

Ripristino da un loop di avvio causato da danneggiamento dell'immagine sui punti di accesso Wave 2 e 11ax (CSCvx32806)

Sommario

[Introduzione](#)

[Condizioni di problema](#)

[Prodotti non interessati](#)

[Prodotti interessati](#)

[Versioni interessate: Sindrome dell'avvio di un'immagine non valida](#)

[Sintomi](#)

[Come ripristinare i punti di accesso in un loop di avvio](#)

[Determinare se gli access point dispongono delle funzionalità Alt-boot](#)

[Ripristino dei punti di accesso in loop di avvio con la funzione Alt-boot](#)

[Se SSH è abilitato sugli access point](#)

[Se il protocollo SSH non è abilitato sugli access point, ma questi hanno la funzione Alt-boot](#)

[Ripristino tramite console](#)

[Per tutti i modelli AP: Determinare La Partizione Di Avvio Danneggiata](#)

[Per i modelli AP 9117, 9124, 9130, 9136](#)

[Per i modelli AP 2802, 3802, 4800, 9105, 9115, 9120](#)

[Domande frequenti](#)

Introduzione

Alcuni access point Cisco (AP) possono scaricare un'immagine danneggiata tramite CAPWAP (Control and Provisioning of Wireless Access Point) da un controller serie 9800. A seconda della versione del software dell'access point, l'access point potrebbe tentare di avviare l'immagine danneggiata, creando un loop di avvio. Questo articolo spiega come ripristinare i punti di accesso bloccati in un loop di avvio. Per ulteriori informazioni sui prodotti e sulle distribuzioni soggetti a questo problema e su come eseguire l'aggiornamento in modo sicuro senza riscontrare il problema del loop di avvio, fare riferimento all'articolo [Aggiornamento sicuro dei punti di accesso per evitare il danneggiamento dell'immagine che causa il loop di avvio](#).

Questo problema è documentato come [avviso sui prodotti: FN74109 - Il danneggiamento dell'immagine del punto di accesso durante l'aggiornamento di CAPWAP potrebbe causare un errore di avvio....](#)

Condizioni di problema

Prodotti non interessati

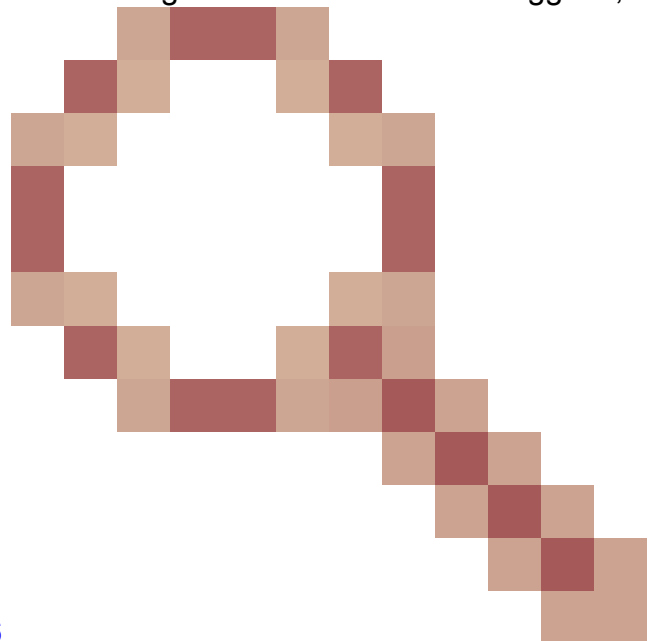
- WLC (Wireless LAN Controller): il download dai access point dai controller LAN wireless AireOS non è influenzato
- Mobility Express, controller wireless integrato
- AP - Aironet serie 1800/1540/1100AC Wave 2 11ac AP e Wave1 11ac Access Point (1700/2700/3700/1570/IW3700) non sono interessati (anche se questi AP sono registrati a 9800 WLC, non ne è influenzato l'impatto)
- AP Wi-Fi 6E introdotti dal 2023: IW9167, IW9165, C9163

Prodotti interessati

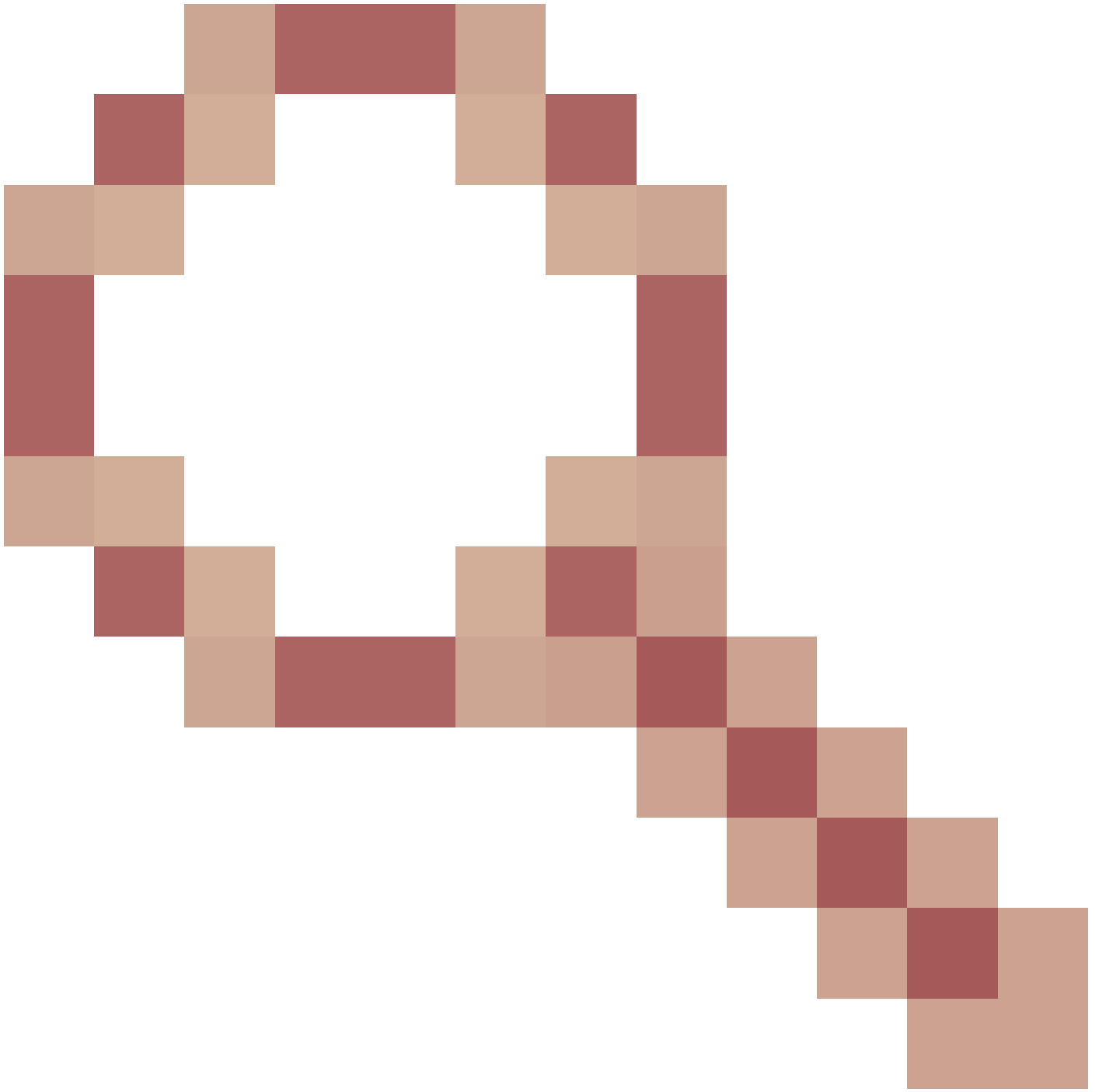
- WLC: Il download degli access point dai Cisco Catalyst serie 9800 Wireless LAN Controller potrebbe essere interessato
- Punti di accesso: Il problema interessa i seguenti modelli AP che si registrano sui Cisco Catalyst serie 9800 Wireless LAN Controller:
 - Access point Aironet Wave2 11ac (2800/3800/4800/1560/IW6330/ESW6300)
 - Access point Catalyst serie 9100 Wi-Fi6 (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
 - Access point Catalyst serie 9100 Wi-Fi6E (9136/9162/9164/9166)

Versioni interessate: Sindrome dell'avvio di un'immagine non valida

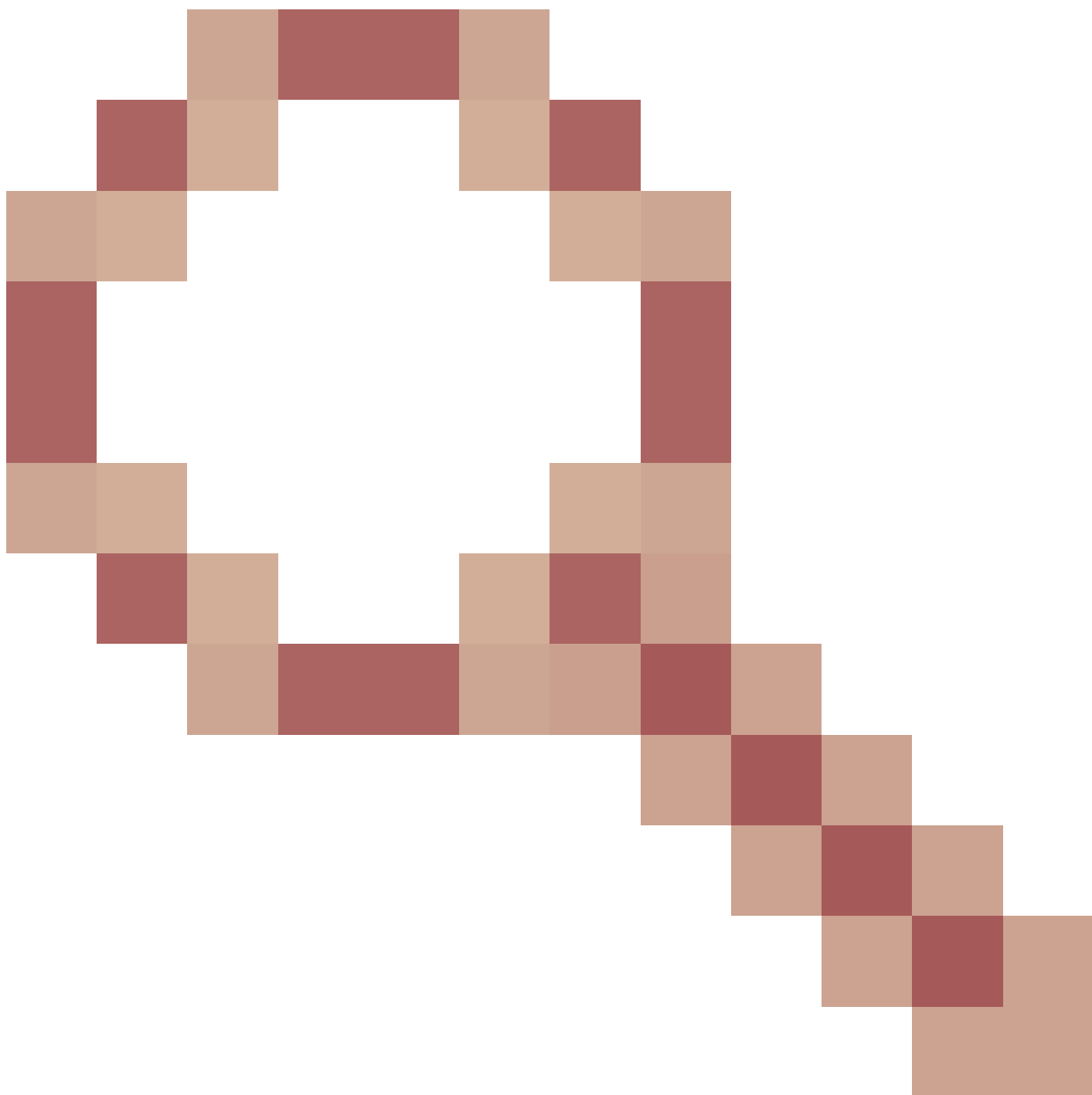
Il problema, quando il punto di accesso tenta di avviare un'immagine che sa essere danneggiata,



viene risolto dai seguenti ID bug Cisco: [CSCvx32806](#)
CSCwc72021



, [CSCwd90081](#)



, che sono fissati nelle seguenti versioni:

- 8.10.185.0 e superiori
- 17.3.7 e oltre
- 17.6.6 e oltre
- 17.9.3 e oltre
- 17.11.1 e oltre

Una volta aggiornato al software con le correzioni di cui sopra, l'access point potrebbe comunque scaricare un'immagine danneggiata; tuttavia, non tenterà di avviare l'immagine, ma continuerà a tentare di eseguire nuovamente il download fino al completamento dell'operazione.

Sintomi

Console AP:

Un punto di accesso che ha già scaricato l'immagine danneggiata e si trova ora in un loop di avvio, visualizzerà un messaggio di console simile al seguente:

```
verifica della firma non riuscita per /bootpart/part1/ramfs_data_cisco.cpio.lzma
```

o

```
verifica firma non riuscita per /bootpart/part2/ramfs_data_cisco.squashfs
```

Prendere nota del messaggio "part1" o "part2", che indica la partizione di avvio danneggiata.

Registrazione syslog o show:

Se il punto di accesso è stato configurato per accedere a un server syslog esterno, prima del tentativo di download dell'immagine verrà registrato il seguente errore:

```
Errore di verifica della firma dell'immagine: -3
```

Questo messaggio di errore può essere visualizzato anche dalla CLI dell'access point (console o SSH), nell'output "show logging". Se il buffer di registrazione è stato sovrascritto dopo il tentativo di aggiornamento dell'immagine, il messaggio di errore potrebbe essere visualizzato nei file syslog archiviati nella memoria flash AP. Se non si visualizzano messaggi di esito positivo o negativo nella registrazione del programma, usare uno dei metodi di ripristino sull'access point per reinstallare l'immagine desiderata tramite TFTP o SFTP.

Porta switch Cisco:

Sugli access point in stato di loop di avvio viene visualizzato il PD IEEE, come mostrato di seguito nell'output Show del comando switchport uplink dell'access point. Se si utilizzano CDP o LLDP, i punti di accesso funzionanti correttamente visualizzeranno il proprio modello nella colonna Dispositivo:

```
<#root>
```

```
switch#show power inline  
Available:195.0(w) Used:159.9(w) Remaining:35.1(w)
```

Interface	Admin	Oper	Power (Watts)	Device	Class	Max
-----	-----	-----	-----	-----	-----	-----
Gi0/1	auto	on	15.4			
Ieee PD						
Gi0/2	auto	on	24.1	C9115AXI-B	4	30.0

Come ripristinare i punti di accesso in un loop di avvio

Determinare se gli access point dispongono delle funzionalità Alt-boot

Se un access point ha scaricato un'immagine danneggiata e sta tentando di avviarla, mostrerà uno dei due comportamenti, a seconda che il suo bootloader u-boot (AP) abbia o meno la funzione di avvio alternativo (Alt-boot)

- Senza Alt-boot: l'access point tenterà indefinitamente di avviare l'immagine danneggiata e dovrà essere ripristinato tramite la porta della console
- Con Alt-boot: l'access point tenterà di avviare l'immagine danneggiata cinque volte, quindi avvierà l'immagine dalla relativa partizione di backup. In questo caso, l'access point può essere ripristinato senza l'accesso alla console, usando uno dei metodi di ripristino Alt-Boot documentati di seguito.

Il miglioramento Alt-boot u-boot è incluso nelle seguenti versioni software:

- 9117/9130/9124 : 8.10.190.0, 17.3.8+, 17.6.6+, 17.9.1+
- 9136: 17.9.1+
- 916x tutte le unità dispongono del miglioramento Alt-boot
- 9105/9115/9120/2800/3800/4800/1560/6300 : 8.10.190.0, 17.3.8+, 17.6.6+, 17.9.4

Si noti che se un access point ha scaricato un'immagine con la funzione Alt-boot, il suo u-boot verrà aggiornato, anche se l'immagine di runtime è danneggiata. Si consideri, ad esempio, questo scenario:

- su un access point serie 9130 è installato 17.3.4c (senza la funzione di avvio con ALT).
- Quindi scarica un'immagine 17.9.5, ma l'immagine viene danneggiata durante il download.
- Poiché la versione 17.3.4c non dispone della correzione per la sindrome dell'avvio di un'immagine non valida, l'access point procede e cerca di avviare l'immagine danneggiata.
- L'avvio della nuova partizione di immagine determinerà l'aggiornamento dell'access point alla versione 17.9.5 di u-boot, prima che tenti di avviare l'immagine di runtime danneggiata.
- L'access point tenterà quindi cinque volte di avviare l'immagine di runtime 17.9.5 danneggiata.
- Quindi, poiché l'access point esegue ora l'u-boot 17.9.5, la logica di avvio ALT cambierà l'access point in modo da avviare l'immagine di runtime nella relativa partizione di backup.
- È ora possibile ripristinare l'access point senza accesso alla console.

Ripristino dei punti di accesso in loop di avvio con la funzione Alt-boot

Se i punti di accesso si trovano in un loop di avvio e il loro riavvio a U presenta la funzione Alt-boot Enhancement, utilizzare una delle seguenti procedure per ripristinarli:

Se SSH è abilitato sugli access point

1. Posizionare nell'area intermedia l'immagine o le immagini AP desiderate su un server TFTP o SFTP accessibile ai punti di accesso interessati. Vedere la [tabella 4 della matrice di](#)

[compatibilità](#) per la versione AP 15.3(3)J* che mappa alla versione Cisco IOS® XE desiderata, quindi scaricare le immagini del software Lightweight AP appropriate per i modelli AP interessati da software.cisco.com.

1. Ad esempio, l'immagine AP 17.9.5 per un CW9162 è [ap1g6b-k9w8-tar.153-3.JPN4.tar](#).
2. Impedire ai punti di accesso interessati di unirsi a un controller che esegue la stessa versione software della partizione danneggiata. Pertanto, aggiungere un ACL CAPWAP sulla porta dello switch dell'access point per impedire che l'access point si unisca nuovamente al controller. Ad esempio, un ACL simile a quello riportato di seguito può essere applicato all'interfaccia del gateway predefinito della subnet dell'access point:

```
Router#show running-config | section access-list 133
access-list 133 deny ip host <wlc_ip> any log
access-list 133 deny ip any host <wlc_ip> log
access-list 133 permit ip any any
```

```
Router#show running-config interface Vlan6
[ ... ]
interface Vlan6
ip address 192.168.6.1 255.255.255.0
ip access-group 133 in
```

3. Lasciare che l'access point si riavvii con l'immagine danneggiata cinque volte, dopodiché dovrebbe passare all'immagine funzionante nella partizione di backup.
 1. È possibile usare il comando `show cdp neighbors <interface>detail` sullo switch dell'access point per verificare la versione del codice presente nella partizione di backup dell'access point. (Se l'access point sta avviando l'immagine danneggiata, il CDP non verrà visualizzato sulla relativa porta.)
4. Una volta che l'access point ha fornito l'immagine di backup funzionante, proverà a unirsi al controller, ma non potrà farlo a causa dell'ACL aggiunto nel passaggio 2.
5. SSH in ciascun access point interessato (se il problema riguarda un numero elevato di access point, questa operazione può essere automatizzata tramite il [controller WLAN](#)).
6. Scaricare ora l'immagine desiderata nella partizione di backup dell'access point utilizzando il comando di download dell'archivio:

```
archive download-sw /no-reload tftp://<indirizzo-ip>/<immagine>
o
archive download-sw /no-reload sftp://<indirizzo-ip>/<immagine>
```

L'immagine danneggiata verrà sovrascritta con l'immagine valida. Una volta completato il download dell'immagine, emettere:

```
test di riavvio capwap
```

Il processo CAPWAP verrà riavviato in modo che l'access point riconosca l'immagine appena installata.
7. A questo punto, rimuovere l'ACL e fare in modo che l'AP si unisca al controller. L'immagine non verrà scaricata di nuovo.

Se il protocollo SSH non è abilitato sugli access point, ma questi hanno la funzione Alt-boot

1. Verificare che gli access point non tentino di collegarsi a un controller che esegue la stessa

versione software della partizione danneggiata. Pertanto, aggiungere un ACL CAPWAP sulla porta dello switch dell'access point per impedire che l'access point si unisca nuovamente al controller.

2. Attivare un controller che esegue una versione software diversa dalla versione danneggiata del punto di accesso.
 1. È possibile usare il comando `show cdp neighbors <interface>detail` sullo switch dell'access point per verificare la versione del codice presente nella partizione di backup dell'access point. (mentre l'access point sta avviando l'immagine danneggiata, il CDP non verrà visualizzato sulla relativa porta.)
 2. Se non è possibile posizionare nell'area intermedia un controller che esegue la versione di backup dell'access point, allora (se 9800), almeno posizionare nell'area intermedia una versione con correzioni per la sindrome dell'avvio di un'immagine non valida e con Alt-boot.
 3. In alternativa, è possibile usare un controller AireOS con versione 8.10.190.0 o successiva, in quanto i download CAPWAP da AireOS non sono soggetti al danneggiamento delle immagini.
3. Configurare l'access point in modo che possa rilevare il controller alternativo, ad esempio tramite l'opzione DHCP 43, un indirizzo dell'helper IP o DNS.
 1. Tenere presente che se sul controller alternativo è in esecuzione una versione di Cisco IOS XE diversa dal backup dell'access point, quest'ultimo potrebbe scaricare un'immagine danneggiata, quindi ripetere la procedura per tutti gli access point che potrebbero essere stati danneggiati di recente.
4. Una volta collegati al controller alternativo, scaricare l'immagine desiderata sugli access point:
 1. Posizionare nell'area intermedia l'immagine o le immagini AP desiderate su un server TFTP o SFTP accessibile ai punti di accesso interessati. Vedere la [tabella 4 della matrice di compatibilità](#) per la versione AP 15.3(3)J* che mappa alla versione Cisco IOS XE desiderata, quindi scaricare le immagini del software Lightweight AP appropriate per i modelli AP interessati da software.cisco.com.
 1. Ad esempio, l'immagine AP 17.9.5 per un CW9162 è [ap1g6b-k9w8-tar.153-3.JPN4.tar](#).
 2. Abilitare il protocollo ssh sugli access point interessati e il protocollo ssh su ciascun access point interessato (se il problema riguarda un numero elevato di access point, questa operazione può essere automatizzata tramite il [poller WLAN](#)).
 1. Scaricare ora l'immagine desiderata nella partizione di backup dell'access point utilizzando il comando di download dell'archivio:

```
archive download-sw /no-reload tftp://<indirizzo-ip>/<immagine>
```

o

```
archive download-sw /no-reload sftp://<indirizzo-ip>/<immagine>
```

L'immagine danneggiata verrà sovrascritta con l'immagine valida.
2. Una volta completato il download dell'immagine, emettere:

```
test di riavvio capwap
```

Il processo CAPWAP verrà riavviato in modo che l'access point riconosca l'immagine appena installata.

3. In alternativa all'esecuzione di `archive download-sw` sugli access point, è possibile usare i seguenti comandi del controller per ottenere gli access point e scaricare l'immagine desiderata da un server TFTP:
 1. In Cisco IOS XE: `Nome ap APNAME tftp-downgrade ip.addr.of.server nomeimmagine.tar`
 2. In AireOS: `config ap tftp-downgrade ip.addr.of.server nomeimmagine.tar NOMEAPP`
 3. Monitorare i registri del server TFTP per verificare che ciascun punto di accesso abbia scaricato correttamente l'immagine. Una volta completato il download, ogni access point si ricarica, eseguendo l'immagine appena scaricata.
5. Rimuovere l'ACL installato nel passaggio 1 e fare in modo che gli AP si uniscano al controller desiderato.

Ripristino tramite console

Se l'access point è in un loop di avvio e non dispone della funzione Alt-boot, deve essere ripristinato tramite console.

Per tutti i modelli AP: Determinare La Partizione Di Avvio Danneggiata

Verificare innanzitutto quale partizione di avvio è danneggiata.

1. Connettersi alla console AP.
2. Controllare il tentativo di avvio dell'access point finché non viene visualizzato il messaggio `verifica della firma non riuscita per /bootpart/part1/ramfs_data_cisco.cpio.lzma`
o
`verifica della firma non riuscita per /bootpart/part2/ramfs_data_cisco.cpio.lzma`
(il messaggio potrebbe essere "ramfs_data_cisco.squashfs" anziché "ramfs_data_cisco.cpio.lzma")
3. Prendere nota della partizione part1 o part2 danneggiata

Per modelli AP 9117, 9124, 9130, 9136

1. Quando è collegato alla console, spegnere e riaccendere il punto di accesso.
2. Durante l'avvio, quando viene visualizzato Premere ESC per arrestare l'avvio automatico, premere il tasto ESC
3. Viene visualizzato uno dei seguenti prompt:
N. BTLDR
o
(avvio da u)>
4. Esegui questi comandi

```
(u-boot)> or (BTLDR)# setenv mtdids nand0=nand0 && setenv mtdparts mtdparts=nand0:0x40000000@0x0(f
(u-boot)> or (BTLDR)# ubi remove part1 (or part2 if corrupted image is in part2)
(u-boot)> or (BTLDR)# ubi create part1 (or part2 if corrupted image is in part2)
(u-boot)> or (BTLDR)# reset
```

Per i modelli AP 2802, 3802, 4800, 9105, 9115, 9120

1. Quando è collegato alla console, spegnere e riaccendere il punto di accesso.
2. Durante l'avvio, quando viene visualizzato Premere ESC per interrompere l'avvio automatico, premere il tasto Esc
3. In questo modo si dovrebbe andare al prompt (u-boot)>.
4. Esegui questi comandi

```
(u-boot)> ubi part fs
(u-boot)> ubi remove part1 (or part2 if corrupted image is in part2)
(u-boot)> ubi create part1 (or part2 if corrupted image is in part2)
(u-boot)> boot
```

Domande frequenti

Q1) Tutti i miei access point sono collegati al 9800 tramite una connessione LAN ad alta velocità, a bassa latenza e a perdita ridotta. È ancora necessario eseguire quanto sopra?

Questo problema è stato segnalato solo quando si aggiornano gli access point su una connessione WAN.

Q2) Ho nuovi punti di accesso non inclusi. Come è possibile distribuirli senza che si verifichi questo problema?

Anche i nuovi access point non inclusi che scaricano codice su un collegamento WAN con perdita di dati potrebbero essere soggetti a questo problema, se sono stati prodotti prima di dicembre 2023. Si consiglia di posizionare questi AP prima su un WLC locale.

Q3) Ho altre domande su questo problema. A chi posso indirizzarli?

A: Inviare un'e-mail a fn74109-questions@cisco.com.

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).