Configurazione di High Availability SSO su Catalyst 9800 | Guida introduttiva

Sommario

Introduzione

In questo documento viene descritto come configurare lo status switchover (SSO) ad alta disponibilità in modalità RP+RMI su un Catalyst 9800 WLC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei

- Catalyst wireless modello 9800.
- Concetti di alta disponibilità illustrati nella guida HA SSO.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C9800-CL v17.9.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Mentre la configurazione HA SSO può richiedere solo 3 di essi, qui sono stati utilizzati 4 indirizzi IP della stessa rete dell'interfaccia di gestione wireless (WMI) per facilitare l'accesso all'interfaccia grafica del controller.

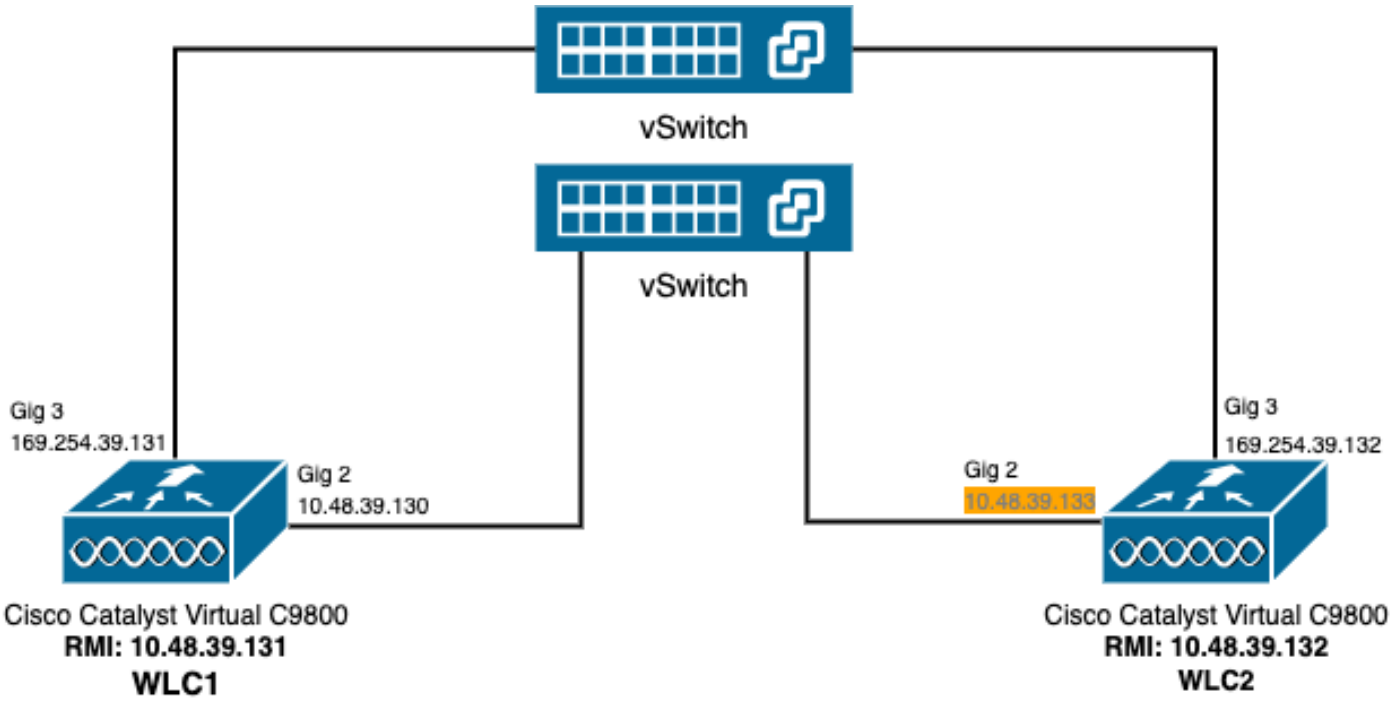
Premesse

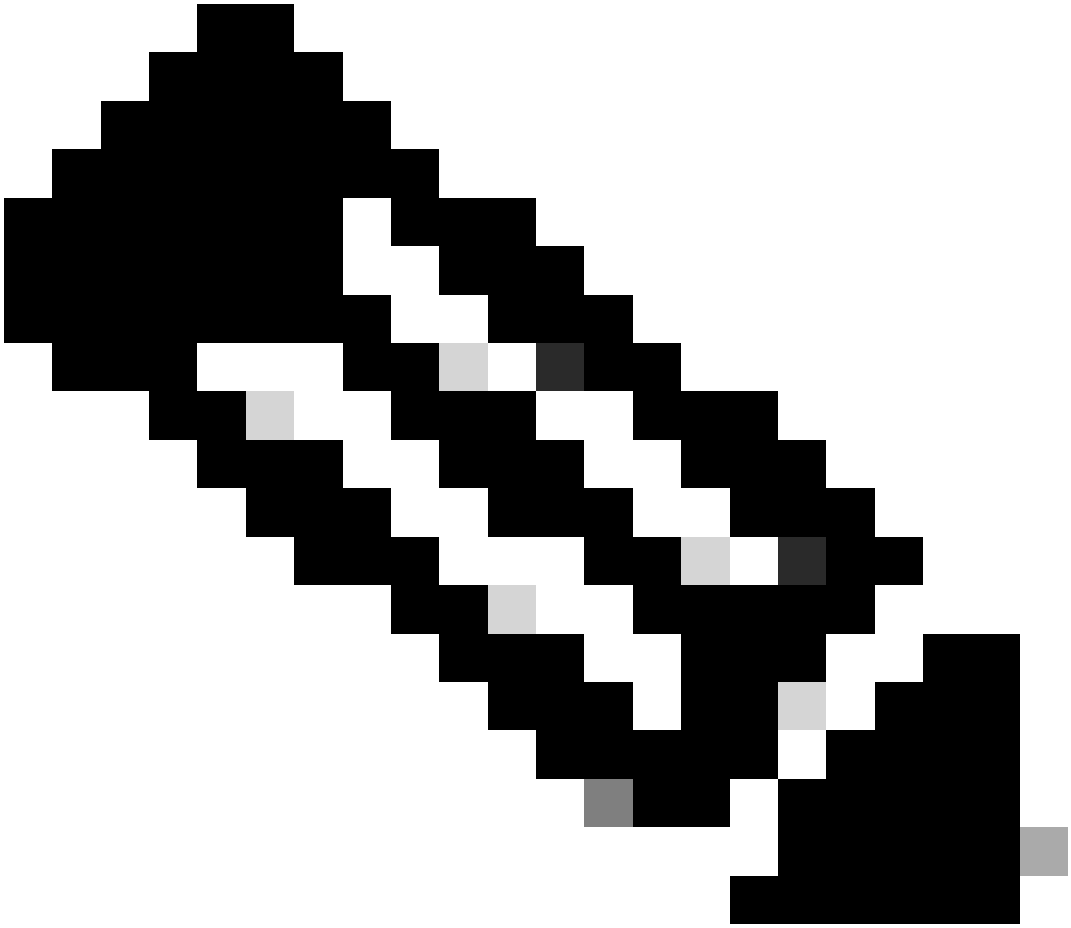
La funzionalità SSO ad alta disponibilità sul controller wireless consente al punto di accesso di stabilire un tunnel CAPWAP con il controller wireless attivo e il controller wireless attivo di condividere una copia mirror del punto di accesso e del database client con il controller wireless in standby. Quando si verificano gli switchover (ovvero il controller attivo si guasta e quindi lo standby prende la mano), gli AP uniti non passano allo stato Discovery e i client non si disconnettono. Tra i punti di accesso e il controller wireless che si trova nello stato Attivo viene mantenuto un solo tunnel CAPWAP alla volta.

Le due unità formano una connessione peer tramite una porta RP dedicata (o un'interfaccia virtuale per le VM) ed entrambi i controller condividono lo stesso indirizzo IP sull'interfaccia di gestione. L'interfaccia RP viene utilizzata per sincronizzare la configurazione in blocco e incrementale in fase di runtime e garantire lo stato operativo di entrambi i controller della coppia HA. Inoltre, quando si utilizza RMI + RP, sia i controller in standby che i controller attivi dispongono di un'interfaccia di gestione della ridondanza (RMI) a cui sono assegnati indirizzi IP, in particolare per garantire la raggiungibilità del gateway. Anche lo stato CAPWAP dei punti di accesso in stato di esecuzione viene sincronizzato dal controller wireless attivo al controller wireless hot-standby, che consente il passaggio completo dallo stato dei punti di accesso in caso di guasto del controller wireless attivo. Gli access point non passano allo stato Discovery quando il controller wireless attivo non funziona e il controller wireless standby diventa il controller wireless attivo che serve la rete.

Configurazione

Esempio di rete


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



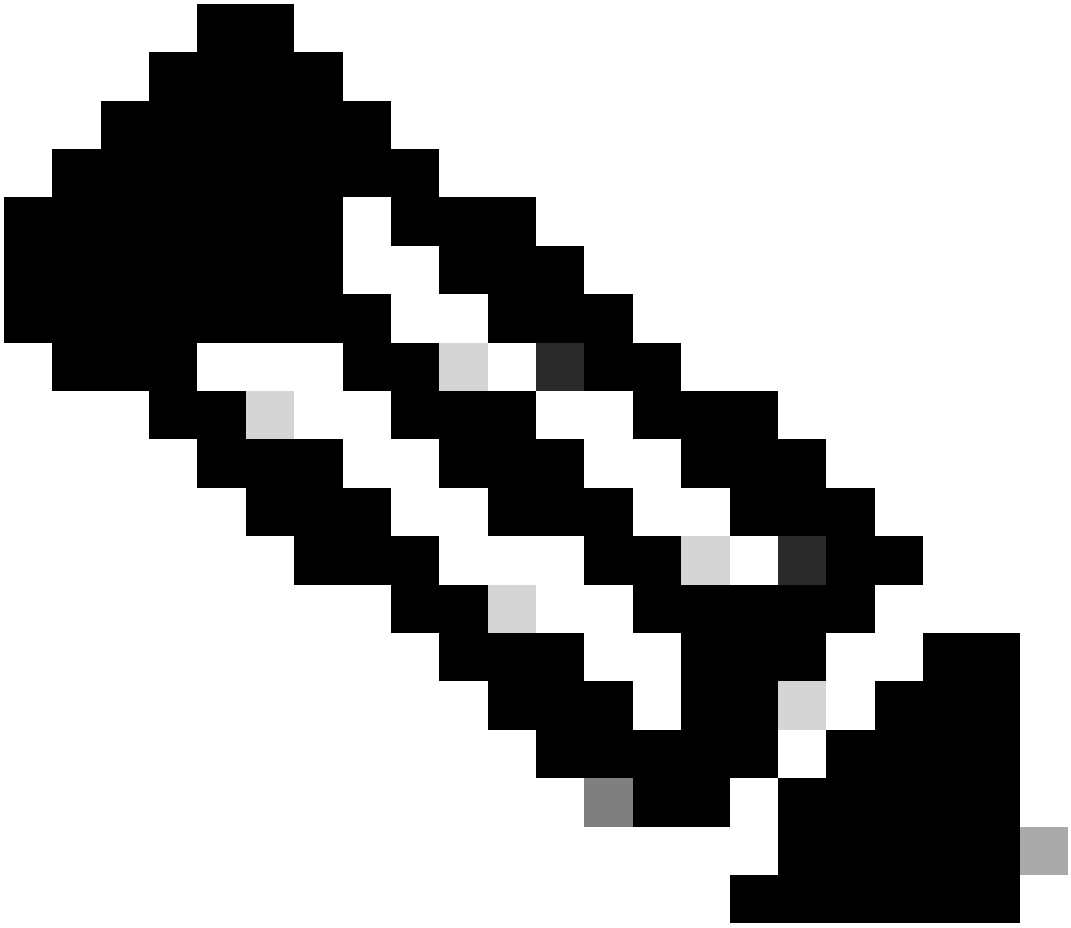
Nota: in arancione viene evidenziato l'indirizzo IP temporaneo assegnato all'interfaccia virtuale Gigabit Ethernet 2 del controller 9800-CL designato come WLC2. Questo indirizzo IP è temporaneamente definito come WMI per WLC2 e consente l'accesso alla GUI di questa istanza per semplificare la configurazione di HA SSO. Una volta configurato HA SSO, questo indirizzo viene liberato poiché per una coppia di controller HA SSO viene utilizzato un solo WMI.

Configurazioni

Nell'esempio, l'SSO (Stateful Switchover) ad alta disponibilità è configurato tra due istanze 9800-CL, che eseguono la stessa versione del software Cisco IOS, configurate con WMI separati e con interfaccia utente accessibile in

- l'indirizzo IP 10.48.39.130 per il primo, indicato come WLC1;
- l'indirizzo IP 10.48.39.133 per il secondo indirizzo, denominato WLC2.

Oltre a questi indirizzi IP, sono stati usati due indirizzi aggiuntivi nella stessa subnet (e VLAN), ossia 10.48.39.131 e 10.48.39.132. Si tratta degli indirizzi IP RMI (Redundancy Management Interface) rispettivamente per lo chassis 1 (WLC1) e lo chassis 2 (WLC2).



Nota: dopo aver configurato HA tra i due controller, 10.48.39.133 viene liberato e 10.48.39.130 diventa l'unico WMI della configurazione. Pertanto, dopo la configurazione, sono in uso solo 3 indirizzi IP, uno dei due WMI e uno degli RMI.

La configurazione delle interfacce per entrambi i dispositivi prima ancora di avviare la configurazione HA deve essere simile a quella fornita in questo esempio.

```
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
```

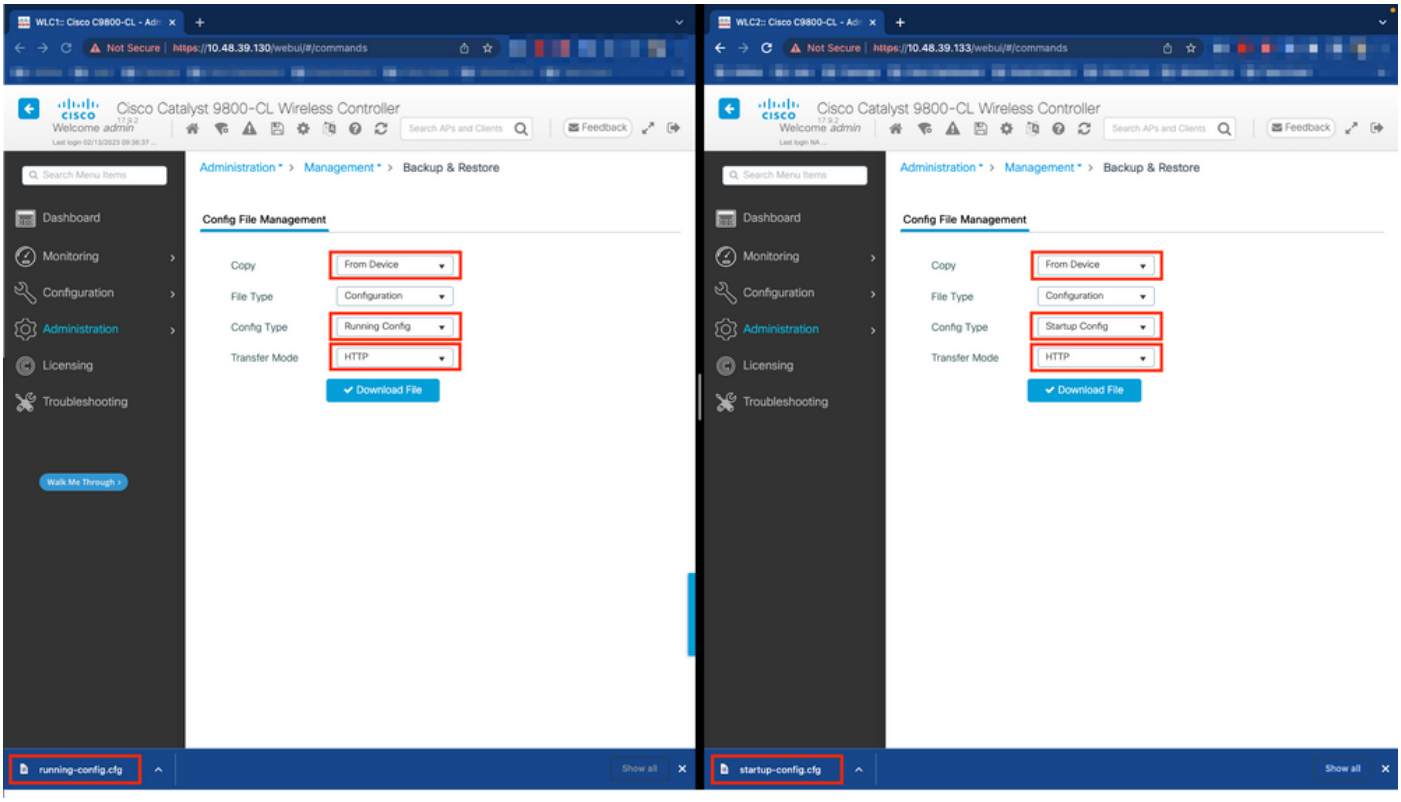
Nell'esempio, il WLC1 è designato come controller primario (ossia chassis 1), mentre il WLC2 è il controller secondario (ossia chassis 2). Ciò significa che la coppia HA costituita dai 2 controller utilizza la configurazione di WLC1 e che quella di WLC2 viene persa dopo il processo.

Passaggio 1. (Facoltativo) Eseguire il backup dei file della configurazione di avvio e della configurazione di esecuzione dei controller.

Una gestione errata può causare la perdita della configurazione. Per evitare questo problema, si consiglia di eseguire il backup della configurazione di avvio e di esecuzione da entrambi i controller utilizzati nella configurazione HA. Questa operazione può essere eseguita facilmente dalla GUI o dalla CLI di 9800.

Dall'interfaccia grafica:

Dalla scheda *Amministrazione → Gestione → Backup & Restore* della GUI 9800 (fare riferimento allo screenshot), è possibile scaricare la configurazione di avvio e di esecuzione attualmente utilizzata dal controller.



Nell'esempio, sia l'avvio (a sinistra) che la configurazione (a destra) vengono scaricati direttamente, tramite HTTP, sul dispositivo che ospita il browser usato per accedere alla GUI del WLC. È possibile regolare facilmente la modalità di trasferimento e la destinazione del file di cui eseguire il backup, utilizzando il campo Transfer Mode (Modalità di trasferimento).

Dalla 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)
```

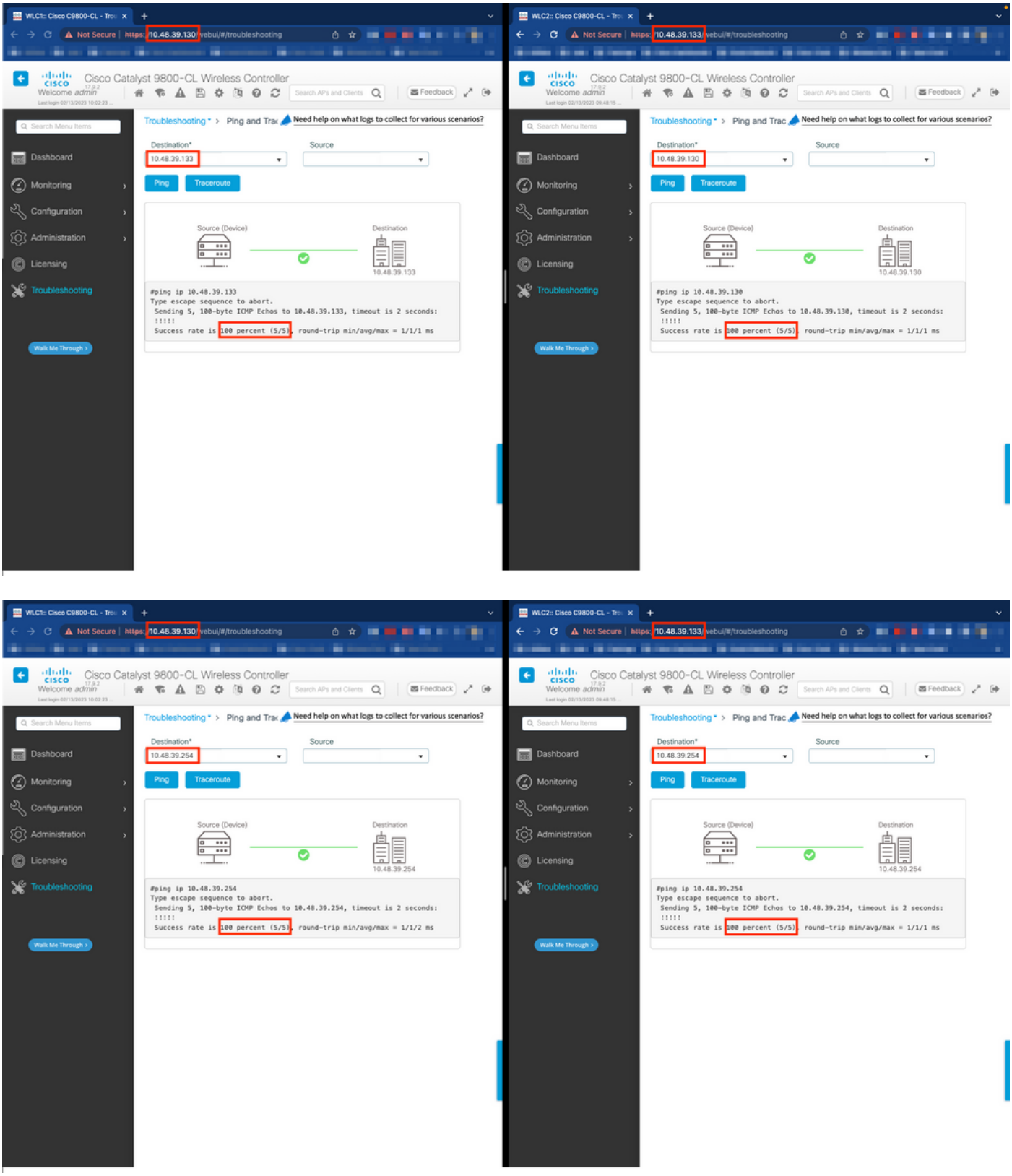
Sostituire con <SERVER-IP> l'indirizzo IP del server TFTP verso cui viene copiato il file di configurazione di avvio/esecuzione.

Passaggio 2. (Facoltativo) Verificare la connettività di rete.

Sia dalle GUI WLC che dalle CLI, è possibile eseguire semplici test di connettività, ossia eseguire il ping del gateway da entrambi i dispositivi ed eseguire il ping dei dispositivi tra di loro. Ciò garantisce che entrambi i controller dispongano della connettività necessaria per configurare HA.

Dall'interfaccia grafica:

Lo strumento *Ping e Traceroute* dalla scheda *Risoluzione dei problemi* della GUI 9800 può essere usato per verificare la connettività tra i controller stessi e tra ciascun WLC e il suo gateway di rete, come mostrato nelle seguenti figure.



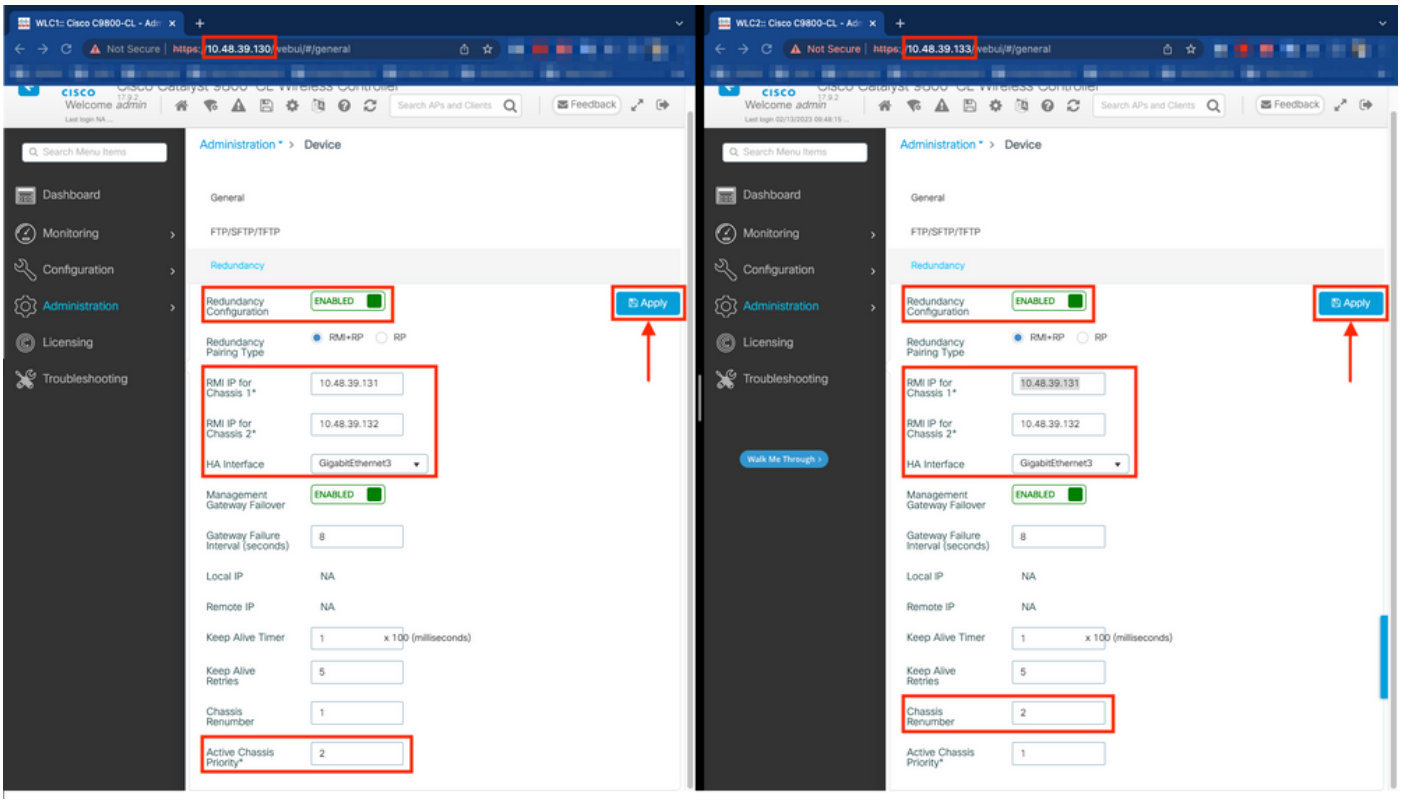
Dalla CLI:

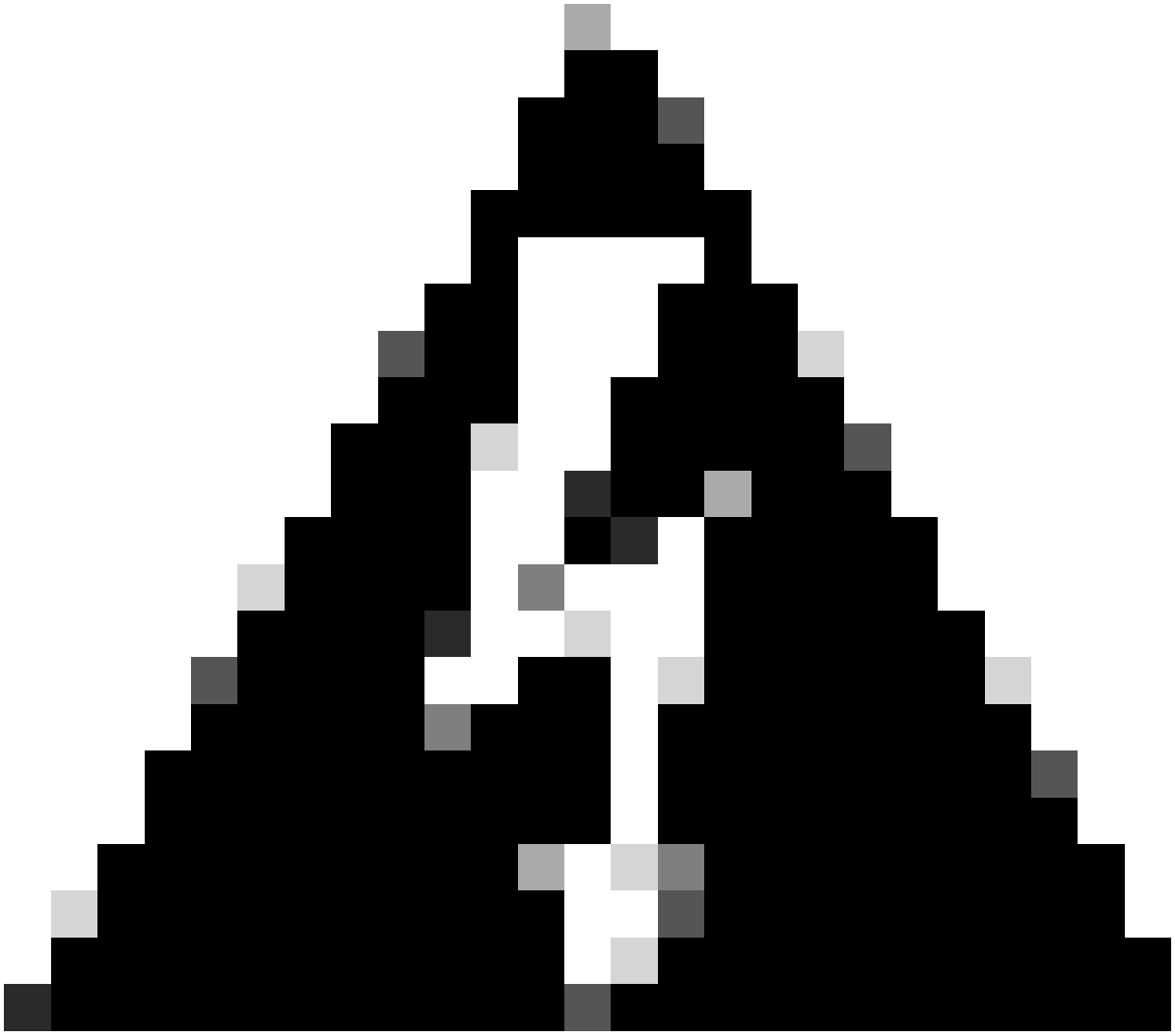
```
WLCx#ping 10.48.39.133 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.48.39.133, t
```

Passaggio 3. Configurare la ridondanza con il tipo di accoppiamento RMI + RP.

Una volta assicurata la connettività tra ciascun dispositivo, è possibile configurare la ridondanza tra i controller. In questa schermata viene

mostrato come eseguire la configurazione dalla scheda *Redundancy (Ridondanza)* della pagina *Administration→ Device* (Amministrazione) dell'interfaccia utente di 9800.





Avviso: nell'esempio, il WLC1 è stato designato come controller primario, ossia è quello la cui configurazione è stata replicata sull'altro controller. Accertarsi di applicare la corretta priorità/rinumerazione dello chassis per utilizzare la configurazione corretta con la coppia HA e di non perdere alcuna parte di essa.

Esaminare i campi configurati e il relativo scopo

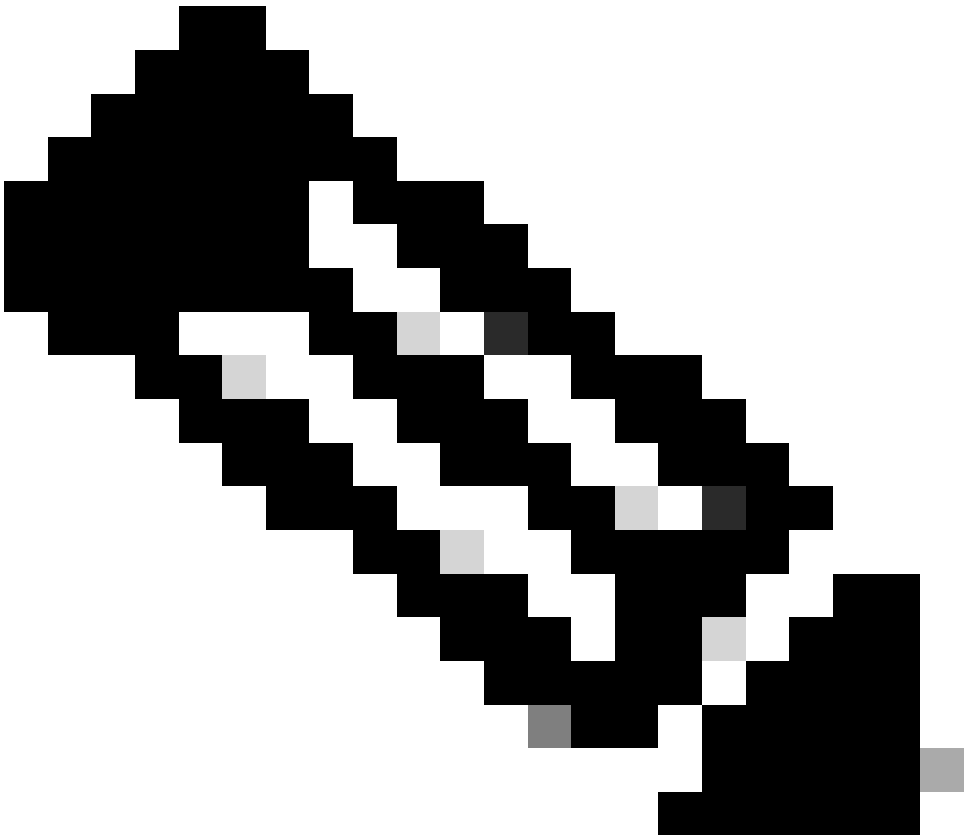
- **Configurazione della ridondanza:** deve essere abilitata per utilizzare la ridondanza tra WLC.

- **Tipo di accoppiamento ridondanza:** poiché questa guida riguarda l'SSO HA utilizzando la configurazione RMI, il tipo di accoppiamento configurato deve essere RMI + RP, utilizzando sia l'interfaccia di gestione della ridondanza che la porta di ridondanza. È

inoltre possibile scegliere di configurare la ridondanza utilizzando solo la porta di ridondanza. Tuttavia, quando si sceglie solo RP, la raggiungibilità del gateway non viene verificata, solo lo stato WLC ridondante è

- **RMI IP per Chassis 1/2:** questi campi assegnano gli indirizzi IP forniti all'interfaccia di ridondanza designata per entrambe le istanze. Nell'esempio, gli IP degli RMI per lo chassis 1 e 2 sono stati configurati rispettivamente come 10.48.39.131 e 10.48.39.132, come descritto in precedenza e mostrato nel diagramma di rete.

- **Interfaccia HA:** quando si utilizzano appliance virtuali, la mappatura tra le schede di interfaccia di rete virtuali (vNIC) dell'hypervisor e le interfacce di rete della macchina virtuale può essere configurata in modi diversi. Pertanto, l'interfaccia utilizzata per la ridondanza è configurabile per Cisco Catalyst 9800-CL. In questo caso, è stato utilizzato Gigabit Ethernet 3, come consigliato dalla guida all'implementazione di 9800-CL.



Nota: quando si utilizzano accessori fisici C9800, l'interfaccia utilizzata in HA e RP è quella predefinita e non è configurabile. In effetti, i WLC 9800 dell'hardware dispongono di un'interfaccia di ridondanza dedicata separata da quelle della rete.

- **Failover del gateway di gestione:** come descritto nella guida alla configurazione di HA SSO, questo metodo di ridondanza implementa il controllo del gateway predefinito, eseguito inviando periodicamente il ping ICMP (Internet Control Message Protocol) al gateway. Sia il controller attivo che quello in standby utilizzano l'indirizzo IP RMI come indirizzo IP di origine per questi controlli. Questi messaggi vengono inviati a un secondo di intervallo.

- **Intervallo errori gateway:** indica per quanto tempo un controllo gateway deve avere esito negativo consecutivo prima che il gateway venga dichiarato non raggiungibile. Per impostazione predefinita, questa impostazione è configurata come 8 secondi. Poiché le verifiche del gateway vengono inviate ogni secondo, si tratta di 8 errori consecutivi che hanno impedito di raggiungere il gateway.

- **IP locale/remoto:** IP RP configurato per lo chassis 1 e 2. Questi indirizzi IP vengono generati automaticamente come 169.254.x.x, dove x.x deriva dagli ultimi due ottetti dell'interfaccia di gestione.

- **Timer keep-alive:** come descritto nella guida alla configurazione HA SSO, gli chassis attivo e standby inviano messaggi keep-alive per garantire che entrambi siano ancora disponibili. Il timer keep-alive indica il periodo di tempo che separa l'invio di due messaggi keepalive tra ogni chassis. Per impostazione predefinita, i messaggi keep-alive vengono inviati ogni 100 ms. Si consiglia spesso di aumentare questo valore con 9800-CL per evitare commutazioni abusive ogni volta che l'infrastruttura VM introduce piccoli ritardi (istantanee e così via...)

- **Tentativi keep-alive:** questo campo configura il valore di ripetizione keepalive del peer prima che asserisca che il peer è inattivo. Se vengono utilizzati sia il timer keep-alive che il valore predefinito retries, un peer viene reclamato inattivo se i 5 messaggi keep-alive inviati a un intervallo di tempo di 100 ms rimangono senza risposta (ossia se il collegamento di ridondanza è inattivo per 500 ms).

- **Rinumerazione chassis:** il numero di chassis che l'accessorio deve utilizzare (1 o 2).

  - Sul WLC2 (10.48.39.133), lo chassis è rinumerato come 2. Per impostazione predefinita, il numero di chassis è 1. Gli indirizzi IP delle porte RP derivano da RMI. Se il numero di chassis è lo stesso su entrambi i controller, la derivazione IP della porta RP locale è la stessa e il rilevamento non riesce. Rinumerare lo chassis per evitare questo scenario denominato attivo-attivo.

- **Priorità chassis attiva:** la priorità utilizzata per definire la configurazione che deve essere utilizzata dalla coppia HA. L'accessorio con la priorità più alta viene replicato sull'altro. La configurazione dello chassis con la priorità più bassa viene quindi persa.

Su WLC1 (10.48.39.130), la priorità dello chassis attivo è stata impostata su 2. In questo modo, lo chassis viene scelto come chassis attivo (e quindi viene utilizzata la relativa configurazione) nella coppia HA creata.

Una volta effettuate queste configurazioni, utilizzare il pulsante *Apply* (Applica) per applicare la configurazione ai controller.

Dalla CLI

In primo luogo, configurare un indirizzo IP secondario nell'interfaccia virtuale utilizzata per configurare l'RMI su entrambi i dispositivi.

```
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
```

Quindi, abilitare la ridondanza su entrambi i dispositivi

```
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
```

Configurare la priorità dello chassis, ad esempio WLC1, che diventa il controller primario

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

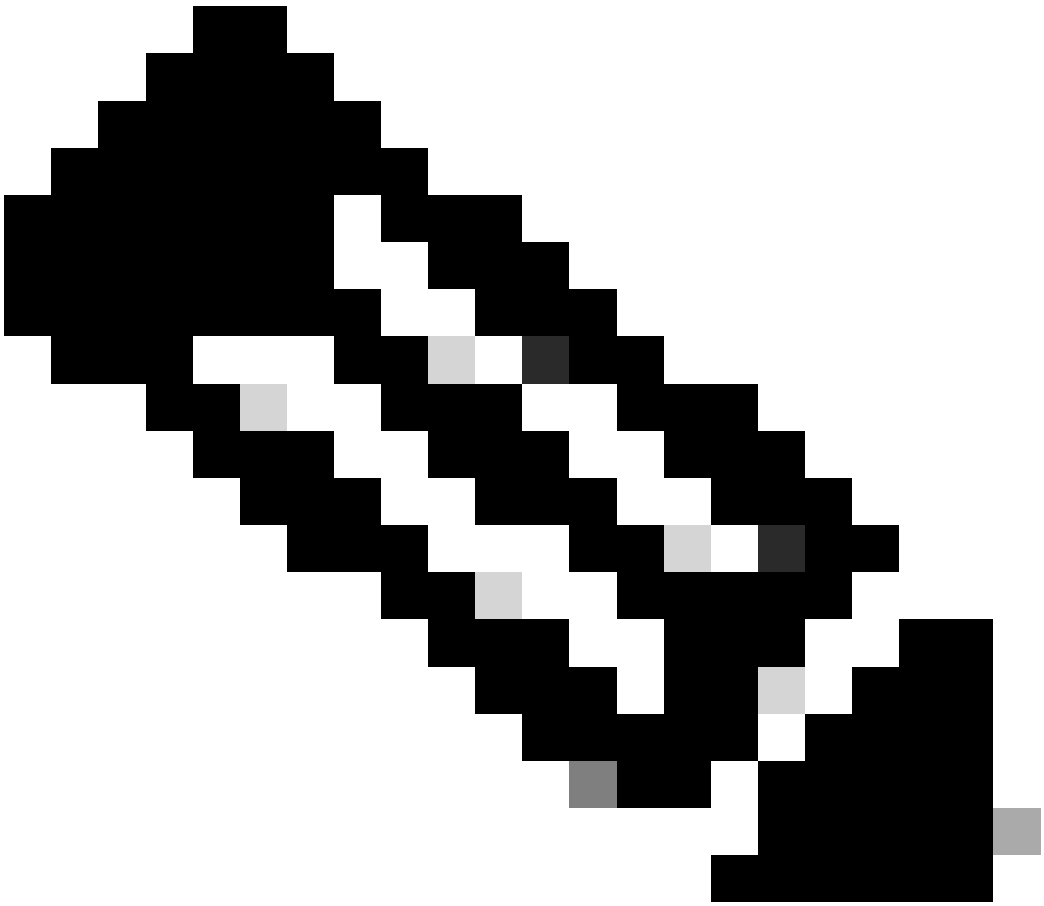
Rinumera lo chassis per WLC2 che diventa il controller secondario

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

Infine, configurare RMI su entrambi i dispositivi

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

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



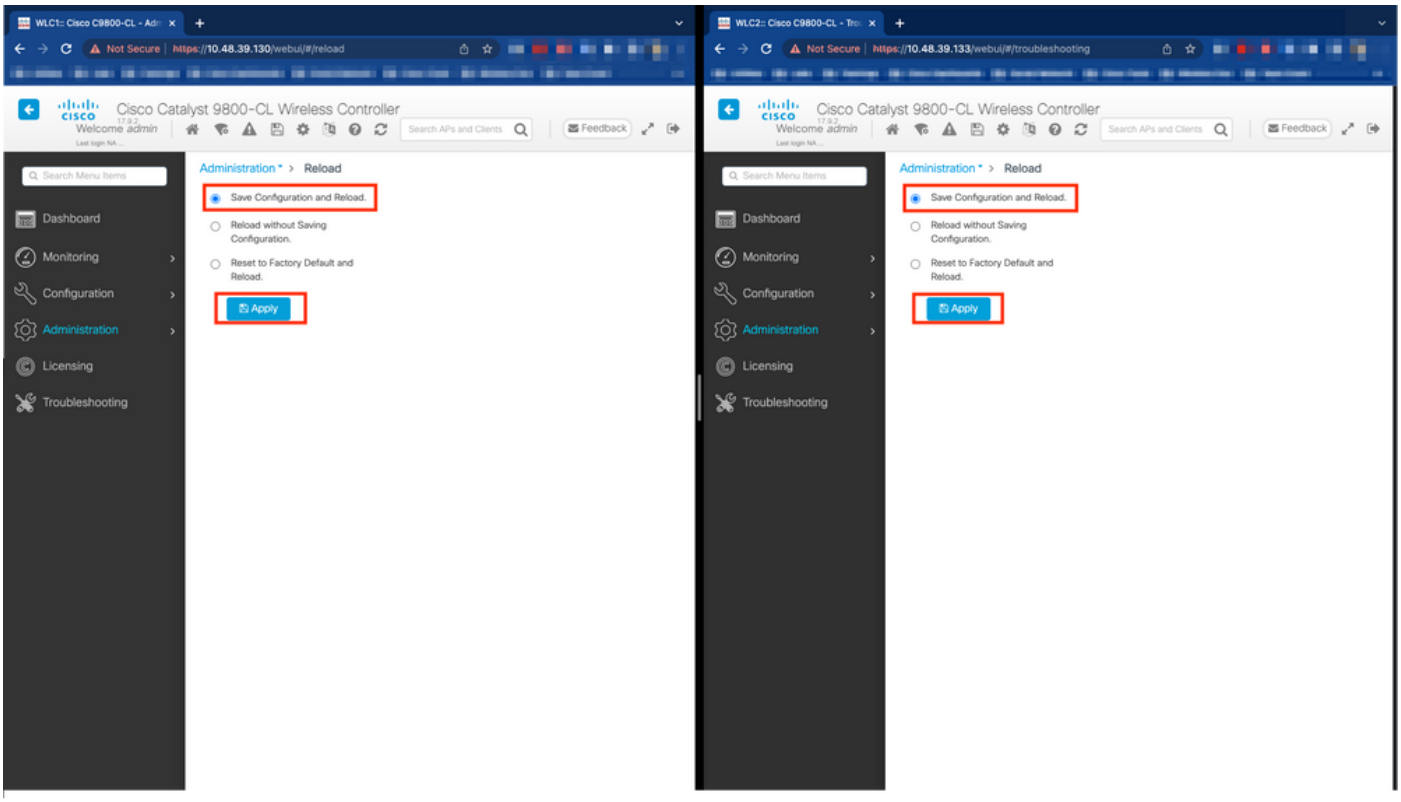
Nota: come per la configurazione GUI, su Virtual Catalyst 9800, l'interfaccia usata dal controller deve essere selezionata tra quelle disponibili. Come consigliato, Gigabit Ethernet 3 viene utilizzato qui e configurato tramite il chassis redundancy ha-interface GigabitEthernet 3 comando. Questo comando non fa parte della configurazione in esecuzione, tuttavia l'interfaccia utilizzata da HA può essere visualizzata nelle variabili di ambiente ROMMON di istanza. Per visualizzarli, usare il show romvar comando.

Passaggio 4. Riavviare i controller.

Affinché la coppia HA si formi e la configurazione sia efficace, entrambi i controller devono essere ricaricati contemporaneamente una volta salvata la configurazione effettuata al passaggio 3.

Dalla GUI:

È possibile utilizzare la pagina Amministrazione - Ricarica di entrambe le GUI per riavviare i controller, come illustrato in questa schermata.



Dalla CLI:

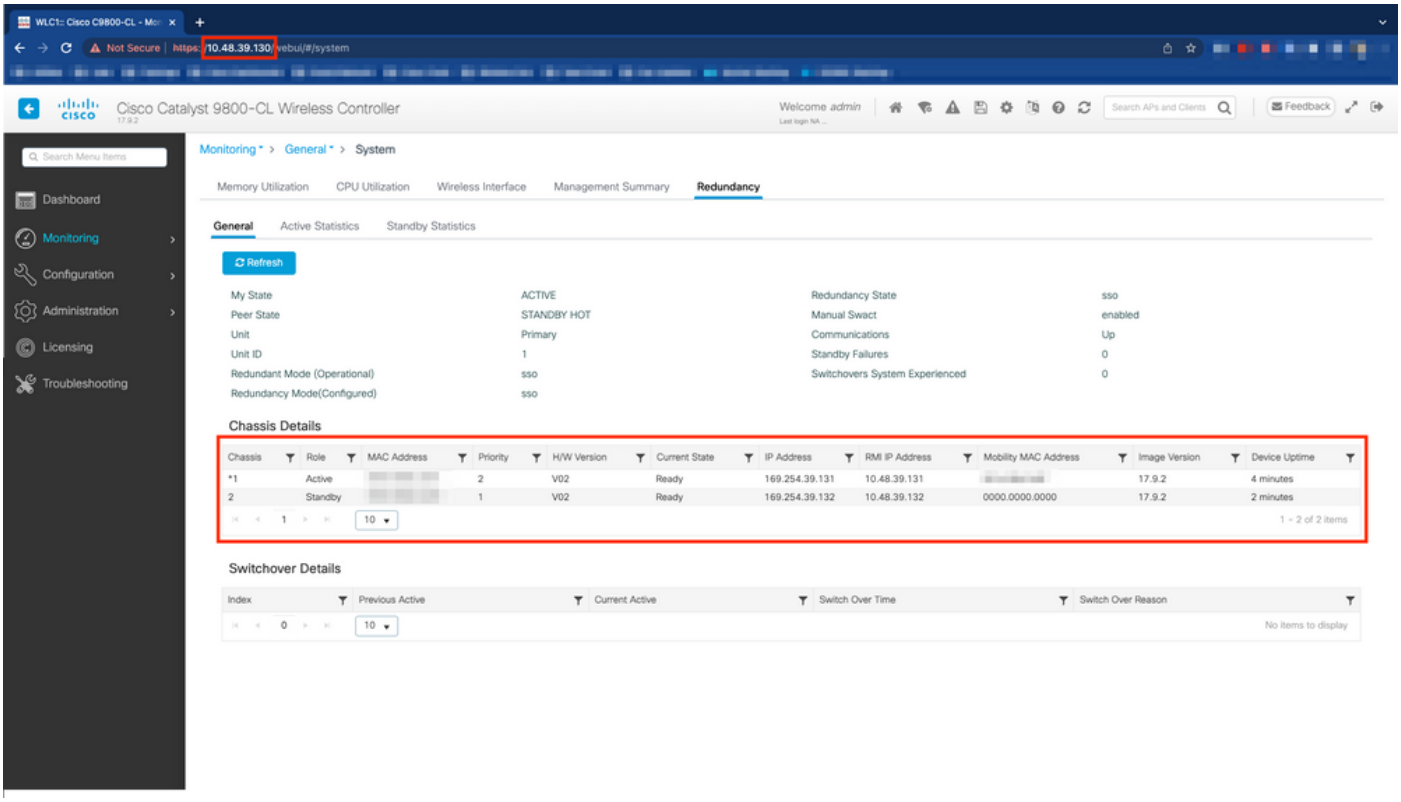
```
WLCx#reload Reload command is being issued on Active unit, this will reload the whole stack Proceed wit
```

Verifica

Quando entrambi i controller della coppia HA si scoprono e creano la coppia HA desiderata, un controller (quello primario) è in grado di monitorare i due chassis dalla GUI o dalla CLI.

Dalla GUI:

Per monitorare la configurazione di ridondanza dalla GUI 9800, passare alla scheda Ridondanza dalla pagina Monitoraggio > Generale > Sistema, come mostrato in questa schermata.



Dalla 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
```

Risoluzione dei problemi

One Stop-Shop Reflex

Il comando usuale show tech wireless non include comandi che consentono di comprendere correttamente i failover HA di una coppia HA né il relativo stato corrente. Raccogli questo comando per avere la maggior parte dei comandi relativi alla disponibilità elevata in una singola operazione:

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

Comandi show

Per lo stato delle porte di ridondanza, è possibile utilizzare questi comandi.

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

Questo comando mostra il numero dello chassis e lo stato della porta di ridondanza, utile come primo passo per la risoluzione dei problemi.

Per verificare i contatori keepalive sulla porta keepalive, è possibile usare questi comandi.

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

Altri comandi

È possibile acquisire un pacchetto sulla porta di ridondanza del controller con questi comandi

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

Le acquisizioni effettuate utilizzando questi comandi vengono salvate nel nome bootflash: del controller, sotto il nome haIntCaptureLo.pcap.

Con questo comando è possibile anche eseguire un test keepalive sulla porta di ridondanza.

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

Ulteriori informazioni

Per visualizzare la configurazione delle variabili ROMMON, che mostra in che modo la configurazione effettiva si riflette sulle variabili, è possibile utilizzare questo comando.

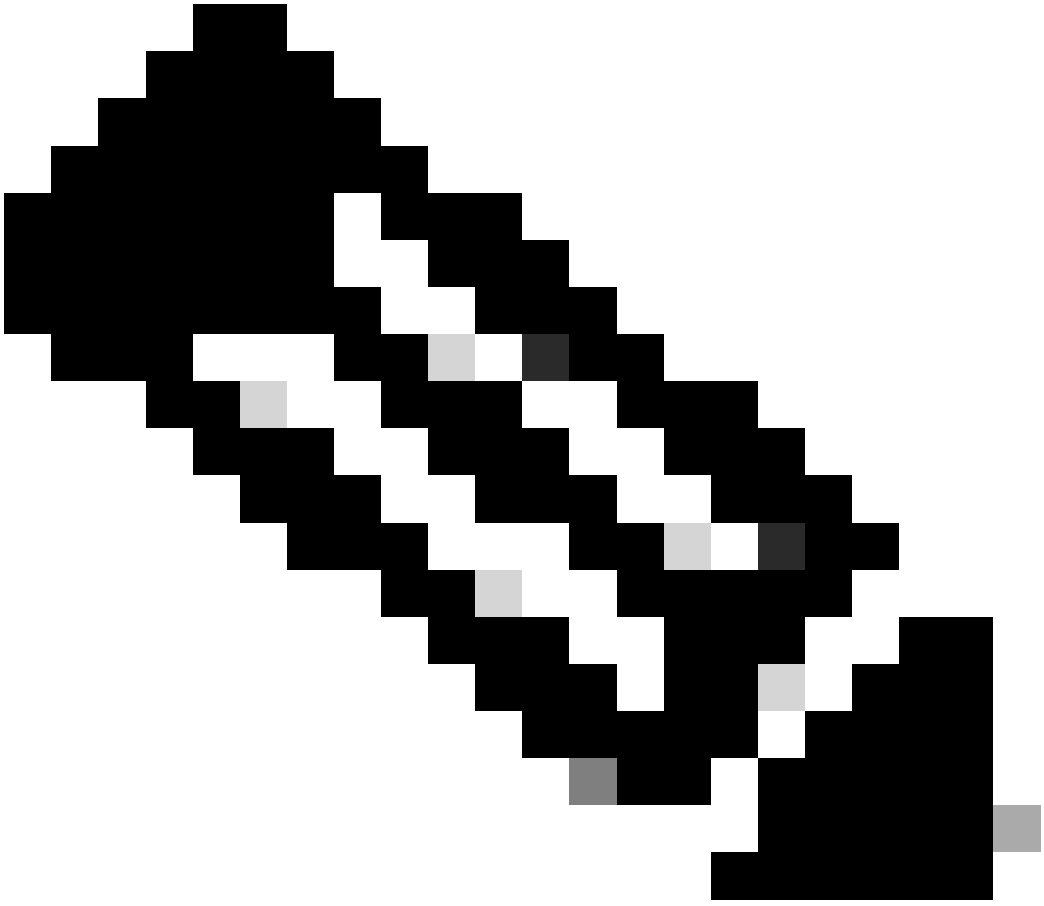
```
WLC#show romvar ROMMON variables: MCP_STARTUP_TRACEFLAGS = 00000000:00000000 SWITCH_NUMBER = 2 CONFIG_F
```

Questo comando mostra la priorità dello chassis, i dettagli RMI e RP, il timeout del peer e dettagli più utili.

Possiamo anche monitorare i processi che eseguono HA SSO sul WLC che sono due processi, ossia stack_mgr e rif_mgr.

A tale scopo, raccogliere le tracce Always On in un file di testo utilizzando il comando, il parametro time qui può essere modificato per coprire l'intervallo di tempo che si desidera risolvere.

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



Nota: è importante notare che la porta di servizio del WLC in standby è disattivata e non raggiungibile mentre il controller funziona in standby.

Scenari tipici

Utente forzato

Se si controlla la cronologia dello switchover, è possibile vedere "user forced" (forzato dall'utente), che appare quando un utente ha avviato uno switchover tra i controller, utilizzando il redundancy force-switchover comando.

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

Unità attiva rimossa

Se si controlla la cronologia dello switchover, è possibile vedere "l'unità attiva rimossa" che indica una perdita di comunicazione sulla porta di ridondanza tra i due controller.

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

Questo può accadere se il collegamento tra i due controller si interrompe, ma può anche verificarsi se un'unità WLC si spegne improvvisamente (interruzione dell'alimentazione) o si blocca. È interessante monitorare entrambi i WLC per vedere se hanno report di sistema che indicano arresti anomali/riavvii imprevisti.

GW perso attivo

Se si controlla la cronologia dello switchover, si può vedere "Active lost GW" che indica una perdita di comunicazione con il gateway sulla porta RMI.

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

Questo si verifica se il collegamento tra il controller attivo e il relativo gateway non è attivo.

Ulteriori considerazioni

HA SSO per Catalyst 9800-CL

Negli ambienti virtuali è necessario accettare l'introduzione della latenza, che non è tollerata correttamente da HA. Ciò è legittimo, in quanto HA SSO tende a rilevare in modo rapido ed efficiente qualsiasi guasto allo chassis. Per ottenere questo risultato, ogni chassis controlla lo stato dell'altro utilizzando keepalive sui collegamenti RP e RMI, nonché ping verso il gateway degli RMI (e questo, quello del loro WMI che deve essere lo stesso). In caso di mancato superamento di una di queste condizioni, lo stack reagisce in base ai sintomi, come descritto in "System and Network Fault Handling" (Gestione degli errori di sistema e di rete) nella guida HA SSO.

Quando si utilizzano stack HA SSO virtuali di Catalyst 9800, è comune osservare gli switchover dovuti alla mancata esecuzione di keepalive sul collegamento RP. Ciò può essere dovuto alla latenza introdotta dall'ambiente virtualizzato.

Per determinare se lo stack HA SSO soffre di perdite keepalive RP, è possibile utilizzare i registri dello stack/rif manager.

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

Se entrambi gli chassis sono in funzione, lo switchover crea un "Dual Active Detection" che è una conseguenza delle cadute su RP.

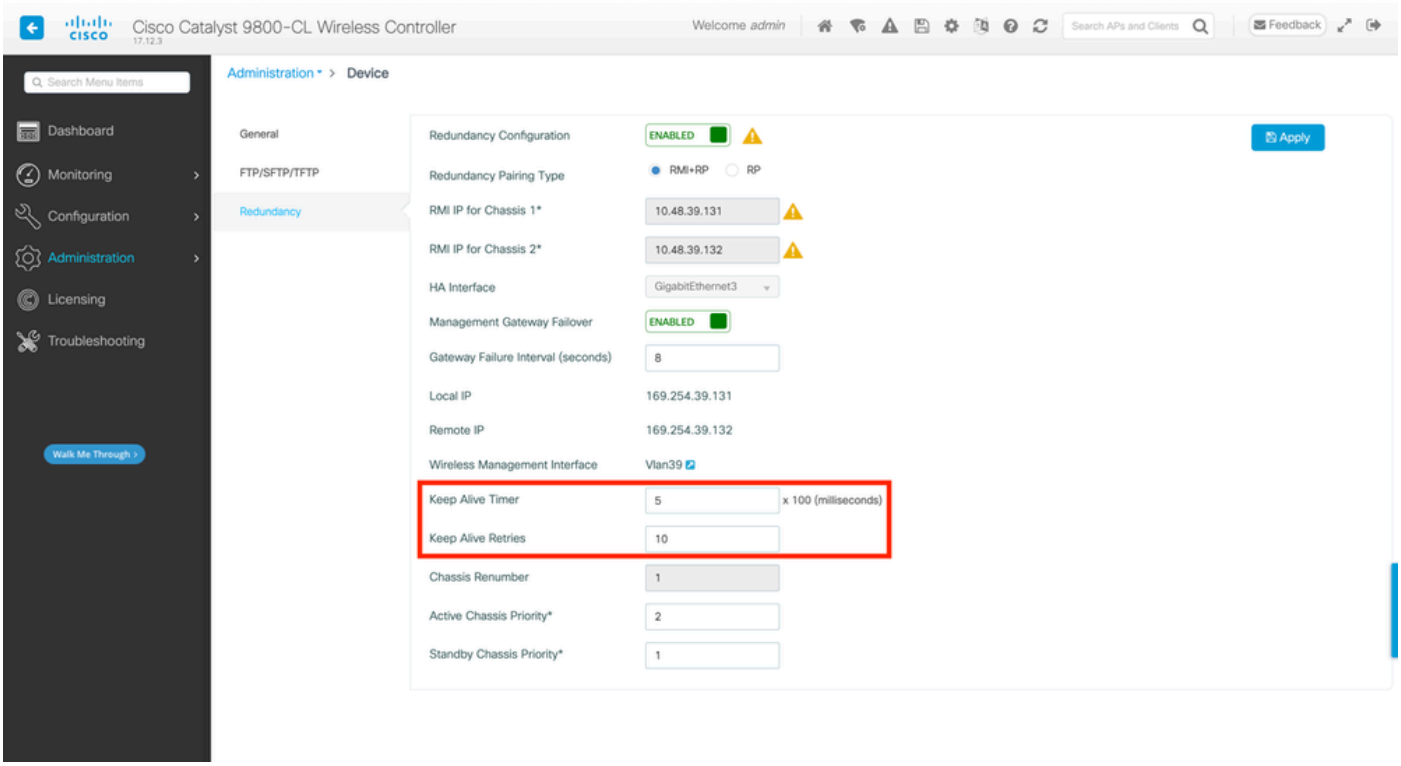
In una situazione di questo tipo, modificare i parametri HA keepalive per evitare questi cambi non necessari può essere di aiuto. È possibile configurare due parametri,

- **Keep Alive Timer:** il periodo di tempo che separa l'invio di due messaggi keepalive tra ogni chassis.
- **Tentativi keep-alive:** il numero di keepalive da omettere per dichiarare un peer down.

Per impostazione predefinita, il timer keep-alive è impostato su 1 ms e i tentativi su 5. Ciò significa che dopo 5 ms di keepalive non riusciti sul collegamento RP, si verifica un switchover. Questi valori possono essere troppo bassi per le distribuzioni virtuali. Se si verifica un passaggio ricorrente a causa della mancata corrispondenza dei pacchetti keepalive RP, provare ad aumentare questi parametri per stabilizzare lo stack.

Dalla GUI:

Per monitorare o modificare i parametri keepalive HA SSO dalla GUI 9800, passare alla scheda Ridondanza dalla pagina *Amministrazione* > *Dispositivo*, come mostrato in questa schermata.



Dalla CLI:

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

Insieme alla configurazione di questi parametri, un'altra ottimizzazione può essere utile per ottenere un comportamento di questo tipo nello stack HA SSO. Per gli accessori fisici, l'hardware consente di collegare uno chassis a un altro utilizzando in genere un singolo filo. In un ambiente virtuale, l'interconnessione della porta RP per ogni chassis deve essere effettuata da uno switch virtuale (vSwitch), che può ancora una volta introdurre la latenza rispetto alle connessioni fisiche. L'utilizzo di uno switch vSwitch dedicato per la creazione del collegamento RP è un'altra ottimizzazione che può impedire la perdita dei pacchetti keepalive HA a causa della latenza. Questa condizione è documentata anche nella guida all'implementazione di Cisco Catalyst 9800-CL Wireless Controller for Cloud. Pertanto, la soluzione migliore consiste nell'utilizzare uno switch vSwitch dedicato per il collegamento RP tra le VM 9800-CL e assicurarsi che non interferisca con il traffico.

Catalyst 9800 HA SSO in implementazioni ACI

Quando si verifica uno switchover in uno stack HA SSO, il nuovo chassis attivo utilizza il meccanismo GRATUITO ARP (GARP) per aggiornare il mapping da MAC a IP nella rete e assicurarsi che riceva il traffico dedicato al controller. In particolare, lo chassis invia GARP per diventare il nuovo "proprietario" di WMI e assicurarsi che il traffico CAPWAP raggiunga lo chassis appropriato.

Lo chassis che sta diventando attivo in realtà non sta inviando un singolo GARP, ma una loro esplosione per garantire che qualsiasi dispositivo nella rete aggiorni la sua mappatura IP a MAC. Questa frammentazione può sovraccaricare la funzione di apprendimento ARP di ACI; pertanto, quando si usa ACI, si consiglia di ridurre al massimo questa frammentazione dalla configurazione di Catalyst 9800.

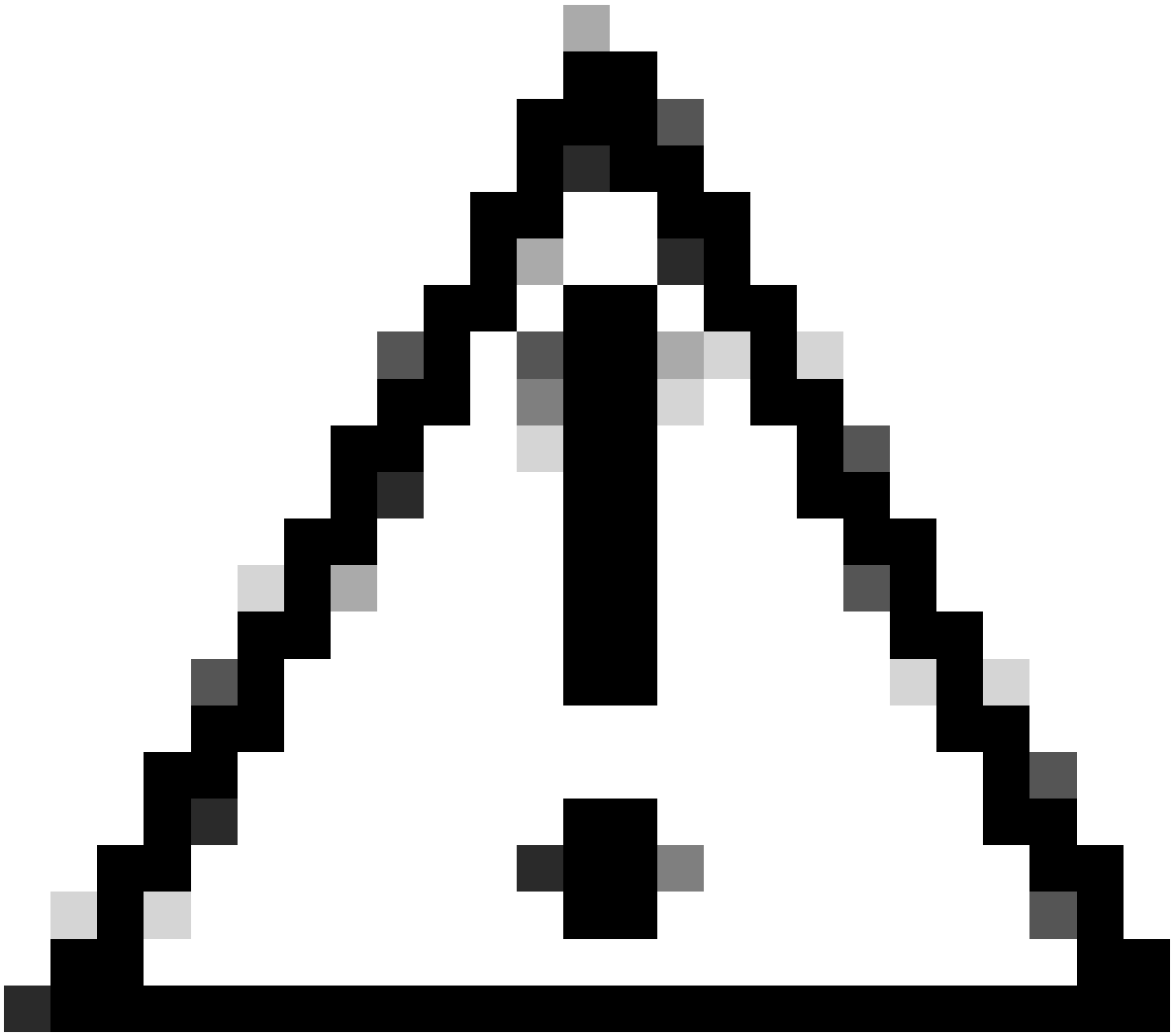
Dalla CLI:

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

Oltre a limitare la frammentazione GARP iniziata dalla 9800 durante un passaggio, si consiglia di disabilitare la funzione di commutazione veloce su questa piattaforma. Quando è configurato lo switchover rapido, il controller attivo invia una notifica esplicita al controller in standby per segnalare che sta per essere disattivato. Quando si utilizza questo tipo di switch, può esistere traffico di interfoliazione (AP e client interrotti) tra entrambi i WLC che formano lo stack HA finché uno di essi non si blocca. Pertanto, la disattivazione di questa funzionalità consente di stabilizzare l'infrastruttura wireless mentre si lavora con le distribuzioni ACI.

Dalla CLI:

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



Attenzione: quando l'opzione di commutazione veloce è disabilitata, il controller in standby si basa esclusivamente sugli errori di timeout keepalive per rilevare quando il controller attivo si è spento. Per questo motivo è necessario procedere con la massima cura alla configurazione.

Per ulteriori informazioni sulle considerazioni relative alle implementazioni di HA SSO per Catalyst 9800 all'interno della rete ACI, vedere la sezione "Information About Deploying ACI Network in Controller" in Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

Riferimenti

- 17.3 Guida SSO HA
- 17.6 Guida SSO HA

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).