Aggiornamento di Catalyst 9800 WLC HA SSO tramite ISSU

Sommario

Introduzione

In questo documento viene descritto come aggiornare una coppia di controller wireless 9800 in HA SSO utilizzando il metodo ISSU (In-Service Software Upgrade).

Requisiti

Il documento descrive la procedura, la limitazione, le precauzioni da adottare e le istruzioni per l'aggiornamento.

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst 9800 Wireless LAN Controller (WLC)
- Switchover stateful ad alta disponibilità (HA SSO)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

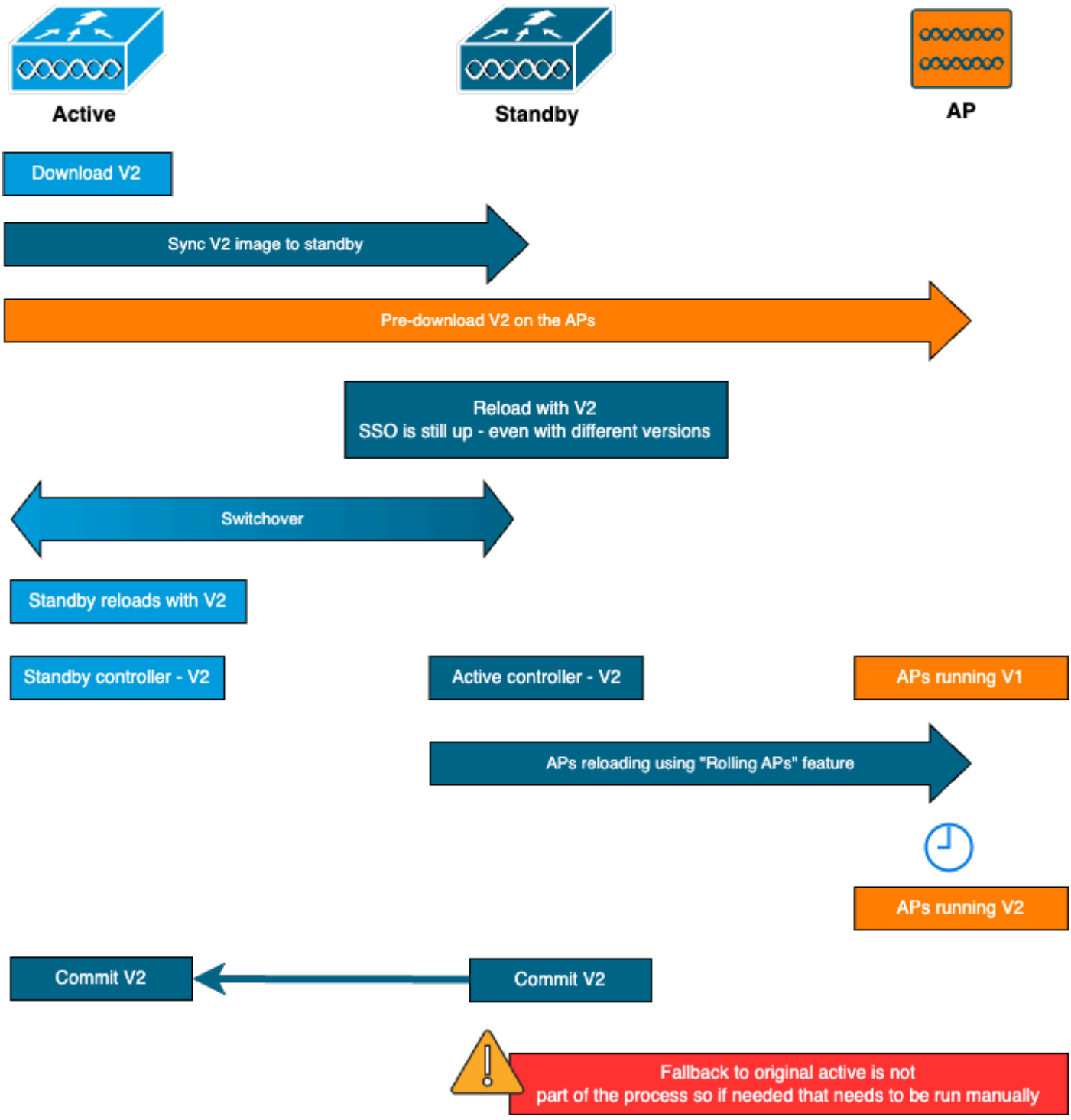
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Funzionamento di ISSU

ISSU è una funzione che consente di aggiornare i controller wireless 9800 con tempi di inattività minimi. Se si dispone di una copertura sufficiente, l'aggiornamento è senza problemi e i client wireless non devono osservare tempi di inattività. Per rendere ciò possibile, l'ISSU ha un meccanismo che aggiorna un controller alla volta e consente ai punti di accesso di eseguire l'aggiornamento in modo scaglionato.

Di seguito è riportata una breve panoramica dei diversi passaggi che si verificano durante l'aggiornamento di un modulo ISSU:

1. L'immagine di destinazione (V2) viene scaricata sul controller primario che esegue V1 ed espansa in pacchetti.
2. L'immagine viene quindi sincronizzata con il controller hot standby tramite la connessione RP. Questo processo è lo stesso per ogni tipo di aggiornamento
3. L'immagine AP corrispondente (V2) viene pre-scaricata sugli access point. Il pre-download di un'immagine non influisce sul servizio.
4. Il controller di standby viene ricaricato e caricato con la nuova immagine (V2). A questo punto, il controller attivo esegue V1 e la modalità standby esegue V2 e formano una coppia SSO. Questa operazione è possibile solo durante l'aggiornamento di ISSU.
5. Quando la coppia HA è pronta (stato attivo/standby caldo), viene eseguito un switchover. Il controller attivo ora esegue V2 e lo standby esegue V1. Il controller di standby si ricarica e viene fornito con V2. In questa fase, entrambi i controller si trovano sulla V2, ma i punti di accesso sono ancora in esecuzione sulla V1.
6. Dopo la fase di attivazione, ai punti di accesso viene richiesto di passare alla versione V2 delle immagini e il loro aggiornamento avviene in sequenza per ridurre al minimo i tempi di inattività. Ciò significa che i sottogruppi di access point vengono ricaricati per ciclo e i client possono connettersi agli access point adiacenti. Quando gli access point tornano a unirsi, si uniscono di nuovo con V2.
7. Il passaggio finale è commit, che rende le modifiche permanenti.



Limitazioni

Di seguito sono riportati i limiti di cui è necessario essere a conoscenza prima di procedere all'aggiornamento di un modulo ISSU:

- L'immagine base deve essere Cisco IOS XE 17.3 o superiore
- L'opzione ISSU è disponibile solo tra versioni principali all'interno dello stesso treno. Ad esempio, il valore da 16.x.x a 17.x.x o da 17.x.x al treno principale successivo non è supportato
- Il downgrade ISSU non è supportato per le piattaforme Cisco Catalyst serie 9800 Wireless Controller

- L'aggiornamento IOS è supportato solo per il controller in modalità INSTALL (modalità BUNDLE non supportata)
- un aggiornamento IOS richiede più tempo rispetto a un aggiornamento standard in base alla progettazione, in quanto un WLC si aggiorna nella coppia HA in un determinato momento, quindi l'aggiornamento AP in modo continuo per ridurre al minimo il downtime. Se i punti di accesso sono dietro un collegamento WAN con una certa latenza, è importante ridurre al minimo il tempo di download dell'immagine, in quanto ciò può aumentare notevolmente il tempo di aggiornamento dell'IOS tramite l'effetto a cascata. Esaminare i metodi di aggiornamento AP o HTTPS fuori banda per velocizzare il tempo di download dell'immagine AP e ridurre al minimo il tempo totale di emissione.

Requisiti e verifiche

Prima di procedere all'aggiornamento dei controller wireless 9800 che utilizzano ISSU, è necessario eseguire alcune verifiche e requisiti per garantire un aggiornamento senza problemi dei controller e dei punti di accesso.

Passaggio 1: verificare che non sia in esecuzione alcuna versione attiva o non vincolata

CLI:

```
show install summary
```

Output previsto:

Viene visualizzata una sola versione con stato "C" (Attivato e Confermato):

```
WLC#show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.04a.0.6
```

Passaggio 2: verificare che il controller sia in modalità INSTALL

Accertarsi che entrambi i controller Active e Standby siano in modalità di installazione e siano avviati da "bootflash:/packages.conf" (vedere il passaggio 3).

CLI:

```
show version | i Installation mode
```

Output previsto:

```
WLC#show version | i Installation mode
Installation mode is INSTALL
```

Passaggio 3: Controllare il file utilizzato per l'avvio ("packages.conf")

Se il controller è in modalità INSTALL, è necessario avviarlo dal file "packages.conf".

CLI:

```
show boot
```

Output previsto:

```
WLC#show boot
BOOT variable = bootflash:packages.conf,12;
CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x102

Standby BOOT variable = bootflash:packages.conf,12;
Standby CONFIG_FILE variable =
Standby BOOTLDR variable does not exist
Standby Configuration register is 0x102
```

Passaggio 4: Controllare gli stati di ridondanza

Il controller attivo deve essere in ATTIVA e il controller di standby deve essere in HOT STANDBY indica che la comunicazione è attiva e che comunicano tra loro.

CLI:

```
show chassis rmi
show redundancy
```

Output previsto:

```
WLC#show chassis rmi
Chassis/Stack Mac Address : 000c.29c4.caff - Local Mac Address
Mac persistency wait time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP                RMI-IP
-------------------------------------------------------------------------------------------------
*1       Active   000c.29c4.caff     2      V02     Ready               169.254.10.9       198.19.10.9
 2       Standby  000c.29d2.4018     1      V02     Ready               169.254.10.10      198.19.10.1

WLC#show redundancy
Redundant System Information :
------------------------------
...
                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
               Maintenance Mode = Disabled
                 Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
...

Peer Processor Information :
----------------------------
              Standby Location = slot 2
        Current Software state = STANDBY HOT
...
```

Passaggio 5: verificare che vi sia spazio sufficiente nel bootflash per memorizzare la nuova immagine

A raccoglitore le dimensioni dell'immagine sono di circa 1 GB. Prima di procedere, accertarsi di disporre di più GB di spazio libero nella memoria flash di avvio.

CLI:

```
dir bootflash:/ | in free
```

Output previsto:

```
WLC#dir bootflash:/ | in free
14785671168 bytes total (11446026240 bytes free)
```

Passaggio 6: verificare che non vi siano altri aggiornamenti in corso

Si tratta di un passaggio cruciale, perché se il controller è bloccato in un aggiornamento precedente, il nuovo aggiornamento non riesce.

CLI:

```
show issu state detail
```

Output previsto:

```
WLC#show issu state detail
Current ISSU Status: Enabled
Previous ISSU Operation: N/A
=====================================================
System Check                        Status
-----------------------------------------------------
Platform ISSU Support               Yes
Standby Online                      Yes
Autoboot Enabled                    Yes
SSO Mode                            Yes
Install Boot                        Yes
Valid Boot Media                    Yes
Operational Mode                    HA-REMOTE
=====================================================
No ISSU operation is in progress
```

Aggiornamento

Dopo aver superato tutti i controlli, è ora possibile procedere all'aggiornamento dei controller wireless. È possibile scegliere di aggiornare i controller utilizzando la GUI o la CLI. Entrambi i metodi presentano vantaggi e svantaggi. La CLI offre un maggiore controllo in quanto è possibile avviare ogni passaggio singolarmente, ma questo richiede un lavoro leggermente superiore rispetto all'aggiornamento tramite la GUI. L'aggiornamento del controller tramite la GUI può essere eseguito con una sola pressione del tasto e tutti i passaggi vengono eseguiti automaticamente. Tuttavia, se si verifica un errore durante l'aggiornamento, è necessario accedere alla CLI per riavviare il passaggio specifico non riuscito. Questa guida mostra solo la procedura di aggiornamento CLI, poiché la procedura GUI può essere eseguita semplicemente eseguendo le istruzioni GUI.

Flusso di lavoro ISSU CLI

Questa sezione mostra un breve riepilogo dei comandi eseguiti per aggiornare i controller. Viene fornita una spiegazione completa di ciascun comando e di tutti i passaggi:

Comando	Descrizione
installare add file <file>	L'immagine scaricata dal CCO al bootflash viene caricata sul controller e

	trasformata in pacchetti
pre-download immagine ap	Le immagini AP corrispondenti all'immagine v2 vengono pre-scaricate sugli access point
installare attivare il problema [auto-abort-timer <30-1200>]	Mette in scena l'orchestrazione di un ricaricamento WLC seguito dall'altro. Il trigger activate esegue la reimpostazione dell'access point in modo sfalsato, tentando nel miglior modo possibile di mantenere la connettività per i client
comando install commit	Il commit rende permanenti le modifiche

Procedura completa

Fase 1: cancellazione delle statistiche pre-download dell'access point

È consigliabile cancellare tali statistiche prima di eseguire l'aggiornamento in modo da ottenere un nuovo output correlato solo all'aggiornamento corrente. Prima di avviare l'aggiornamento non deve essere in corso alcun download preliminare.

CLI:

```
clear ap predownload statistics
show ap image
```

Output previsto:

```
WLC#show ap image
Total number of APs  : 2
Number of APs
        Initiated                   : 0
        Downloading                 : 0
        Predownloading              : 0
        ...
        Predownload in progress     : No
```

Passaggio 2: Rimuovere l'immagine software precedente
Se lo spazio disponibile in bootflash non è sufficiente, è sempre possibile eseguire la pulizia dei vecchi file di installazione utilizzando il comando install remove inactive.

CLI:

```
install remove inactive
```

Passaggio 3: configurare il valore della percentuale di aggiornamento in sequenza del punto di accesso

È possibile impostare questo valore fino al 25% (valore massimo). Se si sceglie il 5% (valore minimo), verrà eseguito l'aggiornamento di un numero inferiore di access point per iterazione e l'aggiornamento richiederà più tempo, ma questo consente anche di ridurre il downtime globale. Scegliere questo valore in base alla distribuzione e alla copertura AP.

CLI:

```
conf t
ap upgrade staggered {5 | 15 | 25 | one-shot}
end
write memory
```

Passaggio 4: scaricare l'immagine .bin sul controller

È possibile caricare questa immagine tramite la CLI o la GUI. Con la GUI, questo avviene quando si avvia il processo di upgrade.

CLI:

```
dir bootflash:*.bin
[OPTIONAL] copy ftp://
```

:

@

/

bootflash:

Passaggio 5: Installare l'immagine

Questo passaggio avvia la prima fase dell'aggiornamento. L'immagine del software del controller viene aggiunta alla memoria flash ed espansa in pacchetti. L'operazione richiede un paio di minuti. Una volta completato il processo di aggiunta dell'installazione, verificare che la nuova immagine venga visualizzata come "Inattiva" dal comando "show install summary".

CLI:

```
install add file bootflash:
```

```
      show install summary
```

Output previsto:

```
WLC#show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.04a.0.6
IMG   I    17.12.02.0.2739
```

Passaggio 6: Pre-scaricare l'immagine nei punti di accesso

Prima di attivare l'immagine, è necessario indicare agli access point di pre-scaricare l'immagine attualmente inattiva (V2). Se il pre-download non viene avviato, l'aggiornamento dell'ISSU non riesce in quanto si tratta di una procedura necessaria per ridurre al minimo i tempi di inattività.

Questa operazione può richiedere alcuni minuti a seconda del numero di access point collegati al controller e della latenza del collegamento.

CLI:

```
ap image predownload
show ap image
```

Output previsto:

```
WLC#show ap image
Total number of APs  : 2

Number of APs
        Initiated                   : 0
        Downloading                 : 0
        Predownloading              : 2
        Completed downloading       : 0
        Completed predownloading    : 0
        Not Supported               : 0
        Failed to Predownload       : 0
        Predownload in progress     : Yes
```

Passaggio 7: Attivare la nuova immagine

Al termine del download preliminare, è possibile attivare la nuova immagine. Questa è la fase più lunga del processo di upgrade. Esegue i controlli di compatibilità, installa il pacchetto e aggiorna i dettagli sullo stato del pacchetto. Facoltativamente, è possibile configurare il limite di tempo per annullare l'aggiunta di nuovo software senza eseguire il commit dell'immagine. I valori validi sono compresi tra 30 e 1200 minuti. Il valore predefinito è 360 minuti (6 ore). Una volta avviato l'aggiornamento, viene eseguito l'intero processo ISSU: gli aggiornamenti in standby, lo switchover, i nuovi aggiornamenti in standby e quindi l'aggiornamento scaglionato dell'AP.

CLI:

```
install activate issu [auto-abort-timer <30-1200 mins>]
```

Output previsto:

```
WLC#install activate issu
install_activate: START Sun Jan 14 08:29:36 EST 2024
install_activate: Activating ISSU
```

```
NOTE: Going to start Activate ISSU install process

STAGE 0: System Level Sanity Check
================================================
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
--- Verifying Platform specific ISSU admission criteria ---
--- Verifying Image ISSU Compatibility ---
Finished Initial System Level Sanity Check

STAGE 1: Installing software on Standby
================================================
--- Starting install_remote ---
[2] install_remote package(s) on chassis 2/R0
WARNING: Found 1545 disjoint TDL objects.
[2] Finished install_remote on chassis 2/R0
install_remote: Passed on [2/R0]
Finished install_remote

STAGE 2: Restarting Standby
================================================
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby to reach terminal redundancy state ---
Finished wait for Standby to reach terminal redundancy state

STAGE 3: Installing software on Active
================================================
--- Starting install_active ---
WARNING: Found 2969 disjoint TDL objects.
[1] install_active package(s) on chassis 1/R0
[1] Finished install_active on chassis 1/R0 install_active: Passed on [1/R0]
Finished install_active

STAGE 4: Restarting Active (switchover to standby)
================================================
--- Starting active reload ---
New software will load after reboot process is completed
```

È consigliabile monitorare periodicamente lo stato corrente dell'aggiornamento utilizzando i comandi "show chassis rmi" e "show redundancy". In questo modo, una volta rimosso un controller dalla coppia HA, quando viene ripristinato e su quale versione. Il processo può richiedere da 20 a 30 minuti circa.

Al termine dell'aggiornamento, l'immagine verrà visualizzata come attiva ma "senza commit":

```
WLC#show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
```

```
IMG   U    17.12.02.0.2739

--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 05:23:37
--------------------------------------------------------------------------------
```

Al termine dell'installazione, il WLC inizierà a ricaricare gli AP in modo scaglionato. Per monitorare l'aggiornamento sfalsato dell'access point, è possibile usare la GUI (in "Statistiche aggiornamento access point" nella sezione "Aggiornamento software") o il comando CLI "show ap uptime", che mostrerà il tempo di attività dell'access point in CAPWAP. Ciò fornisce un'indicazione di quali access point sono già stati ricaricati. È inoltre possibile verificare che l'aggiornamento del punto di accesso sia terminato controllando i log, utilizzando il comando "show logging" sul controller:

```
Jan 20 14:23:22.478: %UPGRADE-6-STAGGERED_UPGRADE_COMPLETE: Chassis 2 R0/0: wncmgrd: Staggered AP Upgra
```

Passaggio 8: [FACOLTATIVO] Interrompere il timer di interruzione automatica

Se sono necessarie più ore di tempo rispetto alle 6 ore predefinite per l'aggiornamento (quando si dispone di molti punti di accesso da aggiornare e si desidera essere certi che funzioni correttamente prima di eseguire il commit dell'immagine), è possibile interrompere questo timer. In questo modo, il rollback automatico non verrà eseguito.

CLI:

```
install auto-abort-timer stop
```

Passaggio 9: Rendere persistente il nuovo software

Eseguire il commit delle modifiche all'attivazione in modo che siano persistenti durante i ricaricamenti utilizzando il comando install commit. Questo è il passaggio finale di un normale processo di aggiornamento. Il comando install commit rende il software persistente dopo il riavvio.

CLI:

```
install commit
```

Output previsto:

```
WLC#show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
```

```
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.12.02.0.2739
```

Una volta eseguito il commit della versione e ricaricati gli access point nella nuova versione, l'aggiornamento dell'ISSU è terminato.

Altre operazioni

È possibile trovare altre operazioni che è possibile eseguire durante o dopo l'aggiornamento di IOS, ad esempio l'interruzione dell'aggiornamento o il ripristino di una versione precedente:

Interrompi problema

Questo passaggio annulla il processo di aggiornamento eseguito finora e riporta il dispositivo allo stato di installazione precedente (V1)in modalità ISSU. Ciò è valido sia per i controller sia per gli access point. Questa operazione può essere eseguita nel caso in cui si noti un forte impatto dovuto all'aggiornamento e se non è stato ancora eseguito il commit dell'immagine. Questo comando ed elaborazione funziona solo se "install commit" non è stato ancora emesso. Una volta eseguito il commit dell'immagine, non è possibile eseguire il rollback in modalità ISSU.

CLI:

```
install abort issu
```

Output previsto:

```
STAGE 1: Rolling Back software on Standby
================================================
--Starting Deactivation at the standby --
--- Starting abort_standby ---
[1] abort_standby package(s) on chassis 1/R0
WARNING: Found 1545 disjoint TDL objects.

[1] Finished abort_standby on chassis 1/R0
abort_standby: Passed on [1/R0]
Finished abort_standby

STAGE 2: Restarting Standby
================================================
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby to reach terminal redundancy state ---
Finished wait for Standby to reach terminal redundancy state
```

```
STAGE 3: Rolling Back software on Active
================================================
--Starting Deactivation at the active --
--- Starting abort_active ---
WARNING: Found 1545 disjoint TDL objects.
[2] abort_active package(s) on chassis 2/R0
[2] Finished abort_active on chassis 2/R0
abort_active: Passed on [2/R0]
Finished abort_active

STAGE 4: Restarting Active (switchover to standby)
================================================
--- Starting active reload ---
New software will load after reboot process is completed
SUCCESS: install_abort  Wed Jan 17 21:58:52 CET 2024
client_loop: send disconnect: Broken pipe
```

Passaggio al controller "primario"

In un ambiente di produzione questo passaggio può essere richiesto se si desidera riattivare il controller originale. Una volta completato l'aggiornamento dell'ISSU, l'unità "secondaria" è il controller attivo. È sempre possibile tornare allo stato originale eseguendo un passaggio manuale. Prima di procedere, è necessario verificare che l'unità peer si trovi nello stato "Standby Hot".

CLI:

```
redundancy force-switchover
```

Ripristino dello stato precedente al termine dell'aggiornamento di ISSU

Una volta eseguito l'aggiornamento, il downgrade ISSU non è supportato per le piattaforme Cisco Catalyst serie 9800 Wireless Controller. A questo punto, un rollback significa che sia i controller wireless che gli access point verranno ricaricati a causa della modifica del codice e questo creerà tempi di inattività. È possibile iniziare controllando i punti di rollback disponibili e quindi decidere a quale di essi eseguire il rollback.

CLI:

```
show install rollback
show install rollback id
```

```
      install rollback to id
```

Output previsto:

```
WLC#sh install rollback
ID      Label                           Description
-------------------------------------------------------
3       No Label                        No Description
2       No Label                        No Description
1       No Label                        No Description

WLC#sh install rollback id 2
Rollback id - 2 (Created on 2024-04-22 10:31:57.000000000 +0000)
Label: No Label
Description: No Description
Reload required: NO
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
-------------------------------------------------------------------------------
Type  St   Filename/Version
-------------------------------------------------------------------------------
IMG   C    17.09.04a.0.6

WLC#install rollback to id 2
install_rollback: START Thu May 30 09:44:38 UTC 2024
install_rollback: Rolling back to id 2

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Rollback ---
Performing Rollback on all members
 [2] Rollback package(s) on Chassis 2/R0
 [1] Rollback package(s) on Chassis 1/R0
 [2] Finished Rollback package(s) on Chassis 2/R0
Checking status of Rollback on [1/R0 2/R0]
Rollback: Passed on [1/R0 2/R0]
Finished Rollback operation

SUCCESS: install_rollback Thu May 30 09:45:40 UTC 2024
```

Risoluzione dei problemi

Se si verifica un problema prima, durante o dopo l'aggiornamento dei controller wireless 9800 tramite ISSU, si consiglia di consultare questo documento che spiega i problemi comuni riscontrati e le relative soluzioni.

Riferimenti

- Alta disponibilità grazie all'applicazione di patch e all'aggiornamento continuo degli access

point sui controller wireless Cisco Catalyst 9800
- Guida alla configurazione di 17.12.X

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).