Comprendere il processo di aggiunta dell'access point con Catalyst 9800 WLC

Sommario

Introduzione

Questo documento descrive in dettaglio il processo di aggiunta dell'access point al Cisco Catalyst 9800 WLC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei punti di accesso wireless (CAPWAP) di controllo e provisioning
- Conoscenze base dell'uso di un controller WLC (Wireless Lan Controller)

Componenti usati

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

- Catalyst 9800-L WLC, Cisco IOS® XE Cupertino 17.9.3
- Access point Catalyst 9120AXE

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.

Premesse

Definizione sessione CAPWAP

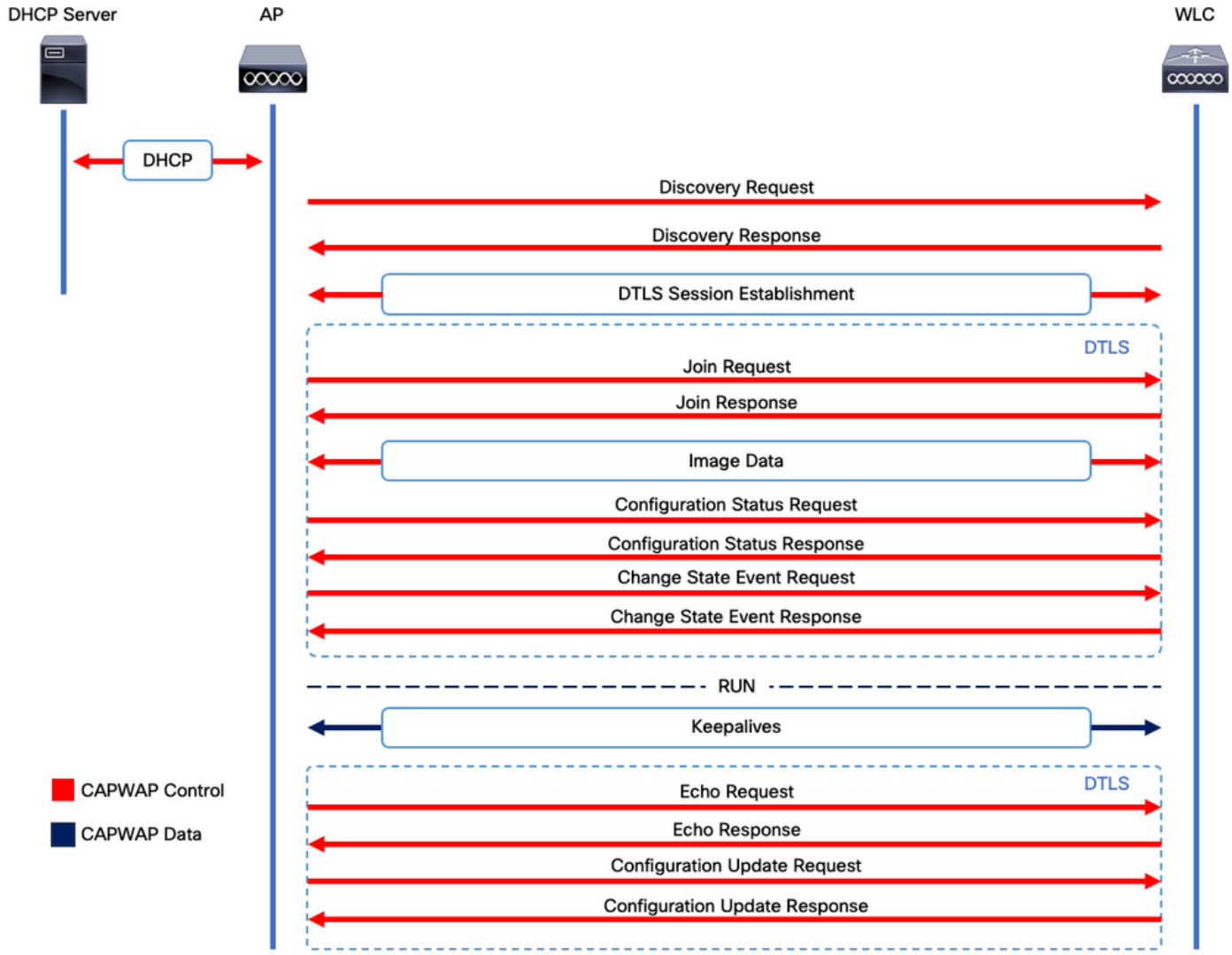
CAPWAP (Control And Provisioning Wireless Access Point) è il protocollo che fornisce il meccanismo di trasporto usato dai punti di accesso (AP) e dai Wireless LAN Controller (WLC) per scambiare le informazioni di controllo e del data plane su un tunnel di comunicazione sicuro (per CAPWAP Control).

Per ulteriori informazioni sul processo di aggiunta all'access point, è importante comprendere il processo di impostazione della sessione CAPWAP (Control And Provisioning Wireless Access Point).

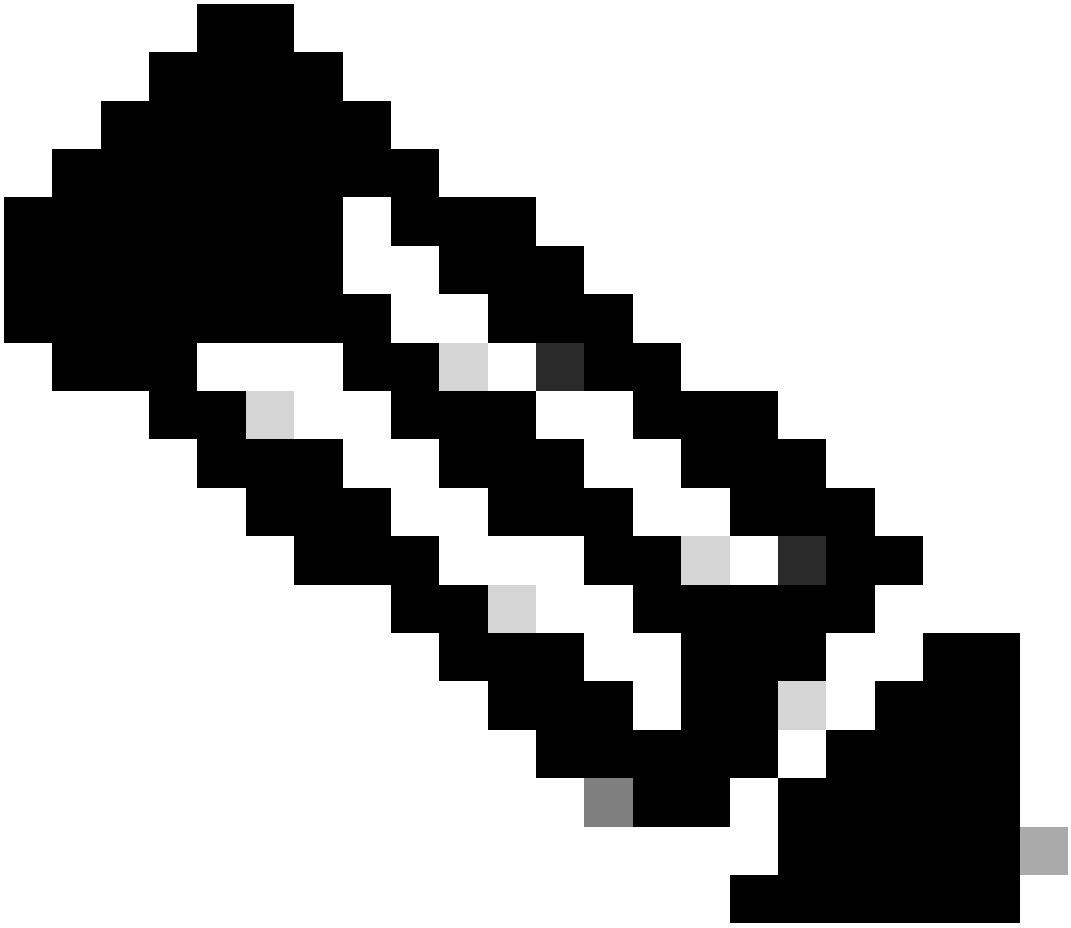
Tenere presente che l'access point deve avere un indirizzo IP prima di poter avviare il processo CAPWAP. Se l'access point non ha un indirizzo IP, non avvia il processo di definizione della sessione CAPWAP.

1. Access Point invia una richiesta di individuazione. Per ulteriori informazioni su questo argomento, vedere la sezione Metodi di rilevamento WLC
2. WLC invia una risposta di individuazione
3. Sessione DTLS stabilita. In seguito, tutti i messaggi vengono crittografati e visualizzati come pacchetti di dati dell'applicazione DTLS in qualsiasi strumento di analisi dei pacchetti.
4. Il punto di accesso invia una richiesta di unione
5. WLC invia una risposta di join
6. AP esegue un controllo dell'immagine. Se ha la stessa versione dell'immagine del WLC, procede con il passaggio successivo. In caso contrario, scarica l'immagine dal WLC e si riavvia per caricare la nuova immagine. In tal caso, ripete il processo dal passaggio 1.

7. Access Point invia una richiesta di stato della configurazione.
8. WLC invia una risposta sullo stato della configurazione
9. Il punto di accesso passa allo stato RUN
10. Durante lo stato RUN, la manutenzione del tunnel CAPWAP viene eseguita in due modi:
    1. I pacchetti keepalive vengono scambiati per gestire il tunnel dei dati CAPWAP
    2. AP invia una richiesta echo al WLC, a cui deve essere risposto con la rispettiva risposta echo. In questo modo si manterrà il tunnel di controllo CAPWAP.



Processo di definizione della sessione CAPWAP



Nota: come da RFC 5415, CAPWAP utilizza le porte UDP 5246 (per il controllo CAPWAP) e 5247 (per i dati CAPWAP).

Definizione sessione DTLS

Dopo che il punto di accesso ha ricevuto una risposta di rilevamento valida dal WLC, viene stabilito un tunnel DTLS tra i due punti per trasmettere tutti i pacchetti successivi su un tunnel protetto. Questo è il processo per stabilire la sessione DTLS:

1. AP invia un messaggio Hello al client
2. WLC invia un messaggio HelloVerifyRequest con un cookie utilizzato per la convalida.
3. AP invia un messaggio ClientHello con un cookie utilizzato per la convalida.
4. WLC invia questi pacchetti in ordine:
    1. ServerHello
    2. Certificato
    3. Scambio chiavi server
    4. Richiesta certificato

    5. FineSalveServer
5. AP invia i pacchetti nel seguente ordine:
    1. Certificato
    2. ScambioChiaviClient
    3. Verifica certificato
    4. CambiaSpecificaCrittografia
6. WLC risponde al ChangeCipherSpec dell'access point con il proprio ChangedCipherSpec:
    1. CambiaSpecificaCrittografia

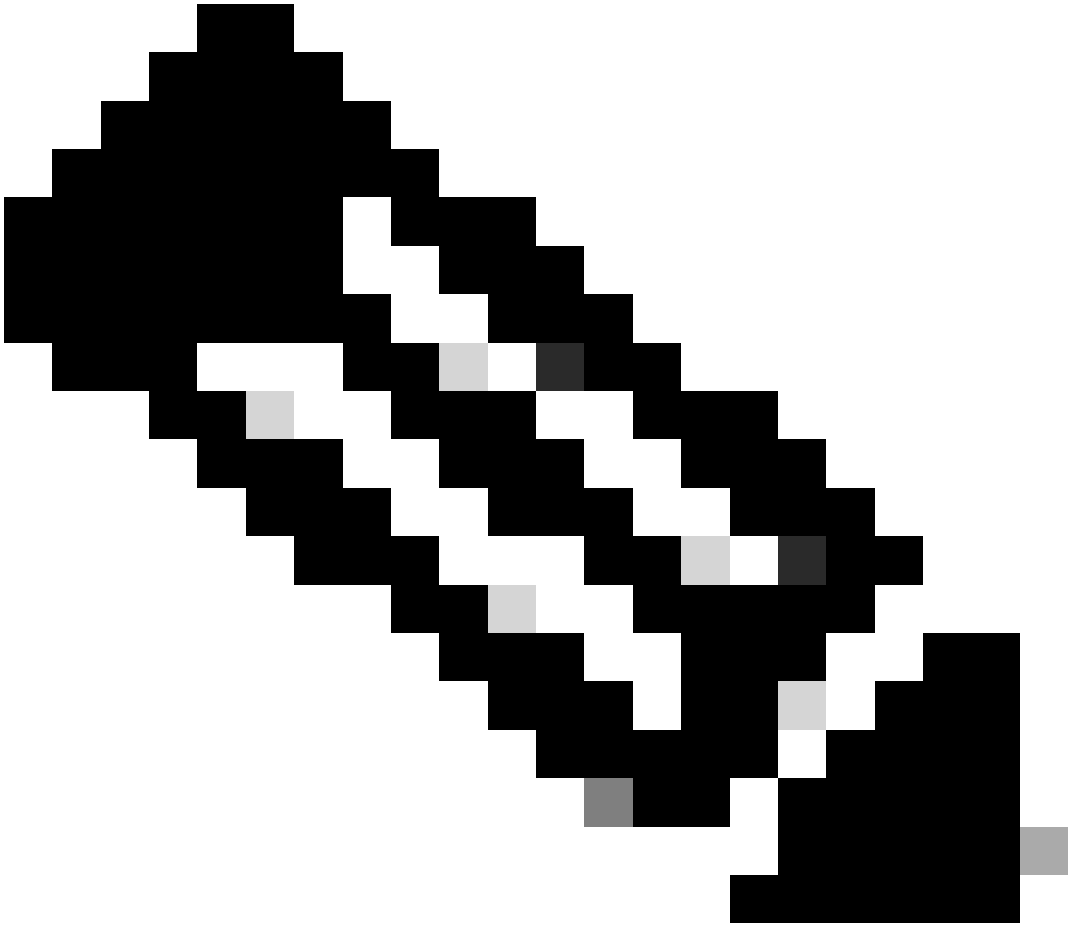
Dopo l'ultimo messaggio ChangedCipherSpec inviato dal WLC, il tunnel sicuro viene stabilito e tutto il traffico inviato in entrambe le direzioni viene ora crittografato.

Metodi di rilevamento controller LAN wireless

Per comunicare ai punti di accesso l'esistenza di un WLC nella rete, sono disponibili diverse opzioni:

- Opzione DHCP 43: questa opzione fornisce agli access point l'indirizzo IPv4 del WLC da unire. Questo processo è utile per installazioni di grandi dimensioni in cui gli AP e il WLC si trovano in siti diversi.
- Opzione DHCP 52: questa opzione fornisce agli access point l'indirizzo IPv6 del WLC da collegare. Il suo utilizzo è comodo nello stesso scenario dell'opzione DHCP 43.
- Individuazione DNS: i punti di accesso eseguono una query sul nome di dominio CISCO-CAPWAP-CONTROLLER.localdomain. È necessario configurare il server DNS per risolvere l'indirizzo IPv4 o IPv6 del WLC da aggiungere. Questa opzione è utile per le distribuzioni in cui i WLC sono archiviati nello stesso sito degli AP.
- Trasmissione di livello 3: gli access point inviano automaticamente un messaggio broadcast a 255.255.255.255. Qualsiasi WLC all'interno della stessa subnet dell'access point deve rispondere a questa richiesta di individuazione.
- Configurazione statica: è possibile usare il comando capwap ap primary-base <wlc-hostname> <wlc-IP-address> per configurare una voce statica per un WLC nell'access point.

    - **Mobility Discovery**: se l'access point è stato precedentemente aggiunto a un WLC che faceva parte di un gruppo di mobilità, l'access point salva anche un record dei WLC presenti in quel gruppo di mobilità.



Nota: i metodi di rilevamento WLC elencati non hanno alcun ordine di precedenza.

Scelta del controller LAN wireless

Dopo aver ricevuto una **risposta di individuazione** da un WLC usando uno dei metodi di individuazione WLC, l'AP seleziona un controller da aggiungere con questo criterio:

- Controller primario (configurato con il comando **capwap ap primary-base <wlc-hostname> <wlc-IP-address>**)
- Controller secondario (configurato con il comando **capwap database-secondario <wlc-hostname> <wlc-IP-address>**)

- Controller terziario (configurato con il comando **capwap ap base-terziary <wlc-hostname> <wlc-IP-address>)**

- Se in precedenza non era stato configurato alcun WLC primario, secondario o terziario, l'AP tenta di unirsi al primo WLC che ha risposto alla richiesta di individuazione con una propria **risposta di individuazione** che ha la capacità massima degli **AP** disponibili (ossia, il **WLC** che può supportare il maggior numero di **AP** in un determinato momento).

Computer di stato CAPWAP

Nella console AP è possibile tenere traccia della macchina a stati CAPWAP, che esegue i passaggi descritti nella sezione Definizione della sessione CAPWAP.

Stato CAPWAP: individuazione

Qui è possibile visualizzare le **richieste di individuazione** e le relative risposte. Osservare come l'access point riceve un IP WLC tramite **DHCP** (opzione 43), e invia anche una **richiesta di rilevamento** ai WLC noti in precedenza:

<#root>

[*09/14/2023 04:12:09.7740]

CAPWAP State: Init

[*09/14/2023 04:12:09.7770]
[*09/14/2023 04:12:09.7770]

CAPWAP State: Discovery

[*09/14/2023 04:12:09.7790]

Discovery Request sent to 172.16.0.20, discovery type STATIC_CONFIG(1)

[*09/14/2023 04:12:09.7800]

Discovery Request

 sent to 172.16.5.11, discovery type STATIC_CONFIG(1)
[*09/14/2023 04:12:09.7800]

Got WLC address 172.16.5.11 from DHCP.

[*09/14/2023 04:12:09.7820]

Discovery Request

 sent to 172.16.0.20, discovery type STATIC_CONFIG(1)
[*09/14/2023 04:12:09.7830]

Discovery Request

 sent to 172.16.5.11, discovery type STATIC_CONFIG(1)
[*09/14/2023 04:12:09.7840]

Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)

[*09/14/2023 04:12:09.7850]

[*09/14/2023 04:12:09.7850]

CAPWAP State: Discovery

[*09/14/2023 04:12:09.7850]

Discovery Response

from 172.16.0.20
[*09/14/2023 04:12:09.8030]

Discovery Response

from 172.16.5.11
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169

Oltre a ricevere una **Discovery Response** da un WLC (172.16.0.20) configurato staticamente e dal WLC indicato dall'opzione DHCP 43 (172.16.5.11), questo access point ha ricevuto una **Discovery Response** da un altro WLC (172.16.5.169) nella stessa subnet perché ha ricevuto il messaggio Broadcast Discovery.

Stato CAPWAP: installazione DTLS.

In questo caso, viene scambiata la sessione DTLS tra l'AP e il WLC.

<#root>

[*09/27/2023 21:50:41.0000]

CAPWAP State: DTLS Setup

```
[*09/27/2023 21:50:41.7140] sudi99_request_check_and_load: Use HARSA SUDI certificat
```

Stato CAPWAP: Join

Dopo aver stabilito la sessione DTLS, viene inviata una **richiesta** di **accesso** al WLC tramite la sessione protetta. Osserva come a questa richiesta viene risposto immediatamente con una **risposta di join** dal WLC

<#root>

[*09/27/2023 21:50:41.9880]

CAPWAP State: Join

[*09/27/2023 21:50:41.9910]

Sending Join request to 172.16.5.11

through port 5270
[*09/27/2023 21:50:41.9950]

Join Response from 172.16.5.11

[*09/27/2023 21:50:41.9950]

AC accepted join request

with result code: 0
[*09/27/2023 21:50:41.9990] Received wlcType 0, timer 30
[*09/27/2023 21:50:41.9990] TLV ID 2216 not found
[*09/27/2023 21:50:41.9990] TLV-DEC-ERR-1: No proc for 2216

Stato CAPWAP: dati immagine

L'access point confronta la sua immagine con l'immagine del WLC. In questo caso, sia la partizione attiva dell'access point che la relativa partizione di backup hanno immagini diverse da quelle del WLC, quindi viene richiamato lo script **upgrade.sh**, che indica all'access point di richiedere l'immagine adeguata al WLC e di scaricarla nella relativa partizione non attiva corrente.

<#root>

[*09/27/2023 21:50:42.0430]

CAPWAP State: Image Data

[*09/27/2023 21:50:42.0430]

AP image version 8.10.185.0 backup 8.10.105.0, Controller 17.9.3.50

[*09/27/2023 21:50:42.0430]

Version does not match.

[*09/27/2023 21:50:42.0680]

upgrade.sh

: Script called with args:[PRECHECK]
[*09/27/2023 21:50:42.1060] do PRECHECK,

part2 is active part

[*09/27/2023 21:50:42.1240]

upgrade.sh

: /tmp space: OK available 101476, required 40000
[*09/27/2023 21:50:42.1250] wtpImgFileReadRequest: request ap1g7, local /tmp/part.tar
[*09/27/2023 21:50:42.1310]

Image Data Request sent to 172.16.5.11

, fileName [ap1g7], slaveStatus 0
[*09/27/2023 21:50:42.1340]

Image Data Response from 172.16.5.11

[*09/27/2023 21:50:42.1340] AC accepted join request with result code: 0
[*09/27/2023 21:50:42.1450] <.....
[*09/27/2023 21:50:55.4980] .....
[*09/27/2023 21:51:11.6290] .....Discarding msg CAPWAP_WTP_EVENT_REQUEST(type
[*09/27/2023 21:51:19.7220] .....
[*09/27/2023 21:51:24.6880] .....
[*09/27/2023 21:51:37.7790] .....
[*09/27/2023 21:51:50.9440] .....> 76738560 bytes, 57055 msgs, 930 last
[*09/27/2023 21:51:59.9160] Last block stored, IsPre 0, WriteTaskId 0
[*09/27/2023 21:51:59.9160]

Image transfer completed from WLC

, last 1

Una volta completato il trasferimento dell'immagine, l'access point avvia un processo di verifica della firma dell'immagine per convalidarla. In seguito, lo script **upgrade.sh** installa l'immagine nella partizione non attiva corrente e scambia la partizione da cui si avvia. Infine, l'access point si ricarica e ripete il processo dall'inizio (**stato CAPWAP: Discover**).

<#root>

[*09/27/2023 21:52:01.1280]

Image signing verify success.

[*09/27/2023 21:52:01.1440]
[*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Shadow is now in-synced with master
[*09/27/2023 21:52:01.1440]
[*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Verifying against bundle image btldr.img...
[*09/27/2023 21:52:01.1570]

upgrade.sh

:

part to upgrade is part1

[*09/27/2023 21:52:01.1780]

upgrade.sh

: AP version1: part1 8.10.105.0, img 17.9.3.50
[*09/27/2023 21:52:01.1960]

upgrade.sh

: Extracting and verifying image in part1...
[*09/27/2023 21:52:01.2080]

upgrade.sh

: BOARD generic case execute
[*09/27/2023 21:52:01.5280]

upgrade.sh

: Untar /tmp/part.tar to /bootpart/part1...
[*09/27/2023 21:52:01.7890]

upgrade.sh

: Sync image to disk...
[*09/27/2023 21:52:31.4970]

upgrade.sh

: status '

Successfully verified image in part1.

'
[*09/27/2023 21:52:32.5270]

upgrade.sh

: AP version2: part1 17.9.3.50, img 17.9.3.50
[*09/27/2023 21:52:32.5540]

upgrade.sh

: AP backup version: 17.9.3.50
[*09/27/2023 21:52:32.5700]

upgrade.sh

:

Finished upgrade task.

[*09/27/2023 21:52:32.5840]

upgrade.sh

: Cleanup for do_upgrade...
[*09/27/2023 21:52:32.5970]

upgrade.sh

: /tmp/upgrade_in_progress cleaned
[*09/27/2023 21:52:32.6090]

upgrade.sh

: Cleanup tmp files ...
[*09/27/2023 21:52:32.6720]

upgrade.sh

: Script called with args:[ACTIVATE]
[*09/27/2023 21:52:32.7100] do ACTIVATE, part2 is active part
[*09/27/2023 21:52:32.7640]

upgrade.sh

: Verifying image signature in part1
[*09/27/2023 21:52:33.7730]

upgrade.sh

: status 'Successfully verified image in part1.'
[*09/27/2023 21:52:33.7850]

upgrade.sh

:

activate part1, set BOOT to part1

[*09/27/2023 21:52:34.2940]

upgrade.sh

:

AP primary version after reload: 17.9.3.50

[*09/27/2023 21:52:34.3070]

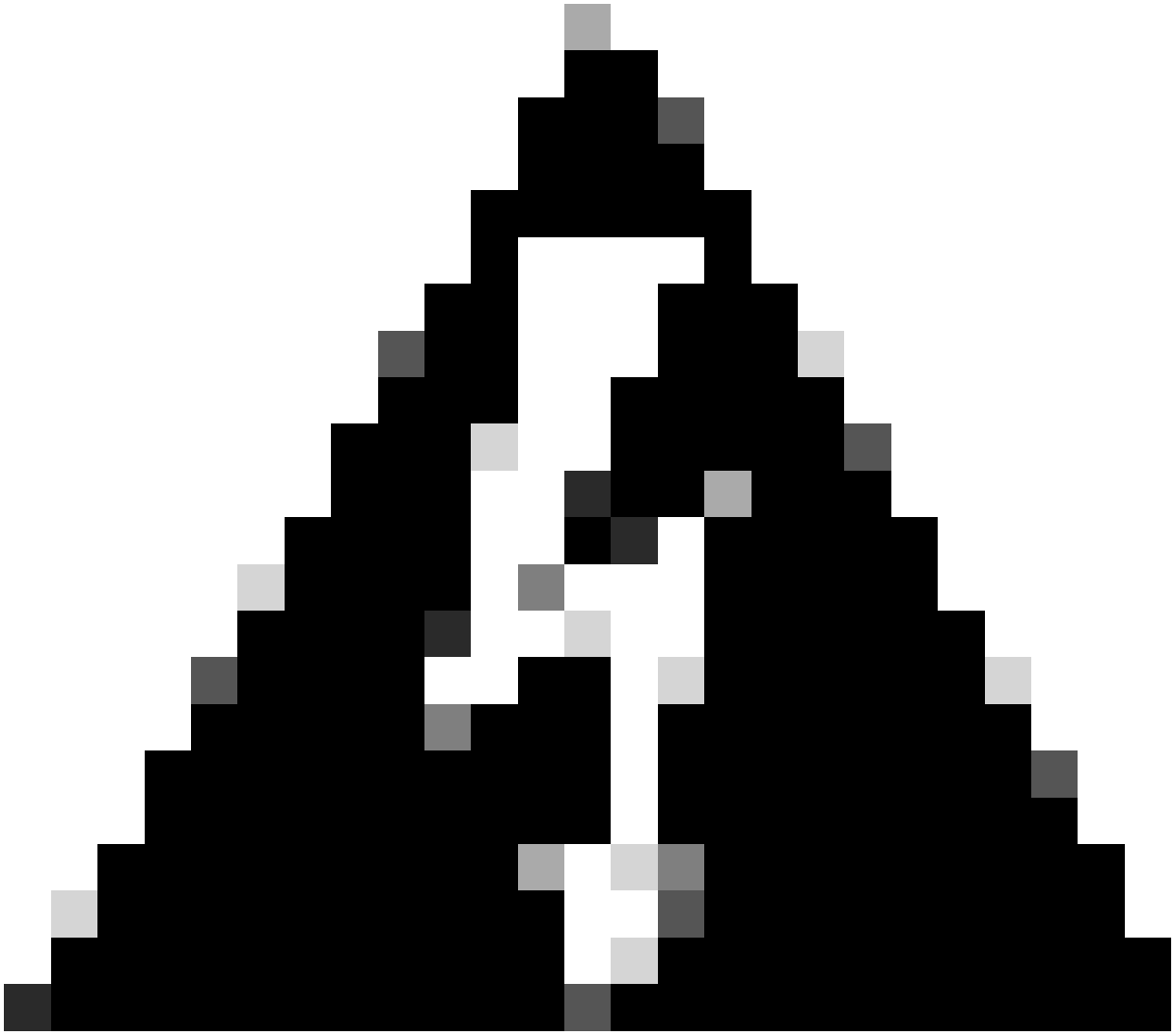
upgrade.sh

: AP backup version after reload: 8.10.185.0
[*09/27/2023 21:52:34.3190]

upgrade.sh

: Create after-upgrade.log
[*09/27/2023 21:52:37.3520]

AP Rebooting: Reset Reason - Image Upgrade



Avviso: i punti di accesso Wave 1 potrebbero non riuscire a scaricare una nuova immagine a causa di un certificato scaduto. Per ulteriori informazioni, fare riferimento all'avviso sui prodotti 72524 e leggere attentamente il documento di supporto relativo al download delle immagini per i punti di accesso IOS non riuscito a causa della scadenza del certificato di firma dell'immagine. Documento di supporto del 4 dicembre 2022 (CSCwd80290) per comprenderne l'impatto e la soluzione.

Una volta che l'access point si ricarica e passa di nuovo attraverso gli stati **CAPWAP Discover** e **Join**, durante lo stato **Image Data** rileva che ora ha l'immagine adeguata.

<#root>

[*09/27/2023 21:56:13.7640]

CAPWAP State: Image Data

[*09/27/2023 21:56:13.7650]

AP image version 17.9.3.50 backup 8.10.185.0, Controller 17.9.3.50

[*09/27/2023 21:56:13.7650]

Version is the same, do not need update.

[*09/27/2023 21:56:13.7650] status '

upgrade.sh: Script called with args:[NO_UPGRADE]

'
[*09/27/2023 21:56:13.7850] do NO_UPGRADE, part1 is active part

Stato CAPWAP: Configurazione

Una volta verificato che ha la stessa versione del WLC, l'AP notifica le sue configurazioni correnti al WLC. In generale, ciò significa che l'access point chiede di mantenere le proprie configurazioni (se sono disponibili nel WLC).

<#root>

[*09/27/2023 21:56:14.8680]

CAPWAP State: Configure

[*09/27/2023 21:56:15.8890] Telnet is not supported by AP, should not encode this payload
[*09/27/2023 21:56:15.8890] Radio [1] Administrative state DISABLED change to ENABLED
[*09/27/2023 21:56:16.0650] Radio [0] Administrative state DISABLED change to ENABLED
[*09/27/2023 21:56:16.0750] DOT11_CFG[1]: Starting radio 1
[*09/27/2023 21:56:16.1150] DOT11_DRV[1]: Start Radio1
[*09/27/2023 21:56:16.1160] DOT11_DRV[1]: set_channel Channel set to 36/20
[*09/27/2023 21:56:16.4380] Started Radio 1
[*09/27/2023 21:56:16.4880] DOT11_CFG[0]: Starting radio 0
[*09/27/2023 21:56:17.5220] DOT11_DRV[0]: Start Radio0
[*09/27/2023 21:56:16.5650] DOT11_DRV[0]: set_channel Channel set to 1/20
[*09/27/2023 21:56:16.5650] Started Radio 0
[*09/27/2023 21:56:16.5890] sensord psage_base init: RHB Sage base ptr a1030000

Stato CAPWAP: Esegui

A questo punto, l'access point è stato aggiunto correttamente al controller. Durante questo stato, il WLC attiva un meccanismo per ignorare la configurazione richiesta dall'AP. È possibile notare che l'access point riceve il push delle **configurazioni di radio e credenziali** e che viene inoltre assegnato al **tag dei criteri predefinito** poiché il WLC non aveva alcuna conoscenza precedente di questo access point.

<#root>

[*09/27/2023 21:56:17.4870]

CAPWAP State: Run

[*09/27/2023 21:56:17.4870]

AP has joined controller

uwu-9800
[*09/27/2023 21:56:17.4940] DOT11_DRV[0]: set_channel Channel set to 1/20
[*09/27/2023 21:56:17.5440] sensord split_glue psage_base: RHB Sage base ptr a1030000
[*09/27/2023 21:56:17.6010] sensord split_glue sage_addr: RHB Sage base ptr a1030000
[*09/27/2023 21:56:17.6230] ptr a1030000
[*09/27/2023 21:56:17.6420]

DOT11_DRV[0]: set_channel Channel set to 1/20

[*09/27/2023 21:56:17.8120]

DOT11_DRV[1]: set_channel Channel set to 36/20

[*09/27/2023 21:56:17.9350] Previous AP mode is 0, change to 0
[*09/27/2023 21:56:18.0160] Current session mode: ssh, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1220] Current session mode: telnet, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1310] Current session mode: console, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1340]

chpasswd: password for user changed

[*09/27/2023 21:56:18.1350]

chpasswd: password for user changed

[*09/27/2023 21:56:18.1520] systemd[1]: Starting Cisco rsyslog client watcher...
[*09/27/2023 21:56:18.1610] Same LSC mode, no action needed
[*09/27/2023 21:56:18.1640] CLSM[00:00:00:00:00:00]: U3 Client RSSI Stats feature is deprecated; can no
[*09/27/2023 21:56:18.1720] systemd[1]: Stopping rsyslog client...
[*09/27/2023 21:56:18.2120] systemd[1]: Starting Cisco syslog service...
[*09/27/2023 21:56:18.2230] systemd[1]: Started Cisco syslog service.
[*09/27/2023 21:56:18.2410] systemd[1]: Started rsyslog client.
[*09/27/2023 21:56:18.2440] AP is in good condition, BLE is off
[*09/27/2023 21:56:18.2510] SET_SYS_COND_INTF: allow_usb state: 1 (up) condition
[*09/27/2023 21:56:18.2530] systemd[1]: Starting dhcpv6 client watcher...
[*09/27/2023 21:56:18.2530] systemd[1]: Stopping DHCPv6 client...
[*09/27/2023 21:56:18.2530] systemd[1]: Starting DHCPv6 client...
[*09/27/2023 21:56:18.2530] systemd[1]: Started DHCPv6 client.
[*09/27/2023 21:56:18.2530] systemd[1]: Started dhcpv6 client watcher.
[*09/27/2023 21:56:18.2560]

Set radio 0 power 4 antenna mask 15

[*09/27/2023 21:56:18.2530]

Set radio 1 power 4 antenna mask 15

[*09/27/2023 21:56:18.2530] Got WSA Server config TLVs
[*09/27/2023 21:56:18.2720]

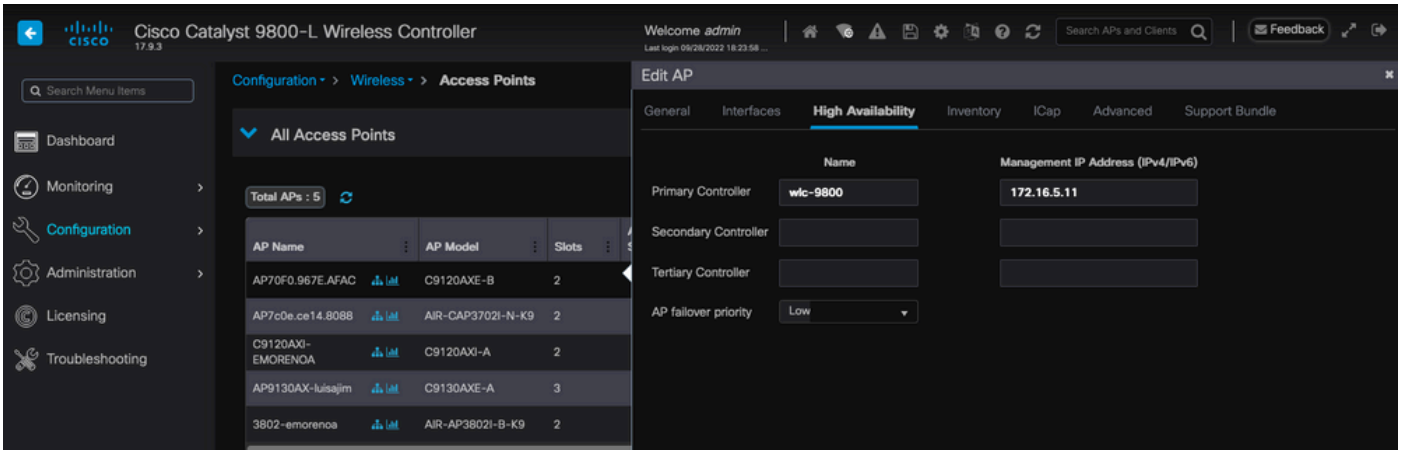
AP tag change to default-policy-tag

[*09/27/2023 21:56:18.2780] Chip flash OK

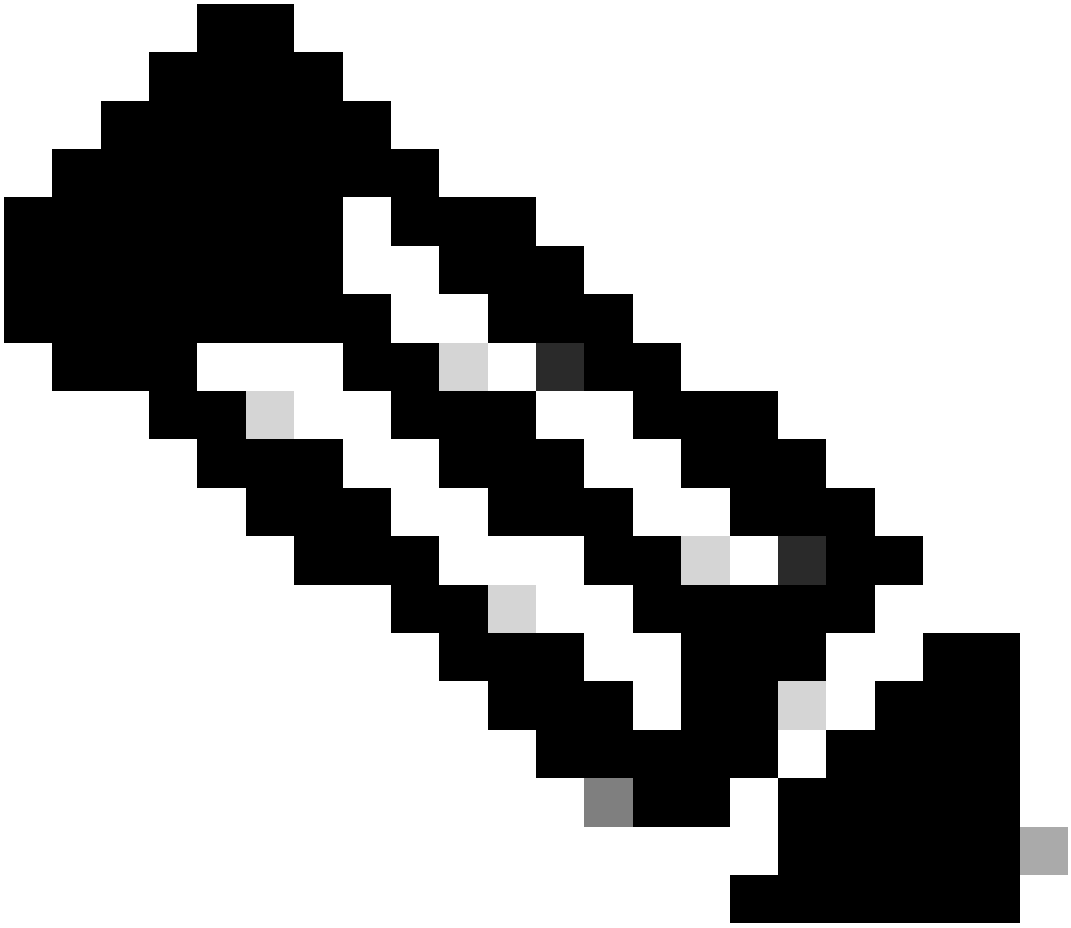
Configurazione

Scelta statica WLC

Dalla GUI, è possibile selezionare **Configuration > Wireless > Access Point**, selezionare un access point e passare alla scheda **High Availability**. È possibile configurare i WLC **principali, secondari e secondari**, come descritto nella sezione Scelta del controller LAN wireless di questo documento. Questa configurazione viene eseguita per punto di accesso.



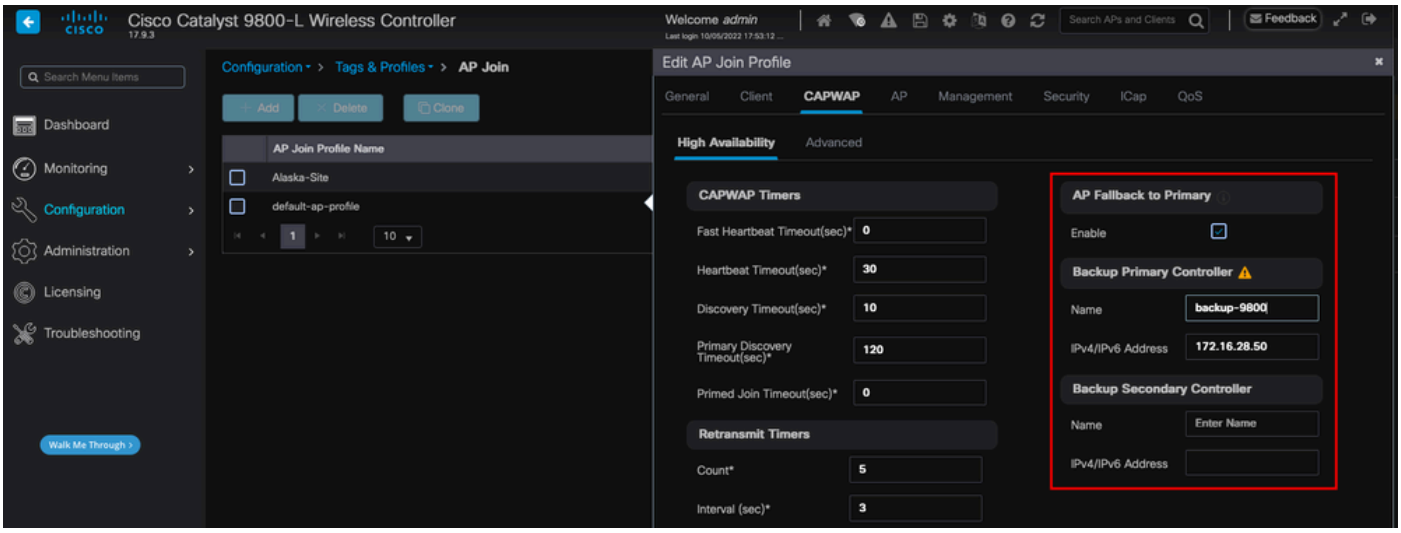
WLC primari, secondari e terziari per un access point.



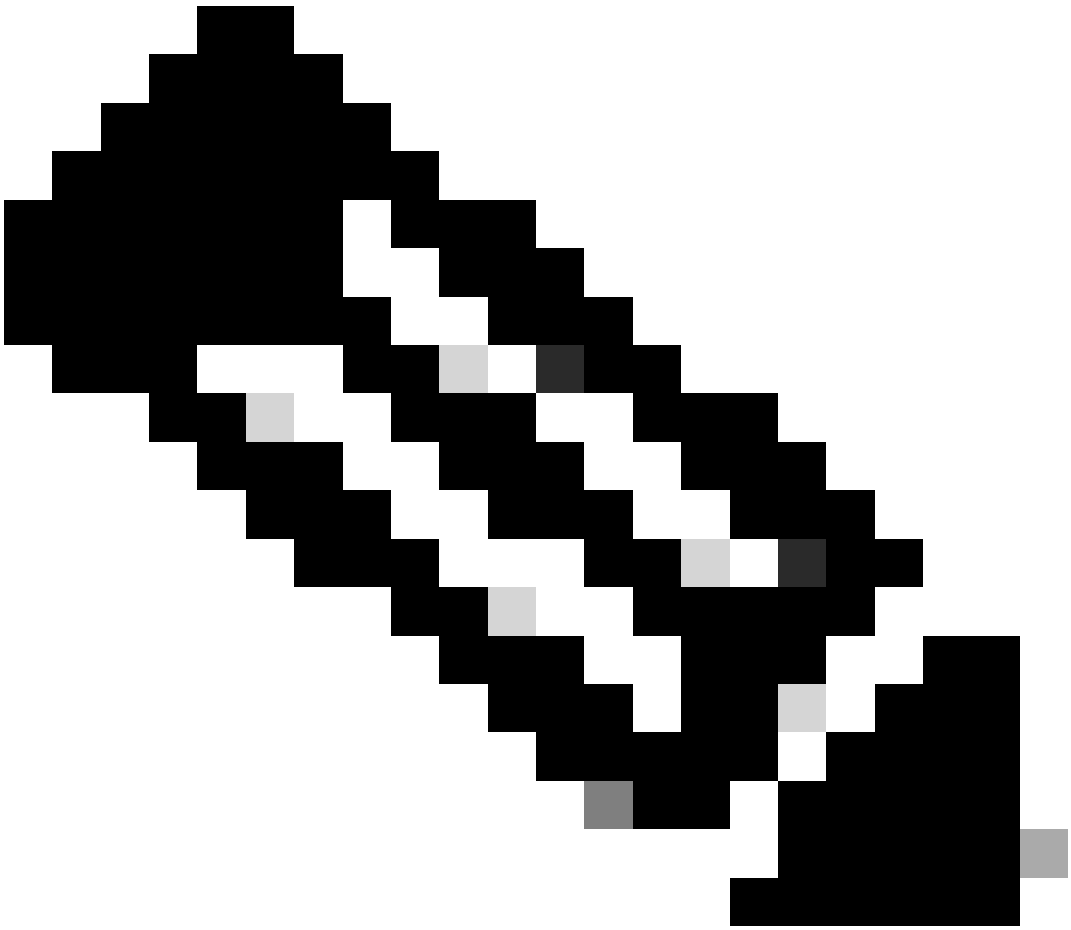
Nota: a partire da Cisco IOS XE 17.9.2, è possibile usare i profili di priming per configurare i controller primario, secondario e terziario per un gruppo di access point che corrispondono alle espressioni regolari (regex) o per un singolo access point. Per ulteriori informazioni, consultare la sezione Fallback dell'access point sui controller configurati in Profilo di priming dell'access point nella guida alla configurazione.

Notare che i controller primario, secondario e terziario configurati nella scheda Alta disponibilità dell'access point sono diversi dai WLC **primari e secondari di backup** che possono essere configurati per **profilo di aggiunta all'access point** nella scheda **CAPWAP > Alta disponibilità.** I **controller primario, secondario e terziario** sono considerati WLC con priorità 1, 2 e 3 rispettivamente, mentre i controller **primario e secondario di backup** sono considerati WLC con priorità 4 e 5.

Se è abilitato il **fallback dell'access point**, l'access point cerca attivamente il **controller primario** quando viene collegato a un **WLC** diverso. L'**AP** cerca solo i **WLC** con priorità 4 e 5 una volta che è presente un evento **CAPWAP Down** e nessuno dei **controller primario e secondario di backup** è disponibile.



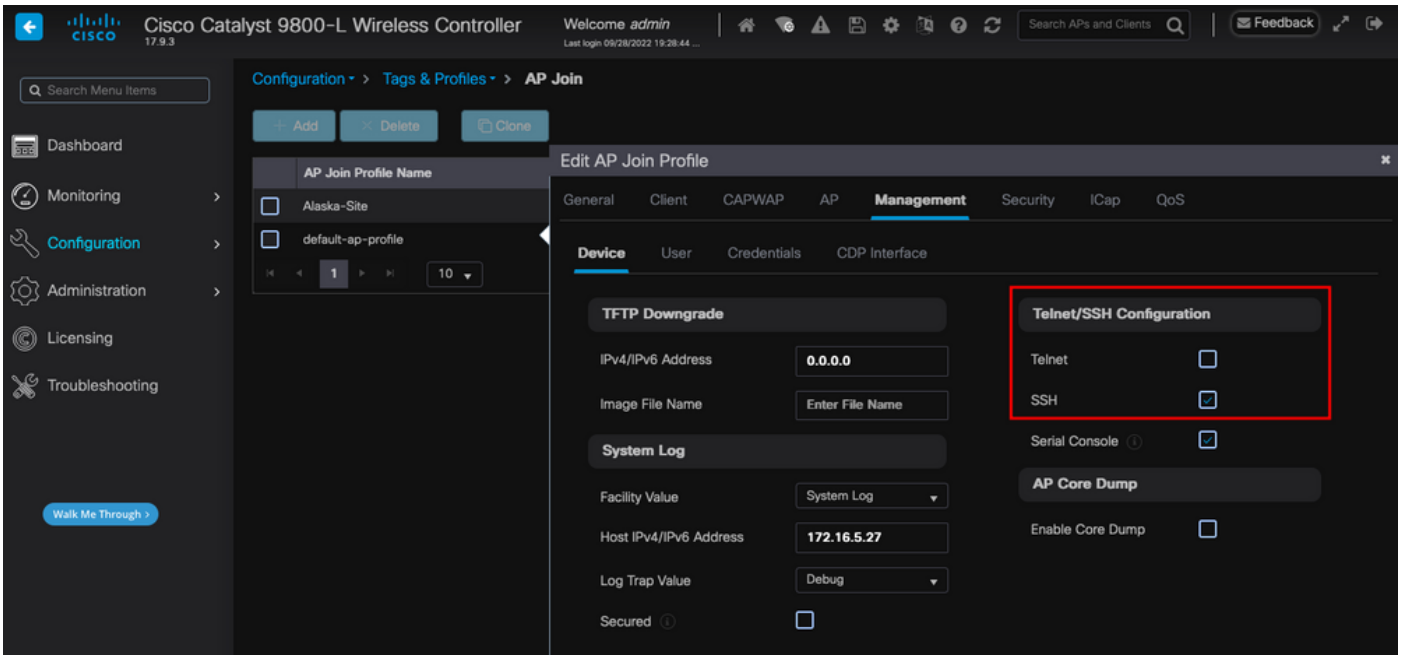
Opzioni di alta disponibilità nel profilo di aggiunta AP



Nota: la configurazione dei WLC primari e secondari di backup nel profilo di join AP non popola le voci **primarie** e **secondarie statiche** nella scheda **Alta disponibilità** del **punto di** accesso.

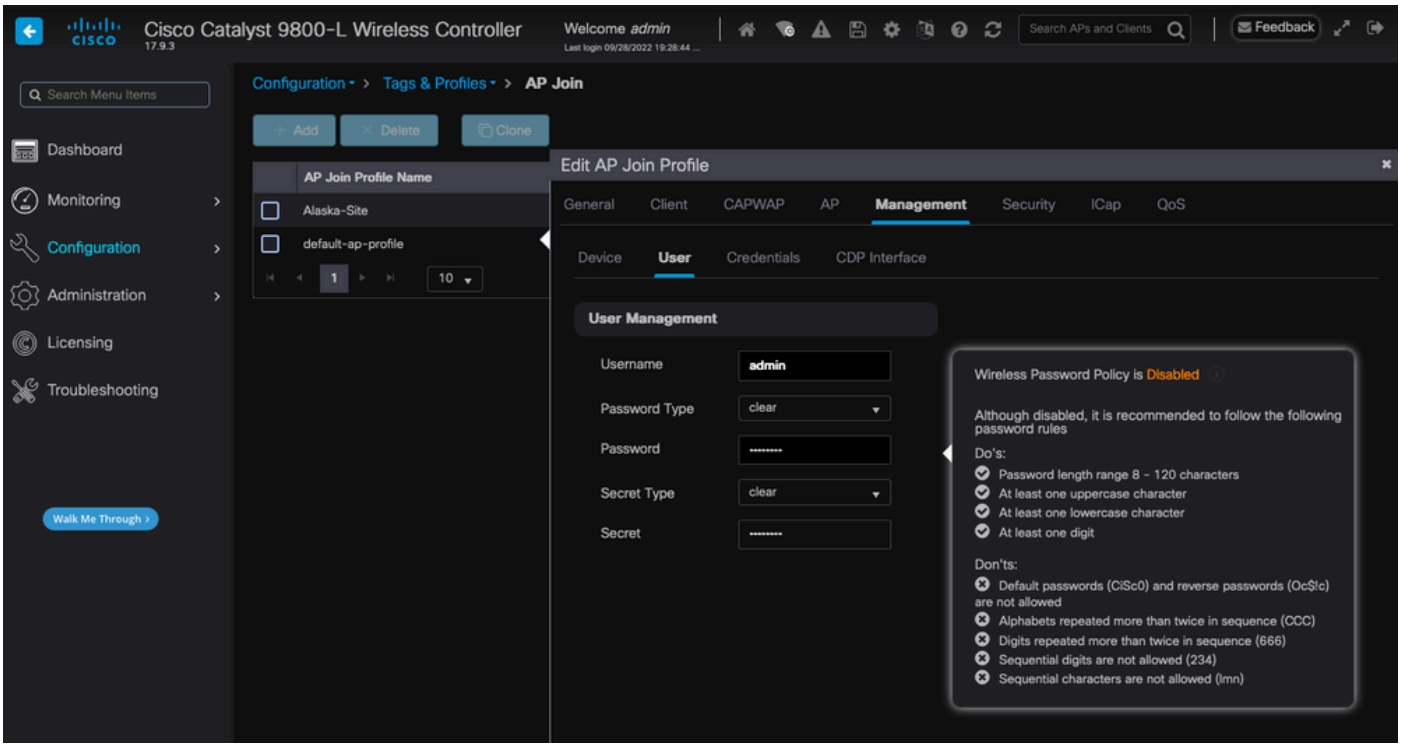
Abilitazione dell'accesso Telnet/SSH all'access point

Selezionare **Configuration > Tags & Profiles > AP Join > Management > Device** (Configurazione > Tag e profili > AP Join > Gestione > Dispositivo), quindi selezionare **SSH** e/o **Telnet**.



Abilitazione dell'accesso Telnet/SSH sul profilo di join AP

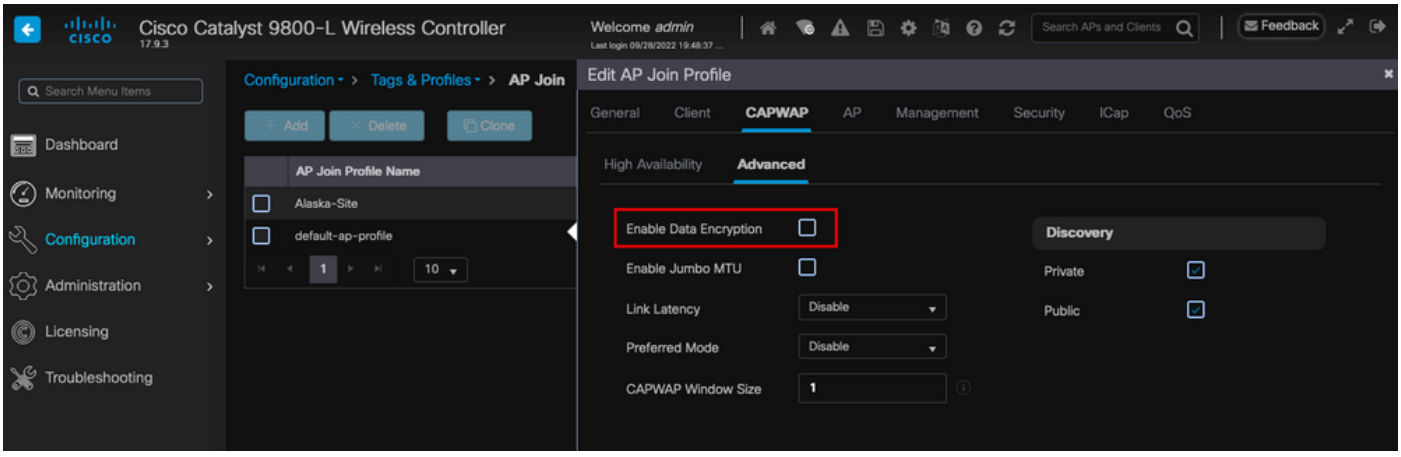
Per configurare le credenziali SSH/Telnet, passare alla scheda **User** (Utente) nella stessa finestra e impostare **Username** (**Nome utente),** **Password** (Password) and **Secret** (Segreto) per accedere all'access point.



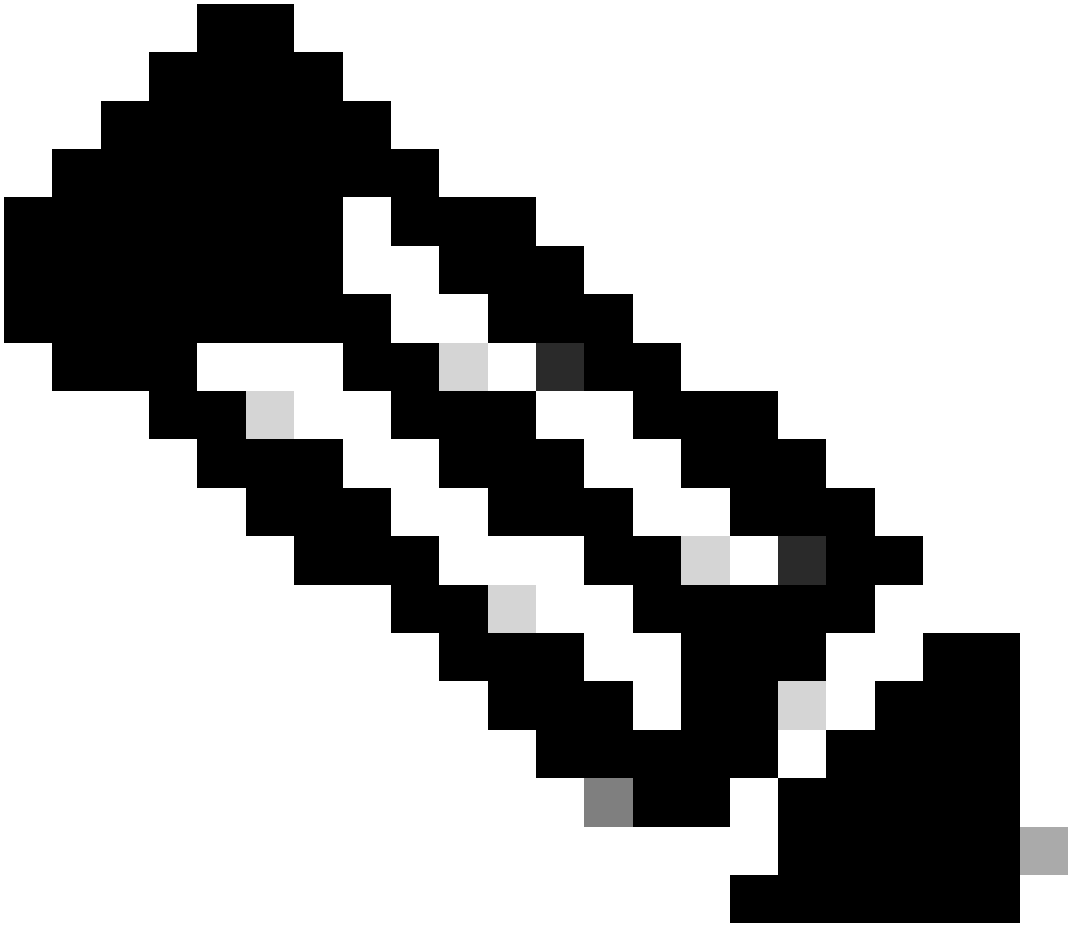
Credenziali SSH e Telnet per l'access point

Crittografia dei collegamenti dati

Per risolvere i problemi dei client che richiedono l'acquisizione di un pacchetto del traffico dell'access point, verificare che **Data Link Encryption** non sia abilitata in **Configuration > Tags & Profiles > AP Join > CAPWAP > Advanced**. In caso contrario, il traffico verrà crittografato.



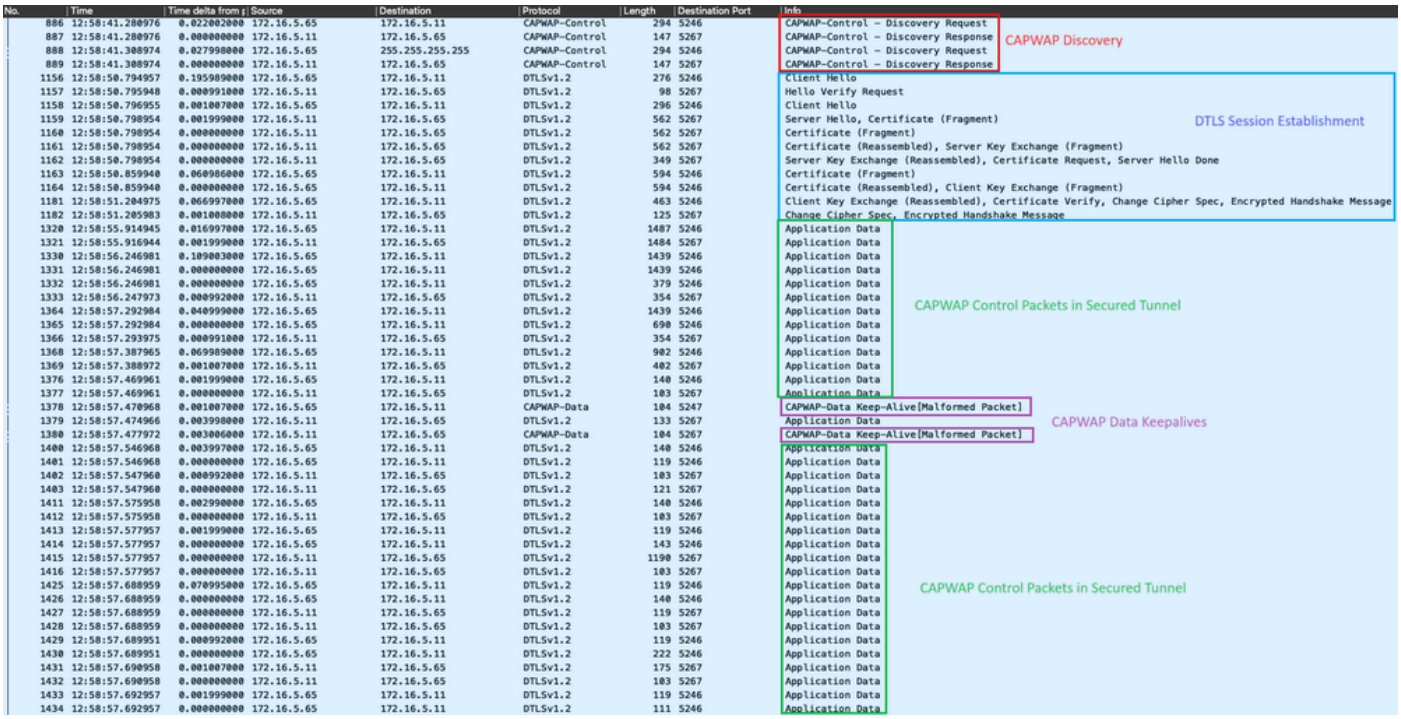
Crittografia dei collegamenti dati



Nota: Data Encryption esegue la crittografia solo del traffico di dati CAPWAP. Il traffico CAPWAP Control è già crittografato tramite DTLS.

Verifica

Oltre a tenere traccia del computer di stato CAPWAP nella console dell'access point, è possibile usare Embedded Packet Capture nel WLC per analizzare il processo di aggiunta dell'access point:



Processo di aggiunta dell'access point rilevato in un'acquisizione di pacchetto incorporata nel WLC

Notare che tutto il traffico successivo al pacchetto **Chance Cipher Spec** (pacchetto n. 1182) viene visualizzato solo come **dati dell'applicazione** su **DTLSv1.2**. Questi sono tutti i dati crittografati dopo la **creazione** della **sessione DTLS**.

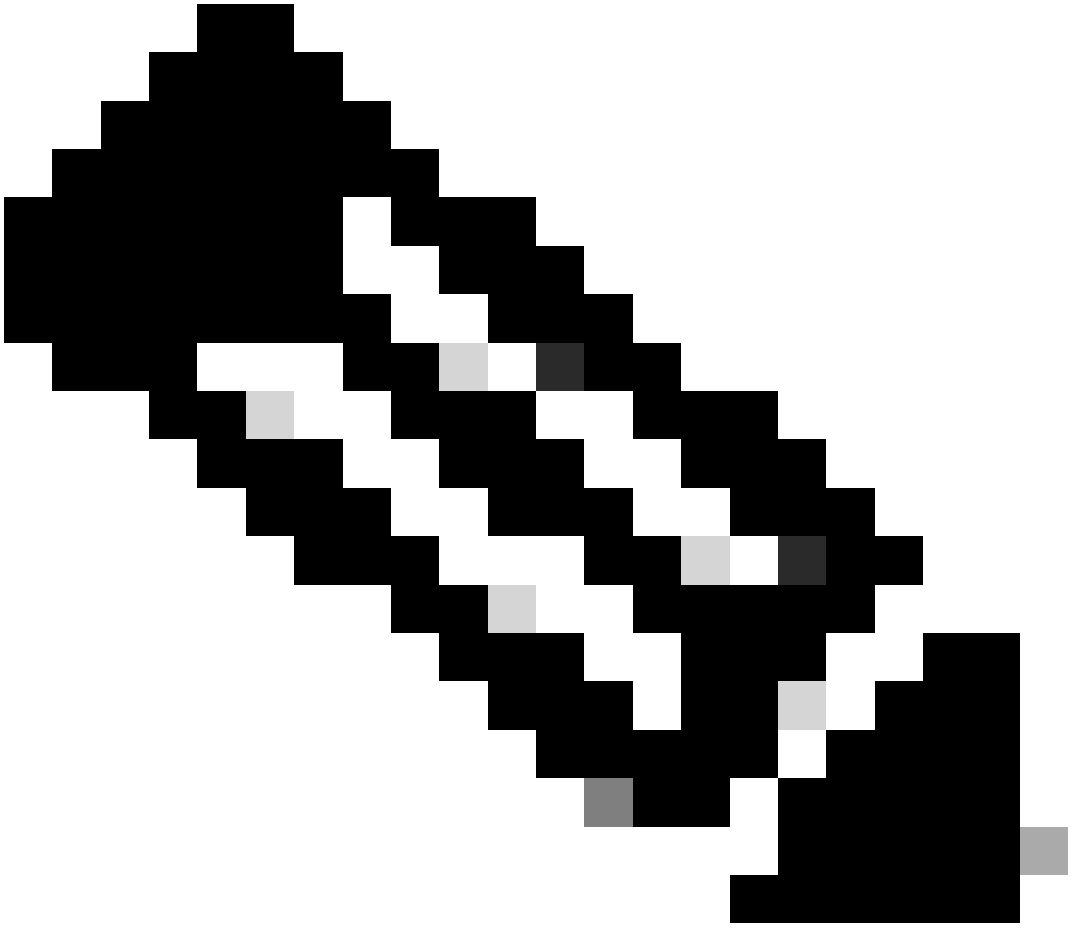
Risoluzione dei problemi

Problemi noti

Fare riferimento ai problemi noti che potrebbero impedire agli access point di unirsi al WLC.

- AP sul loop di avvio a causa di immagine danneggiata nei punti di accesso Catalyst 11ax Wave 2 (CSCvx32806)
- Avviso 72424: i punti di accesso C9105/C9120/C9130 prodotti a partire da settembre 2022 potrebbero richiedere aggiornamenti del software per il collegamento ai Wireless LAN Controller.
- Notifica 72524: durante il downgrade o l'aggiornamento del software, i Cisco IOS AP potrebbero rimanere in stato di download dopo il 4 dicembre 2022. Scadenza del certificato. Si consiglia un aggiornamento del software
- ID bug Cisco CSCwb13784: i punti di accesso non sono in grado di unirsi a 9800 a causa di una MTU del percorso non valida nella richiesta di unione dei punti di accesso
- ID bug Cisco CSCvu22886: C9130: messaggio "unlzma: write: No space left on device" on upgrade to 17.7 Increase max size of /tmp

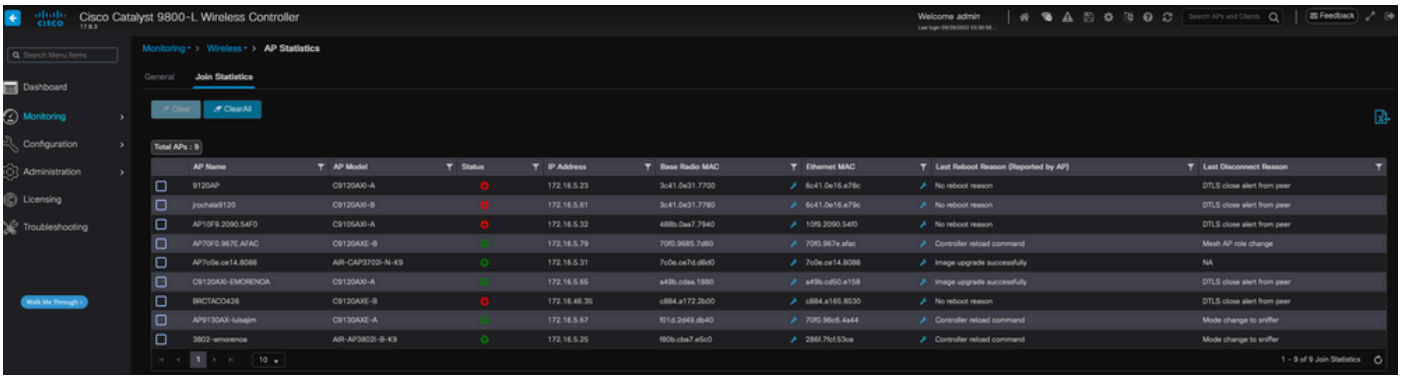
Prima di eseguire l'aggiornamento, consultare sempre la sezione **Percorso** di **aggiornamento** delle Note sulla versione di ciascuna versione.



Nota: a partire da Cisco IOS XE Cupertino 17.7.1, il controller wireless Cisco Catalyst 9800-CL non accetta più di 50 access point se la licenza smart non è connessa e attiva.

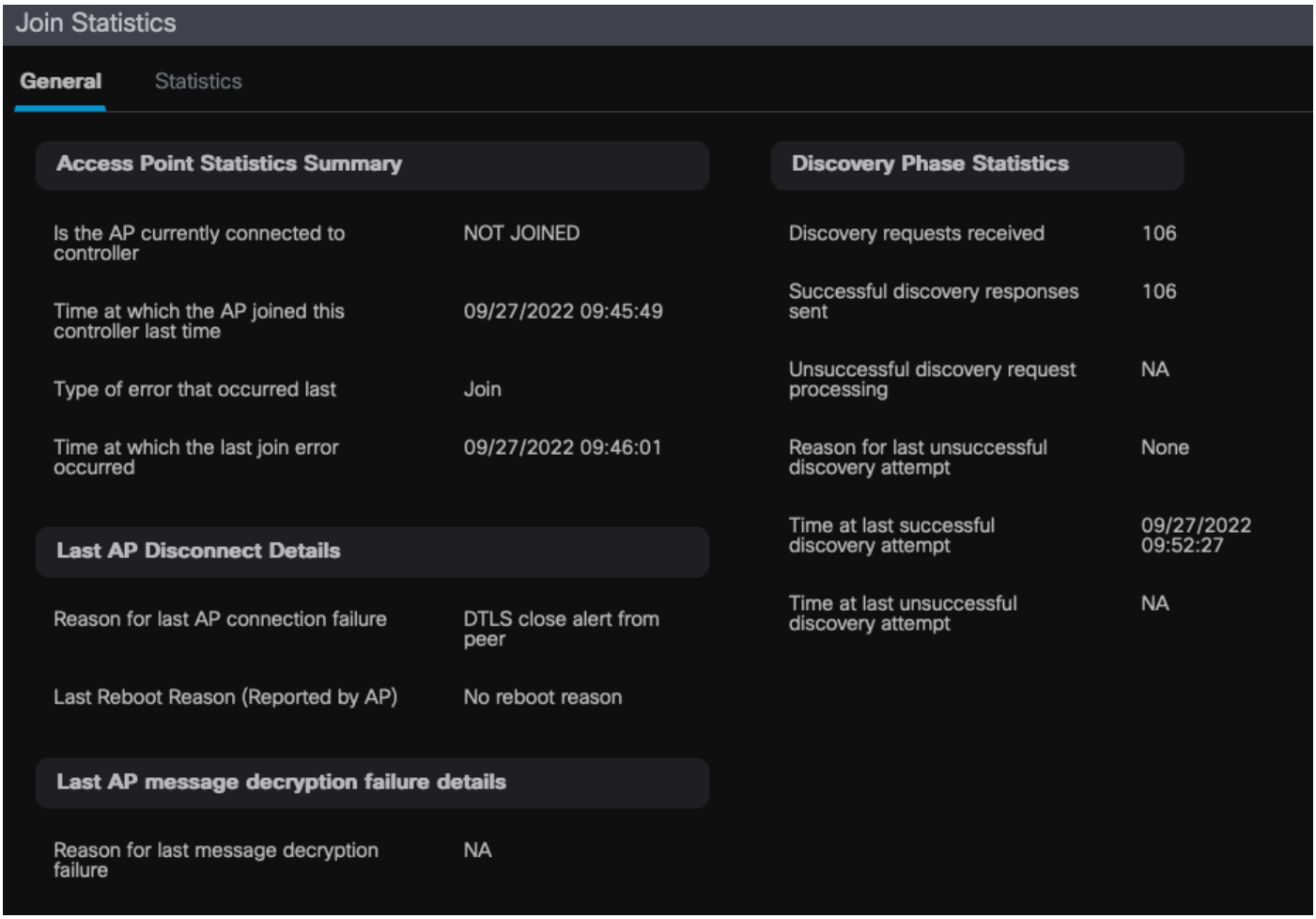
Controlli GUI WLC

Sul WLC, selezionare **Monitoraggio > Wireless > Statistiche access point > Statistiche di accesso** è possibile visualizzare il **motivo dell'ultimo riavvio** segnalato da qualsiasi access point e il motivo dell'**ultima disconnessione** registrato dal WLC.



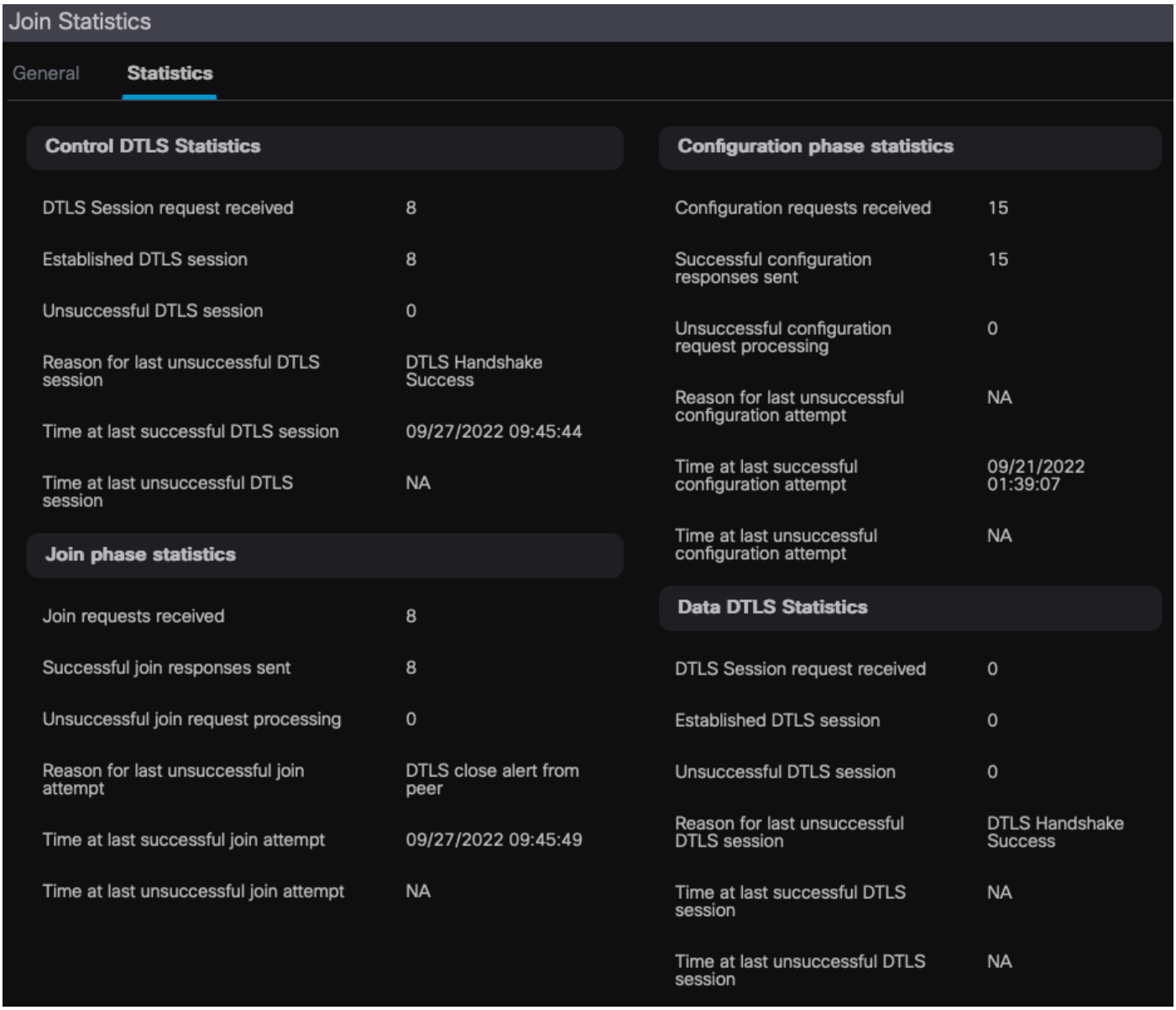
Pagina Statistiche join AP sul WLC

È possibile fare clic su qualsiasi punto di accesso e controllare i dettagli relativi alle statistiche di accesso. Qui è possibile vedere informazioni più dettagliate, come la data e l'ora in cui l'access point è entrato a far parte del WLC e ha tentato di scoprirlo.



Statistiche generali di join AP

Per informazioni più dettagliate, andare alla scheda Statistiche della stessa finestra. Qui è possibile confrontare la quantità di **risposte di join inviate** con la quantità di **richieste di join ricevute**, nonché le **risposte di configurazione inviate** rispetto alle **richieste di configurazione ricevute**.



Statistiche dettagliate di join AP

Comandi

Questi comandi sono utili per risolvere i problemi relativi all'aggiunta dell'access point:

Dal WLC

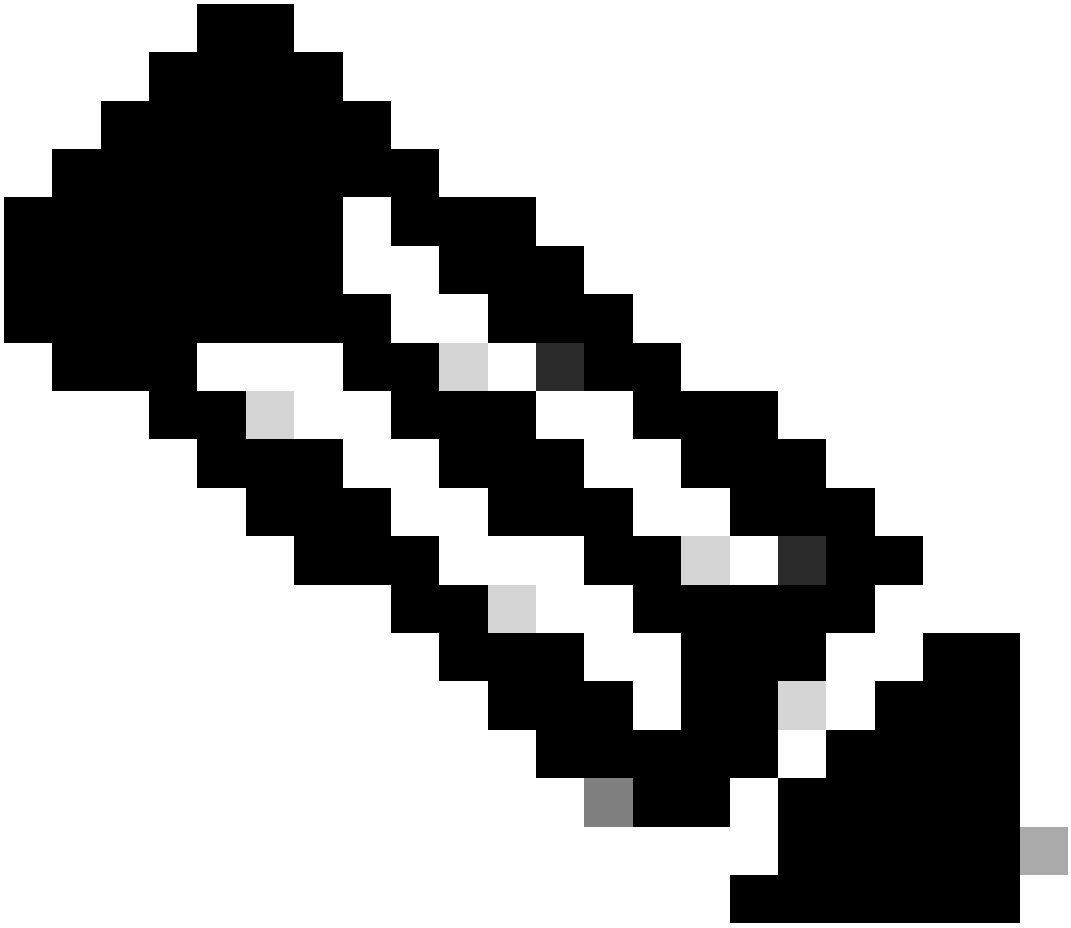
- mostra riepilogo app
- errore debug capwap
- debug capwap packet

Dalla Wave 2 ai Catalyst 11ax AP

    - debug capwap client events
- debug capwap client error
- errore del client debug dtls
- debug evento client dtls
- debug capwap client keepalive
- test di riavvio capwap
- capwap ap erase all

Da access point Wave 1

- cli console debug capwap
- debug capwap client - nessun ricaricamento
- mostra statistiche dtls
- clear cawap ap all-config



Nota: quando si esegue la connessione agli access point in modalità Telnet/SSH per risolvere il problema, usare sempre il comando **terminal monitor** durante la riproduzione del problema dopo aver abilitato i debug sugli access point. In caso contrario, non sarà possibile visualizzare alcun output dai debug.

Tracce radioattive

Un buon punto di partenza per la risoluzione dei problemi di aggiunta all'access point è prendere tracce radioattive degli indirizzi MAC radio ed Ethernet di un access point che ha problemi di aggiunta. Per i dettagli sulla generazione di questi log, consultare la raccolta dei log e del debug sul documento Catalyst 9800 WLC.

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).