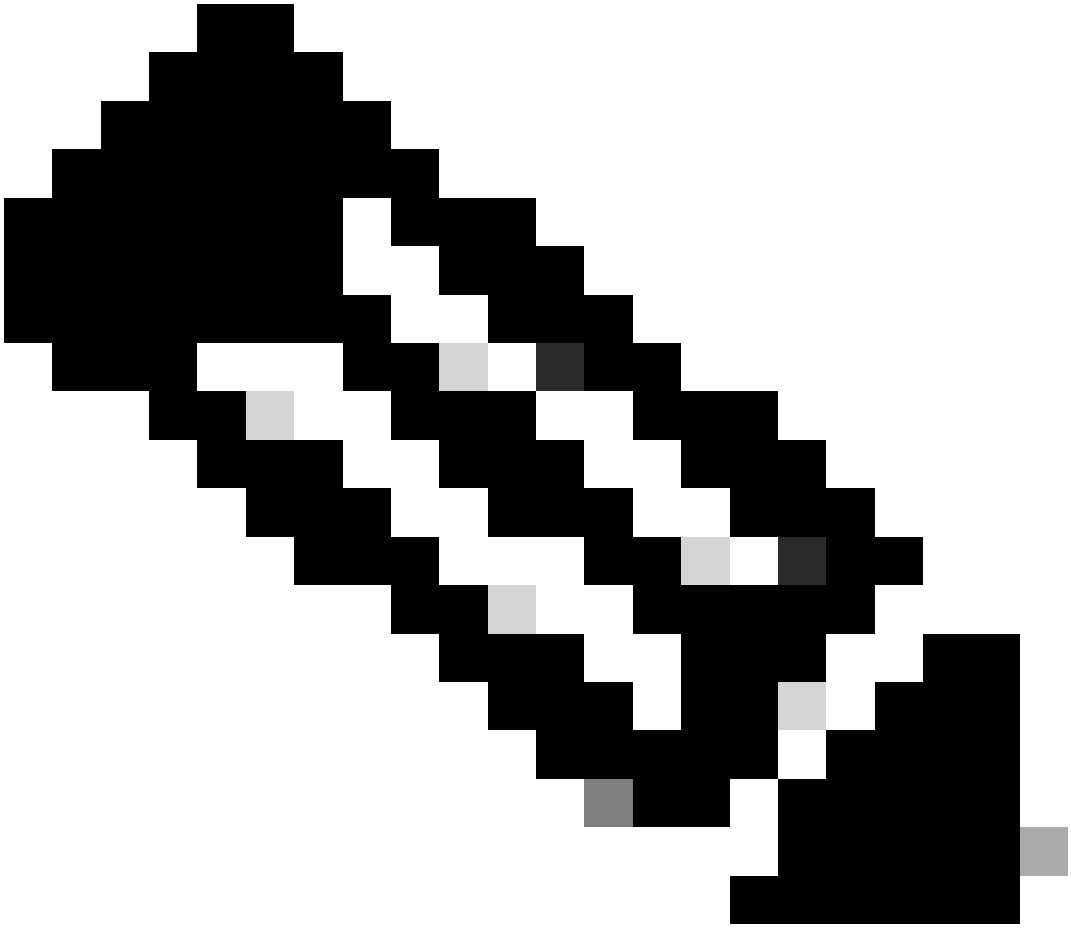
Die Hochverfügbarkeits-SSO-Funktion des Wireless Controllers ermöglicht dem Access Point die Einrichtung eines CAPWAP-Tunnels mit dem aktiven Wireless Controller und dem aktiven Wireless Controller, um eine Spiegelkopie des AP und der Client-Datenbank mit dem Standby-Wireless Controller gemeinsam zu nutzen. Bei einem Switchover (d. h. wenn der aktive Controller ausfällt und der Standby-Access Point die Hand übernimmt), werden verbundene APs nicht in den Erkennungsstatus versetzt, und die Verbindung der Clients wird nicht getrennt. Es wird jeweils nur ein CAPWAP-Tunnel zwischen den APs und dem Wireless-Controller im aktiven Zustand verwaltet.

Die beiden Einheiten bilden eine Peer-Verbindung über einen dedizierten RP-Port (oder eine virtuelle Schnittstelle für VMs), und beide Controller verwenden dieselbe IP-Adresse auf der Management-Schnittstelle. Die RP-Schnittstelle dient zum Synchronisieren umfangreicher und inkrementeller Konfigurationen zur Laufzeit und zum Sicherstellen des Betriebsstatus beider Controller des HA-Paars. Darüber hinaus verfügen Standby- und Active-Controller bei Verwendung von RMI + RP über eine Redundanz-Management-Schnittstelle (RMI), der IP-Adressen zugewiesen werden, um die Gateway-Erreichbarkeit zu gewährleisten. Der CAPWAP-Status der Access Points, die sich im Ausführungszustand befinden, wird ebenfalls vom aktiven Wireless Controller zum Hot-Standby Wireless Controller synchronisiert. Auf diese Weise können die Access Points bei einem Ausfall des aktiven Wireless Controllers vollständig umgeschaltet werden. Wenn der aktive Wireless-Controller ausfällt, werden die APs nicht erkannt, und der Standby-Wireless-Controller übernimmt die Rolle des aktiven Wireless-Controllers für den Netzwerkbetrieb.

Konfigurieren

Netzwerkdiagramm


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



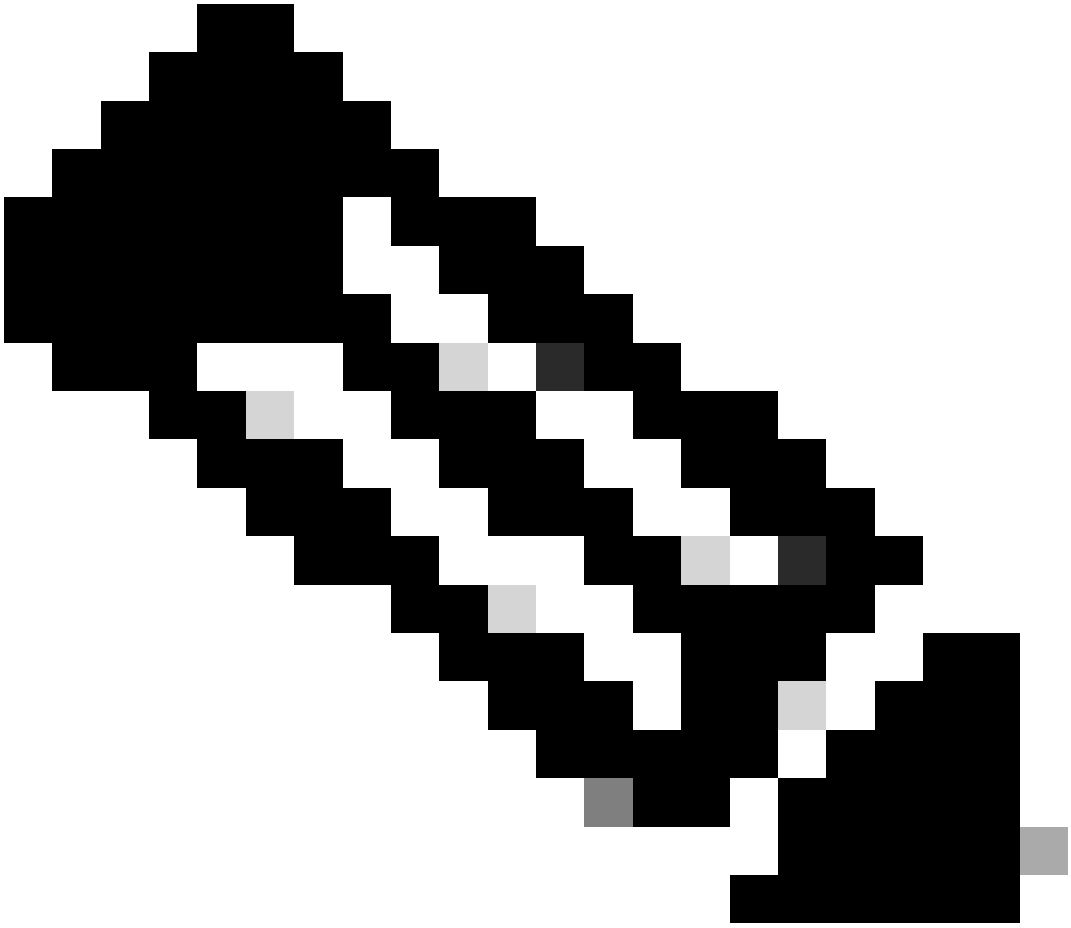
Hinweis: In orange ist die temporäre IP-Adresse hervorgehoben, die der virtuellen Schnittstelle GigabitEthernet 2 des 9800-CL-Controllers zugewiesen ist, der als WLC2 bezeichnet wird. Diese IP-Adresse wird vorübergehend als WMI für WLC2 definiert und ermöglicht den Zugriff auf die grafische Benutzeroberfläche dieser Instanz, um die HA SSO-Konfiguration zu vereinfachen. Nach der Konfiguration von HA SSO wird diese Adresse freigegeben, da für ein HA SSO-Controller-Paar nur ein WMI verwendet wird.

Konfigurationen

In diesem Beispiel wird ein Stateful Switchover (SSO) mit hoher Verfügbarkeit zwischen zwei 9800-CL-Instanzen konfiguriert, auf denen dieselbe Cisco IOS-Softwareversion ausgeführt wird. Diese wurden mit separaten WMIs konfiguriert und verfügen über eine Benutzeroberfläche, auf die unter

- die IP-Adresse 10.48.39.130 für die erste Adresse, die als WLC1 bezeichnet wird;
- Die zweite IP-Adresse lautet 10.48.39.133 und wird als WLC2 bezeichnet.

Neben diesen IP-Adressen wurden zwei weitere Adressen im gleichen Subnetz (und VLAN) verwendet, nämlich 10.48.39.131 und 10.48.39.132. Dies sind die RMI-IP-Adressen (Redundancy Management Interface) für Chassis 1 (WLC1) und Chassis 2 (WLC2).



Hinweis: Wenn HA zwischen den beiden Controllern konfiguriert ist, wird 10.48.39.133 freigegeben, und 10.48.39.130 wird zum einzigen WMI meiner Konfiguration. Daher werden nach der Konfiguration nur drei IP-Adressen verwendet, die der WMI und die der RMIs.

Die Schnittstellenkonfiguration für beide Geräte muss ähnlich wie in diesem Beispiel sein, bevor die HA-Konfiguration überhaupt initiiert wird.

```
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 diesem Beispiel ist WLC1 als primärer Controller (d. h. Chassis 1) festgelegt, während WLC2 als sekundärer Controller (d. h. Chassis 2) festgelegt ist. Das bedeutet, dass das aus den beiden Controllern bestehende HA-Paar die Konfiguration des WLC1 verwendet und dass nach dem Prozess der eine des WLC2 verloren geht.

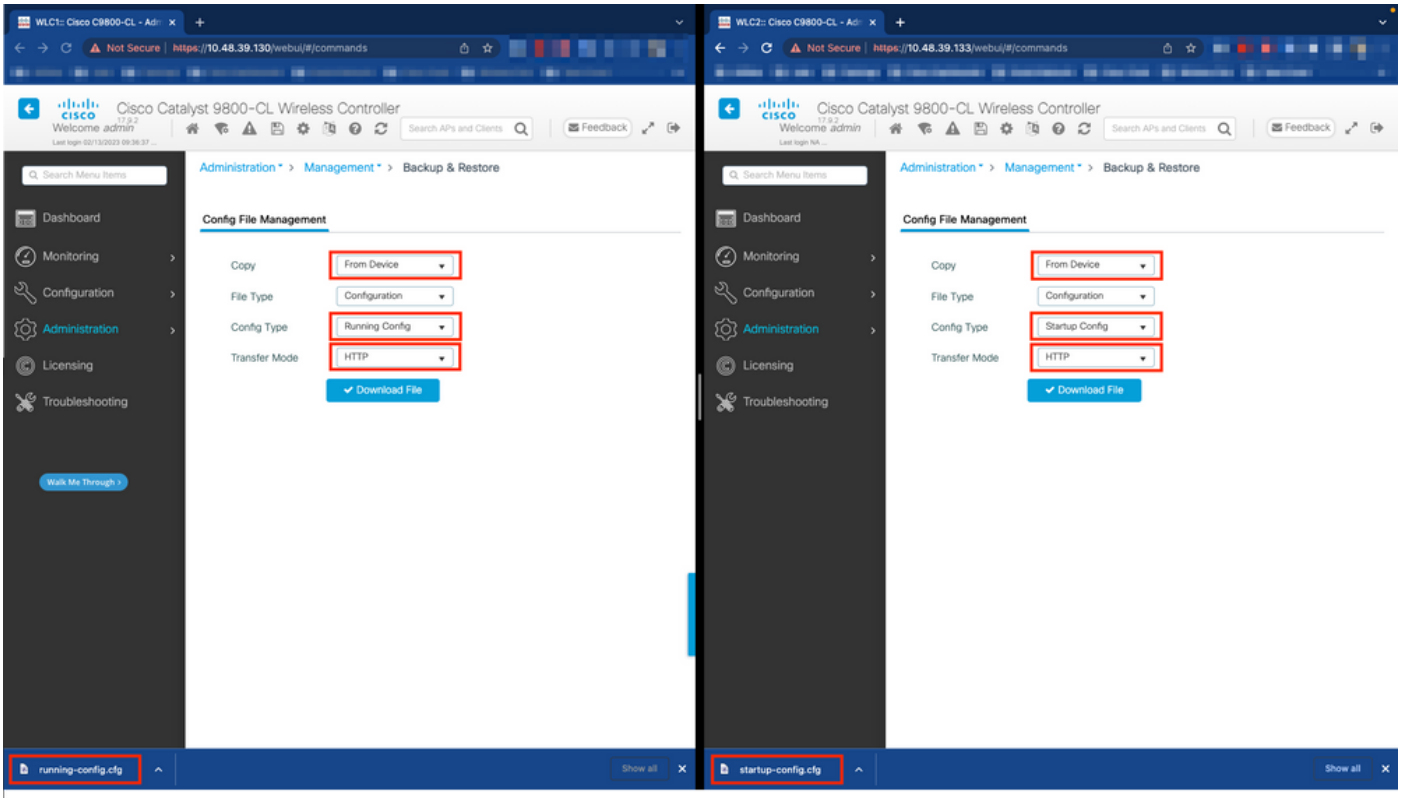
Schritt 1: Sichern Sie optional die Startkonfigurations- und Ausführungskonfigurationsdateien der Controller.

Falsche Handhabung kann passieren und dazu führen, dass die Konfiguration verloren geht. Um dies zu vermeiden, wird dringend empfohlen, sowohl die Start- als auch die aktuelle Konfiguration von beiden in der HA-Konfiguration verwendeten Controllern zu sichern. Dies ist über die Benutzeroberfläche oder die Kommandozeile des 9800 ganz einfach möglich.

Über die GUI:

Über die Registerkarte *Administration → Management → Backup & Restore (Verwaltung* und *Verwaltung Sicherung und Wiederherstellung)* der Benutzeroberfläche des 9800 (siehe Screenshot) können Sie die aktuell vom Controller verwendete Start- und Ausführungskonfiguration

herunterladen.



In diesem Beispiel werden sowohl der Startvorgang (linke Seite) als auch die Konfiguration (rechte Seite) direkt über HTTP auf das Gerät heruntergeladen, das den Browser hostet, der für den Zugriff auf die grafische Benutzeroberfläche des WLC verwendet wird. Der Übertragungsmodus und das Ziel der zu sichernden Datei können mit dem Feld Übertragungsmodus leicht angepasst werden.

Über die 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)
```

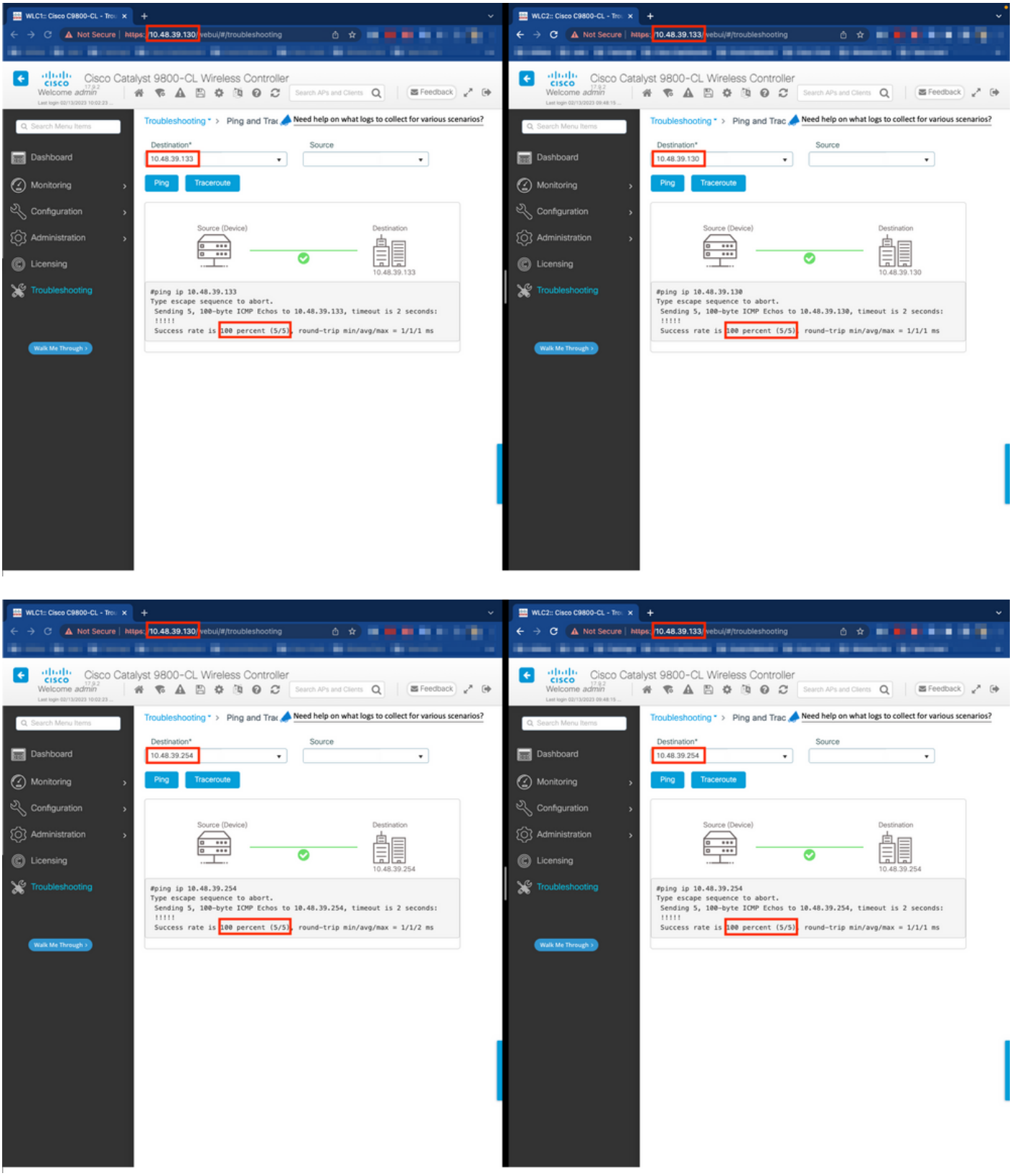
Ersetzen Sie die <SERVER-IP> durch die TFTP-Server-IP-Adresse, in die die Start-/aktuelle Konfigurationsdatei kopiert wird.

Schritt 2: (Optional) Sicherstellen der Netzwerkverbindung

Von beiden WLC-GUIs oder CLIs können einfache Verbindungstests durchgeführt werden, bei denen ein Ping an das Gateway von beiden Geräten und ein Ping an die Geräte untereinander gesendet wird. Dadurch wird sichergestellt, dass beide Controller über die erforderliche Konnektivität für die Konfiguration von HA verfügen.

Über die GUI:

Mit dem Tool *Ping und Traceroute* auf der Registerkarte *Troubleshooting (Fehlerbehebung)* der Benutzeroberfläche des Cisco 9800 können die Verbindungen zwischen den Controllern selbst sowie zwischen den einzelnen WLCs und ihren Netzwerk-Gateways getestet werden.



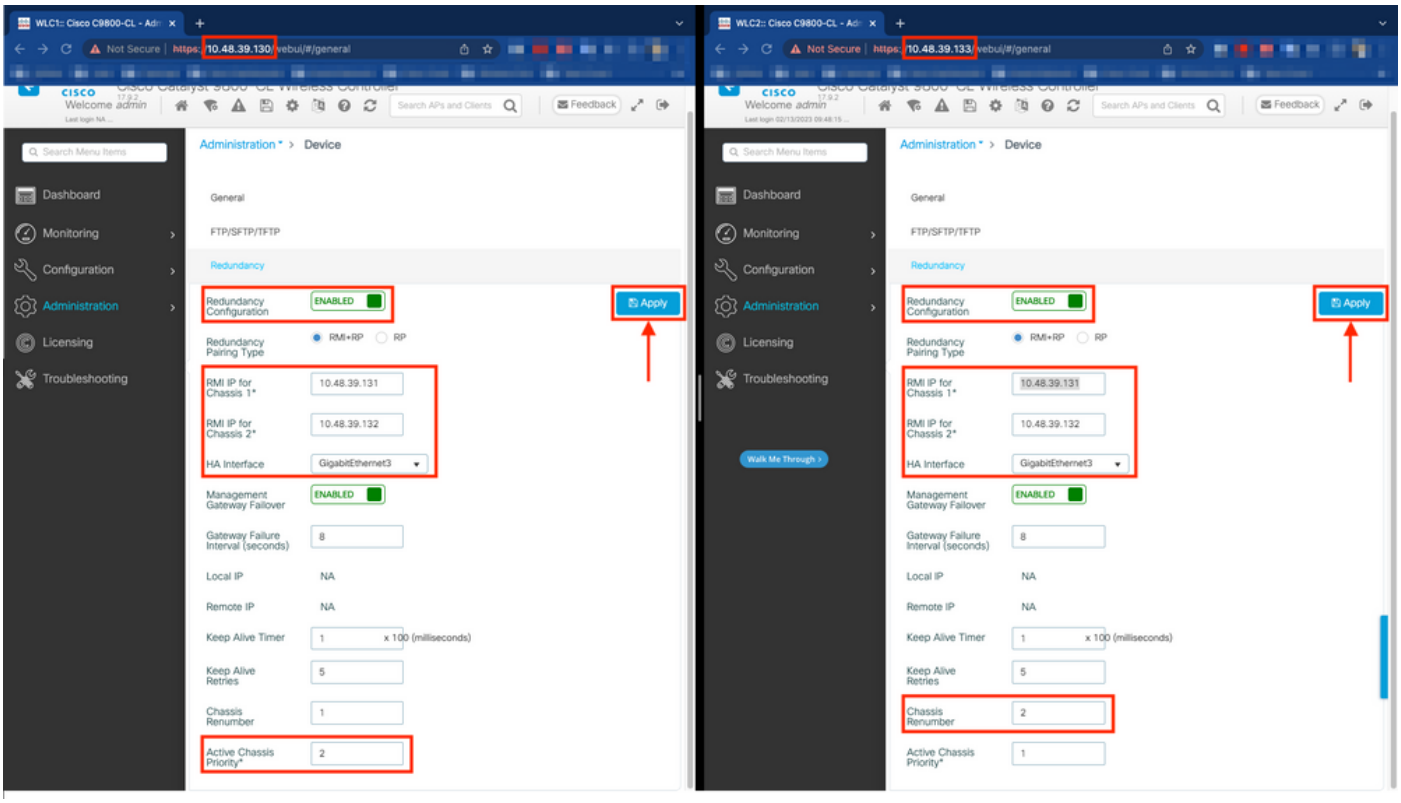
Über die CLI:

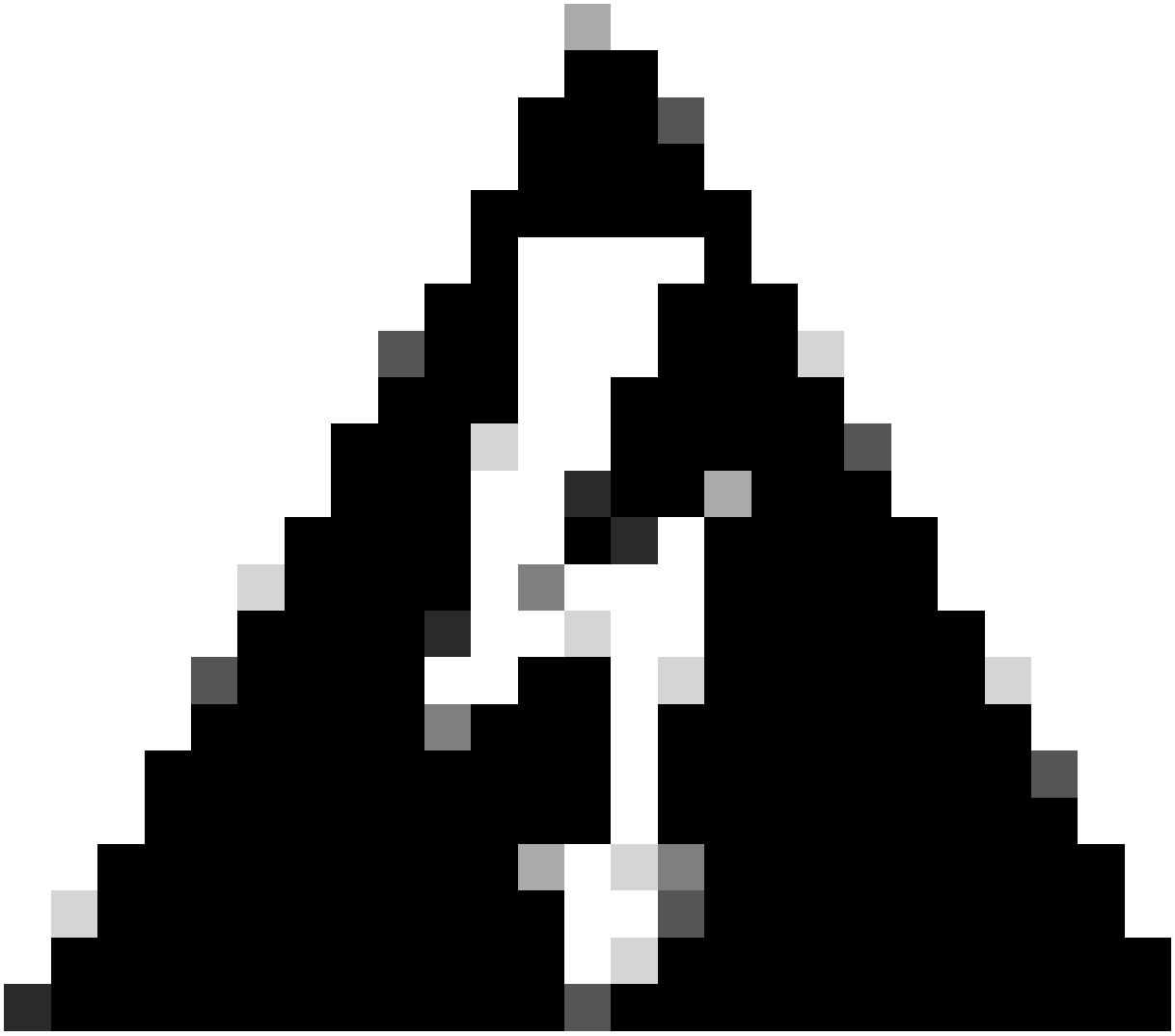
```
WLCx#ping 10.48.39.133 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.48.39.133, t
```

Schritt 3: Konfigurieren der Redundanz mithilfe des RMI + RP-Paarungstyps

Bei gesicherter Verbindung zwischen den einzelnen Geräten kann zwischen den Controllern Redundanz konfiguriert werden. Dieser Screenshot

zeigt, wie die Konfiguration auf der Registerkarte *Redundanz* der Seite *Administration→ Device* der 9800-Benutzeroberfläche vorgenommen wird.





Warnung: In diesem Beispiel wurde WLC1 als primärer Controller festgelegt, d. h. dieser ist derjenige, dessen Konfiguration auf den anderen Controller repliziert wird. Stellen Sie sicher, dass Sie die richtige Chassis-Priorität/-Umnummerierung anwenden, damit die richtige Konfiguration für das HA-Paar verwendet wird und kein Teil davon verloren geht.

Sehen wir uns nun die konfigurierten Felder und deren Zweck an.

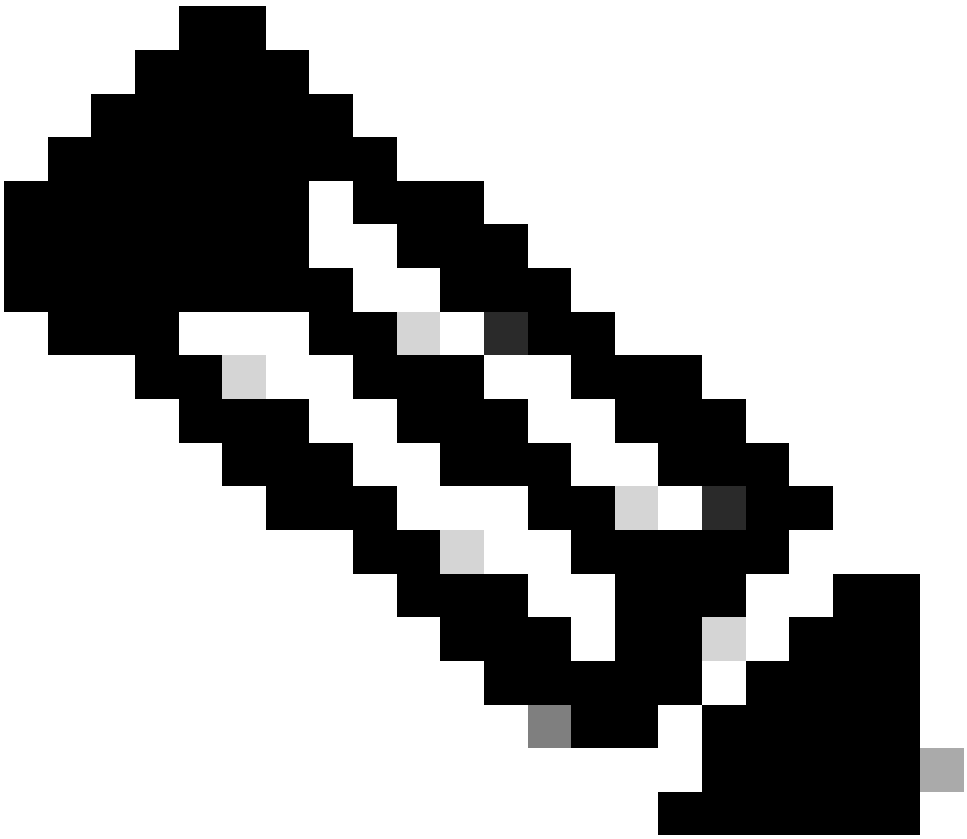
- **Redundanzkonfiguration:** Diese muss aktiviert sein, um die Redundanz zwischen WLCs zu nutzen.

- **Redundanzpaarungstyp:** Da in diesem Handbuch HA SSO mit RMI-Konfiguration behandelt wird, muss als Paarungstyp RMI + RP konfiguriert werden. Dabei werden sowohl die Redundanzverwaltungsschnittstelle als auch der Redundanzport verwendet. Sie

können die Redundanz auch mithilfe des Redundanz-Ports konfigurieren. Wenn jedoch nur der RP ausgewählt wird, wird die Erreichbarkeit des Gateways nicht geprüft, sondern nur der redundante WLC-Status.

- **RMI-IP für Chassis 1/2:** Diese Felder weisen der designierten Redundanzschnittstelle für beide Instanzen die bereitgestellten IP-Adressen zu. In diesem Beispiel wurden beide RMI-IPs für Chassis 1 und 2 als 10.48.39.131 bzw. 10.48.39.132 konfiguriert, wie zuvor beschrieben und im Netzwerkdiagramm dargestellt.

- **HA-Schnittstelle:** Bei Verwendung virtueller Appliances kann die Zuordnung zwischen den virtuellen Netzwerkschnittstellenkarten (vNIC) des Hypervisors und den Netzwerkschnittstellen des virtuellen Systems auf unterschiedliche Weise konfiguriert werden. Die für die Redundanz verwendete Schnittstelle kann daher für Cisco Catalyst 9800-CLs konfiguriert werden. In diesem Fall wurde GigabitEthernet 3 verwendet, wie im Bereitstellungsleitfaden für 9800-CL empfohlen.



Hinweis: Bei Verwendung von physischen C9800-Appliances werden in HA und RP standardmäßig Schnittstellen verwendet, die nicht konfigurierbar sind. Die Hardware-9800-WLCs verfügen über eine dedizierte Redundanzschnittstelle, die von den Netzwerkschnittstellen getrennt ist.

- **Management-Gateway-Failover:** Wie im HA SSO-Konfigurationsleitfaden beschrieben, führt diese Redundanzmethode eine Standard-Gateway-Prüfung durch. Hierzu wird regelmäßig ein ICMP-Ping (Internet Control Message Protocol) an das Gateway gesendet. Sowohl der aktive als auch der Standby-Controller verwenden die RMI-IP als Quell-IP für diese Prüfungen. Diese Nachrichten werden in einem Intervall von 1 Sekunde gesendet.

- **Gateway-Fehlerintervall:** Dieser Parameter gibt die Zeit an, für die eine Gateway-Prüfung nacheinander fehlschlagen muss, bevor das Gateway als nicht erreichbar deklariert wird. Standardmäßig ist dies auf 8 Sekunden konfiguriert. Da Gateway-Prüfungen jede Sekunde gesendet werden, sind dies 8 aufeinander folgende Fehler beim Erreichen des Gateways.

- **Lokale/Remote-IP**: Dies ist die RP-IP, die für Chassis 1 und 2 konfiguriert wurde. Diese IP-Adressen werden automatisch als 169.254.x.x generiert, wobei x.x von den letzten beiden Oktetten der Verwaltungsschnittstelle abgeleitet wird.

- **Keep Alive Timer:** Wie im HA SSO-Konfigurationsleitfaden beschrieben, senden das aktive und das Standby-Chassis Keep-Alive-Nachrichten miteinander, um sicherzustellen, dass beide weiterhin verfügbar sind. Der Keep-Alive-Timer gibt die Zeitspanne zwischen dem Senden von zwei Keepalive-Nachrichten zwischen den einzelnen Chassis an. Standardmäßig werden Keepalive-Nachrichten alle 100 ms gesendet. Es wird oft empfohlen, diesen Wert mit 9800-CL zu erhöhen, um missbräuchliche Switchovers zu vermeiden, wenn die VM-Infrastruktur zu kleinen Verzögerungen (Snapshots usw.) führt.

- **Keep Alive Retries (Erneut aktive Verbindungsversuche halten)**: In diesem Feld wird der Peer-Keepalive-Wiederholungswert konfiguriert, bevor behauptet wird, dass der Peer ausgefallen ist. Wenn sowohl der Keep-Alive-Timer als auch der wiederholte Standardwert verwendet werden, wird ein Peer deaktiviert, wenn die 5 Keep-Alive-Nachrichten, die in einem Zeitintervall von 100 ms gesendet wurden, nicht beantwortet werden (d. h., wenn die Redundanzverbindung für 500 ms deaktiviert ist).

- **Chassis-Neunummerierung:** die Chassis-Nummer, die die Appliance verwenden muss (1 oder 2).

    - Auf WLC2 (10.48.39.133) wird die Chassis-Nummer in 2 geändert. Standardmäßig lautet die Gehäusenummer 1. Die IP-Adressen der RP-Ports werden von RMI abgeleitet. Wenn die Gehäusenummer auf beiden Controllern identisch ist, wird die lokale RP-Port-IP-Ableitung identisch sein, und die Erkennung schlägt fehl. Nummerieren Sie das Gehäuse neu, um dieses so genannte Aktiv-Aktiv-Szenario zu vermeiden.

-

Aktive Chassis-Priorität: die Priorität, mit der definiert wird, welche Konfiguration vom HA-Paar verwendet werden muss. Die Appliance mit der höchsten Priorität ist diejenige, die auf die andere repliziert wird. Die Konfiguration des Chassis mit der niedrigsten Priorität geht somit verloren.

Für WLC1 (10.48.39.130) wurde die aktive Chassis-Priorität auf 2 festgelegt. Dadurch soll sichergestellt werden, dass das Chassis als aktives Chassis ausgewählt wird (und daher seine Konfiguration verwendet wird).

Nachdem diese Konfigurationen vorgenommen wurden, können Sie die Konfiguration über die Schaltfläche *Apply* (Anwenden) auf die Controller anwenden.

Über die Kommandozeile

Konfigurieren Sie zunächst eine sekundäre IP-Adresse in der virtuellen Schnittstelle, die zum Konfigurieren des RMI auf beiden Geräten verwendet wird.

```
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
```

Aktivieren Sie dann die Redundanz auf beiden Geräten.

```
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
```

Konfiguration der Chassis-Priorität wie WLC1 wird zum primären Controller

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

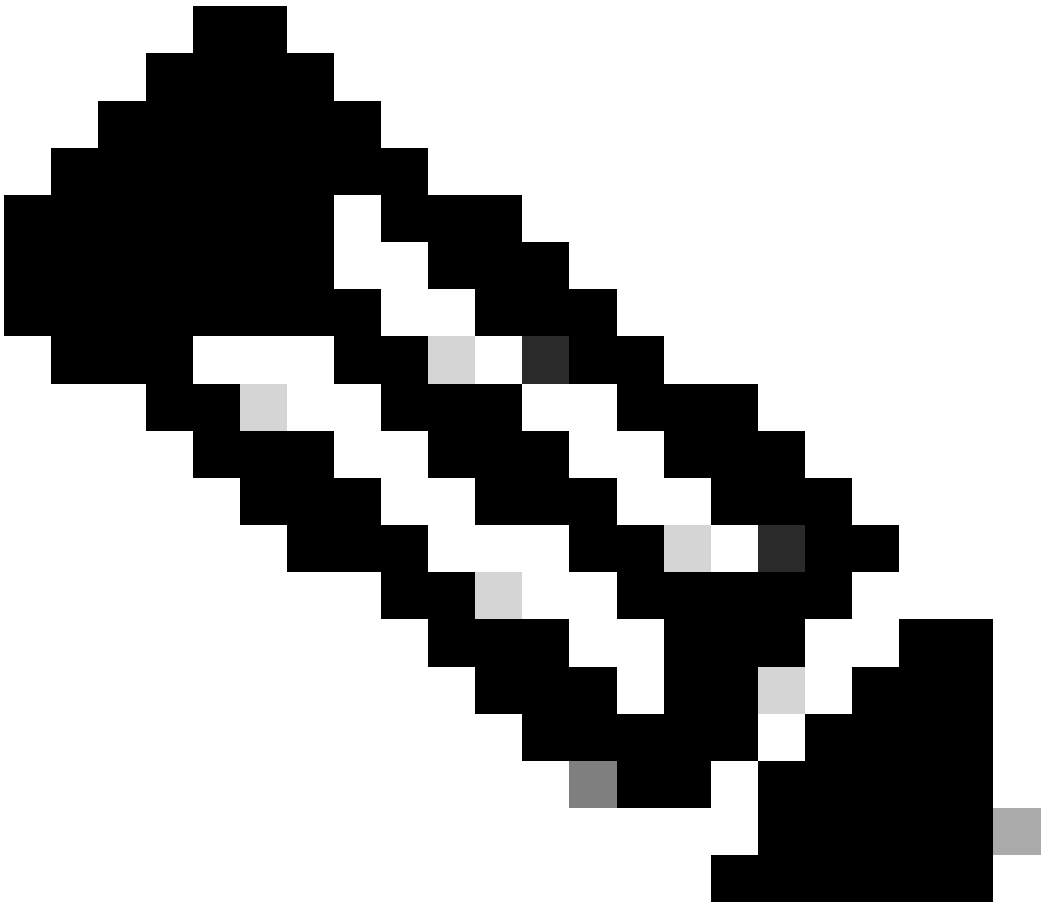
Nummerierung des Chassis für WLC2, das zum sekundären Controller wird

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

RMI auf beiden Geräten konfigurieren

```
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
```



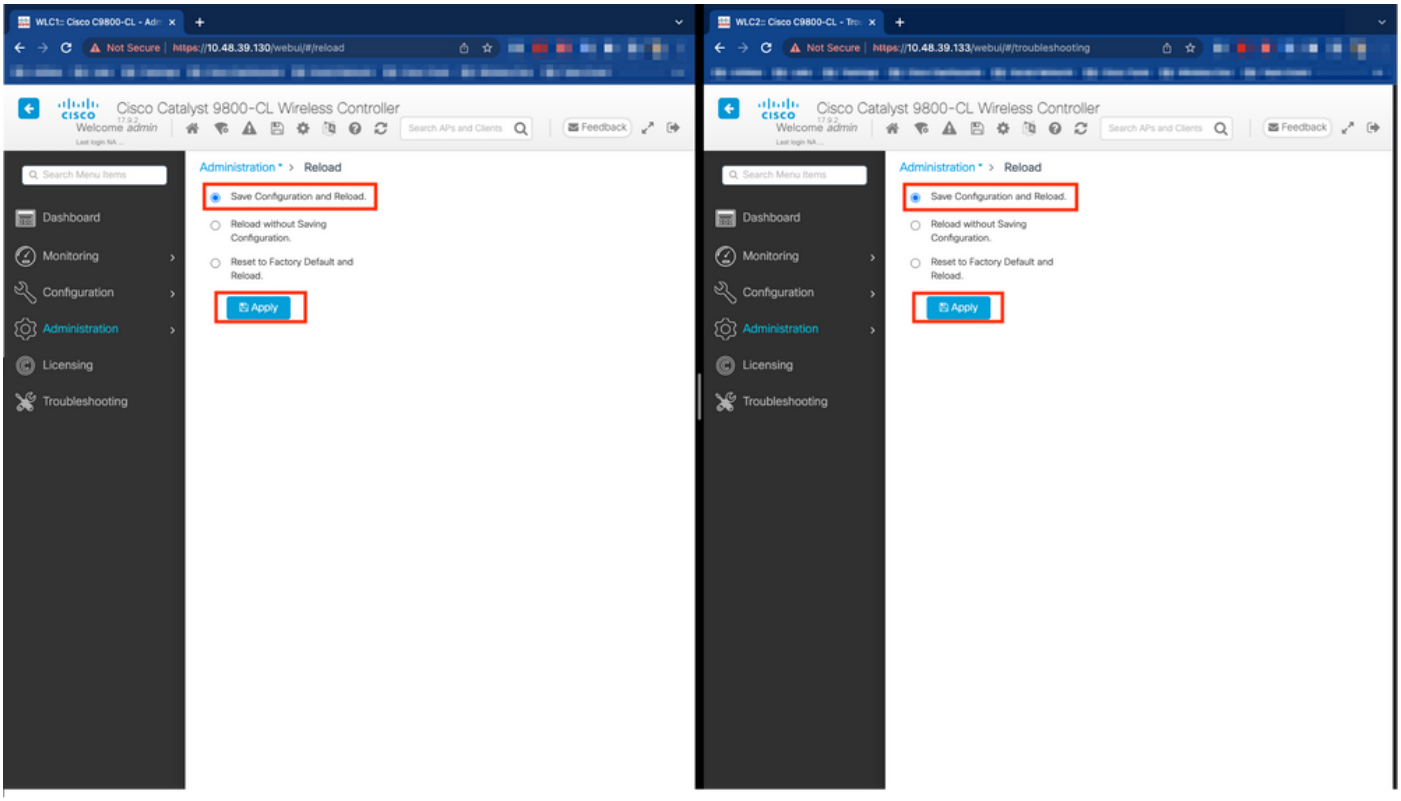
Hinweis: Für die GUI-Konfiguration auf dem virtuellen Catalyst 9800 muss die vom Controller verwendete Schnittstelle zwischen den verfügbaren Schnittstellen ausgewählt werden. Wie empfohlen wird hier GigabitEthernet 3 verwendet und mithilfe des chassis redundancy ha-interface GigabitEthernet 3 Befehls konfiguriert. Dieser Befehl ist nicht Teil der aktuellen Konfiguration. Die von HA verwendete Schnittstelle ist jedoch in den Umgebungsvariablen der Instanz ROMMON zu sehen. Diese werden mithilfe des show romvar Befehls angezeigt.

Schritt 4: Controller neu laden.

Damit sich das HA-Paar bildet und die Konfiguration wirksam ist, müssen beide Controller gleichzeitig neu geladen werden, nachdem die in Schritt 3 vorgenommene Konfiguration gespeichert wurde.

Über GUI:

Sie können die Seite "Administration Reload" (Verwaltung neu laden) beider GUI verwenden, um die Controller neu zu starten, wie in diesem Screenshot dargestellt.



Aus CLI:

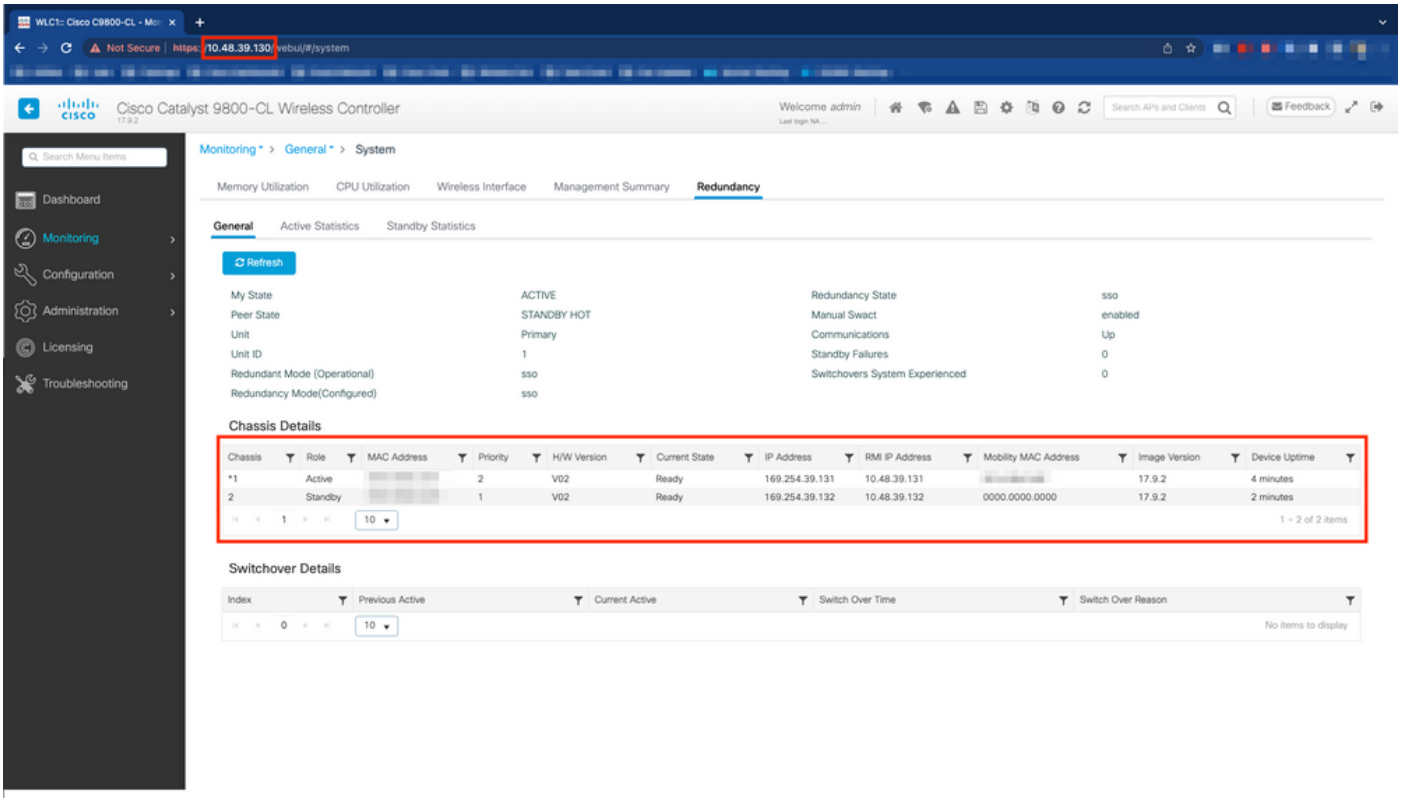
```
WLCx#reload Reload command is being issued on Active unit, this will reload the whole stack Proceed wit
```

Überprüfung

Sobald beide Controller des HA-Paars sich gegenseitig erkennen und das gewünschte HA-Paar erstellen, kann ein Controller (der primäre Controller) die beiden Chassis über die GUI oder CLI überwachen.

Über GUI:

Um die Redundanzkonfiguration über die 9800-Benutzeroberfläche zu überwachen, navigieren Sie von der Seite Monitoring > General > System zur Registerkarte Redundancy (Redundanz), wie in diesem Screenshot dargestellt.



Aus 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
```

Fehlerbehebung

Ein Stopp-Shop-Reflex

Die gängigen Befehle enthalten show tech wireless keine Befehle, die ein korrektes Verständnis der HA-Failovers eines HA-Paares oder seines aktuellen Status ermöglichen. Erfassen Sie diesen Befehl, um die meisten Befehle in Bezug auf die hohe Verfügbarkeit in einem Arbeitsgang zu erhalten:

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

Befehle anzeigen

Für den Status der Redundanz-Ports können diese Befehle verwendet werden.

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

Dieser Befehl zeigt die Gehäusenummer und den Redundanz-Portstatus an. Dies ist hilfreich bei der Fehlerbehebung im ersten Schritt.

Um die Keepalive-Zähler auf dem Keepalive-Port zu überprüfen, können Sie diese Befehle verwenden.

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

Andere Befehle

Mit diesen Befehlen ist es möglich, eine Paketerfassung auf dem Redundanz-Port des Controllers durchzuführen.

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

Mit diesen Befehlen erstellte Aufnahmen werden im bootflash: des Controllers unter dem Namen haIntCaptureLo.pcapgespeichert.

Mit diesem Befehl kann auch ein Keepalive-Test am Redundancy Port durchgeführt werden.

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

Mehr Details

Mit diesem Befehl können Sie die Konfiguration der ROMMON-Variablen anzeigen, die anzeigt, wie sich die aktuelle Konfiguration auf die Variablen auswirkt.

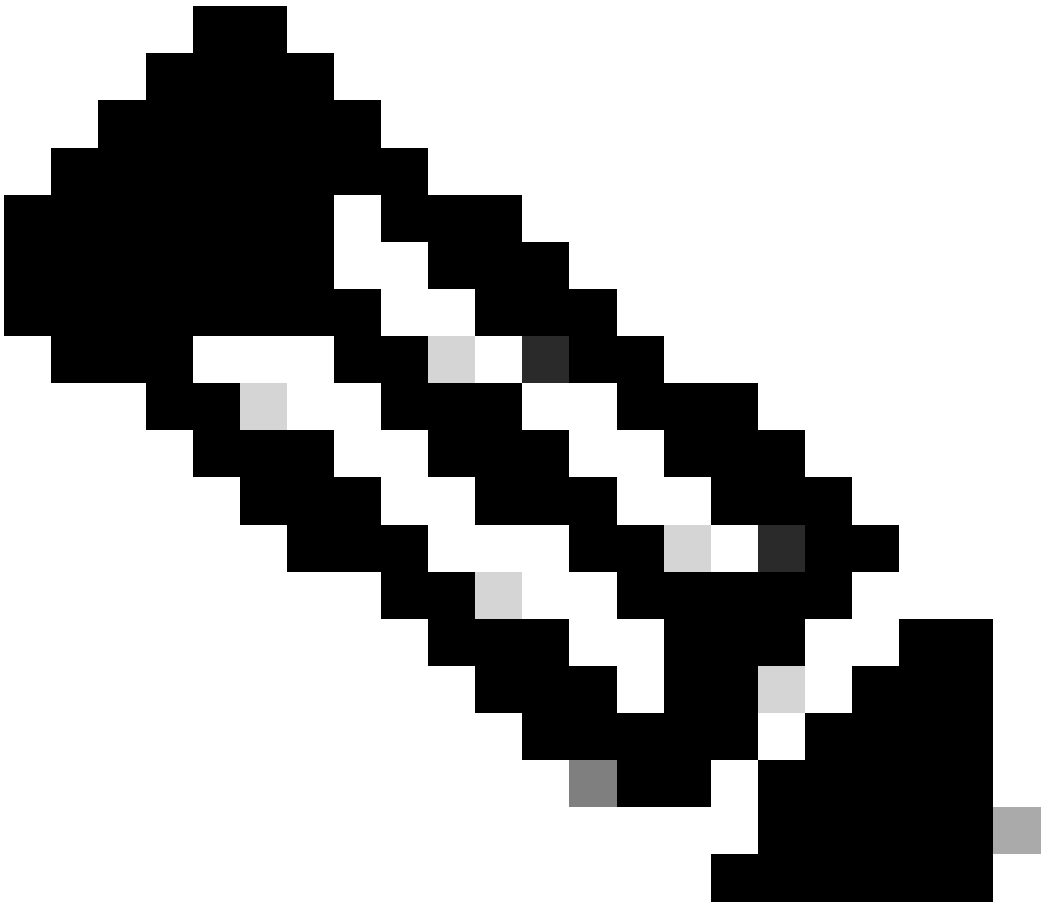
```
WLC#show romvar ROMMON variables: MCP_STARTUP_TRACEFLAGS = 00000000:00000000 SWITCH_NUMBER = 2 CONFIG_F
```

Dieser Befehl zeigt die Priorität für das Chassis an, sowohl RMI- als auch RP-Details, Peer-Timeout und weitere hilfreiche Details.

Wir können auch die Prozesse überwachen, die HA SSO auf dem WLC ausführen. Dabei handelt es sich um zwei Prozesse, nämlich stack_mgr und rif_mgr.

Zu diesem Zweck sammeln Sie die immer auf Traces zu einer Textdatei mit dem Befehl, kann der Zeit-Parameter hier angepasst werden, um den Zeitrahmen, den wir zu beheben.

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



Hinweis: Es ist wichtig zu beachten, dass der Service-Port des Standby-WLC deaktiviert ist und nicht erreichbar ist, während der Controller als Standby-Gerät agiert.

Typische Szenarien

Vom Benutzer erzwungen

Wenn Sie sich den Switchover-Verlauf ansehen, sehen Sie, dass "user forced" (vom Benutzer erzwungen) angezeigt wird, wenn ein Benutzer

mit dem redundancy force-switchover Befehl einen Switchover zwischen den Controllern initiiert hat.

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

Aktive Einheit entfernt

Wenn Sie sich den Switchover-Verlauf ansehen, sehen Sie, dass die "aktive Einheit entfernt" wurde, was auf einen Kommunikationsverlust am Redundanz-Port zwischen den beiden Controllern hindeutet.

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

Dies kann passieren, wenn die Verbindung zwischen den beiden Controllern ausfällt, es kann aber auch passieren, wenn ein WLC plötzlich ausfällt (Stromausfall) oder abstürzt. Es ist interessant, beide WLCs zu überwachen, um festzustellen, ob sie Systemberichte haben, die auf unerwartete Abstürze/Neustarts hinweisen.

Aktiv Verloren GW

Wenn Sie sich den Switchover-Verlauf ansehen, sehen Sie "Active lost GW", was auf einen Verlust der Kommunikation mit dem Gateway am RMI-Port hinweist.

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

Dies ist der Fall, wenn die Verbindung zwischen dem aktiven Controller und seinem Gateway ausfällt.

Weitere Überlegungen

HA SSO für Catalyst 9800-CL

Wenn Sie in virtuellen Umgebungen arbeiten, müssen Sie akzeptieren, dass Latenz eingeführt wird, und Latenz ist nicht etwas, das HA richtig toleriert. Dies ist legitim, da Hochverfügbarkeits-SSO dazu neigt, Chassis-Fehler schnell und effizient zu erkennen. Um dies zu erreichen, überprüft jedes Chassis den Status des jeweils anderen mithilfe von Keepalives für RP- und RMI-Verbindungen sowie Pings zum Gateway ihrer RMIs (und zwar zu dem ihres WMI, der identisch sein muss). Wenn eine dieser Optionen nicht erkannt wird, reagiert der Stack abhängig von den Symptomen, die im HA SSO-Leitfaden unter "System and Network Fault Handling" (Behebung von System- und Netzwerkfehlern) beschrieben sind.

Bei der Arbeit mit virtuellen HA SSO-Stacks von Catalyst 9800 ist es üblich, Switchovers zu beobachten, da Keepalive über die RP-Verbindung versäumt hat. Dies kann auf die durch die virtualisierte Umgebung verursachte Latenz zurückzuführen sein.

Um festzustellen, ob der HA SSO-Stack unter RP-Keepalive-Drops leidet, können Sie die Stack-/Rif-Manager-Protokolle verwenden.

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

Wenn beide Chassis in Betrieb sind, führt der Switchover zu einer "Dual Active Detection", die eine Folge des Herunterfahrens des RPs ist.

In einer solchen Situation kann das Anpassen der HA-Keepalive-Parameter helfen, um diese unnötigen Switchovers zu vermeiden. Es können zwei Parameter konfiguriert werden:

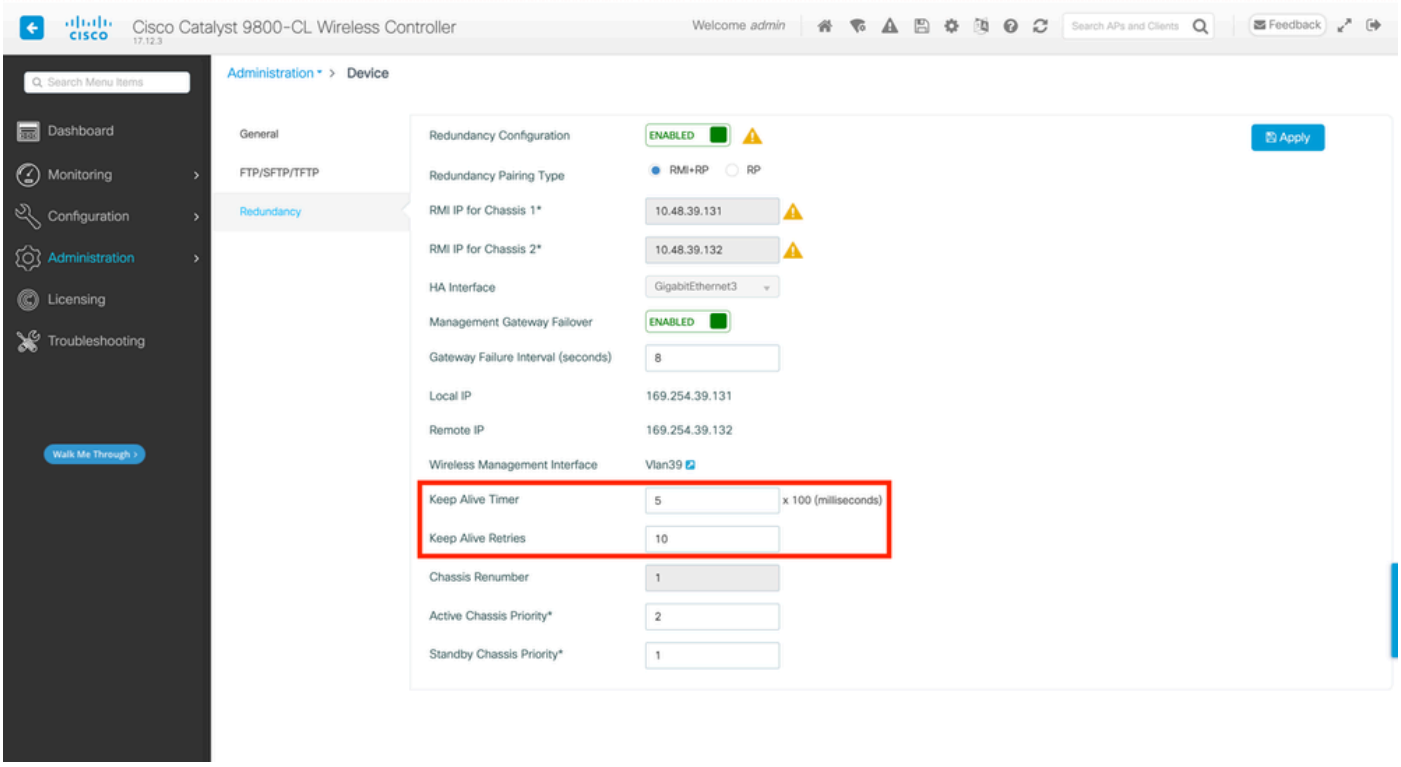
- **Keep Alive Timer**: Die Zeitspanne zwischen dem Senden von zwei Keepalive-Nachrichten zwischen den einzelnen Chassis.

- **Keep Alive Retries (**Erneut aktive Keepalives): Die Anzahl der Keepalives, die übersehen werden müssen, um einen Peer als inaktiv zu erklären.

Standardmäßig ist der Keep-Alive-Timer auf 1ms und der Wiederholungsversuch auf 5 gesetzt. Das bedeutet, dass nach 5ms fehlender Keepalive-Wartezeit auf der RP-Verbindung ein Switchover stattfindet. Diese Werte können für virtuelle Bereitstellungen zu niedrig sein. Wenn Sie regelmäßige Switchover-Vorgänge feststellen, weil RP-Keepalives fehlen, erhöhen Sie diese Parameter, um den Stack zu stabilisieren.

Über GUI:

Um die HA SSO-Keepalive-Parameter der 9800-GUI zu überwachen oder zu ändern, navigieren Sie von der Seite *Administration* > *Device* zur Registerkarte Redundancy (Redundanz), wie in diesem Screenshot dargestellt.



Aus CLI:

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

Neben der Konfiguration dieser Parameter kann eine weitere Optimierung bei einem solchen Verhalten im HA SSO-Stack helfen. Bei physischen Appliances ermöglicht die Hardware das Verbinden eines Chassis mit einem anderen, in der Regel über ein einziges Kabel. In einer virtuellen Umgebung muss die Verbindung des RP-Ports für jedes Chassis über einen virtuellen Switch (vSwitch) erfolgen, der im Vergleich zu physischen Verbindungen erneut Latenz erzeugen kann. Die Verwendung eines dedizierten vSwitch zum Erstellen der RP-Verbindung ist eine weitere Optimierung, die verhindern kann, dass HA-Keepalives aufgrund von Latenz verloren gehen. Dies wird auch im Cisco Catalyst 9800-CL Wireless Controller for Cloud Deployment Guide dokumentiert. Daher ist es am besten, einen dedizierten vSwitch für die RP-Verbindung zwischen den virtuellen Systemen der Serie 9800-CL zu verwenden und sicherzustellen, dass dieser durch keinen anderen Datenverkehr beeinträchtigt wird.

Catalyst 9800 HA SSO in ACI-Bereitstellungen

Wenn ein Switchover in einem HA SSO-Stack stattfindet, verwendet das neu aktive Chassis den Gratis-ARP-Mechanismus (GARP), um die MAC-IP-Zuordnung im Netzwerk zu aktualisieren und sicherzustellen, dass der für den Controller reservierte Datenverkehr empfangen wird.

Insbesondere sendet das Chassis GARP, um der neue "Eigentümer" des WMI zu werden, und stellt sicher, dass der CAPWAP-Datenverkehr das richtige Chassis erreicht.

Das Chassis, das aktiv wird, sendet eigentlich nicht nur einen einzigen GARP, sondern einen Burst davon, um sicherzustellen, dass jedes Gerät im Netzwerk seine IP-MAC-Zuordnung aktualisiert. Dieser Burst kann die ARP-Learning-Funktion der ACI überlasten. Wenn die ACI verwendet wird, wird daher empfohlen, diesen Burst in der Catalyst 9800-Konfiguration so weit wie möglich zu reduzieren.

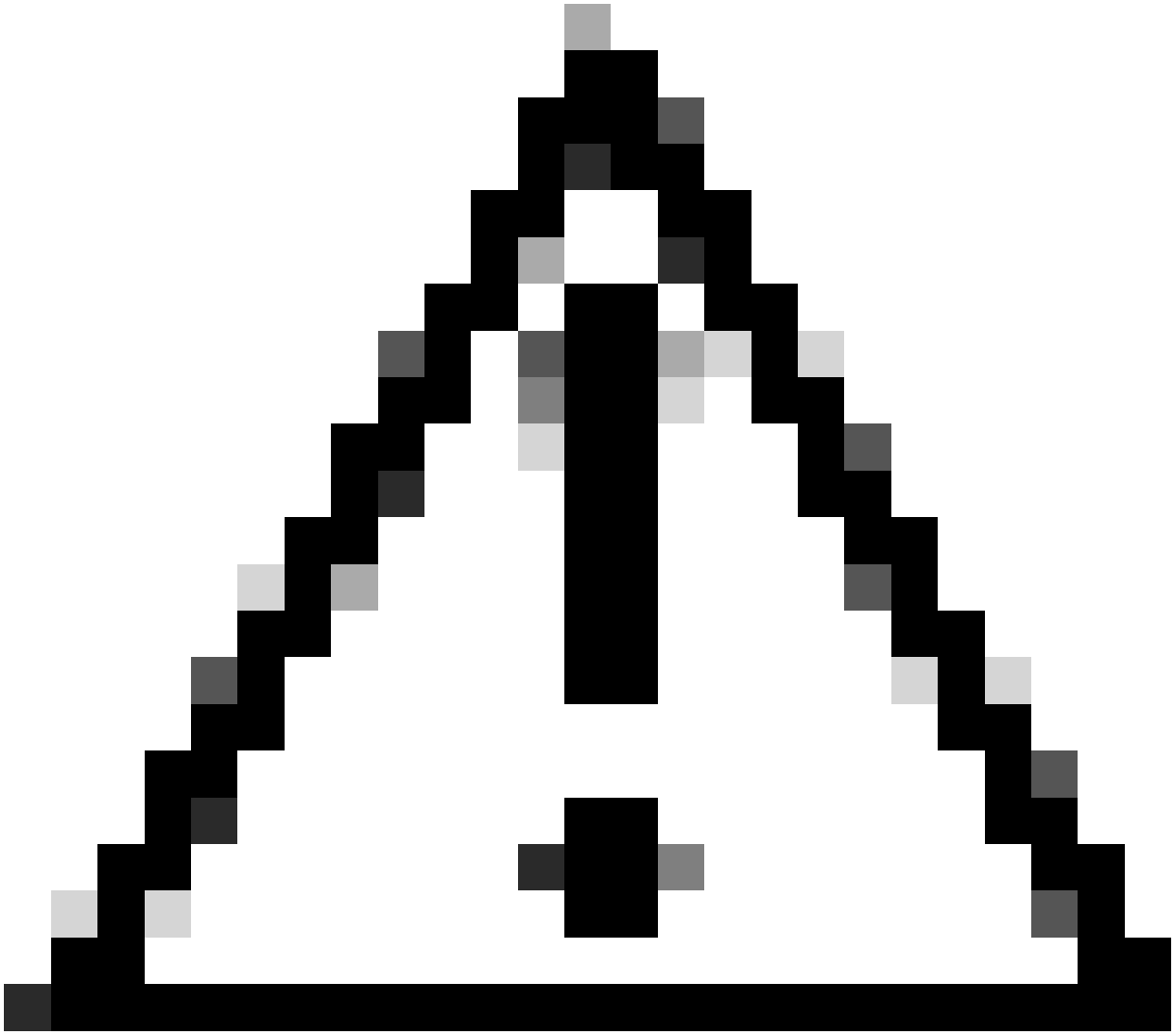
Aus CLI:

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

Neben der Begrenzung des vom 9800 während eines Switchovers initiierten GARP-Bursts wird auch empfohlen, die Funktion für schnelles Switchover auf dieser Plattform zu deaktivieren. Wenn Fast Switchover konfiguriert ist, sendet der aktive Controller eine explizite Benachrichtigung an den Standby-Controller, die besagt, dass dieser ausfällt. Auf diese Weise kann zwischen den beiden WLCs, die den HA-Stack bilden, Datenverkehr entstehen, der die Datenpakete verschachtelt (APs und Clients werden verworfen), bis einer von ihnen ausfällt. Wenn Sie diese Funktion deaktivieren, stabilisieren Sie Ihre Wireless-Infrastruktur und arbeiten gleichzeitig mit ACI-Bereitstellungen.

Aus CLI:

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



Vorsicht: Beachten Sie, dass der Standby-Controller bei deaktiviertem schnellen Switchover nur auf Fehler beim Keepalive-Timeout angewiesen ist, um zu erkennen, wann der aktive Controller ausgefallen ist. Diese müssen daher mit größter Sorgfalt konfiguriert werden.

Einzelheiten zu Überlegungen bezüglich Hochverfügbarkeits-SSO-Bereitstellungen für Catalyst 9800 im ACI-Netzwerk finden Sie im Abschnitt "Informationen zur Bereitstellung des ACI-Netzwerks im Controller" im Software-Konfigurationsleitfaden für Cisco Catalyst Wireless Controller der Serie 9800.

Referenzen

- 17.3 HA SSO-Leitfaden
- 17.6 HA SSO-Leitfaden

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.