

瞭解Catalyst 9800 WLC的AP加入過程

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[建立CAPWAP會話](#)

[DTLS會話建立](#)

[無線LAN控制器探索方法](#)

[無線LAN控制器選擇](#)

[CAPWAP狀態機](#)

[CAPWAP狀態：發現](#)

[CAPWAP狀態：DTLS設定。](#)

[CAPWAP狀態：加入](#)

[CAPWAP狀態：影像資料](#)

[CAPWAP狀態：配置](#)

[CAPWAP狀態：運行](#)

[設定](#)

[靜態WLC選擇](#)

[啟用Telnet/SSH訪問AP](#)

[資料連結加密](#)

[驗證](#)

[疑難排解](#)

[已知的問題](#)

[WLC GUI檢查](#)

[命令](#)

[從WLC](#)

[從Wave 2和Catalyst 11ax AP](#)

[從Wave 1 AP](#)

[放射性痕跡](#)

簡介

本文檔詳細介紹了Cisco Catalyst 9800 WLC的AP加入過程。

必要條件

需求

思科建議您瞭解以下主題：

- 對控制和調配無線存取點(CAPWAP)的基本瞭解
- 基本瞭解無線Lan控制器(WLC)的用法

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9800-L WLC、Cisco IOS® XE Cupertino 17.9.3
- Catalyst 9120AXE存取點

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

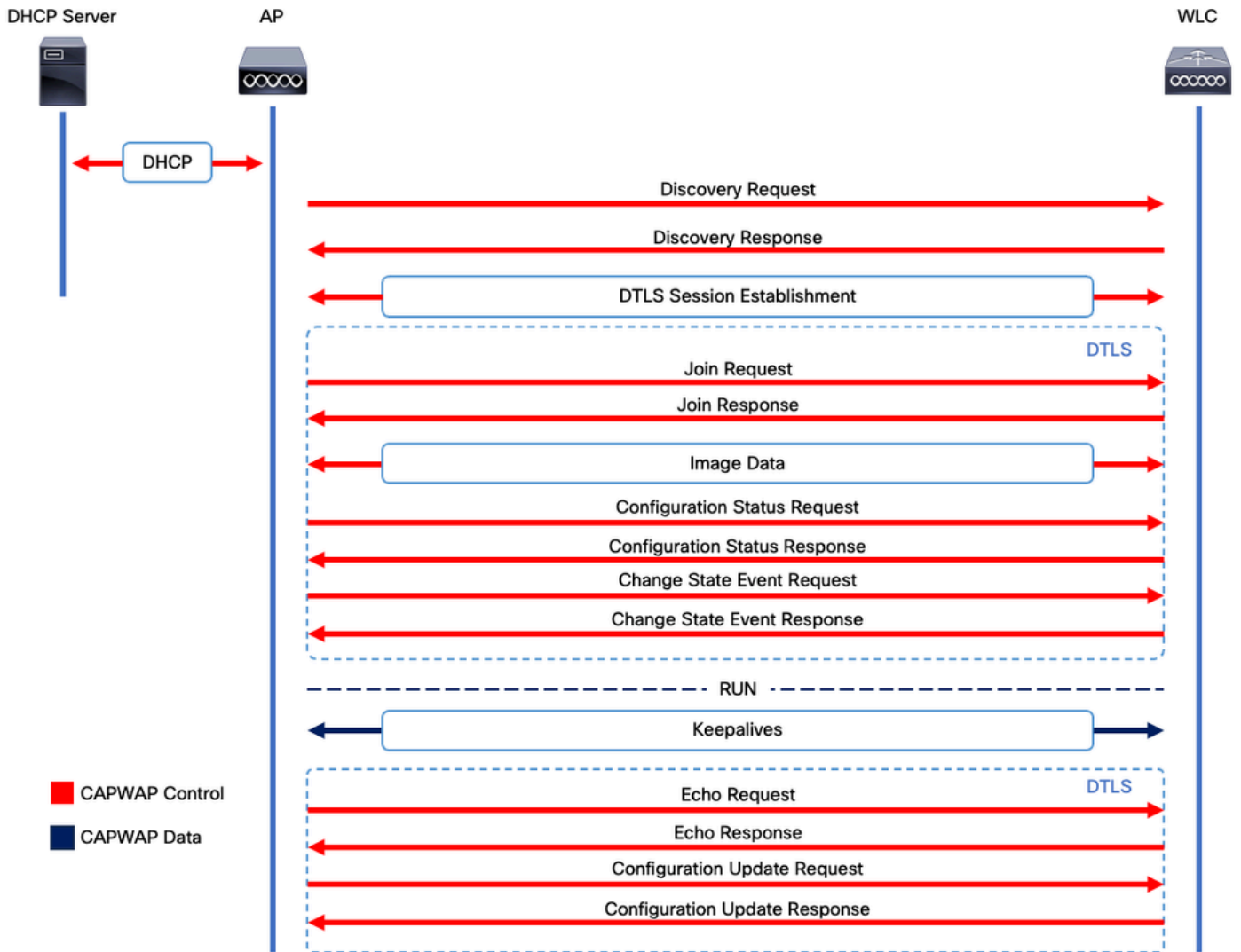
建立CAPWAP會話

控制和設定無線存取點(CAPWAP)是提供存取點(AP)和無線區域網控制器(WLC)使用的傳輸機制的協定，用於透過安全通訊隧道（用於CAPWAP控制）交換控制和資料平面資訊。

要詳細介紹AP加入過程，請務必瞭解控制和調配無線存取點(CAPWAP)會話建立過程。

請記住，AP需要有IP地址才能啟動CAPWAP進程。如果AP沒有IP地址，則不會啟動CAPWAP會話建立過程。

1. 存取點傳送發現請求。有關此過程的詳細資訊，請參閱WLC發現方法部分
2. WLC傳送發現響應
3. DTLS會話建立。之後，所有在此之後傳送的訊息都會經過加密，並在任何封包分析工具中顯示為DTLS應用程式資料封包。
4. 存取點傳送加入請求
5. WLC傳送加入響應
6. AP執行映像檢查。如果它的映像版本與WLC相同，則會繼續進行下一個步驟。如果沒有，則會從WLC下載映像並重新啟動，以載入新映像。在這種情況下，它會重複步驟1中的過程。
7. 存取點傳送配置狀態請求。
8. WLC傳送配置狀態響應
9. 存取點進入RUN狀態
10. 在RUN狀態時，會透過兩種方式執行CAPWAP隧道維護：
 1. 交換Keepalive以維護CAPWAP資料隧道
 2. AP向WLC傳送回應請求，WLC必須使用相應的回應響應做出響應。這是為了維護CAPWAP控制隧道。



CAPWAP會話建立過程

注意：根據RFC 5415，CAPWAP使用UDP埠5246（用於CAPWAP控制）和5247（用於CAPWAP資料）。

DTLS會話建立

一旦存取點收到來自WLC的有效發現響應，就會在它們之間建立DTLS隧道，以透過安全隧道傳輸所有後續資料包。這是建立DTLS會話的過程：

1. AP傳送客戶端Hello消息
2. WLC傳送一條HelloVerifyRequest消息，其中包含用於驗證的Cookie。
3. AP傳送一條ClientHello消息，其中包含用於驗證的cookie。
4. WLC按照以下順序傳送這些資料包：
 1. ServerHello
 2. 憑證
 3. 伺服器金鑰交換
 4. 憑證要求
 5. ServerHelloDone

5. AP按照以下順序傳送這些資料包：

1. 憑證
2. ClientKeyExchange
3. 憑證驗證
4. ChangeCipherSpec

6. WLC使用自己的ChangedCipherSpec響應AP的ChangeCipherSpec：

1. ChangeCipherSpec

在WLC傳送最後一個ChangedCipherSpec消息後，安全隧道建立完成，雙向傳送的所有流量現在都將進行加密。

無線LAN控制器探索方法

有幾種選項可讓存取點知道網路中有一個WLC的存在：

- DHCP選項43：此選項為AP提供要加入的WLC的IPv4地址。對於AP和WLC位於不同站點的大型部署，此過程非常方便。
- DHCP選項52：此選項為AP提供WLC要加入的IPv6地址。在與DHCP選項43相同的場景中，其使用是方便的。
- DNS發現：AP查詢域名CISCO-CAPWAP-CONTROLLER.localdomain。您必須設定DNS伺服器，以解析WLC要加入的IPv4或IPv6位址。對於WLC與AP儲存在同一站點的部署，此選項非常方便。
- 第3層廣播：AP自動向255.255.255.255傳送廣播消息。與AP位於同一子網中的任何WLC都應響應此發現請求。
- 靜態配置：您可以使用 `capwap primary-base <wlc-hostname> <wlc-IP-address>`命令在AP中為WLC配置靜態條目。
- 移動性發現：如果AP之前已加入屬於移動組的WLC，則AP還會儲存該移動組中駐留的WLC的記錄。

注意：列出的WLC發現方法沒有任何優先順序。

無線LAN控制器選擇

一旦AP使用任何WLC發現方法從任何WLC收到發現響應，它將選擇一個控制器加入以下條件：

- 主控制器(使用`capwap primary-base <wlc-hostname> <wlc-IP-address>` 命令配置)
- 輔助控制器(使用`capwap secondary-base <wlc-hostname> <wlc-IP-address>` 命令配置)
- 第三級控制器(使用`capwap tertiary-base <wlc-hostname> <wlc-IP-address>` 命令配置)

- 如果之前未配置任何主WLC、輔助WLC或第三WLC，則AP會嘗試加入第一個WLC(用其自己的發現響應具有最大可用AP容量的發現響應)(即可在指定時間支援最多AP的WLC)。

CAPWAP狀態機

在AP控制檯中，您可以跟蹤CAPWAP狀態機，該狀態機將執行CAPWAP會話建立一節中描述的步驟。

CAPWAP狀態：發現

您可以在此處檢視發現請求和響應。觀察AP如何透過DHCP (選項43) 接收WLC IP，以及如何向先前已知的WLC傳送發現請求：

```
<#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

此AP除了從靜態配置的WLC (172.16.0.20)和透過DHCP選項43 (172.16.5.11)指示的WLC接收發現響應外，還從同一子網中的另一個WLC (172.16.5.169)接收了發現響應，因為它收到了廣播發現消息。

CAPWAP狀態：DTLS設定。

此處，交換AP與WLC之間的DTLS會話。

<#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 HARSА SUDI certificat

CAPWAP狀態：加入

建立DTLS會話後，現在將透過安全會話向WLC傳送加入請求。觀察此請求如何立即從WLC得到加入響應的響應

<#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

CAPWAP狀態：影像資料

AP將其映像與WLC映像進行比較。在這種情況下，AP的活動分割槽及其備份分割槽與WLC的映像不同，因此它會呼叫**upgrade.sh**指令碼，該指令碼指示AP向WLC請求足夠的映像，並將其下載到當前的非活動分割槽中。

<#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 msg, 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

映像傳輸完成後，AP將啟動映像簽名驗證過程以驗證映像傳輸。執行此操作後，upgrade.sh指令碼將映像安裝到當前非活動分割槽，並交換該映像啟動時所在的分割槽。最後，AP重新載入自己並從頭重複該過程(CAPWAP狀態：發現)。

<#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]

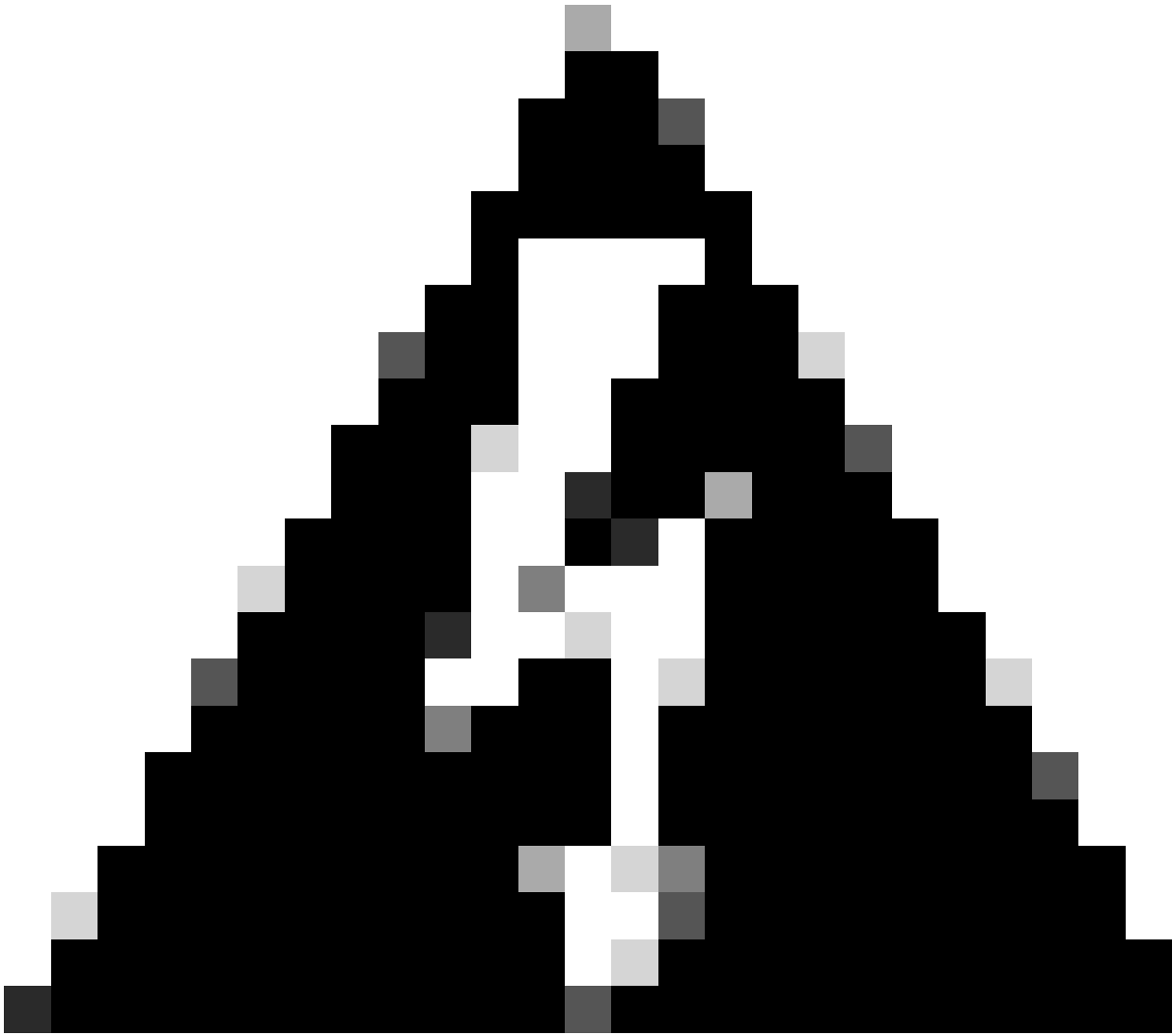
upgrade.sh

: 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



警告：由於證書過期，Wave 1存取點可能無法下載新映像。有關詳細資訊，請參閱[Field Notice 72524](#)，並仔細閱讀[2022年12月4日以後由於映像簽名證書過期而導致的IOS AP映像下載失敗\(CSCwd80290\)支援文檔](#)以瞭解其影響和解決方案。

一旦AP重新載入並再次進入CAPWAP Discover和Join狀態，在Image Data狀態期間，它會檢測到它現在已有足夠的映像。

<#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

CAPWAP狀態：配置

AP驗證其版本與WLC相同後，會向WLC通知其當前配置。一般而言，這表示AP會要求維護其組態（如果WLC中有這些組態）。

<#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

CAPWAP狀態：運行

此時，AP已成功加入控制器。在此狀態下，WLC會觸發一個機制來覆蓋AP請求的配置。您可以看到，AP被推送了無線電和憑據配置，並且它還被分配到預設策略標籤，因為WLC之前不知道此AP。

<#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]
```

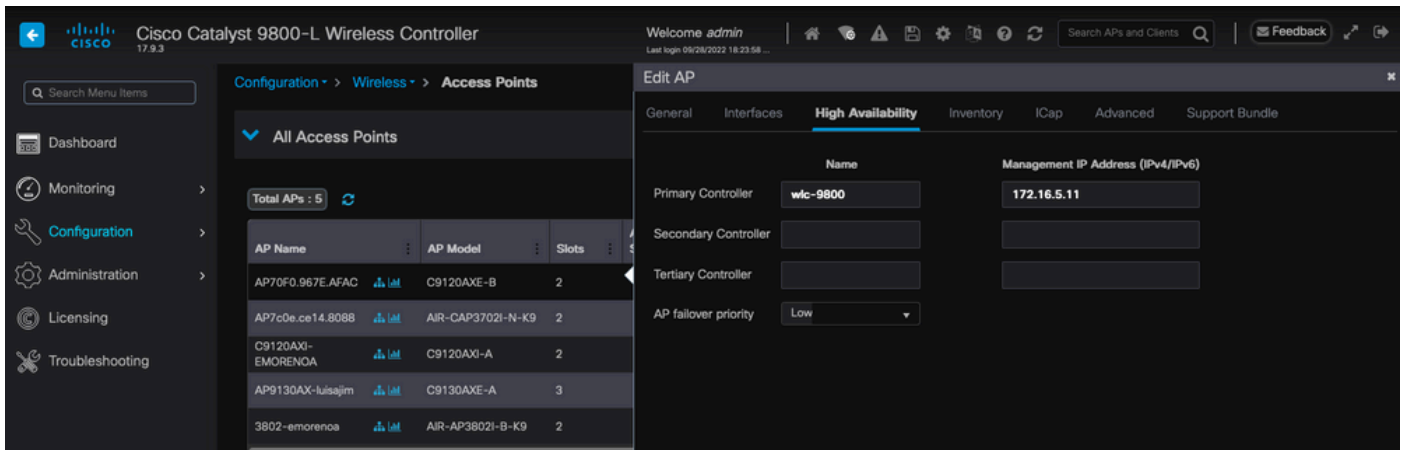
AP tag change to default-policy-tag

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

設定

靜態WLC選擇

在GUI中，您可以轉到**Configuration > Wireless > Access Points**，選擇AP並轉到**High Availability**頁籤。在這裡，您可以配置主、輔助和第三WLC，如本文檔的無線LAN控制器選擇部分所述。此配置按存取點進行。

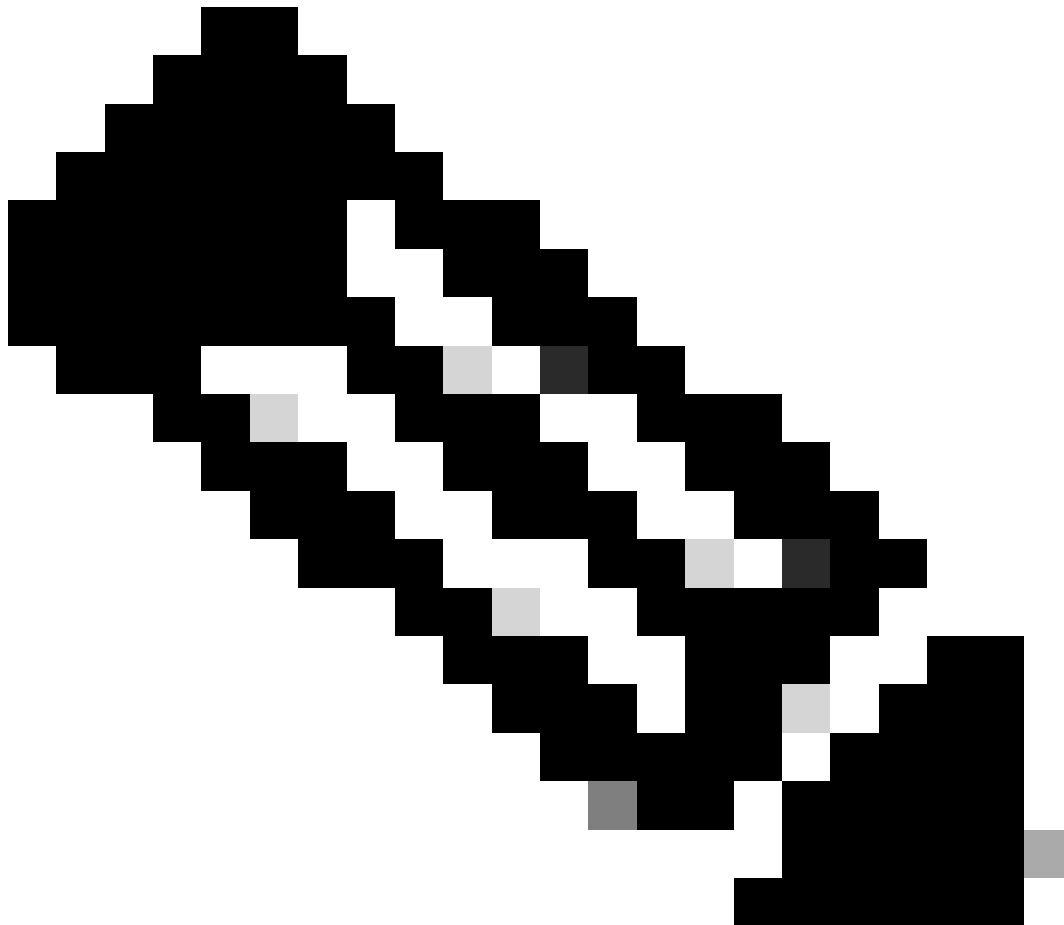


The screenshot displays the Cisco Catalyst 9800-L Wireless Controller GUI. The main navigation pane on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The central pane shows the 'All Access Points' configuration, with a table listing five APs. The right pane is the 'Edit AP' configuration, specifically the 'High Availability' tab, which allows setting the Primary, Secondary, and Tertiary controllers and the AP failover priority.

AP Name	AP Model	Slots
AP70F0.967E.AFAC	C9120AXE-B	2
AP7c0e.ce14.8088	AIR-CAP3702I-N-K9	2
C9120AXI-EMORENOA	C9120AXI-A	2
AP9130AX-luisajlm	C9130AXE-A	3
3802-emorenoa	AIR-AP3802I-B-K9	2

Field	Name	Management IP Address (IPv4/IPv6)
Primary Controller	wlc-9800	172.16.5.11
Secondary Controller		
Tertiary Controller		
AP failover priority	Low	

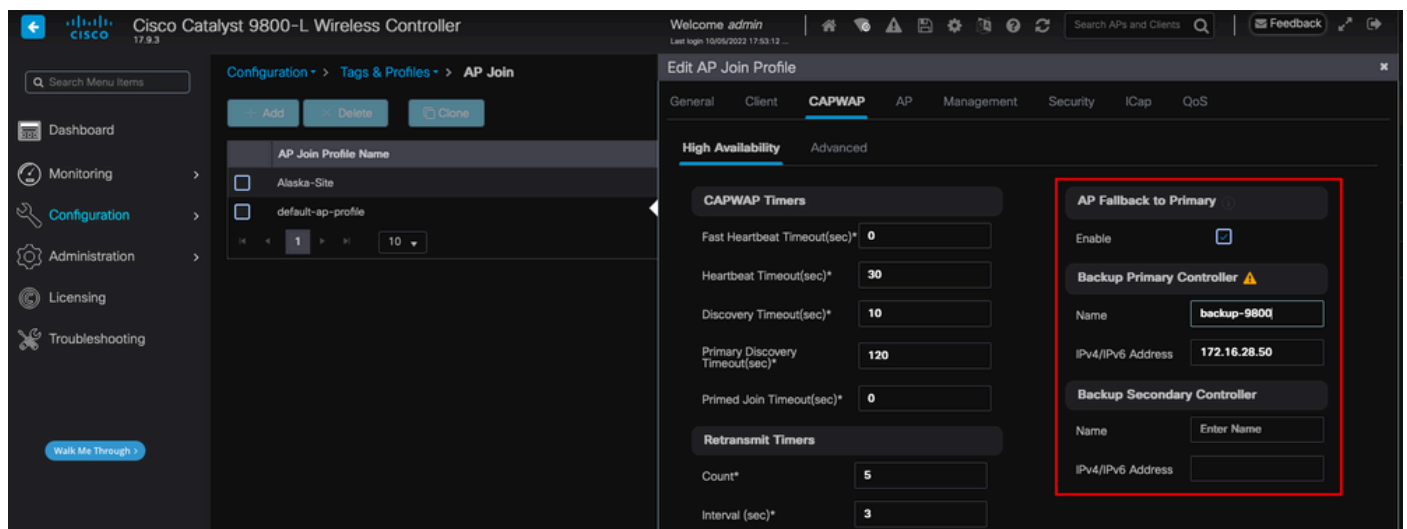
AP的主WLC、輔助WLC和第三WLC。



注意：從Cisco IOS XE 17.9.2開始，您可以使用啟動配置檔案，為匹配正規表示式(regex)的一組AP或單個AP配置主要、次要和第三控制器。有關更多資訊，請參閱[配置指南](#)的[AP回退到在AP啟動配置檔案下配置的控制器](#)部分。

請注意，在AP High Availability頁籤中配置的主要、次要和第三控制器與Backup Primary和Secondary WLC不同，後者可在CAPWAP > High Availability頁籤下根據AP加入配置檔案進行配置。主要、次要和第三控制器分別被視為具有優先順序1、2和3的WLC，而備份主要和輔助控制器則被視為具有優先順序4和5的WLC。

如果啟用了AP Fallback，當加入另一個WLC時，AP將主動查詢主控制器。只有發生CAPWAP Down事件並且沒有可用的備份主控制器和備用控制器時，AP才會查詢優先順序為4和5的WLC。



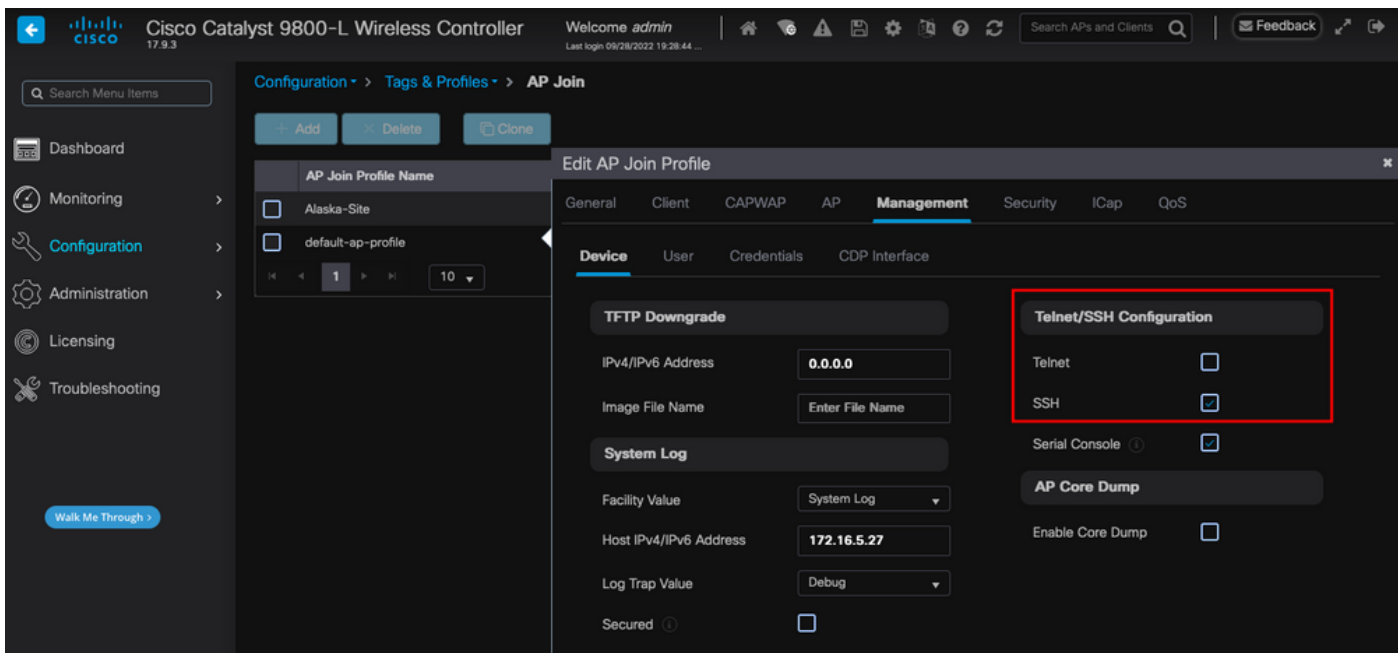
AP加入配置檔案中的高可用性選項



注意：在AP加入配置檔案中備份主WLC和備份輔助WLC的配置不填充存取點的High Availability頁籤中的Static Primary和Secondary條目。

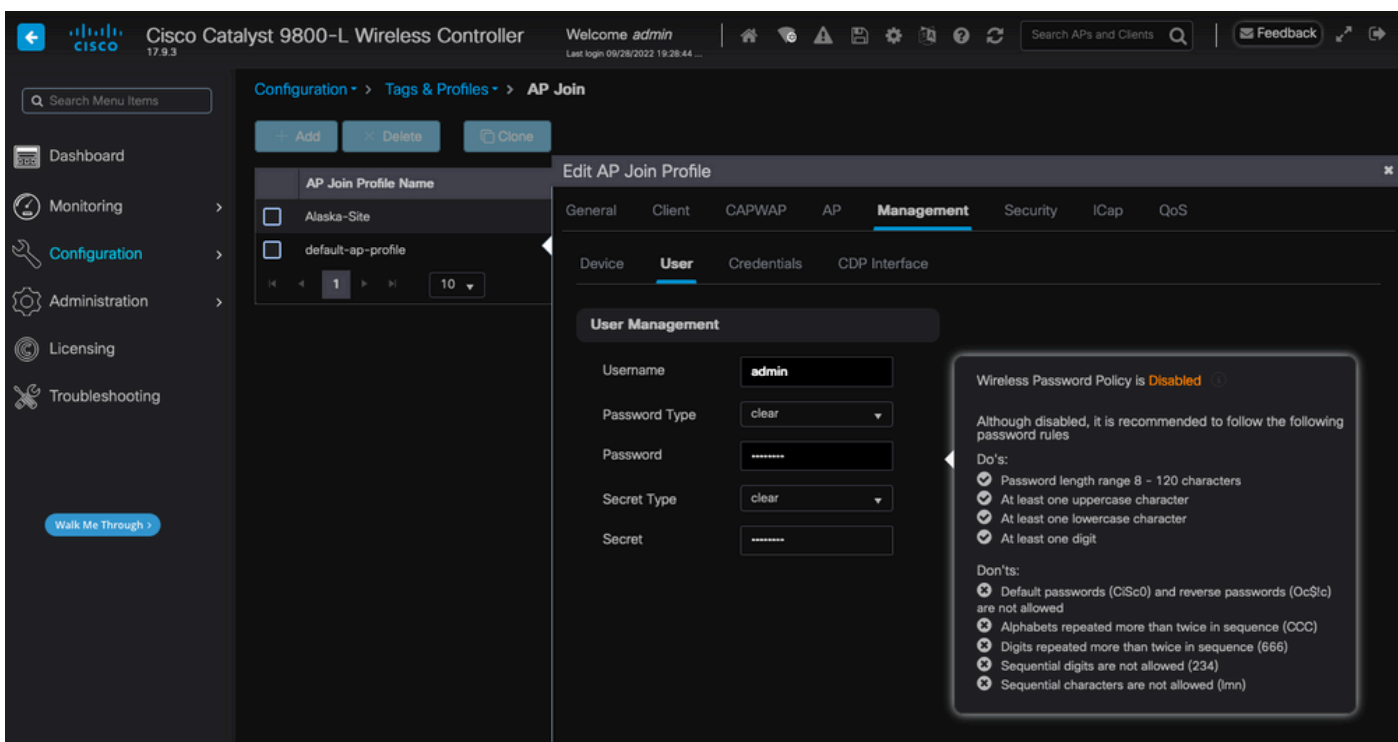
啟用Telnet/SSH訪問AP

轉至Configuration > Tags & Profiles > AP Join > Management > Device，然後選擇SSH和/或Telnet。



在AP加入配置檔案中啟用Telnet/SSH訪問

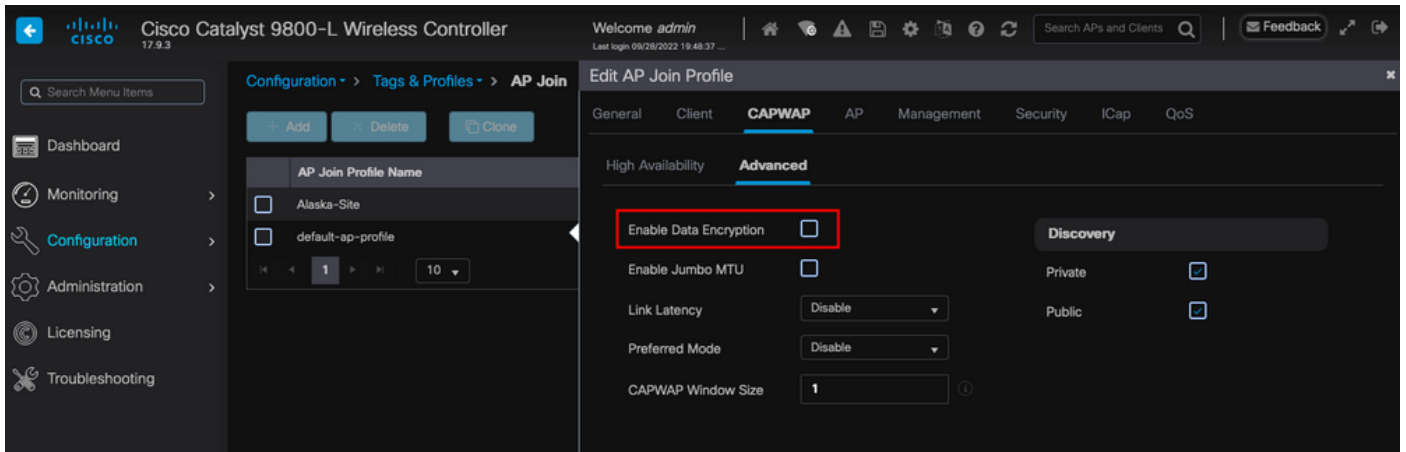
要配置SSH/Telnet憑證，請導航到同一窗口中的User頁籤，然後設定Username、Password和Secret以訪問AP。



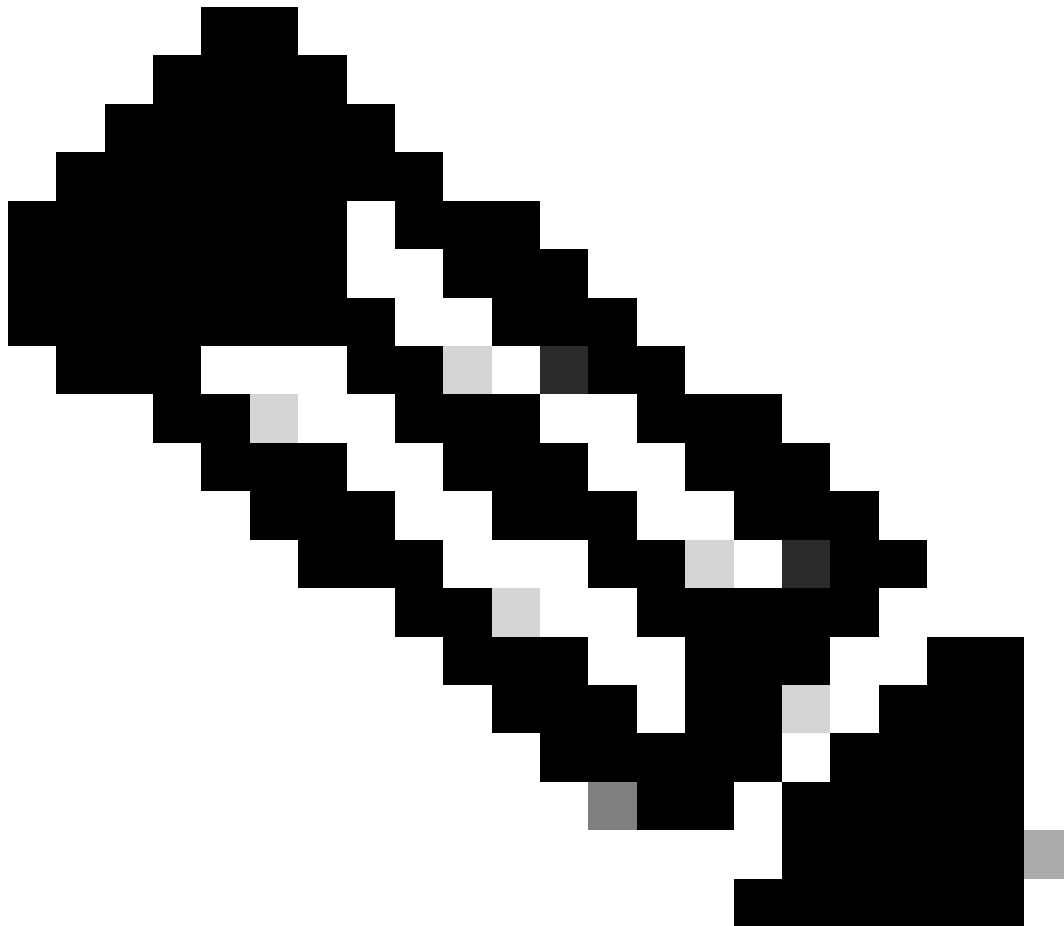
AP的SSH和Telnet憑證

資料連結加密

如果需要排除要求對AP資料流進行資料包捕獲的任何客戶端問題，請確保未在Configuration > Tags & Profiles > AP Join > CAPWAP > Advanced下啟用Data Link Encryption。否則，您的流量會經過加密。



資料連結加密



注意：資料加密僅加密CAPWAP資料流量。CAPWAP控制流量已透過DTLS加密。

驗證

除了在AP的控制檯中跟蹤CAPWAP狀態機外，您還可以在WLC中使用[嵌入式資料包捕獲](#)來分析AP加入過程：

No.	Time	Time della from Source	Destination	Protocol	Length	Destination Port	Info
886	12:58:41.280976	0.022002000	172.16.5.65	172.16.5.11	CAPWAP-Control	294 5246	CAPWAP-Control - Discovery Request
887	12:58:41.280976	0.000000000	172.16.5.11	172.16.5.65	CAPWAP-Control	147 5267	CAPWAP-Control - Discovery Response
888	12:58:41.388974	0.027998000	172.16.5.65	255.255.255.255	CAPWAP-Control	294 5246	CAPWAP-Control - Discovery Request
889	12:58:41.388974	0.000000000	172.16.5.11	172.16.5.65	CAPWAP-Control	147 5267	CAPWAP-Control - Discovery Response
1156	12:58:50.794957	0.135909000	172.16.5.65	172.16.5.11	DTLSv1.2	276 5246	Client Hello
1157	12:58:50.795948	0.000991000	172.16.5.11	172.16.5.65	DTLSv1.2	98 5267	Hello Verify Request
1158	12:58:50.796955	0.001007000	172.16.5.65	172.16.5.11	DTLSv1.2	296 5246	Client Hello
1159	12:58:50.798954	0.001999000	172.16.5.11	172.16.5.65	DTLSv1.2	562 5267	Server Hello, Certificate (Fragment)
1160	12:58:50.798954	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	562 5267	Certificate (Fragment)
1161	12:58:50.798954	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	562 5267	Certificate (Reassembled), Server Key Exchange (Fragment)
1162	12:58:50.798954	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	349 5267	Server Key Exchange (Reassembled), Certificate Request, Server Hello Done
1163	12:58:50.859948	0.000990000	172.16.5.65	172.16.5.11	DTLSv1.2	594 5246	Certificate (Fragment)
1164	12:58:50.859948	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	594 5246	Certificate (Reassembled), Client Key Exchange (Fragment)
1181	12:58:51.204975	0.066997000	172.16.5.65	172.16.5.11	DTLSv1.2	463 5246	Client Key Exchange (Reassembled), Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1182	12:58:51.205983	0.001000000	172.16.5.11	172.16.5.65	DTLSv1.2	125 5267	Change Cipher Spec, Encrypted Handshake Message
1328	12:58:55.914945	0.016997000	172.16.5.65	172.16.5.11	DTLSv1.2	1487 5246	Application Data
1329	12:58:55.914945	0.001999000	172.16.5.11	172.16.5.65	DTLSv1.2	1484 5267	Application Data
1330	12:58:56.246981	0.109003000	172.16.5.65	172.16.5.11	DTLSv1.2	1439 5246	Application Data
1331	12:58:56.246981	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	1439 5246	Application Data
1332	12:58:56.246981	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	379 5246	Application Data
1333	12:58:56.247973	0.000992000	172.16.5.11	172.16.5.65	DTLSv1.2	354 5267	Application Data
1364	12:58:57.292984	0.040999000	172.16.5.65	172.16.5.11	DTLSv1.2	1439 5246	Application Data
1365	12:58:57.292984	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	690 5246	Application Data
1366	12:58:57.293975	0.000991000	172.16.5.11	172.16.5.65	DTLSv1.2	354 5267	Application Data
1368	12:58:57.387965	0.069989000	172.16.5.65	172.16.5.11	DTLSv1.2	982 5246	Application Data
1369	12:58:57.387965	0.001007000	172.16.5.11	172.16.5.65	DTLSv1.2	482 5267	Application Data
1376	12:58:57.469961	0.001999000	172.16.5.65	172.16.5.11	DTLSv1.2	146 5246	Application Data
1377	12:58:57.469961	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1378	12:58:57.470968	0.001007000	172.16.5.65	172.16.5.11	CAPWAP-Data	104 5247	CAPWAP-Data Keep-Alive(Malformed Packet)
1379	12:58:57.474966	0.003998000	172.16.5.11	172.16.5.65	DTLSv1.2	133 5267	Application Data
1380	12:58:57.477972	0.003006000	172.16.5.11	172.16.5.65	CAPWAP-Data	104 5267	CAPWAP-Data Keep-Alive(Malformed Packet)
1400	12:58:57.546968	0.003997000	172.16.5.65	172.16.5.11	DTLSv1.2	140 5246	Application Data
1401	12:58:57.546968	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1402	12:58:57.547968	0.000992000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1403	12:58:57.547968	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	121 5267	Application Data
1411	12:58:57.575958	0.002999000	172.16.5.65	172.16.5.11	DTLSv1.2	140 5246	Application Data
1412	12:58:57.575958	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1413	12:58:57.577957	0.001999000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1414	12:58:57.577957	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	143 5246	Application Data
1415	12:58:57.577957	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	1190 5267	Application Data
1416	12:58:57.577957	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1425	12:58:57.688959	0.070950000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1426	12:58:57.688959	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	140 5246	Application Data
1427	12:58:57.688959	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	119 5267	Application Data
1428	12:58:57.688959	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1429	12:58:57.689951	0.000992000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1430	12:58:57.689951	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	222 5246	Application Data
1431	12:58:57.690958	0.001007000	172.16.5.11	172.16.5.65	DTLSv1.2	175 5267	Application Data
1432	12:58:57.690958	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1433	12:58:57.692957	0.001999000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1434	12:58:57.692957	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	111 5246	Application Data

在WLC中的嵌入式資料包捕獲中看到的AP加入過程

請注意，Change Cipher Spec資料包（資料包編號1182）後的所有流量如何僅顯示為DTLSv1.2上的應用資料。這是建立DTLS會話後所有加密的資料。

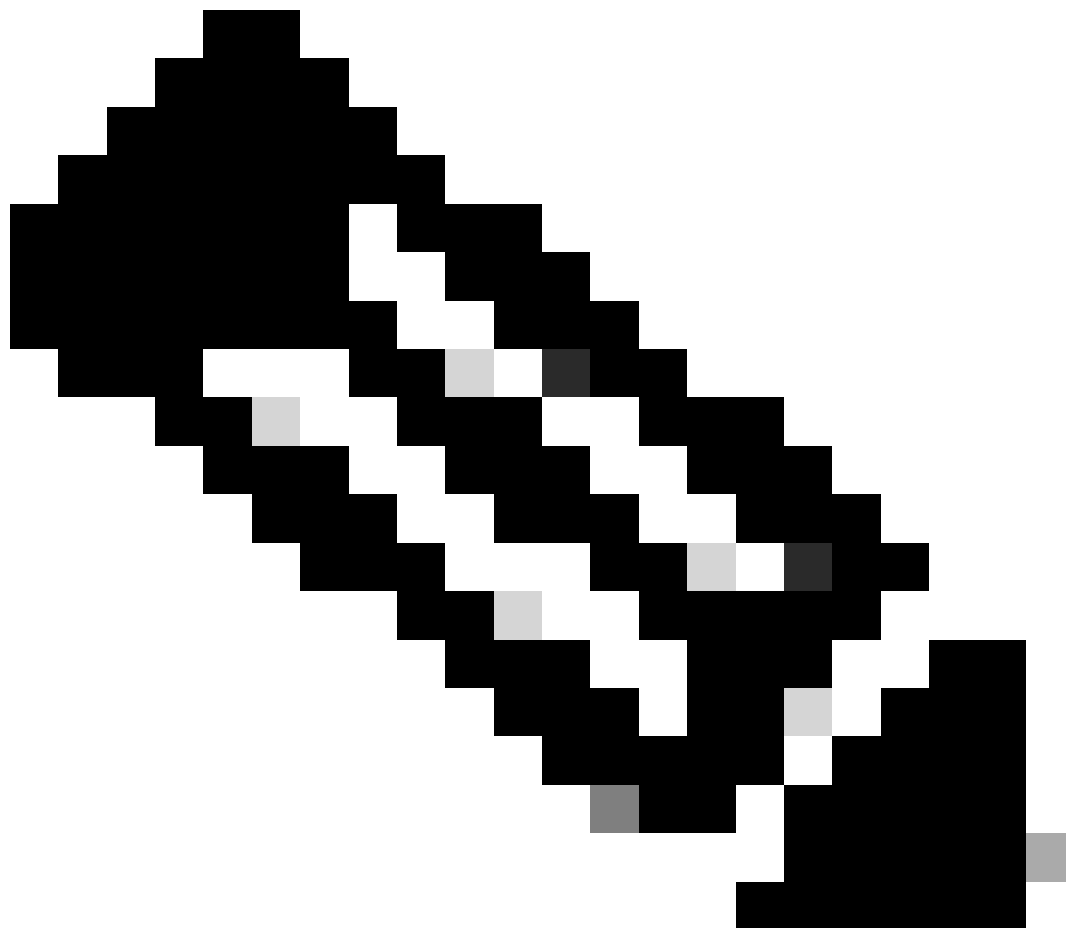
疑難排解

已知的問題

請參閱可能阻止您的AP加入WLC的已知問題。

- [AP由於在Wave 2和Catalyst 11ax存取點\(CSCvx32806\)中損毀的影像而處於開機回圈中](#)
- [現場通知72424：從2022年9月開始生產的C9105/C9120/C9130存取點可能需要軟體升級才能加入無線LAN控制器。](#)
- [現場通知72524：在軟體升級/降級期間，由於證書過期，Cisco IOS AP可能會在2022年12月4日後保持下載狀態-建議進行軟體升級](#)
- [思科漏洞ID CSCwb13784：由於AP加入請求中的路徑MTU無效，AP無法加入9800](#)
- [思科漏洞ID CSCvu22886：C9130：升級到17.7時出現「unlzma：write：No space left on device」消息「Increase max size of /tmp」](#)

在升級之前，請始終參閱每個版本的[發行版本註釋](#)的升級路徑部分。



注意：從Cisco IOS XE Cupertino 17.7.1開始，如果智慧許可未連線且未運行，則Cisco Catalyst 9800-CL無線控制器接受的AP數不會超過50個。

WLC GUI檢查

在WLC上，轉到**Monitoring > Wireless > AP Statistics > Join Statistics**，您可以看到任何AP報告的上次重新引導原因以及WLC註冊的上次斷開原因。

AP Name	AP Model	Status	IP Address	Base Radio MAC	Ethernet MAC	Last Reboot Reason (Reported by AP)	Last Disconnect Reason
9120AP	C9120AXI-A	Red	172.16.5.23	3c41.0a31.7780	6c41.0e16.e79c	No reboot reason	DTLS close alert from peer
josuhel9120	C9120AXI-B	Red	172.16.5.61	3c41.0a31.7780	6c41.0e16.e79c	No reboot reason	DTLS close alert from peer
AP19F9.2096.54F0	C9106AXI-A	Red	172.16.5.32	488b.0aa7.7940	1095.2096.54f0	No reboot reason	DTLS close alert from peer
AP72F9.9876.AFAC	C9120AXI-B	Green	172.16.5.79	7090.9885.7980	7090.9876.afac	Controller reload command	Mesh AP role change
AP710e.ca14.8088	AR-CA93702I-N-K9	Green	172.16.5.31	710e.ca14.8088	710e.ca14.8088	Image upgrade successfully	NA
C9120AXI-EMORENCA	C9120AXI-A	Green	172.16.5.65	a49b.cdaa.1880	a49b.c050.a158	Image upgrade successfully	DTLS close alert from peer
BRCTAC0428	C9120AXI-B	Red	172.16.46.35	c884.a172.2600	c884.a165.8530	No reboot reason	DTLS close alert from peer
AP9130AXI-tulajim	C9130AXI-A	Green	172.16.5.67	011a.2a89.d840	7090.9806.4a44	Controller reload command	Mode change to sniffer
3802-emorenea	AR-AP9802I-B-K9	Green	172.16.5.25	802b.caa7.a5c0	286f.7a15.53ae	Controller reload command	Mode change to sniffer

WLC上的「AP加入統計資訊」頁

您可以按一下任何AP並檢查AP加入統計資訊的詳細資訊。您可以在此處看到更多詳細資訊，例如AP上次加入並嘗試發現WLC的時間和日期。

Join Statistics

General | Statistics

Access Point Statistics Summary

Is the AP currently connected to controller	NOT JOINED
Time at which the AP joined this controller last time	09/27/2022 09:45:49
Type of error that occurred last	Join
Time at which the last join error occurred	09/27/2022 09:46:01

Discovery Phase Statistics

Discovery requests received	106
Successful discovery responses sent	106
Unsuccessful discovery request processing	NA
Reason for last unsuccessful discovery attempt	None
Time at last successful discovery attempt	09/27/2022 09:52:27
Time at last unsuccessful discovery attempt	NA

Last AP Disconnect Details

Reason for last AP connection failure	DTLS close alert from peer
Last Reboot Reason (Reported by AP)	No reboot reason

Last AP message decryption failure details

Reason for last message decryption failure	NA
--------------------------------------------	----

一般AP加入統計資料

如需更多詳細資訊，請移至同一視窗的「統計資料」標籤。在此，您可以比較傳送的加入響應與接收的加入請求數量，以及傳送的配置響應與接收的配置請求。

Join Statistics

General

Statistics

Control DTLS Statistics

DTLS Session request received	8
Established DTLS session	8
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	09/27/2022 09:45:44
Time at last unsuccessful DTLS session	NA

Join phase statistics

Join requests received	8
Successful join responses sent	8
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	DTLS close alert from peer
Time at last successful join attempt	09/27/2022 09:45:49
Time at last unsuccessful join attempt	NA

Configuration phase statistics

Configuration requests received	15
Successful configuration responses sent	15
Unsuccessful configuration request processing	0
Reason for last unsuccessful configuration attempt	NA
Time at last successful configuration attempt	09/21/2022 01:39:07
Time at last unsuccessful configuration attempt	NA

Data DTLS Statistics

DTLS Session request received	0
Established DTLS session	0
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	NA
Time at last unsuccessful DTLS session	NA

詳細的AP加入統計資訊

命令

以下命令可用於排除AP加入問題：

從WLC

- show ap summary
- debug capwap error
- debug capwap packet

從Wave 2和Catalyst 11ax AP

- 偵錯 capwap 用戶端事件
- debug capwap client error
- debug dtls client error
- debug dtls client event
- debug capwap client keepalive
- test capwap restart
- capwap ap erase all

從Wave 1 AP

- debug capwap console cli
- debug capwap client no-reload
- show dtls stats
- clear cawap ap all-config



註：透過Telnet/SSH連線到AP以進行故障排除時，在啟用AP調試後重現問題時請始終發出**terminal monitor**命令。否則，您將看不到來自調試的任何輸出。

放射性痕跡

排除AP加入問題的一個好起點是獲取存在加入問題的AP的無線電和乙太網MAC地址的放射性蹤跡。有關生成這些日誌的詳細資訊，請參閱[Catalyst 9800 WLC上的調試和日誌收集](#)。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。