AP-Join-Prozess mit dem Catalyst 9800 WLC verstehen

Inhalt

Einleitung

In diesem Dokument wird der Beitrittsprozess des Access Points mit dem Cisco Catalyst 9800 WLC ausführlich beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis der Control and Provisioning Wireless Access Points (CAPWAP)
- Grundlegendes Verständnis der Verwendung eines Wireless LAN Controllers (WLC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9800-L WLC, Cisco IOS® XE Cupertino 17.9.3
- Access Point Catalyst 9120AX

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

CAPWAP-Sitzungserstellung

CAPWAP (Control And Provisioning Wireless Access Point) ist das Protokoll, das den Transportmechanismus bereitstellt, der von Access Points (APs) und Wireless LAN Controllern (WLCs) verwendet wird, um Kontroll- und Datenebeneninformationen über einen sicheren Kommunikationstunnel (für CAPWAP Control) auszutauschen.

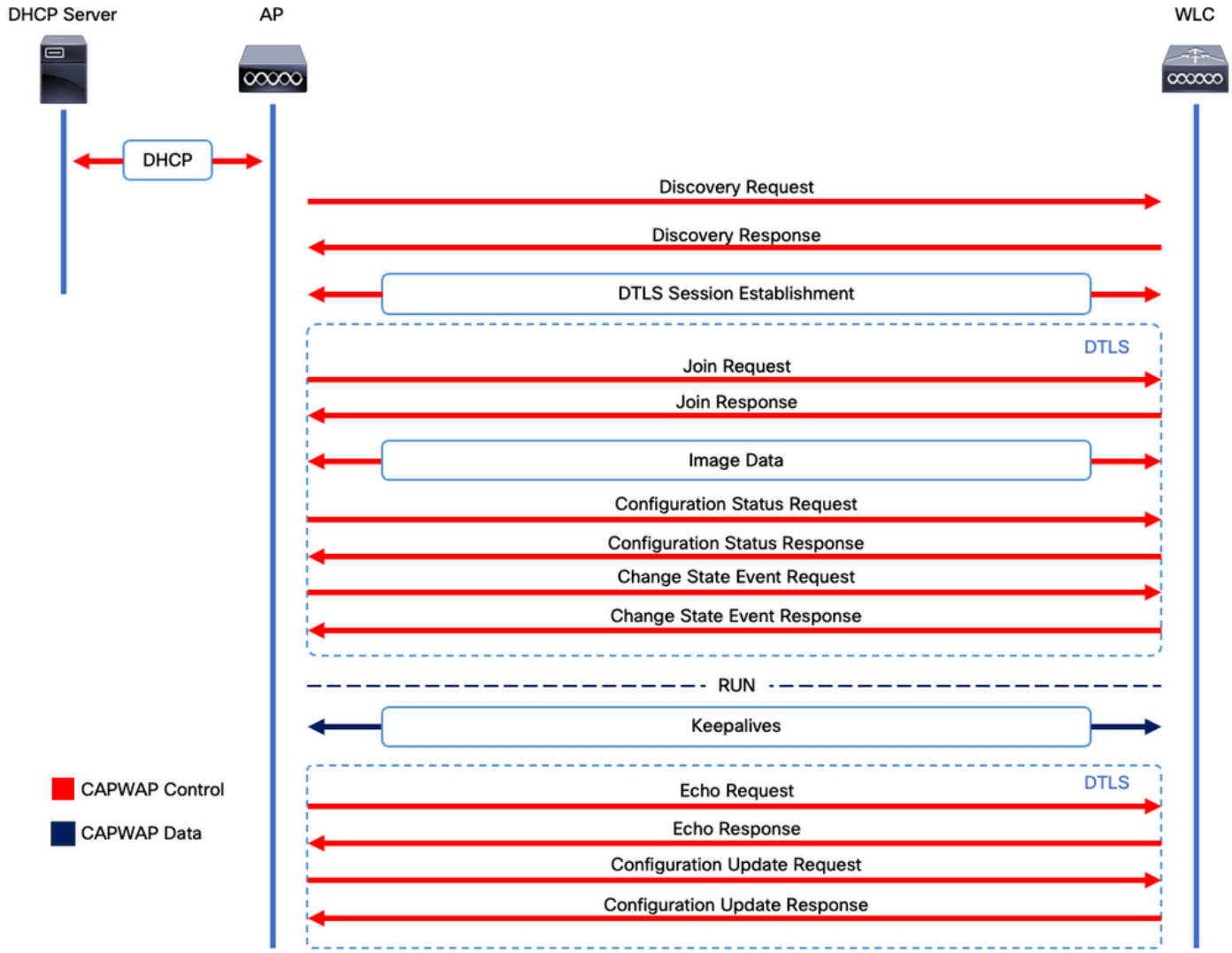
Um den Prozess der Zugehörigkeit zum Access Point genauer zu erläutern, ist es wichtig, dass Sie mit dem Prozess der CAPWAP-Sitzungserstellung (Control And Provisioning Wireless Access Point) vertraut sind.

Beachten Sie, dass der AP über eine IP-Adresse verfügen muss, bevor der CAPWAP-Prozess gestartet werden kann. Wenn der WAP über keine IP-Adresse verfügt, initiiert er nicht den CAPWAP-Sitzungsetablierungsprozess.

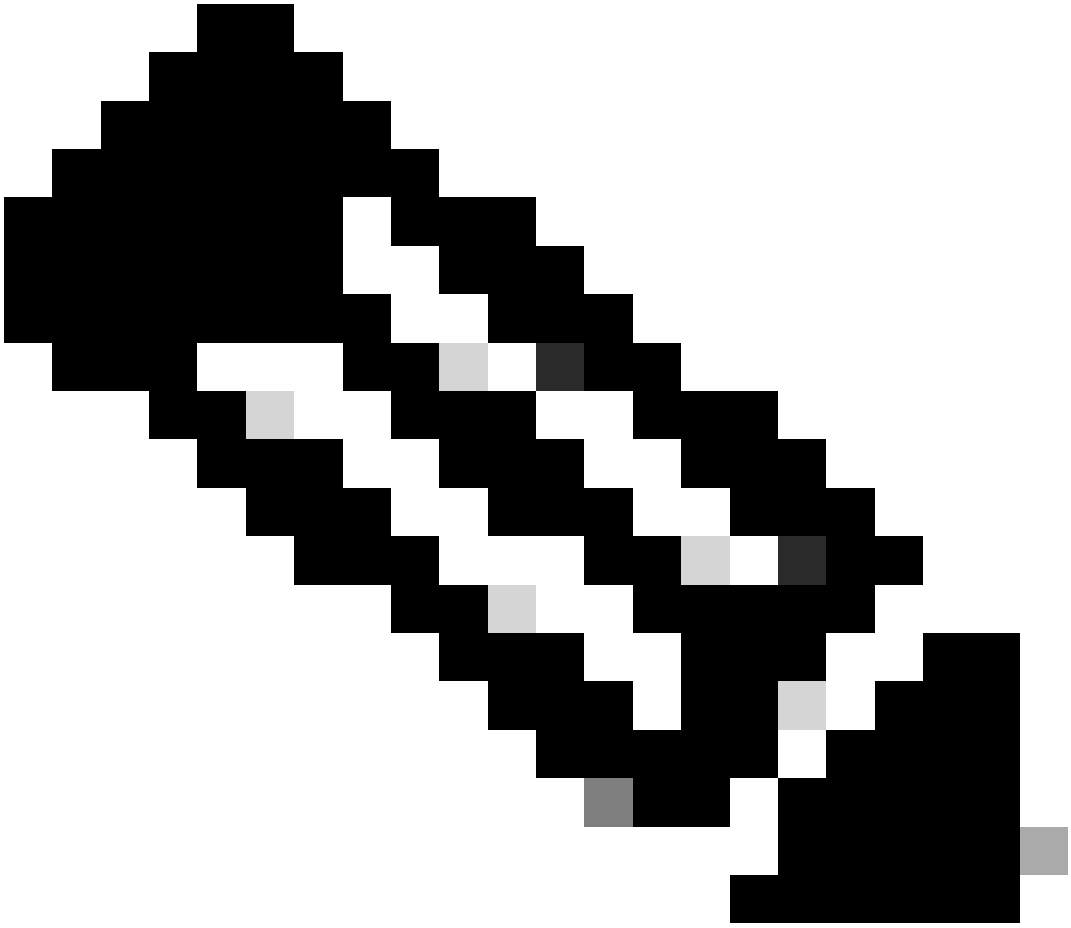
1. Der Access Point sendet eine Ermittlungsanforderung. Weitere Informationen hierzu finden Sie im Abschnitt zu den WLC-Erkennungsmethoden.
2. WLC sendet Erkennungsantwort
3. DTLS-Sitzungsaufbau. Danach werden alle Nachrichten verschlüsselt und in jedem Paketanalyse-Tool als DTLS-Anwendungsdatenpakete angezeigt.
4. Access Point sendet Beitrittsanfrage
5. WLC sendet Join-Antwort
6. AP führt eine Bildprüfung durch. Wenn es die gleiche Image-Version wie der WLC hat, wird mit dem nächsten Schritt fortgefahren. Wenn dies nicht der Fall ist, lädt er das Image vom

WLC herunter und startet neu, um das neue Image zu laden. In diesem Fall wiederholt er den Vorgang aus Schritt 1.

7. Der Access Point sendet eine Konfigurationsstatusanfrage.
8. WLC sendet Konfigurationsstatusantwort
9. Access Point wechselt in RUN-Status
10. Im RUN-Status gibt es zwei Möglichkeiten für die CAPWAP-Tunnelwartung:
    1. Keepalives werden ausgetauscht, um den CAPWAP-Datentunnel zu warten
    2. AP sendet eine Echoanfrage an den WLC, die mit der jeweiligen Echoantwort beantwortet werden muss. Dies dient zur Wartung des CAPWAP Control Tunnels.



Prozess zur Einrichtung von CAPWAP-Sitzungen



Hinweis: Gemäß RFC 5415 verwendet CAPWAP die UDP-Ports 5246 (für CAPWAP-Steuerung) und 5247 (für CAPWAP-Daten).

DTLS-Sitzungsaufbau

Sobald der Access Point eine gültige Discovery-Antwort vom WLC erhält, wird ein DTLS-Tunnel zwischen den Access Points eingerichtet, um alle nachfolgenden Pakete über einen gesicherten Tunnel zu übertragen. So wird die DTLS-Sitzung eingerichtet:

1. AP sendet Client-Hello-Nachricht
2. WLC sendet eine HelloVerifyRequest-Nachricht mit einem zur Validierung verwendeten Cookie.
3. AP sendet eine ClientHello-Nachricht mit einem zur Validierung verwendeten Cookie.
4. WLC sendet diese Pakete in der folgenden Reihenfolge:
    1. ServerHallo
    2. Zertifikat
    3. Serverschlüsselaustausch

    4. Zertifikatanforderung
    5. ServerHalloFertig
5. AP sendet diese Pakete in der folgenden Reihenfolge:
    1. Zertifikat
    2. ClientSchlüsselaustausch
    3. Überprüfung des Zertifikats
    4. CipherSpec ändern
6. WLC reagiert auf die ChangeCipherSpec des AP mit einer eigenen ChangedCipherSpec:
    1. CipherSpec ändern

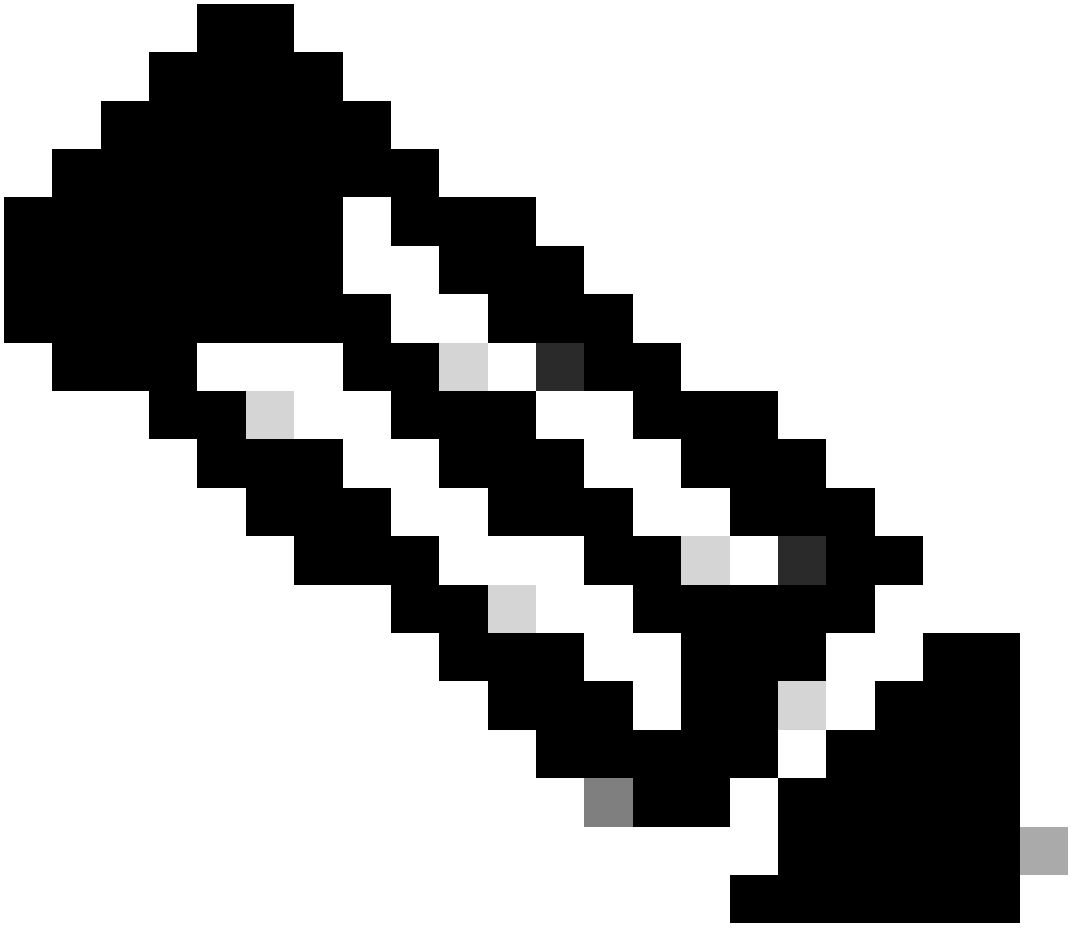
Nach der letzten vom WLC gesendeten ChangedCipherSpec-Nachricht wird der sichere Tunnel eingerichtet, und der gesamte in beide Richtungen gesendete Datenverkehr wird jetzt verschlüsselt.

Wireless LAN Controller-Erkennungsmethoden

Es gibt mehrere Möglichkeiten, den Access Points das Vorhandensein eines WLC im Netzwerk mitzuteilen:

- DHCP-Option 43: Diese Option stellt den APs die IPv4-Adresse des WLC bereit, dem sie beitreten möchten. Dieser Prozess eignet sich für große Bereitstellungen, bei denen sich die APs und der WLC an verschiedenen Standorten befinden.
- DHCP-Option 52: Diese Option stellt den APs die IPv6-Adresse des WLC bereit, dem sie beitreten möchten. Die Nutzung ist im selben Szenario wie bei der DHCP-Option 43 möglich.
- DNS Discovery (DNS-Erkennung): APs fragen den Domänennamen CISCO-CAPWAP-CONTROLLER.localdomain ab. Sie müssen Ihren DNS-Server so konfigurieren, dass er entweder die IPv4- oder die IPv6-Adresse des WLC auflöst, dem Sie beitreten möchten. Diese Option eignet sich für Bereitstellungen, in denen die WLCs am gleichen Standort wie die APs gespeichert werden.
- Layer 3 Broadcast: Die APs senden automatisch eine Broadcast-Nachricht an 255.255.255.255. Jeder WLC innerhalb desselben Subnetzes wie der WAP muss auf diese Erkennungsanfrage antworten.
- Statische Konfiguration: Sie können den Befehl capwap ap primary-base <wlc-hostname> <wlc-IP-address> verwenden, um einen statischen Eintrag für einen WLC im AP zu konfigurieren.

    - **Mobilitätserkennung:** Wenn der WAP zuvor einem WLC hinzugefügt wurde, der Teil einer Mobilitätsgruppe war, speichert der WAP auch einen Datensatz der WLCs in dieser Mobilitätsgruppe.



Hinweis: Die aufgeführten WLC-Ermittlungsmethoden haben keine Rangfolge.

Wahl des Wireless LAN-Controllers

Sobald der Access Point mithilfe einer der WLC-Erkennungsmethoden eine **Erkennungsantwort** von einem beliebigen WLC erhalten hat, wählt er einen Controller aus, dem die folgenden Kriterien zugewiesen werden:

- Primärer Controller (konfiguriert mit dem Befehl **capwap ap primary-base <wlc-hostname> <wlc-IP-Adresse>**)
- Sekundärer Controller (konfiguriert mit dem Befehl **capwap ap second-base <wlc-hostname> <wlc-IP-address**>)

- Tertiärer Controller (konfiguriert mit dem Befehl **capwap ap tertiary-base <wlc-hostname> <wlc-IP-Adresse>)**

- Wenn zuvor kein primärer, sekundärer oder tertiärer WLC konfiguriert wurde, versucht der WAP, dem ersten WLC beizutreten, der auf die Ermittlungsanforderung mit einer eigenen **Ermittlungsantwort** reagiert hat, die über die maximale Kapazität der verfügbaren **WAPs** verfügt (d. h. dem **WLC,** der zu einem bestimmten Zeitpunkt die meisten **WAP** unterstützen kann).

CAPWAP-Zustandsautomat

In der AP-Konsole können Sie den CAPWAP-Statuscomputer verfolgen, der die im Abschnitt CAPWAP Session Establishment beschriebenen Schritte durchläuft.

CAPWAP-Status: Erkennung

Hier sehen Sie die **Ermittlungsanfragen** und Antworten. Beobachten Sie, wie der Access Point eine WLC-IP über **DHCP** empfängt (Option 43) und außerdem eine **Ermittlungsanforderung** an zuvor bekannte WLCs sendet:

<#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

Neben der **Entdeckungsantwort** von einem statisch konfigurierten WLC (172.16.0.20) und dem WLC, die über die DHCP-Option 43 (172.16.5.11) angezeigt werden, hat dieser AP auch eine **Entdeckungsantwort** von einem anderen WLC (172.16.5.5.11) erhalten. 169) im gleichen Subnetz übertragen, da die Broadcast-Discovery-Nachricht eingegangen ist.

CAPWAP-Status: DTLS-Einrichtung.

Hier wird die DTLS-Sitzung zwischen dem AP und dem WLC ausgetauscht.

<#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

CAPWAP-Status: Beitreten

Nach Einrichtung der DTLS-Sitzung wird nun eine **Join Request** an den WLC über die sichere Sitzung gesendet. Beobachten Sie, wie diese Anfrage sofort mit einer **Join-Antwort** des WLC beantwortet wird.

<#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-Status: Bilddaten

Der AP vergleicht sein Image mit dem Image des WLC. In diesem Fall haben sowohl die aktive Partition des Access Points als auch seine Backup-Partition unterschiedliche Images als der WLC. Daher ruft er das Skript **upgrade.sh** auf, das den Access Point anweist, das entsprechende Image beim WLC anzufordern und in die aktuelle nicht aktive Partition herunterzuladen.

<#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

Sobald die Bildübertragung abgeschlossen ist, initiiert der Access Point eine Überprüfung der Bildsignatur, um diese zu validieren.

Anschließend wird das Image vom Skript **upgrade.sh** in die aktuell nicht aktive Partition installiert und die Partition, von der es gestartet wird, ausgetauscht. Schließlich lädt sich der Access Point selbst neu und wiederholt den Vorgang von Anfang an (**CAPWAP State: 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]

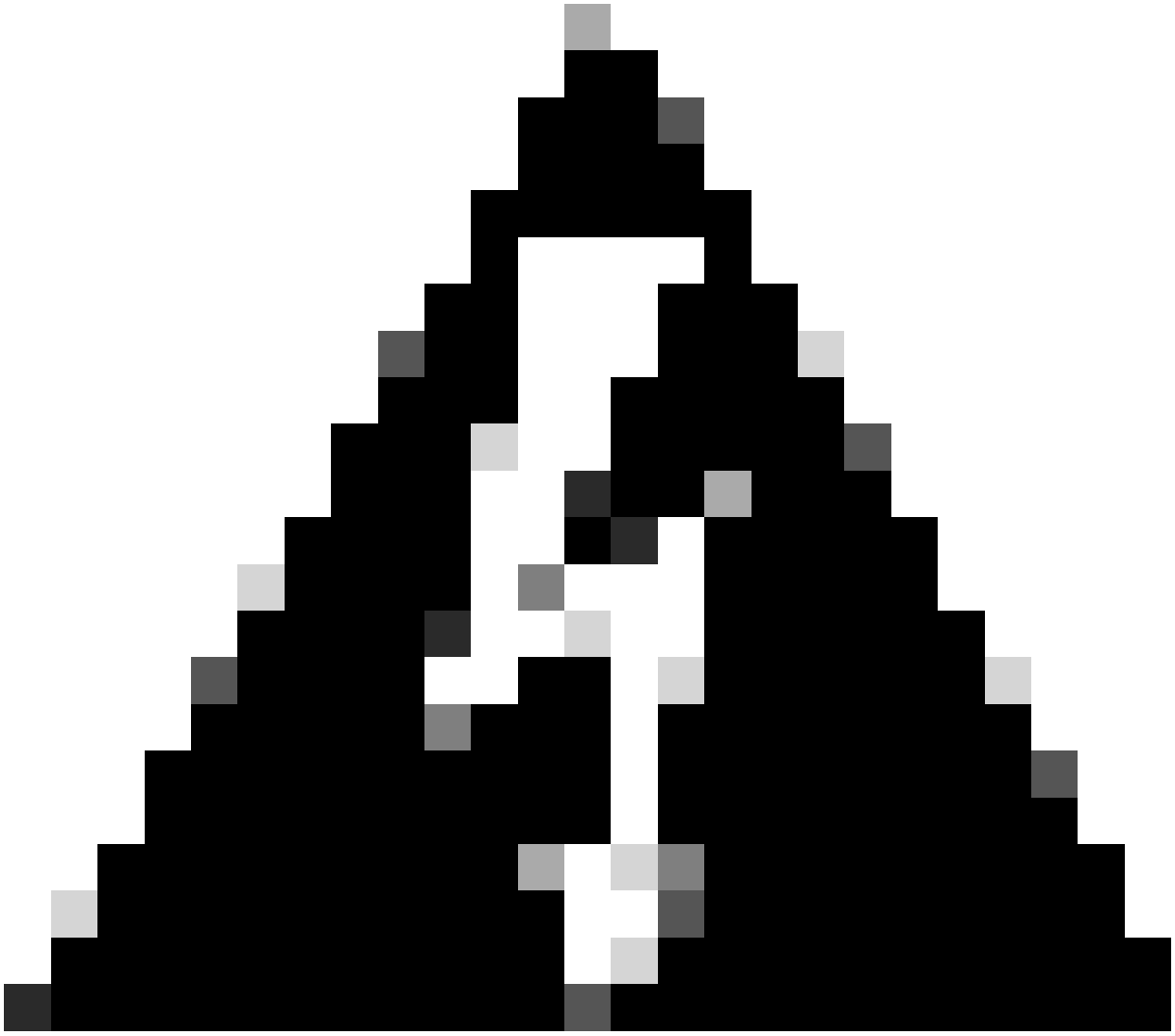
upgrade.sh

: 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



Warnung: Wave 1 Access Points können aufgrund eines abgelaufenen Zertifikats möglicherweise kein neues Image herunterladen. Weitere Informationen finden Sie in der Problembeschreibung 72524. Lesen Sie das IOS AP Image Download Fails Due to Expired Image Signing Certificate Past December 4th, 2022 (CSCwd80290) Support Document sorgfältig durch, um die Auswirkungen und die Lösung zu verstehen.

Sobald der Access Point neu geladen wurde und den **CAPWAP**-Status **"Erkennen** und **Beitreten"** erneut durchläuft, erkennt er im **Bilddatenstatus,** dass er nun über das entsprechende Image verfügt.

<#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-Status: Konfigurieren

Nachdem der WAP überprüft hat, dass die Version mit der des WLC übereinstimmt, benachrichtigt er den WLC über seine aktuellen Konfigurationen. Im Allgemeinen bedeutet dies, dass der Access Point die Aufrechterhaltung seiner Konfigurationen verlangt (sofern diese im WLC verfügbar sind).

<#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-Status: Ausführen

Zu diesem Zeitpunkt wurde der Access Point erfolgreich mit dem Controller verbunden. In diesem Zustand löst der WLC einen Mechanismus aus, um die vom WAP angeforderte Konfiguration zu überschreiben. Wie Sie sehen, erhält der Access Point **Konfigurationen** für **Funkmodule und Anmeldedaten** per Push und wird außerdem dem **Standard-Policy-Tag** zugewiesen, da der WLC keine Vorkenntnisse über diesen Access Point hatte.

<#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]

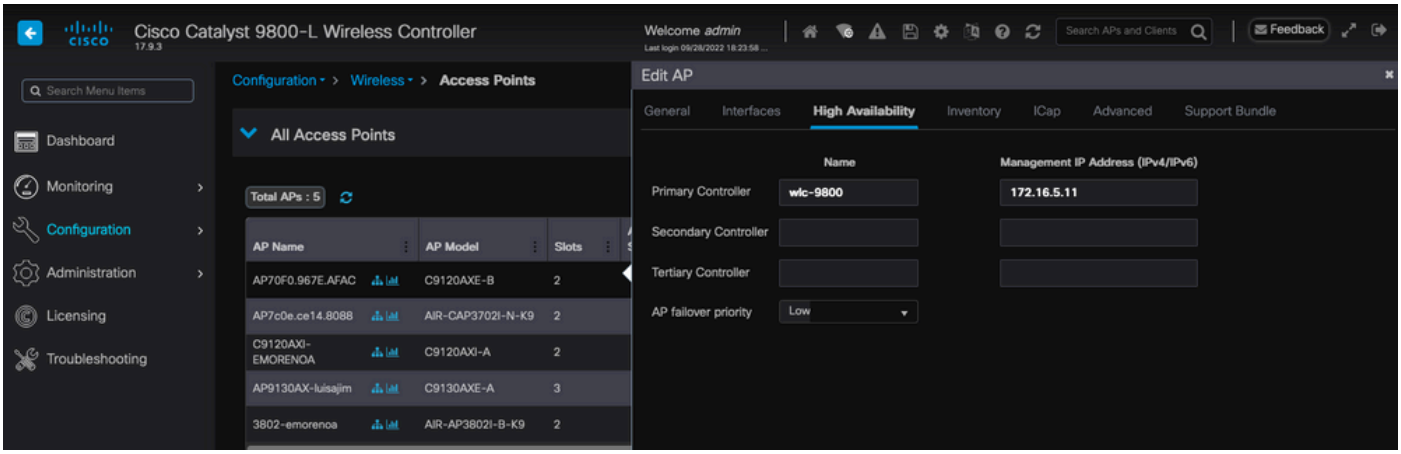
AP tag change to default-policy-tag

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

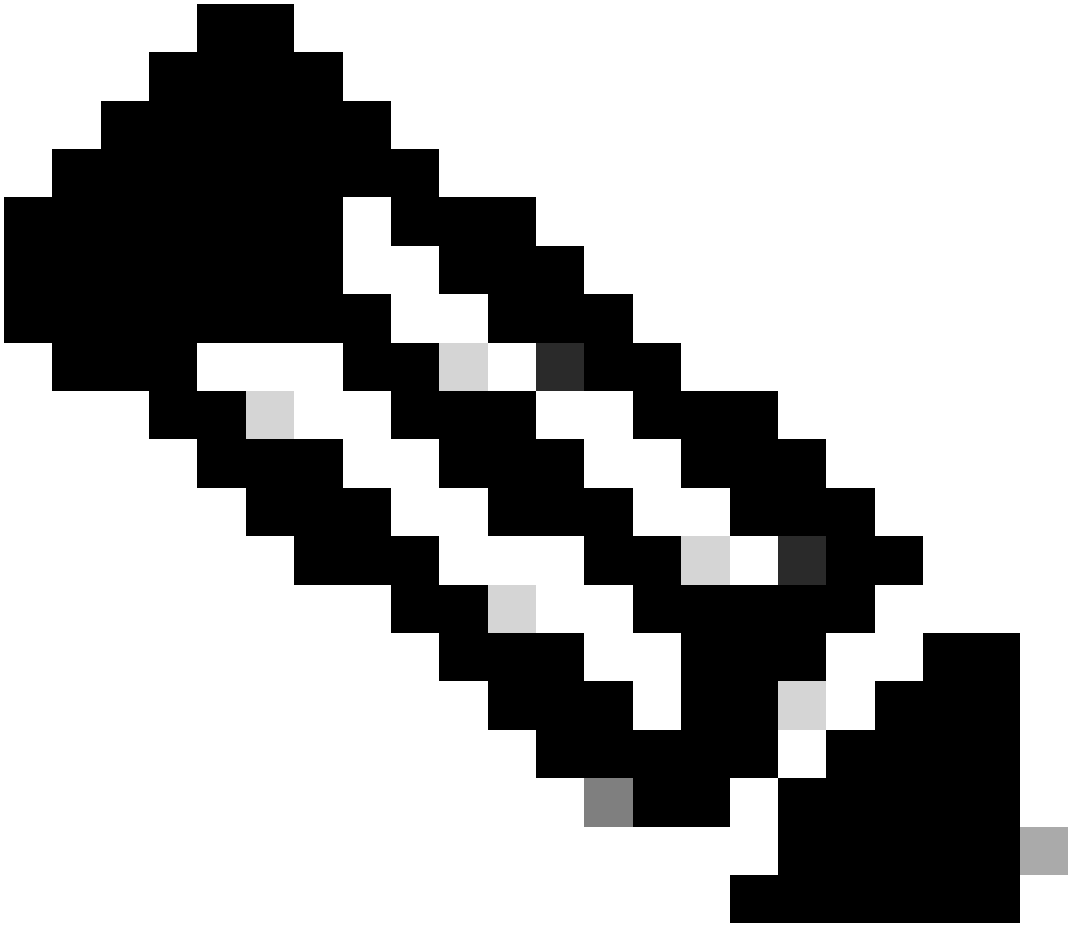
Konfigurieren

Statische WLC-Wahl

In der GUI können Sie zu **Configuration > Wireless > Access Points** wechseln, einen Access Point auswählen und zur Registerkarte **High Availability** wechseln. Hier können Sie die **primären, sekundären und tertiären** WLCs konfigurieren, wie im Abschnitt zur Wahl des Wireless LAN-Controllers in diesem Dokument beschrieben. Diese Konfiguration erfolgt pro Access Point.



Primäre, sekundäre und tertiäre WLCs für einen AP.

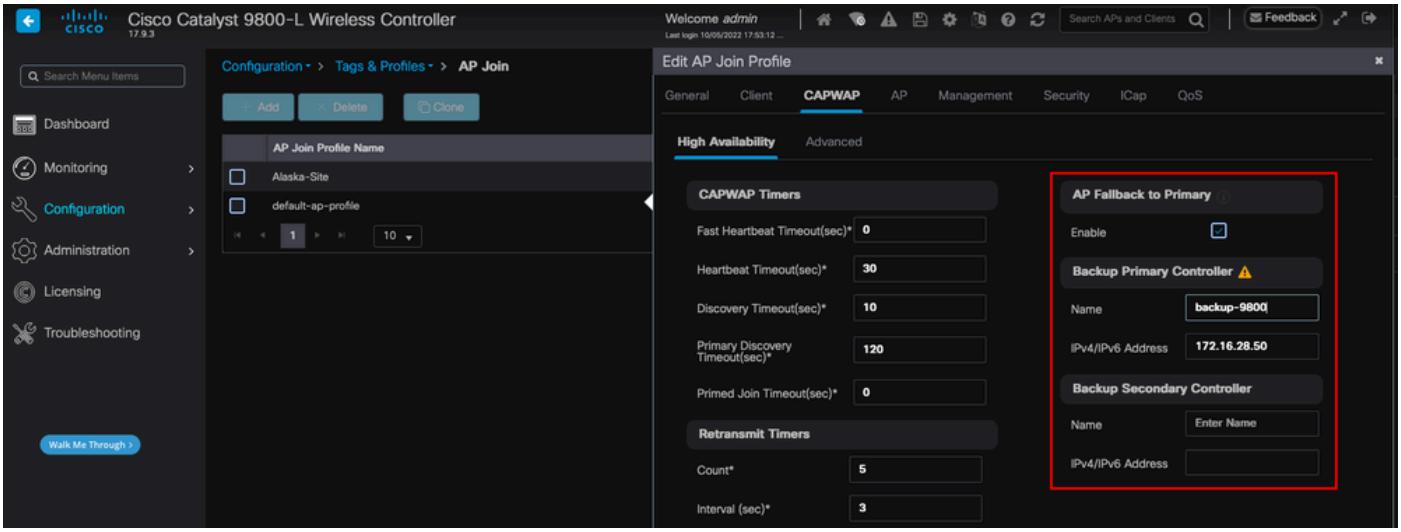


Hinweis: Ab Cisco IOS XE 17.9.2 können Sie mithilfe von Priming Profiles primäre, sekundäre und tertiäre Controller für eine Gruppe von APs konfigurieren, die regulären Ausdrücken (regulären Ausdrücken) entsprechen, oder für einen einzelnen AP. Weitere Informationen finden Sie im Abschnitt AP Fallback to Controllers Configured Under AP Priming Profile (AP-Fallback zu Controllern, die unter dem AP-Priming-Profil konfiguriert wurden) im Konfigurationsleitfaden.

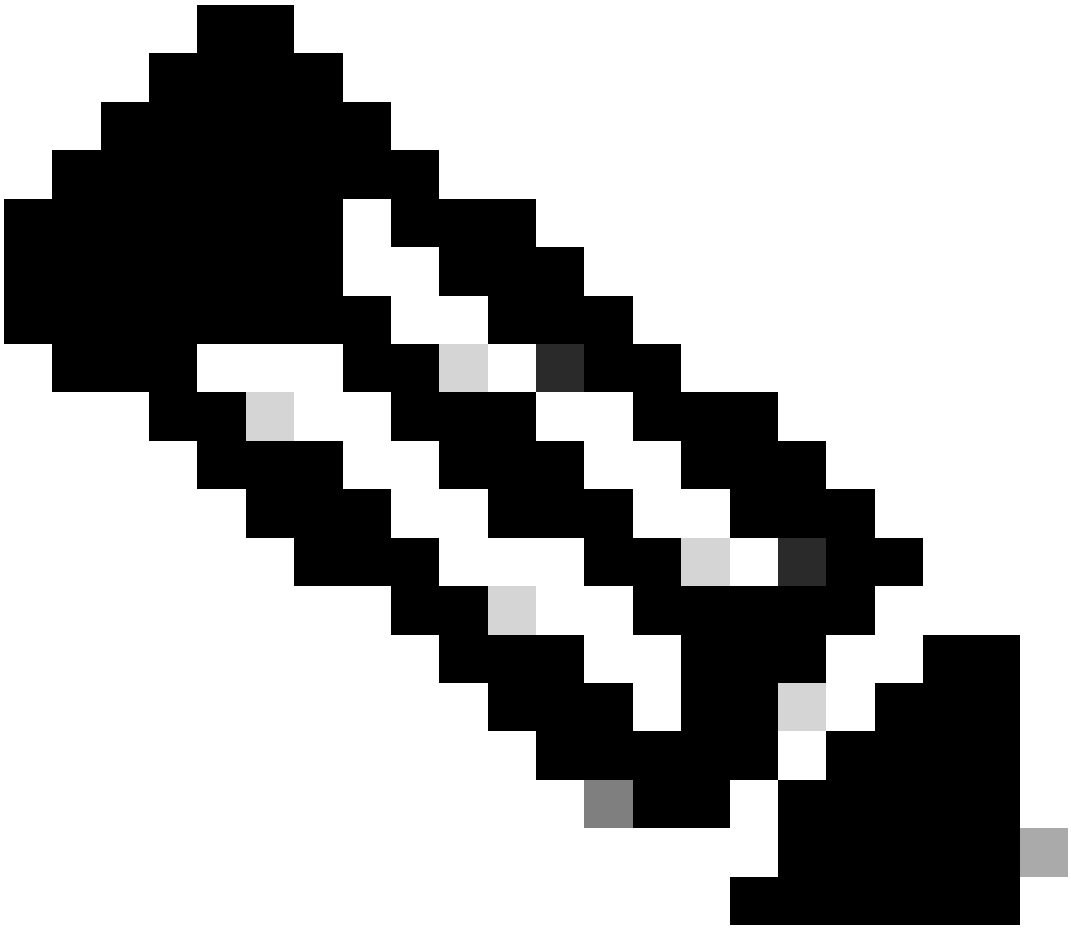
Bitte beachten Sie, dass sich die auf der Registerkarte "AP High Availability" (Hochverfügbarkeit des Access Points) konfigurierten primären, sekundären und tertiären Controller von den **primären und sekundären Backup-**WLCs unterscheiden, die pro **AP-Join-Profil** auf der **Registerkarte "CAPWAP > High Availability" (Hochverfügbarkeit)** konfiguriert werden können**.** Die **primären, sekundären und tertiären Controller** gelten als WLCs mit den Prioritäten 1, 2 bzw. 3, während die **primären und sekundären Backup-Controller** als WLCs mit den Prioritäten 4 und 5 angesehen werden.

Wenn **AP-Fallback** aktiviert ist, sucht der AP aktiv nach dem **primären Controller,** wenn er mit einem anderen **WLC** verbunden wird. Der **AP** sucht nur nach **WLCs** mit den Prioritäten 4 und 5, wenn ein **CAPWAP-Down**-Ereignis vorliegt und keiner der **primären und sekundären**

Backup-Controller verfügbar ist.



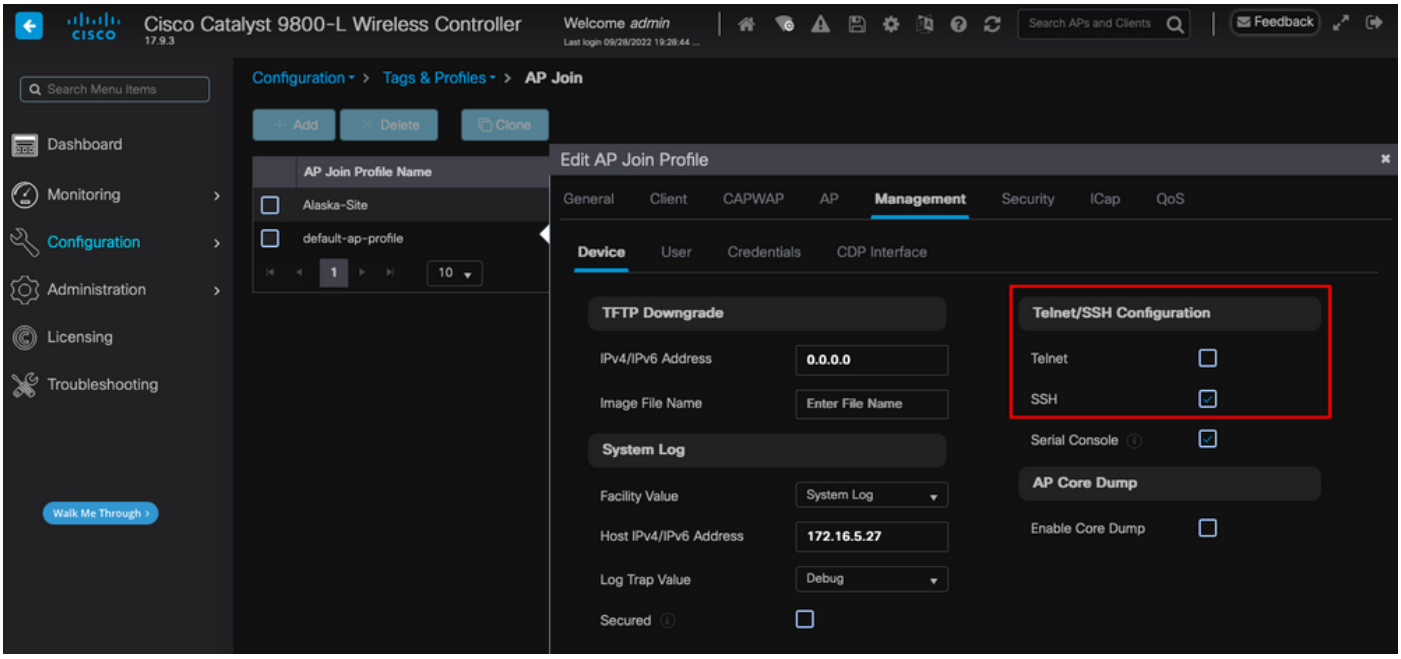
Hochverfügbarkeitsoptionen im Zugangsprofil des Access Points



Hinweis: Bei der Konfiguration der primären und sekundären Backup-WLCs im AP-Join-Profil werden die statischen primären und **sekundären** Einträge auf der Registerkarte für die **hohe Verfügbarkeit** des Access Points **nicht ausgefüllt**.

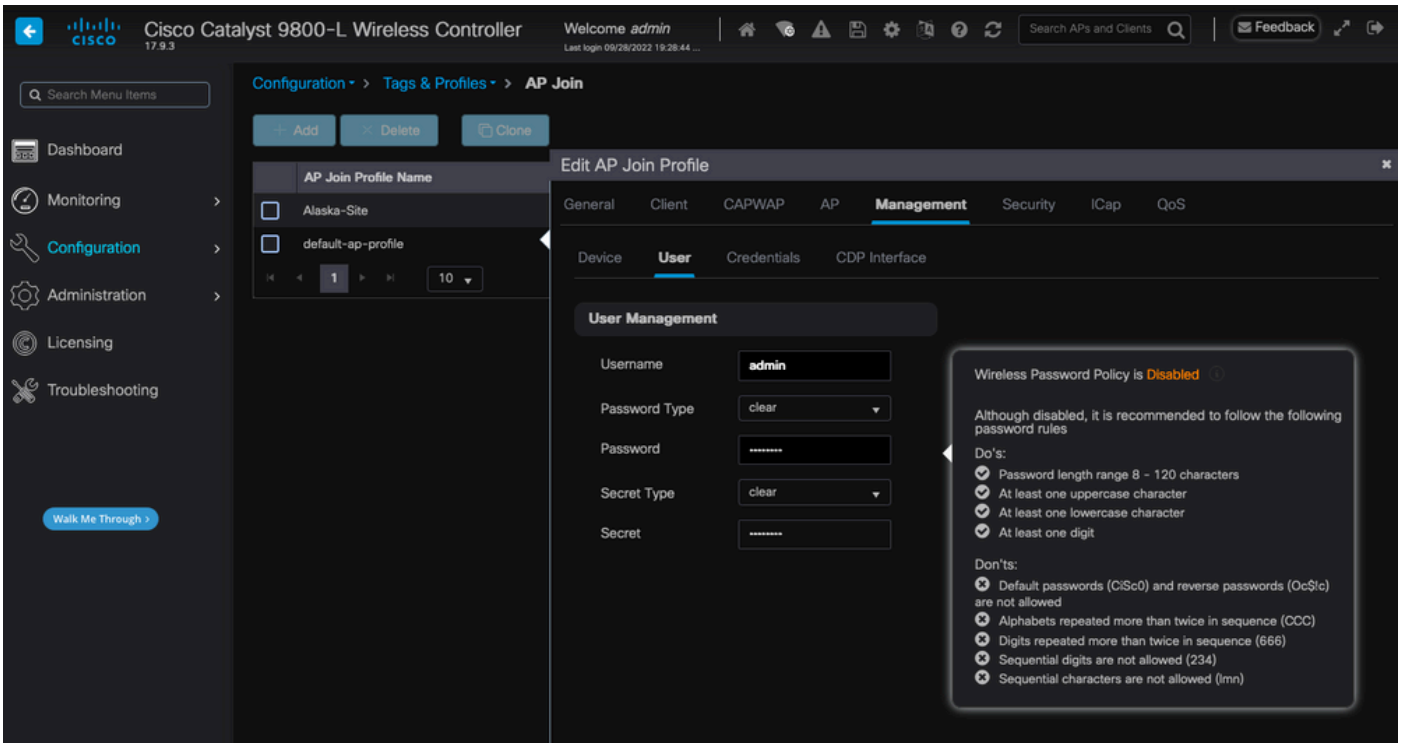
Aktivieren des Telnet-/SSH-Zugriffs auf den AP

Gehen Sie zu **Configuration > Tags & Profiles > AP Join > Management > Device,** und wählen Sie **SSH** und/oder **Telnet aus**.



Aktivieren des Telnet-/SSH-Zugriffs auf dem AP-Join-Profil

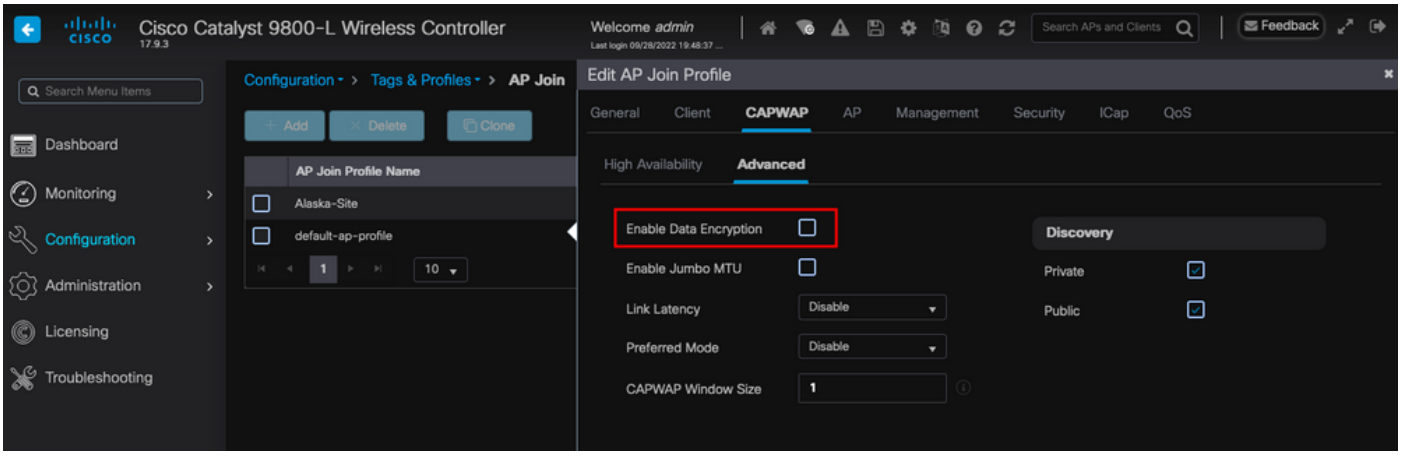
Um die SSH-/Telnet-Anmeldeinformationen zu konfigurieren, navigieren Sie zur Registerkarte **Benutzer** im gleichen Fenster, und legen Sie **Benutzername, Kennwort** und **Schlüssel** fest, um auf den Access Point zuzugreifen.



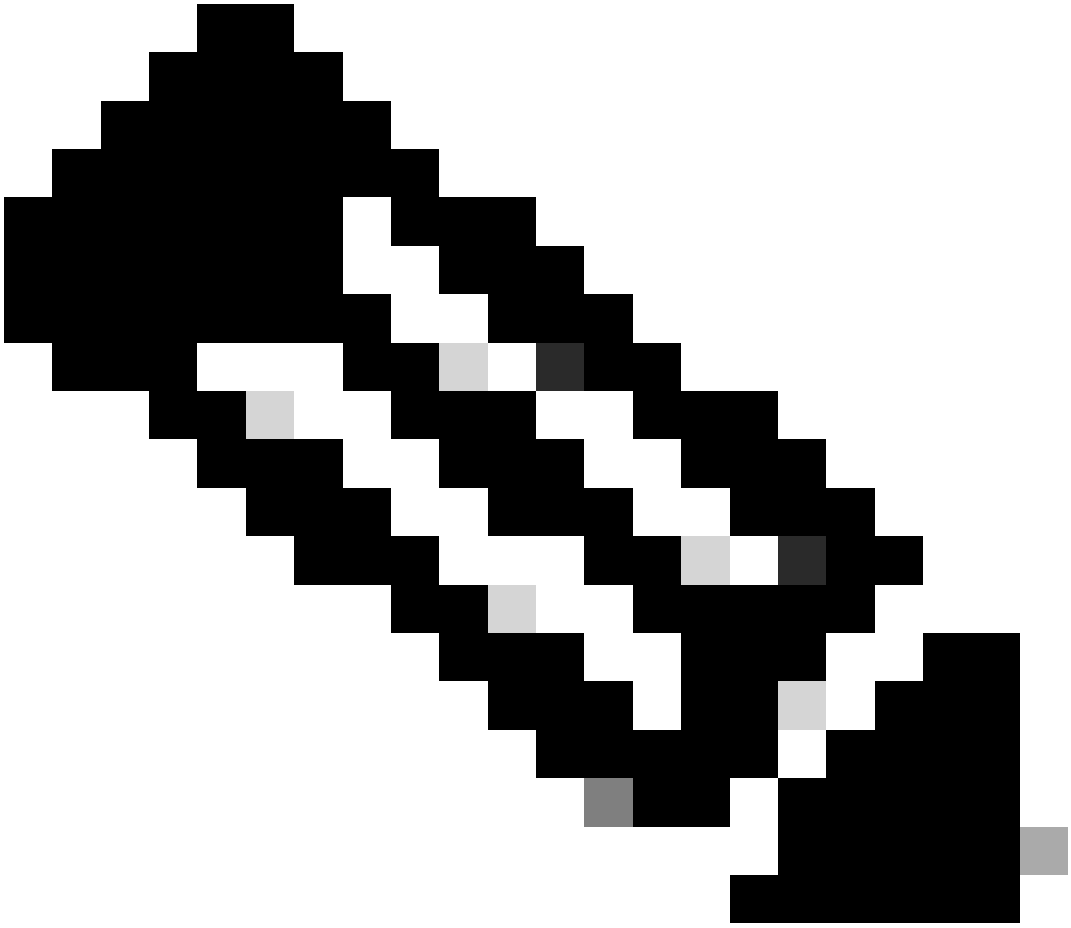
SSH- und Telnet-Anmeldedaten für den AP

Datenverbindungsverschlüsselung

Wenn Sie ein Client-Problem beheben müssen, bei dem eine Paketerfassung des AP-Datenverkehrs erforderlich ist, stellen Sie sicher, dass **Data Link Encryption** unter **Configuration > Tags & Profiles > AP Join > CAPWAP > Advanced** nicht aktiviert ist. Andernfalls wird Ihr Datenverkehr verschlüsselt.



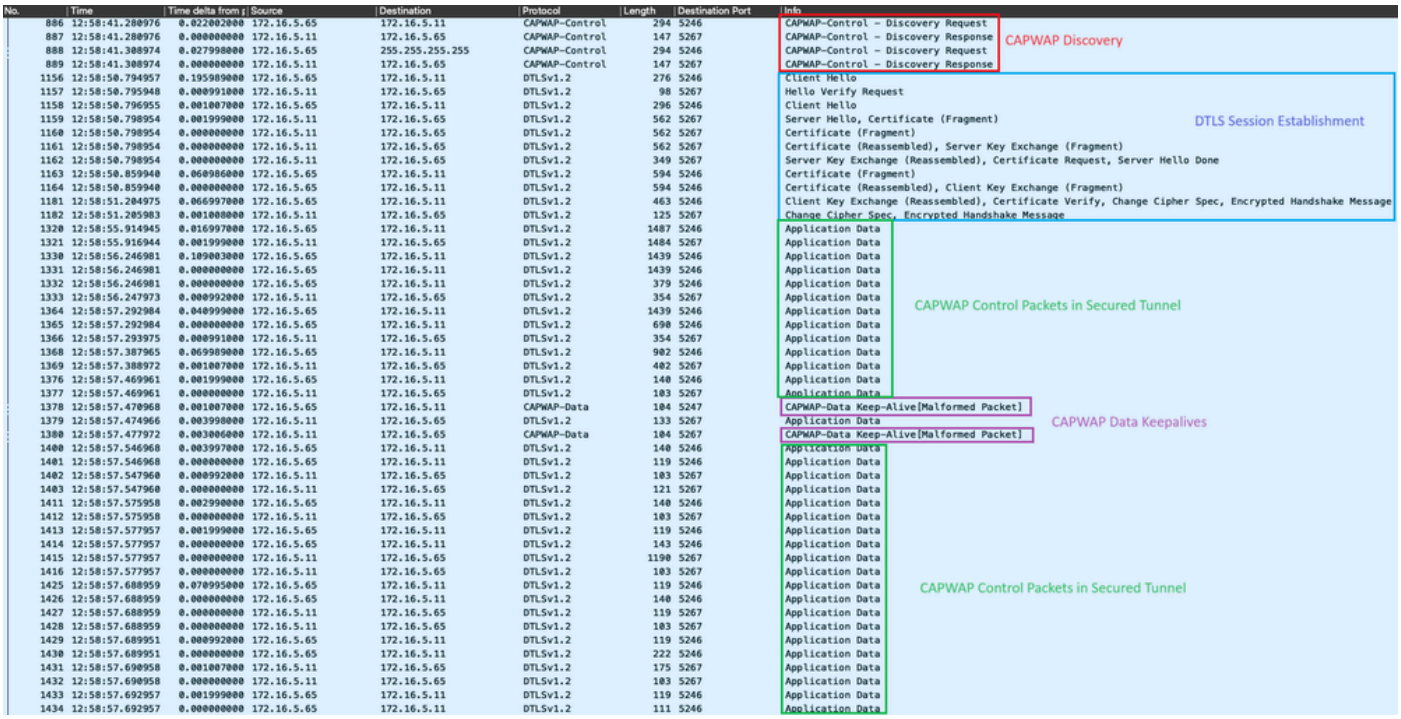
Datenverbindungsverschlüsselung



Hinweis: Datenverschlüsselung verschlüsselt nur CAPWAP-Datenverkehr. CAPWAP-Steuerungsdatenverkehr ist bereits über DTLS verschlüsselt.

Überprüfung

Zusätzlich zur Nachverfolgung des CAPWAP-Statuscomputers in der Konsole des AP können Sie auch eine eingebettete Paketerfassung im WLC durchführen, um den AP-Join-Prozess zu analysieren:



AP-Join-Prozess bei eingebetteter Paketerfassung im WLC

Beachten Sie, dass der gesamte Datenverkehr nach dem Paket **Chance Cipher Spec (**Paket Nr. 1182) nur als **Anwendungsdaten** über **DTLSv1.2** angezeigt wird. Dies sind alle verschlüsselten Daten nach dem **Aufbau** der **DTLS-Sitzung**.

Fehlerbehebung

Bekannte Probleme

Bitte beziehen Sie sich auf die bekannten Probleme, die Ihre APs daran hindern könnten, dem WLC beizutreten.

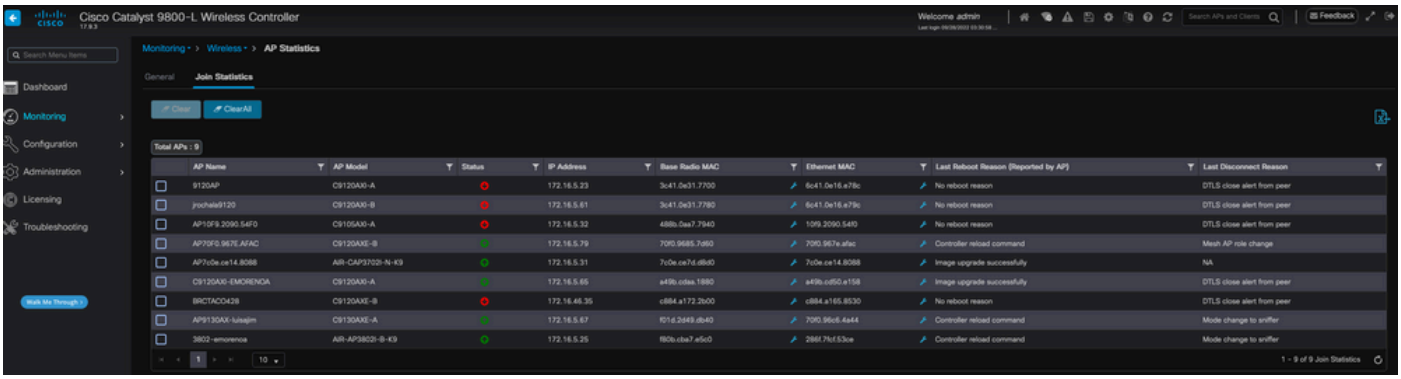
- APs im Boot-Loop aufgrund eines beschädigten Images in Wave 2 und Catalyst 11ax Access Points (CSCvx32806)
- Problemhinweis 72424: Bei Access Points der Serien C9105/C9120/C9130, die ab September 2022 hergestellt werden, sind möglicherweise Software-Upgrades erforderlich, um den Wireless LAN Controllern beizutreten.
- Problemhinweis 72524: Während des Software-Upgrades/-Downgrades befinden sich die Cisco IOS APs möglicherweise auch nach dem 4. Dezember 2022 im Download-Status. Aufgrund des Zertifikatsablaufs wird ein Software-Upgrade empfohlen.
- Cisco Bug-ID CSCwb13784: APs können 9800 wegen ungültiger Pfad-MTU in AP-Beitrittsanfrage nicht beitreten
- Cisco Bug-ID CSCvu22886: C9130: Meldung "unlzma: write: no space left on device" beim Upgrade auf 17.7 Increase max size of /tmp

Vor dem Upgrade sollten Sie stets den Abschnitt **Upgrade Path** der Versionshinweise der jeweiligen Version lesen.

Hinweis: Ab Cisco IOS XE Cupertino 17.7.1 sind für den Cisco Catalyst 9800-CL Wireless Controller nicht mehr als 50 APs zulässig, wenn die Smart Licensing-Technologie nicht ordnungsgemäß verbunden ist.

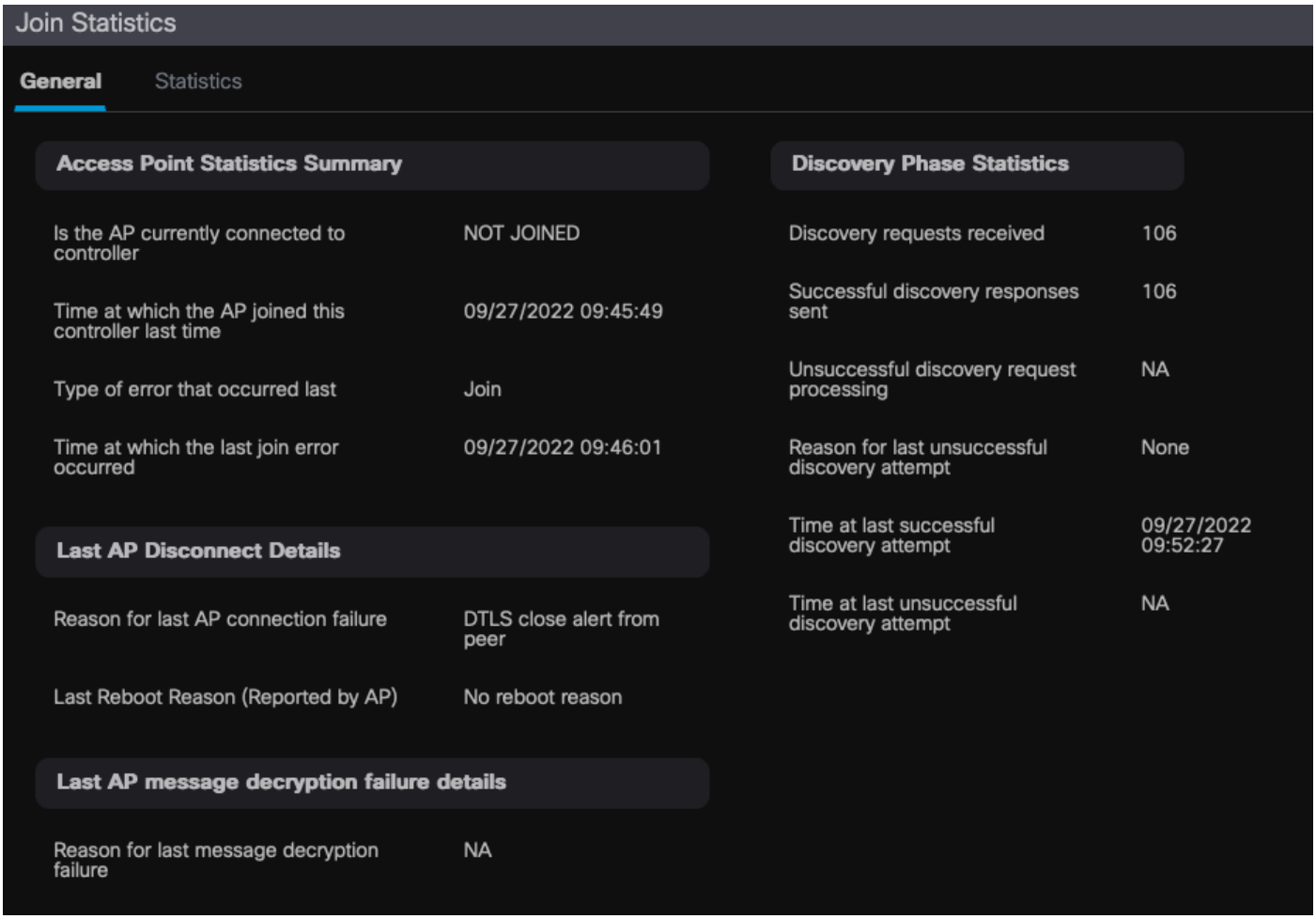
WLC-GUI-Prüfungen

Gehen Sie auf Ihrem WLC zu **Monitoring > Wireless > AP Statistics > Join Statistics, und** Sie können den **Grund für** den **letzten Neustart** sehen, der von einem AP gemeldet wurde, sowie den Grund für den **letzten Verbindungsabbruch,** der vom WLC registriert wurde.



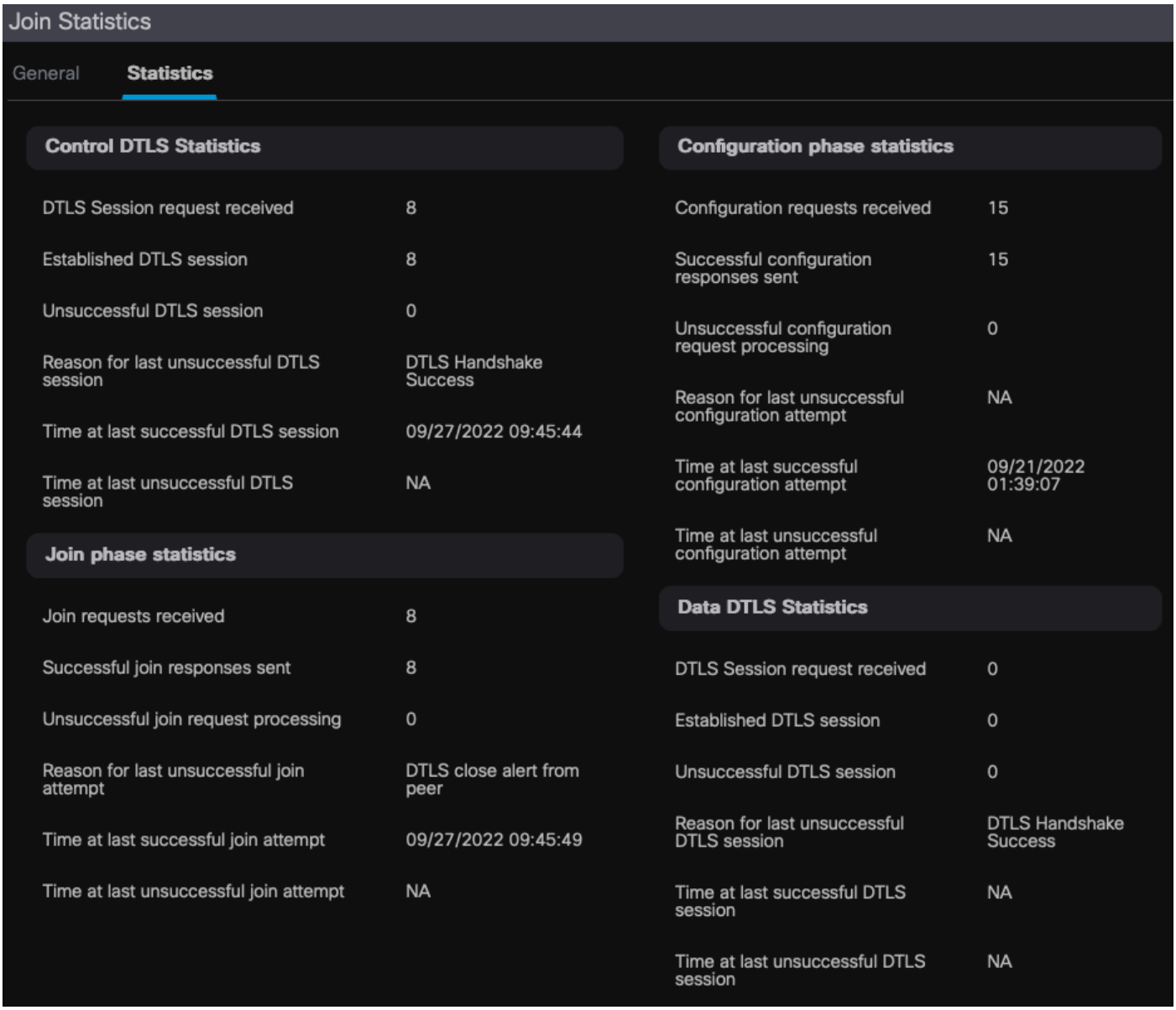
Seite "AP Join Statistics" auf dem WLC

Sie können auf einen beliebigen Access Point klicken und nach Details zur AP-Join-Statistik suchen. Hier finden Sie ausführlichere Informationen, z. B. zu Zeitpunkt und Datum, zu dem der Access Point zuletzt beigetreten ist und versucht hat, den WLC zu erkennen.



Allgemeine AP-Join-Statistik

Ausführlichere Informationen finden Sie auf der Registerkarte Statistik des gleichen Fensters. Hier können Sie die Anzahl der **gesendeten Join-Antworten** mit der Anzahl der **empfangenen Join-Anfragen** sowie die **gesendeten Konfigurationsantworten** mit den **empfangenen Konfigurationsanfragen** vergleichen**vergleichen**.



Detaillierte AP-Join-Statistik

Befehle

Diese Befehle sind nützlich, um Probleme mit der AP-Verbindung zu beheben:

Vom WLC

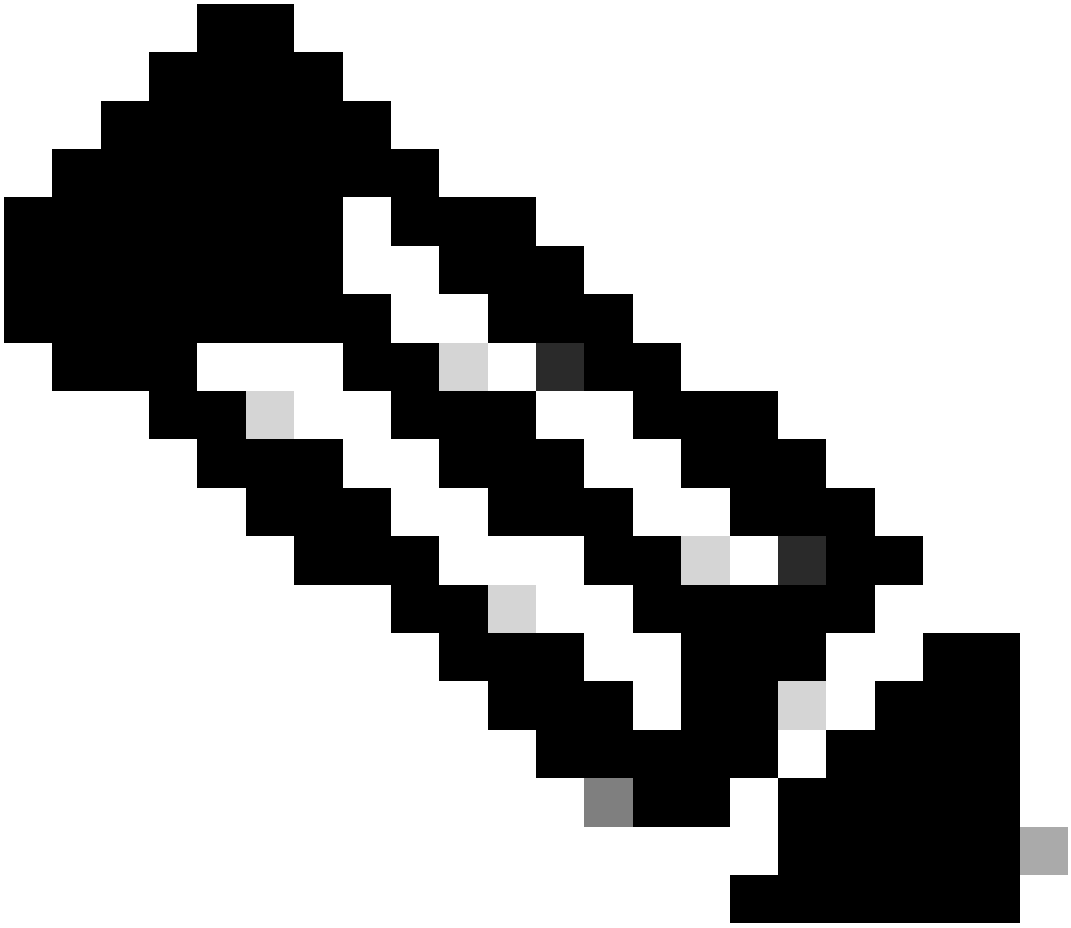
- show ap summary
- Fehler beim Debuggen von Capwap
- debug capwap-Paket

Von Wave 2 und Catalyst 11ax APs

    - debuggen capwap-Clientereignisse
- debug capwap client error
- debuggen dtls-Clientfehler
- debuggen dtls-Clientereignis
- debuggen capwap client keepalive
- Test-Capwap-Neustart
- capwap ap alle löschen

Von APs der Phase 1

- debug capwap console cli
- debug capwap client no-reload
- dtls-Statistiken anzeigen
- clear cawap ap all-config



Hinweis: Wenn Sie zur Fehlerbehebung eine Verbindung zu den APs über Telnet/SSH herstellen, geben Sie nach der Aktivierung von Debug-Vorgängen auf den APs immer den Befehl **terminal monitor** ein, während Sie das Problem reproduzieren. Andernfalls können Sie keine Ausgabe der Debugs sehen.

Radioaktive Spuren

Ein guter Ausgangspunkt für die Behebung von AP-Join-Problemen ist die Erfassung radioaktiver Spuren sowohl der Radio- als auch der Ethernet-MAC-Adresse eines AP, bei dem Probleme beim Join bestehen. Einzelheiten zur Generierung dieser Protokolle finden Sie in der Debug & Log-Auflistung im Catalyst 9800 WLC-Dokument.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.