Comprendre le processus de jonction du point d’accès avec le contrôleur LAN sans fil (WLC) Catalyst 9800

Table des matières

Introduction

Le présent document décrit en détail le processus de jonction du point d’accès avec le contrôleur LAN sans fil (WLC) Cisco Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base des points d'accès sans fil de contrôle et de mise en service (CAPWAP)
- Compréhension de base de l'utilisation d'un contrôleur LAN sans fil (WLC)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC Catalyst 9800-L, Cisco IOS® XE Cupertino 17.9.3
- Point d'accès Catalyst 9120AX

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Établissement de session CAPWAP

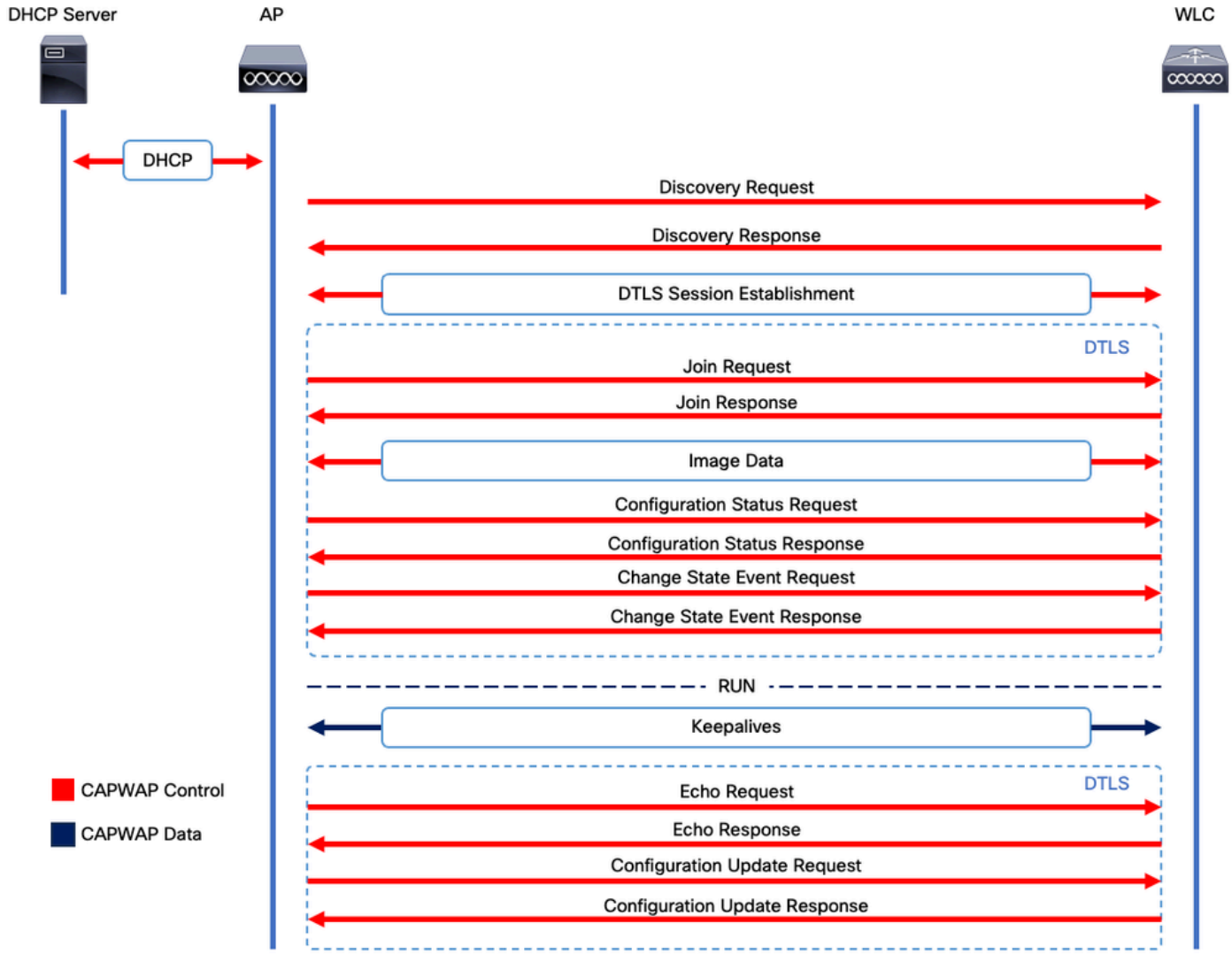
Le protocole CAPWAP (Control And Provisioning Wireless Access Point) fournit le mécanisme de transport utilisé par les points d'accès (AP) et les contrôleurs de réseau local sans fil (WLC) pour échanger des informations de plan de données et de contrôle via un tunnel de communication sécurisé (pour le contrôle CAPWAP).

Afin d'élaborer sur le processus de jointure de point d'accès, il est important que vous compreniez le processus d'établissement de session de point d'accès sans fil de contrôle et de mise en service (CAPWAP).

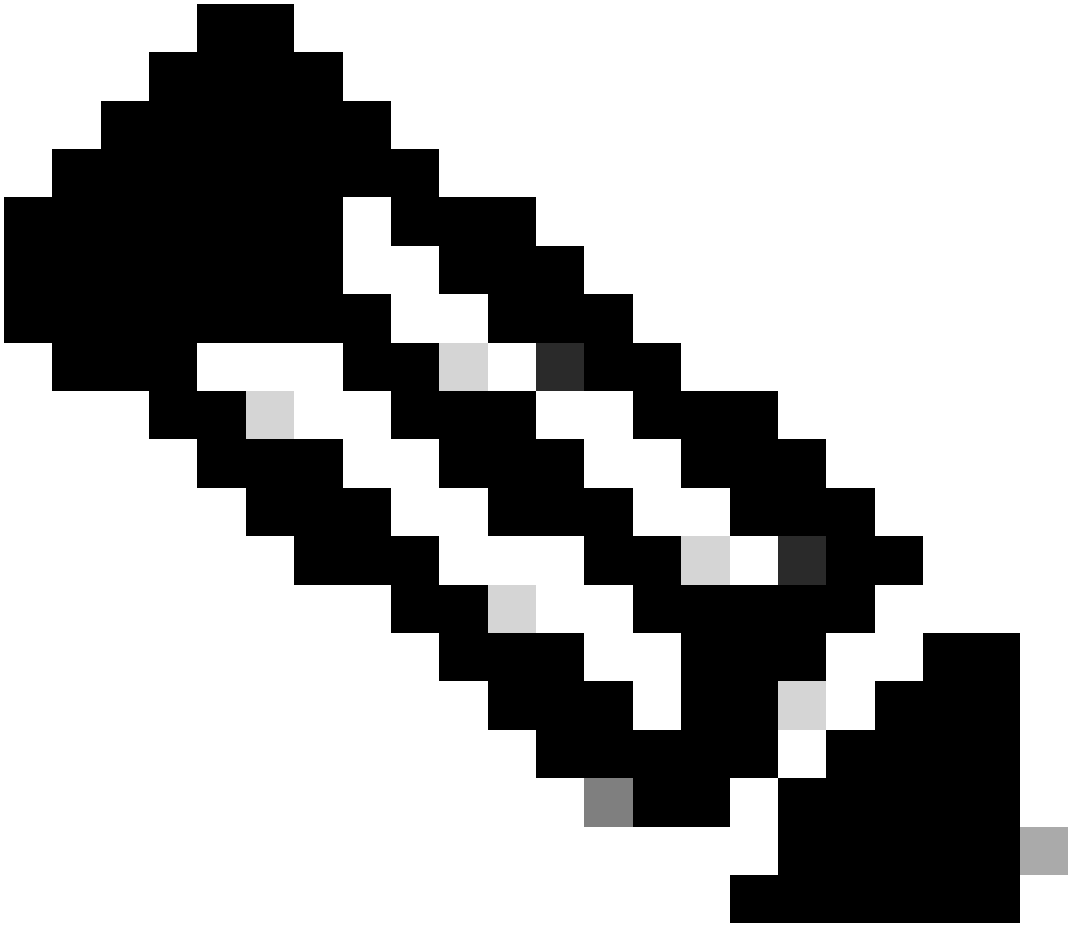
Gardez à l'esprit que le point d'accès doit avoir une adresse IP avant de pouvoir démarrer le processus CAPWAP. Si le point d'accès n'a pas d'adresse IP, il ne lance pas le processus d'établissement de session CAPWAP.

1. Le point d'accès envoie une demande de détection. Voir la section Méthodes de détection de WLC pour plus d'informations sur cela
2. Le WLC envoie une réponse de détection
3. Établissement de session DTLS. Ensuite, tous les messages qui suivent sont chiffrés et sont affichés sous forme de paquets de données d'application DTLS dans n'importe quel outil d'analyse de paquets.
4. Le point d'accès envoie une demande de jointure

5. Le WLC envoie une réponse de jointure
6. Le point d’accès effectue un contrôle d’image. S'il a la même version d'image que le WLC, alors il passe à l'étape suivante. Si ce n'est pas le cas, il télécharge l'image à partir du WLC et redémarre pour charger la nouvelle image. Dans ce cas, il répète le processus de l'étape 1.
7. Le point d'accès envoie une demande d'état de configuration.
8. WLC envoie une réponse d'état de configuration
9. Le point d'accès passe à l'état RUN
10. Pendant l'état RUN, la maintenance du tunnel CAPWAP est effectuée de deux manières :
    1. Des messages de test sont échangés pour maintenir le tunnel de données CAPWAP
    2. AP envoie une requête d'écho au WLC, qui doit recevoir une réponse avec sa réponse d'écho respective. Ceci permet de maintenir le tunnel de contrôle CAPWAP.



Processus d'établissement de session CAPWAP



Remarque : Conformément à la RFC 5415, CAPWAP utilise les ports UDP 5246 (pour le contrôle CAPWAP) et 5247 (pour les données CAPWAP).

Établissement de session DTLS

Une fois que le point d'accès reçoit une réponse de détection valide du WLC, un tunnel DTLS est établi entre eux pour transmettre tous les paquets suivants sur un tunnel sécurisé. Il s'agit du processus d'établissement de la session DTLS :

1. AP envoie un message Hello client
2. Le WLC envoie un message HelloVerifyRequest avec un cookie utilisé pour la validation.
3. AP envoie un message ClientHello avec un cookie utilisé pour la validation.
4. WLC envoie ces paquets dans l'ordre suivant :
    1. ServerHello
    2. Certificat
    3. Échange de clés de serveur
    4. requête de certificat

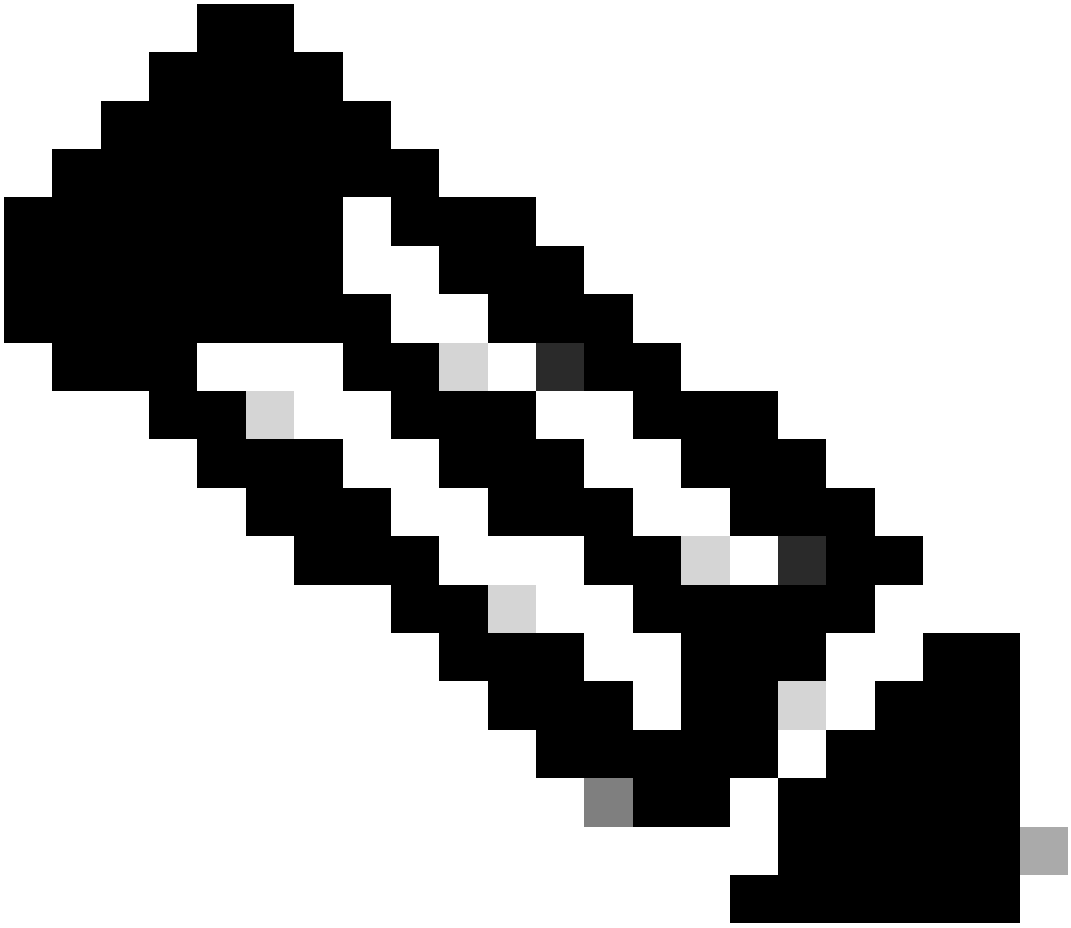
    5. ServeurHelloTerminé
5. AP envoie ces paquets dans l'ordre :
    1. Certificat
    2. ÉchangeCléClient
    3. Vérification du certificat
    4. ModifierSpécificationChiffre
6. WLC répond aux AP ChangeCipherSpec avec son propre ChangedCipherSpec :
    1. ModifierSpécificationChiffre

Après le dernier message ChangedCipherSpec envoyé par le WLC, le tunnel sécurisé est établi et tout le trafic envoyé dans les deux directions est maintenant chiffré.

Méthodes de détection de contrôleur LAN sans fil

Il existe plusieurs options pour informer les points d'accès de l'existence d'un WLC dans le réseau :

- Option DHCP 43 : Cette option fournit aux AP l'adresse IPv4 du WLC à joindre. Ce processus est pratique pour les grands déploiements dans lesquels les AP et le WLC sont dans des sites différents.
- Option DHCP 52 : Cette option fournit aux AP l'adresse IPv6 du WLC à joindre. Son utilisation est pratique dans le même scénario que l'option DHCP 43.
- Détection DNS : Les AP interrogent le nom de domaine CISCO-CAPWAP-CONTROLLER.localdomain. Vous devez configurer votre serveur DNS pour résoudre l'adresse IPv4 ou IPv6 du WLC à joindre. Cette option est pratique pour les déploiements dans lesquels les WLC sont stockés dans le même site que les AP.
- Diffusion de couche 3 : Les points d’accès envoient automatiquement un message de diffusion à 255.255.255.255. Tout WLC dans le même sous-réseau que le point d’accès est censé répondre à cette demande de détection.
- Configuration statique : Vous pouvez utiliser la commande capwap primary-base **<**wlc-hostname**>** **<**wlc-IP-address**>** pour configurer une entrée statique pour un WLC dans le point d'accès.
- Découverte de la mobilité : Si l'AP était précédemment joint à un WLC qui faisait partie d'un groupe de mobilité, l'AP enregistre également un enregistrement des WLC présents dans ce groupe de mobilité.



Remarque : Les méthodes de détection WLC répertoriées n'ont pas d'ordre de priorité.

Choix du contrôleur LAN sans fil

Une fois que le point d'accès a reçu une réponse de détection de n'importe quel WLC utilisant l'une des méthodes de détection de WLC, il sélectionne un contrôleur à joindre avec ce critère :

1. Contrôleur principal (configuré avec la commande capwap primary-base <wlc-hostname> <wlc-IP-address>)
2. Contrôleur secondaire (configuré avec la commande capwap secondary-base <wlc-hostname> <wlc-IP-address>)
3. Tertiary Controller (configuré avec la commande capwap tertiary-base <wlc-hostname> <wlc-IP-address>)
4. Si aucun WLC primaire, secondaire ou tertiaire n'a été configuré précédemment, alors l'AP tente de joindre le premier WLC qui a répondu à la demande de détection avec sa propre réponse de détection qui a la capacité maximale des AP disponibles (c'est-à-dire, le WLC qui peut prendre en charge le plus d'AP à un moment donné).

Machine d'état CAPWAP

Dans la console AP, vous pouvez suivre la machine d'état CAPWAP, qui passe en revue les étapes décrites dans la section Établissement de session CAPWAP.

État CAPWAP : Découverte

Ici, vous pouvez voir les demandes et les réponses de détection. Observez comment l'AP reçoit une IP de WLC via DHCP (Option 43), et envoie également une requête de découverte aux WLC connus précédemment :

<#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

En plus de la réception d'une réponse de détection à la fois d'un WLC configuré statiquement (172.16.0.20) et du WLC indiqué par l'option DHCP 43 (172.16.5.11), cet AP a également reçu une réponse de détection d'un autre WLC (172.16.5.169) dans le même sous-réseau parce qu'il a reçu le message de détection de diffusion.

État CAPWAP : Configuration DTLS.

Ici, la session DTLS entre l'AP et le WLC est échangée.

<#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

État CAPWAP : Se Joindre

Après avoir établi la session DTLS, une demande de jonction au WLC est maintenant envoyée sur la session sécurisée. Observez comment cette demande reçoit immédiatement une réponse Join Response du 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

État CAPWAP : Données d'image

Le point d'accès compare son image avec l'image du WLC. Dans ce cas, à la fois la partition active des AP et sa partition de sauvegarde ont des images différentes du WLC, de sorte qu'il appelle le script upgrade.sh, qui demande à l'AP de demander l'image adéquate au WLC et de la télécharger dans sa partition non active actuelle.

<#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
```

Une fois le transfert d'image terminé, le point d'accès lance un processus de vérification de signature d'image pour le valider. Après cela, le script upgrade.sh installe l'image dans la partition non active actuelle, et échange la partition à partir de laquelle elle démarre. Enfin, l'AP se recharge et répète le processus depuis le début (CAPWAP State : Découvrir).

<#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]

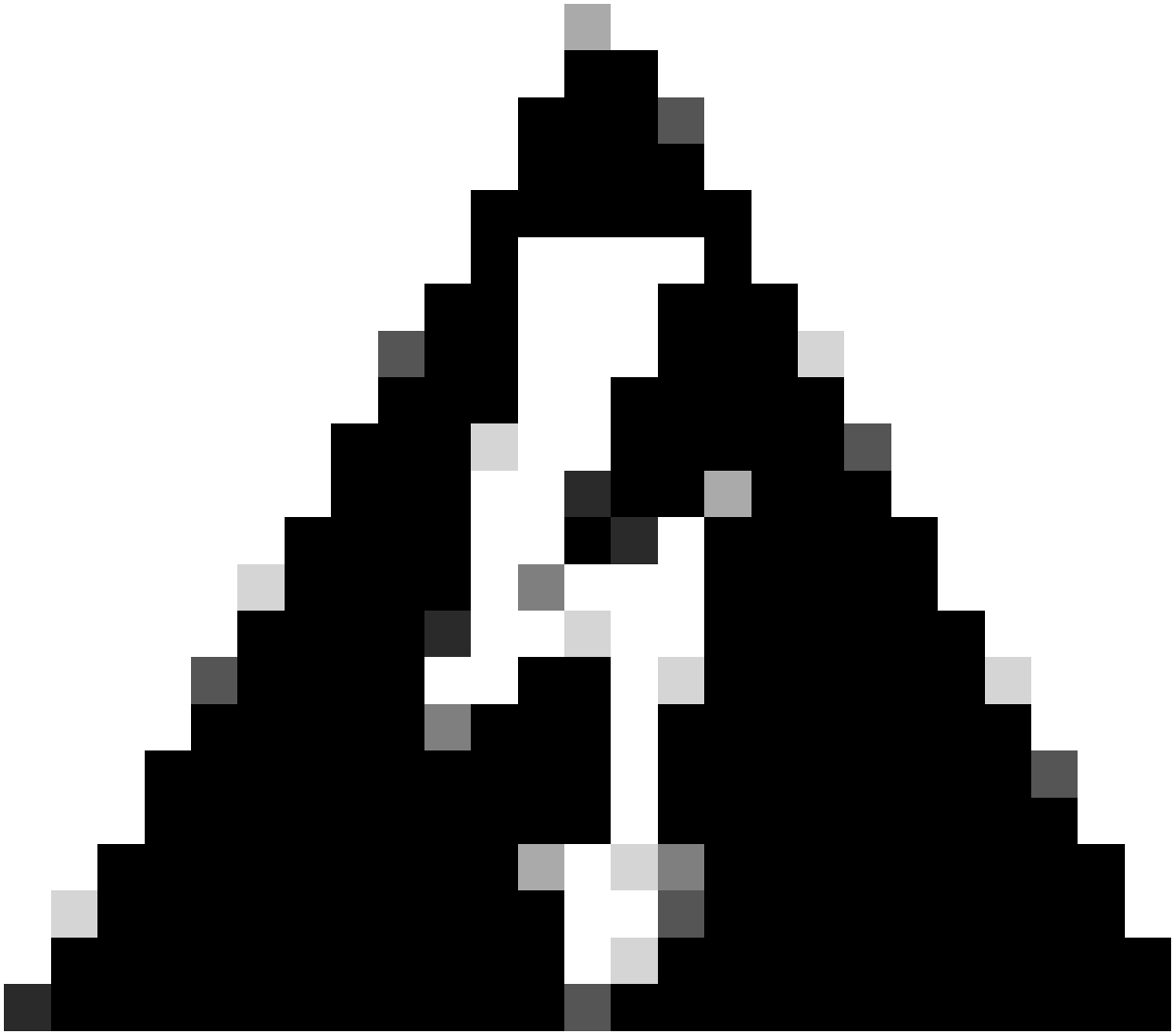
upgrade.sh

: 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



Avertissement : Le téléchargement d'une nouvelle image par les points d'accès de phase 1 peut échouer en raison de l'expiration d'un certificat. Veuillez vous reporter à la notice 72524 pour plus d'informations et lire attentivement le document d'assistance Cisco IOS AP Image Download Fails Due to Expired Image Signing Certificate Past December 4th, 2022 (CSCwd80290) Support Document pour comprendre son impact et sa solution.

Une fois que l'AP se recharge et passe à nouveau par les états CAPWAP Discover et Join, pendant l'état Image Data, il détecte qu'il a maintenant l'image adéquate.

<#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
```

État CAPWAP : Configurer

Une fois que l'AP a validé qu'il a la même version que le WLC, il notifie ses configurations actuelles au WLC. En général, cela signifie que l'AP demande de maintenir ses configurations (si elles sont disponibles dans le 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
```

État CAPWAP : Exécutez la commande

À ce stade, le point d'accès a rejoint avec succès le contrôleur. Pendant cet état, le WLC déclenche un mécanisme pour remplacer la configuration demandée par l'AP. Vous pouvez voir que l'AP obtient des configurations Radio et Credentials poussées, et il est également assigné à la balise de stratégie par défaut puisque le WLC n'avait aucune connaissance précédente de cet 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]

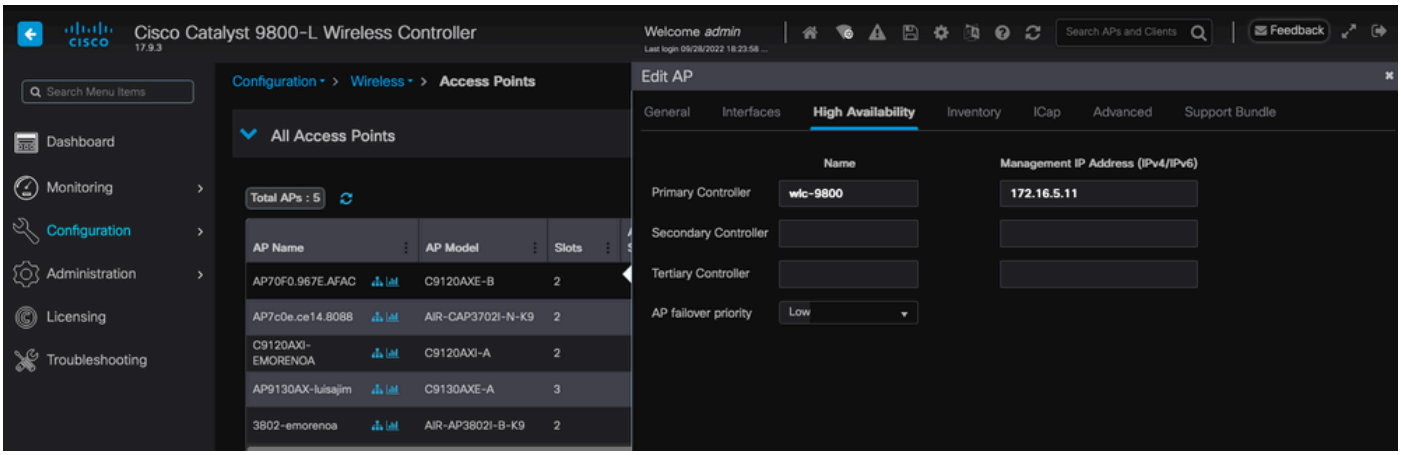
AP tag change to default-policy-tag

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

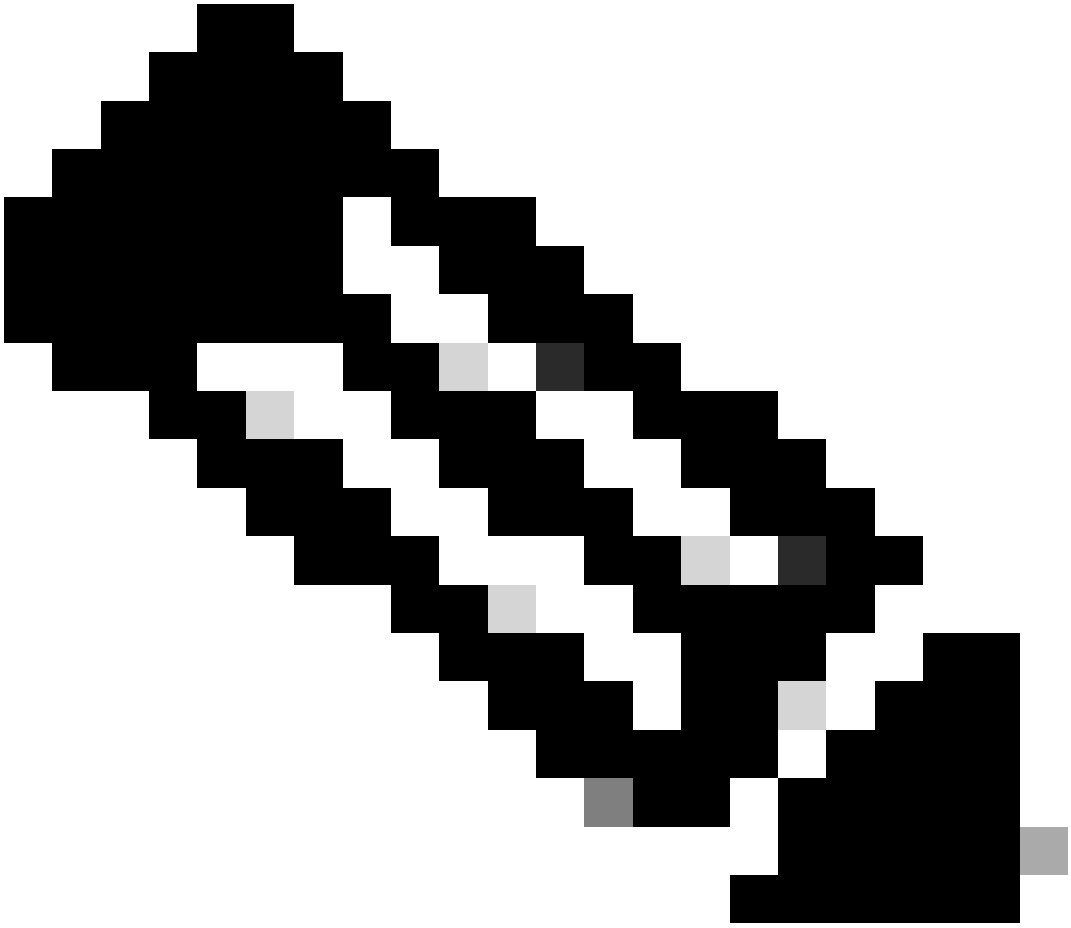
Configurer

Choix du WLC statique

Dans l'interface graphique utilisateur, vous pouvez aller à Configuration > Wireless > Access Points, sélectionnez un AP et naviguez jusqu'à l'onglet High Availability. Ici, vous pouvez configurer les WLC principal, secondaire et tertiaire, comme décrit dans la section Sélection du contrôleur LAN sans fil de ce document. Cette configuration est effectuée par point d'accès.



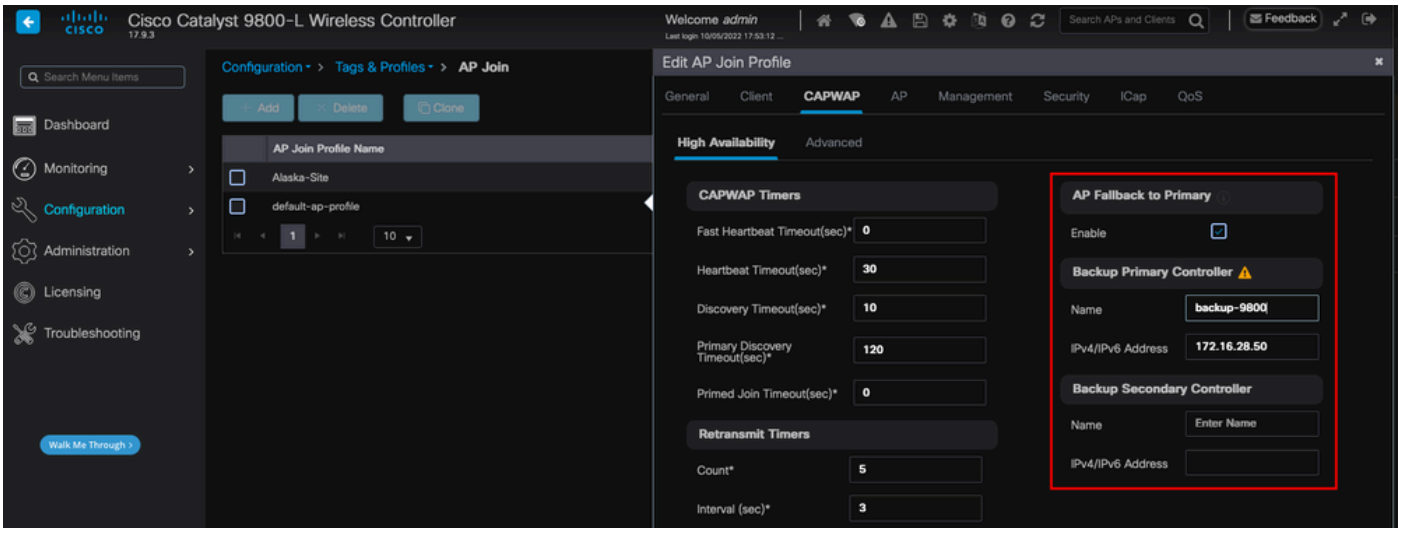
WLC principaux, secondaires et tertiaires pour un point d'accès.



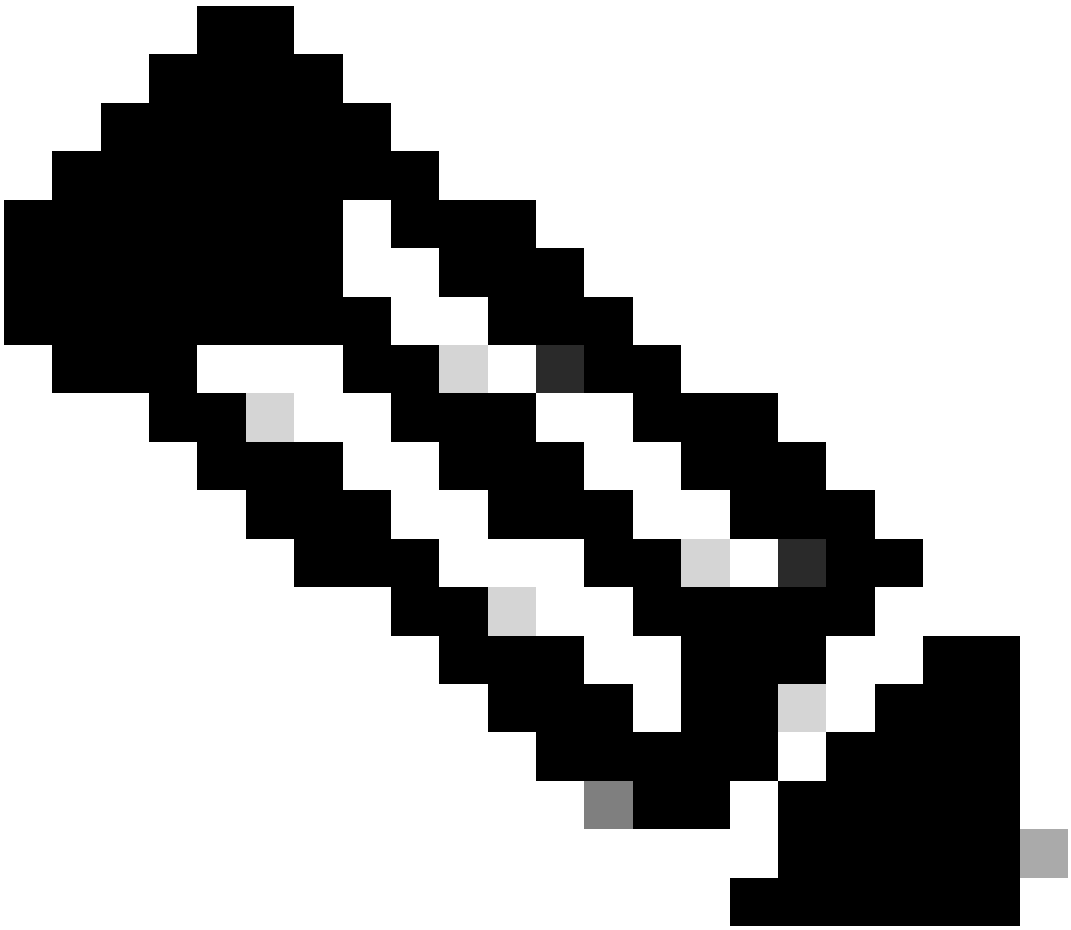
Remarque : À partir de Cisco IOS XE 17.9.2, vous pouvez utiliser les profils d'amorçage pour configurer des contrôleurs principaux, secondaires et tertiaires pour un groupe d'AP correspondant à une expression régulière (regex) ou pour un AP individuel. Référez-vous à la section AP Fallback to Controllers Configured Under AP Priming Profile du Guide de configuration pour plus d'informations.

Veuillez noter que les contrôleurs principal, secondaire et tertiaire configurés dans l'onglet AP High Availability diffèrent des WLC principaux et secondaires de sauvegarde qui peuvent être configurés par AP Join Profile sous l'onglet CAPWAP > High Availability. Les contrôleurs principal, secondaire et tertiaire sont considérés comme des WLC avec les priorités 1, 2 et 3, respectivement, tandis que les contrôleurs principal et secondaire de secours sont considérés comme des WLC avec les priorités 4 et 5.

Si AP Fallback est activé, l'AP recherche activement le contrôleur principal lorsqu'il est joint à un autre WLC. Le point d'accès recherche uniquement les WLC avec les priorités 4 et 5 une fois qu'il y a un événement CAPWAP Down et aucun des contrôleurs principal et secondaire de secours n'est disponible.



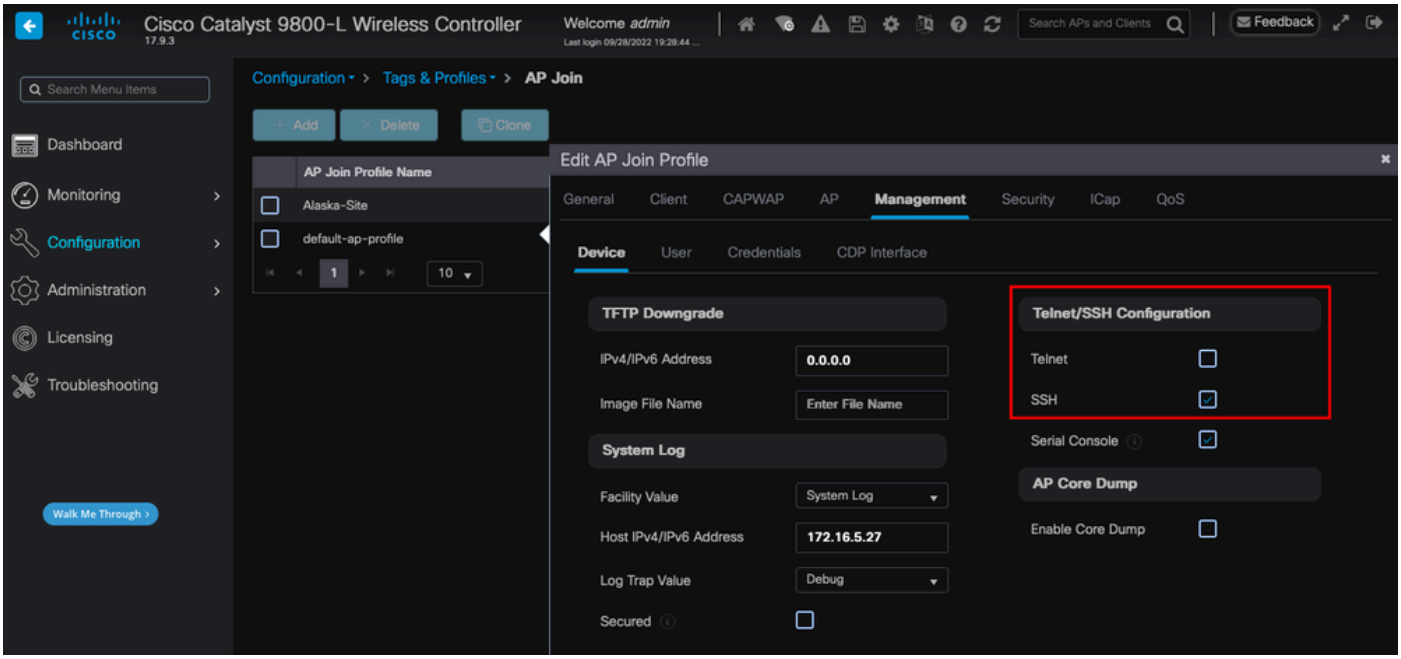
Options de haute disponibilité dans le profil de jonction AP



Remarque : La configuration des WLC principal et secondaire de secours dans le profil de jonction AP ne remplit pas les entrées Static Primary et Secondary dans l'onglet High Availability du point d'accès.

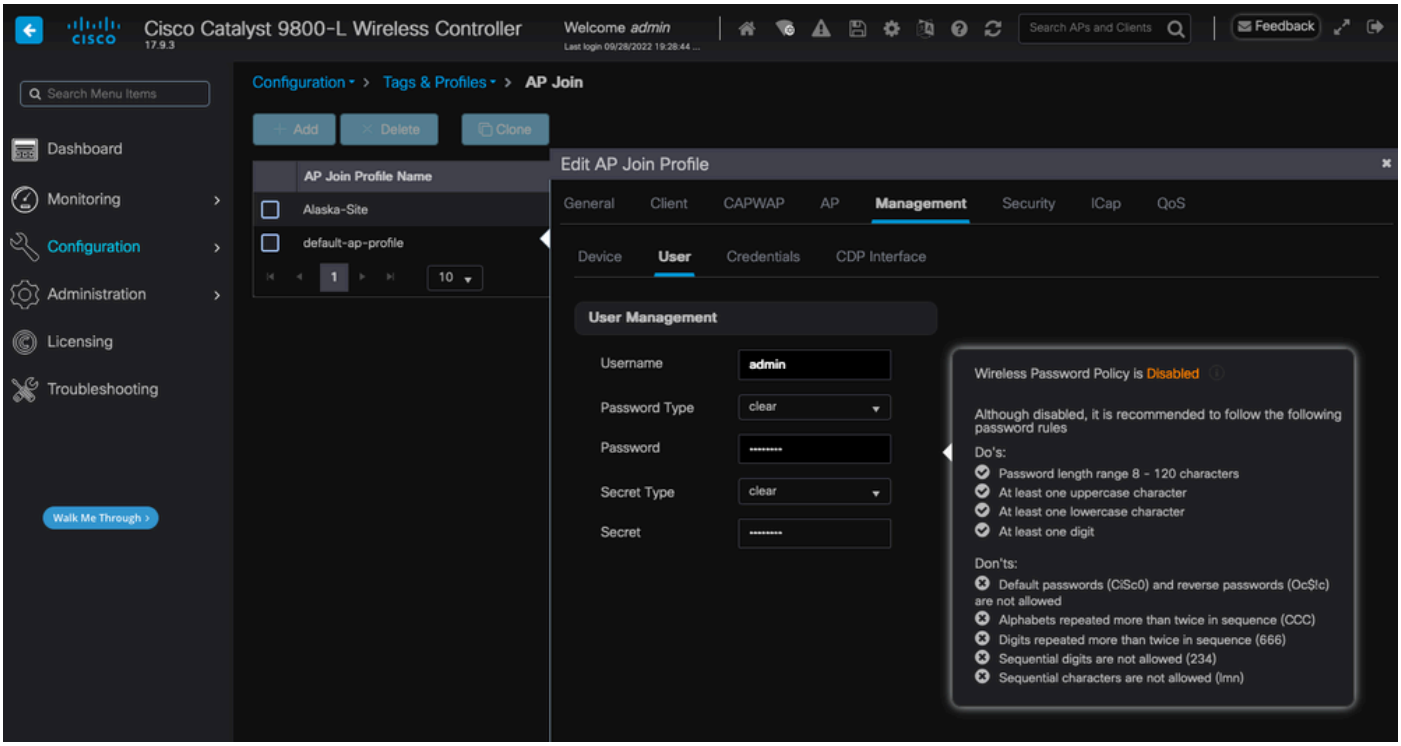
Activation de l'accès Telnet/SSH au point d'accès

Accédez à Configuration > Tags & Profiles > AP Join > Management > Device et sélectionnez SSH et/ou Telnet.



Activer l'accès Telnet/SSH sur le profil de jonction AP

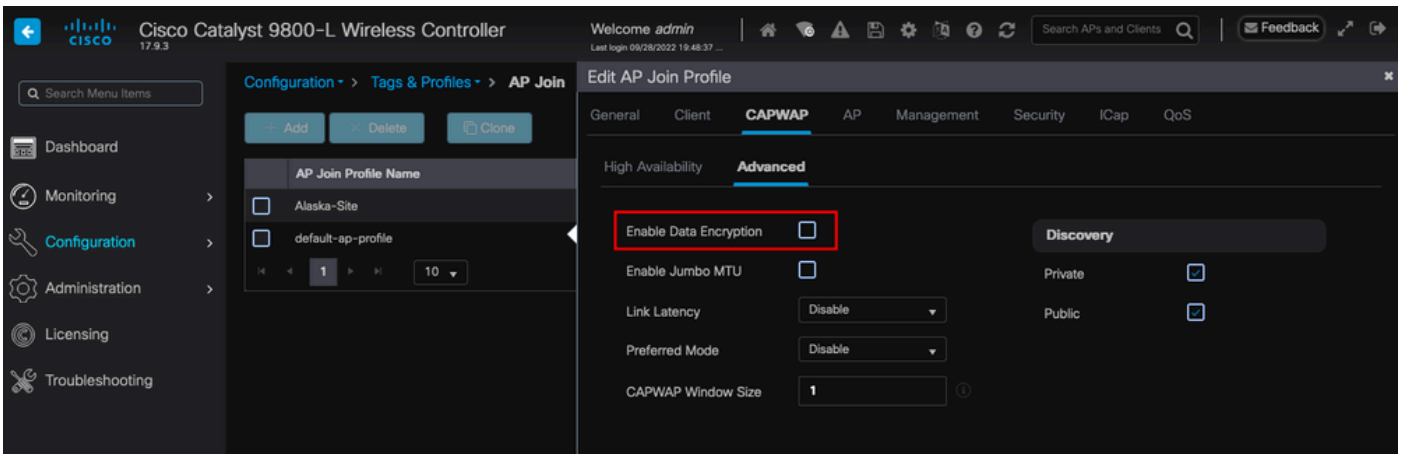
Pour configurer les informations d'identification SSH/Telnet, accédez à l'onglet User dans la même fenêtre et définissez le nom d'utilisateur, le mot de passe et le secret pour accéder à l'AP.



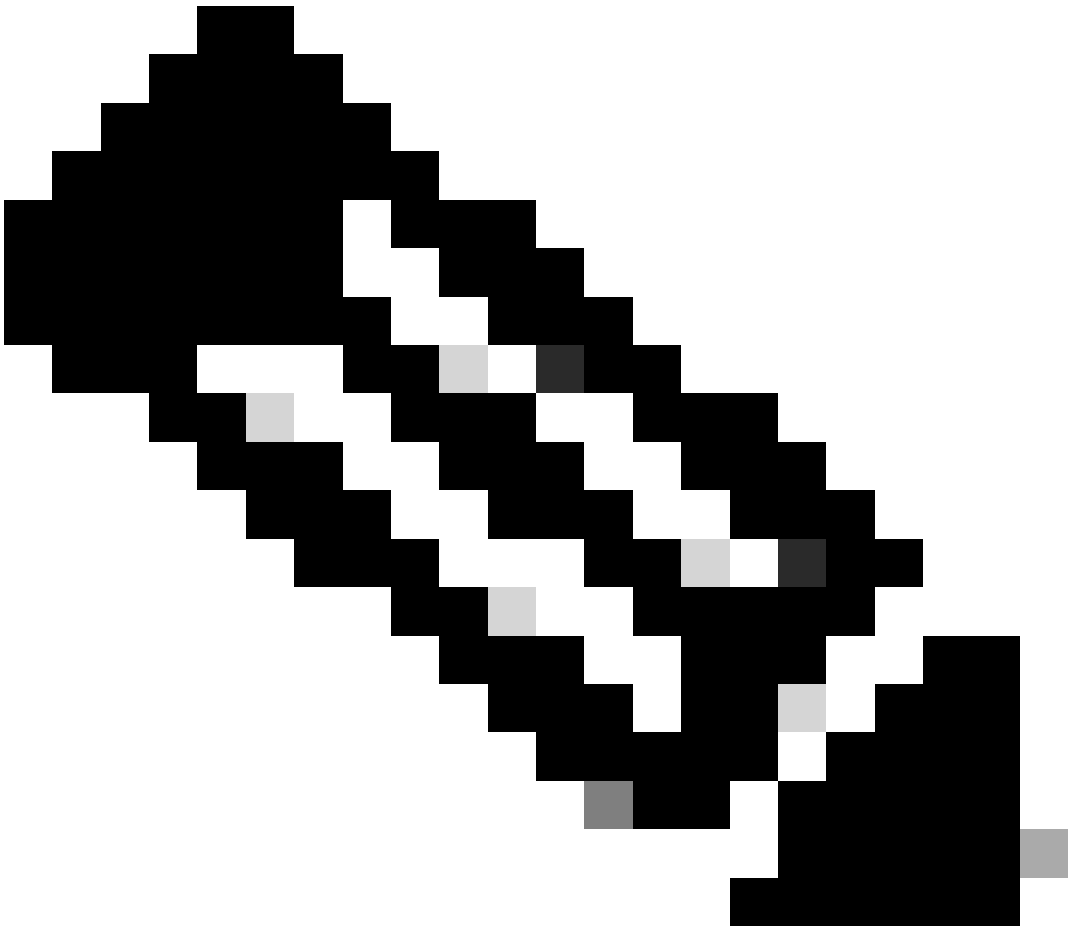
Identifiants SSH et Telnet pour l'AP

Chiffrement de liaison de données

Si vous avez besoin de dépanner un problème client qui vous oblige à prendre une capture de paquet du trafic des AP, assurez-vous que le cryptage de liaison de données n'est pas activé sous Configuration > Tags & Profiles > AP Join > CAPWAP > Advanced. Sinon, votre trafic est chiffré.



Chiffrement de liaison de données

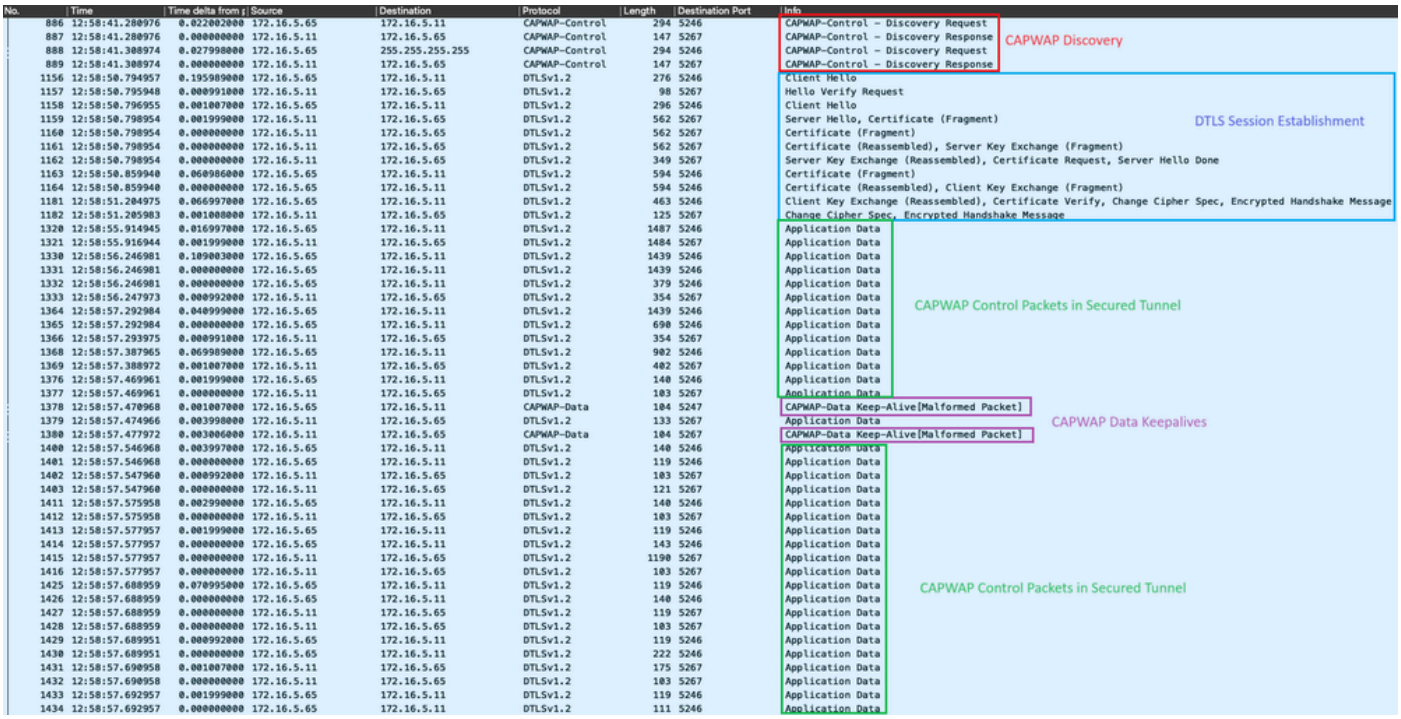


Remarque : Chiffrement des données chiffre uniquement le trafic de données CAPWAP.

Le trafic de contrôle CAPWAP est déjà chiffré via DTLS.

Vérifier

En plus du suivi de la machine d'état CAPWAP dans la console des AP, vous pouvez également prendre une capture de paquets incorporée dans le WLC pour analyser le processus de jointure d'AP :



Processus de jointure d'AP vu dans une capture de paquets intégrée dans le WLC

Notez que tout le trafic après le paquet Chance Cipher Spec (paquet n° 1182) est affiché uniquement comme données d'application sur DTLSv1.2. Il s'agit de toutes les données chiffrées après l'établissement de la session DTLS.

Dépannage

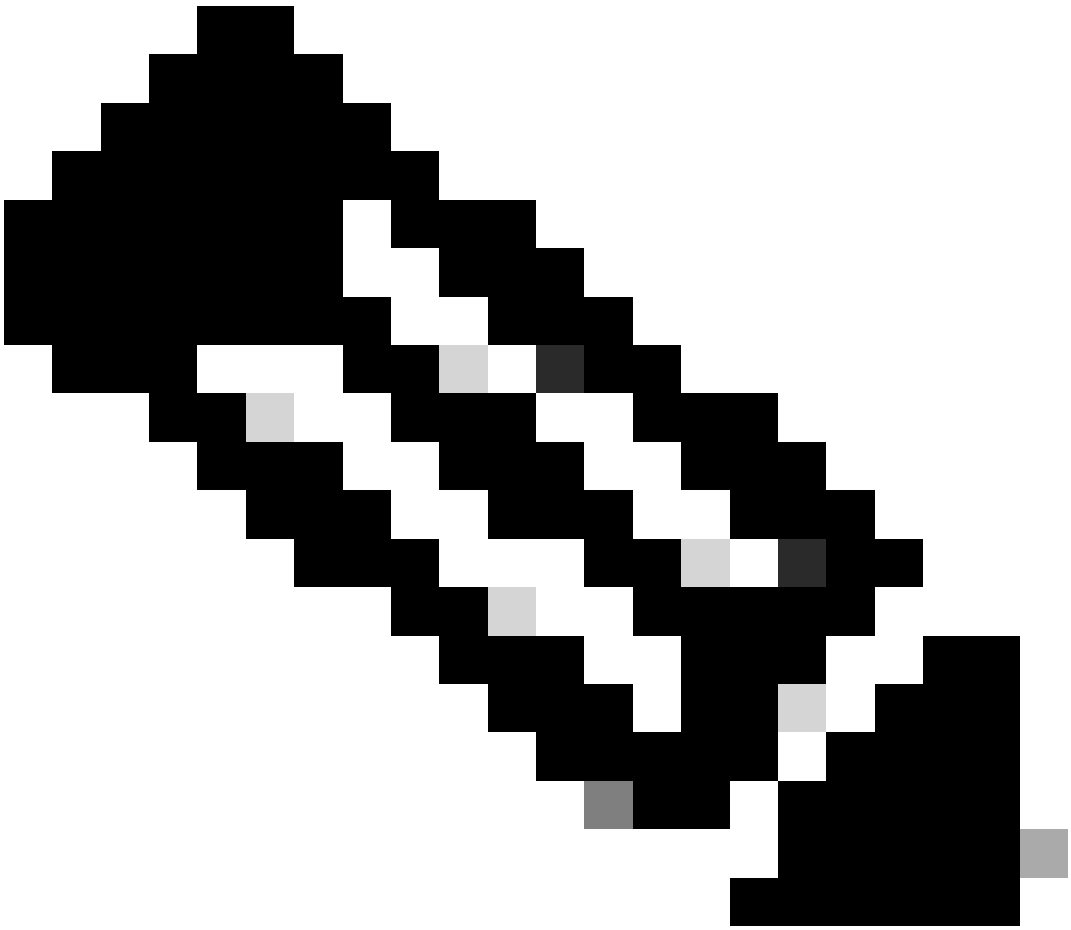
Problèmes identifiés

Veuillez vous reporter aux problèmes connus qui pourraient empêcher vos AP de rejoindre le WLC.

- Points d'accès sur la boucle de démarrage en raison d'une image corrompue dans les points d'accès Wave 2 et Catalyst 11ax (CSCvx32806)
- Avis de champ 72424 : Les points d'accès C9105/C9120/C9130 fabriqués à partir de septembre 2022 peuvent nécessiter des mises à niveau logicielles pour rejoindre les contrôleurs LAN sans fil.
- Avis de champ 72524 : Pendant la mise à niveau/rétrogradation du logiciel, les points

d'accès Cisco IOS peuvent rester à l'état de téléchargement après le 4 décembre 2022 en raison de l'expiration du certificat - Mise à niveau du logiciel recommandée
- ID de bogue Cisco CSCwb13784 : Les AP ne peuvent pas joindre 9800 en raison d'un MTU de chemin non valide dans la demande de jointure AP
- ID de bogue Cisco CSCvu22886 : C9130 : message "unlzma : écrire : Pas d'espace restant sur le périphérique lors de la mise à niveau vers 17.7 Augmenter la taille maximale de /tmp

Consultez toujours la section Chemin de mise à niveau des Notes de publication de chaque version avant de procéder à la mise à niveau.

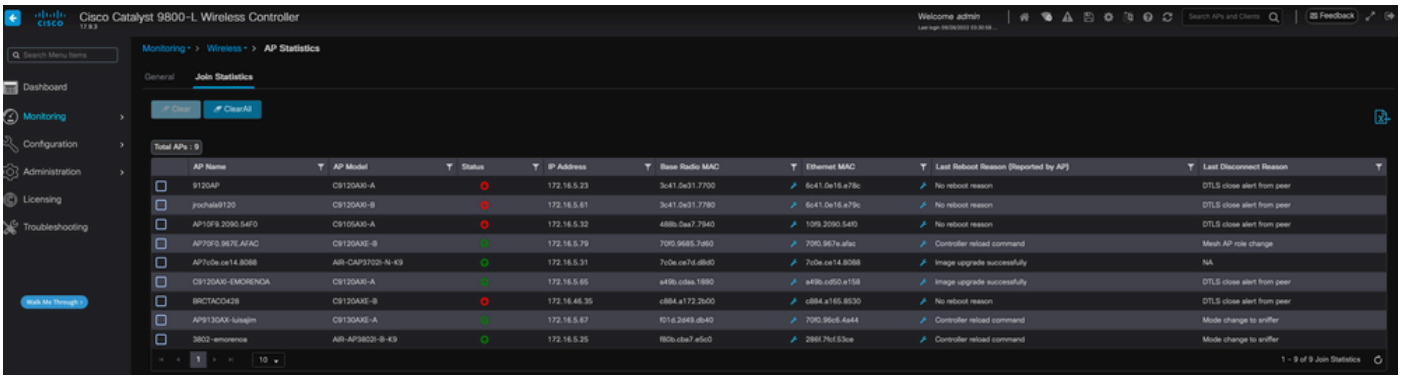


> Remarque : À partir de Cisco IOS XE Cupertino 17.7.1, le contrôleur sans fil Cisco Catalyst 9800-CL n'accepte pas plus de 50 points d'accès si la licence Smart n'est pas connectée et active.

Vérifications de GUI WLC

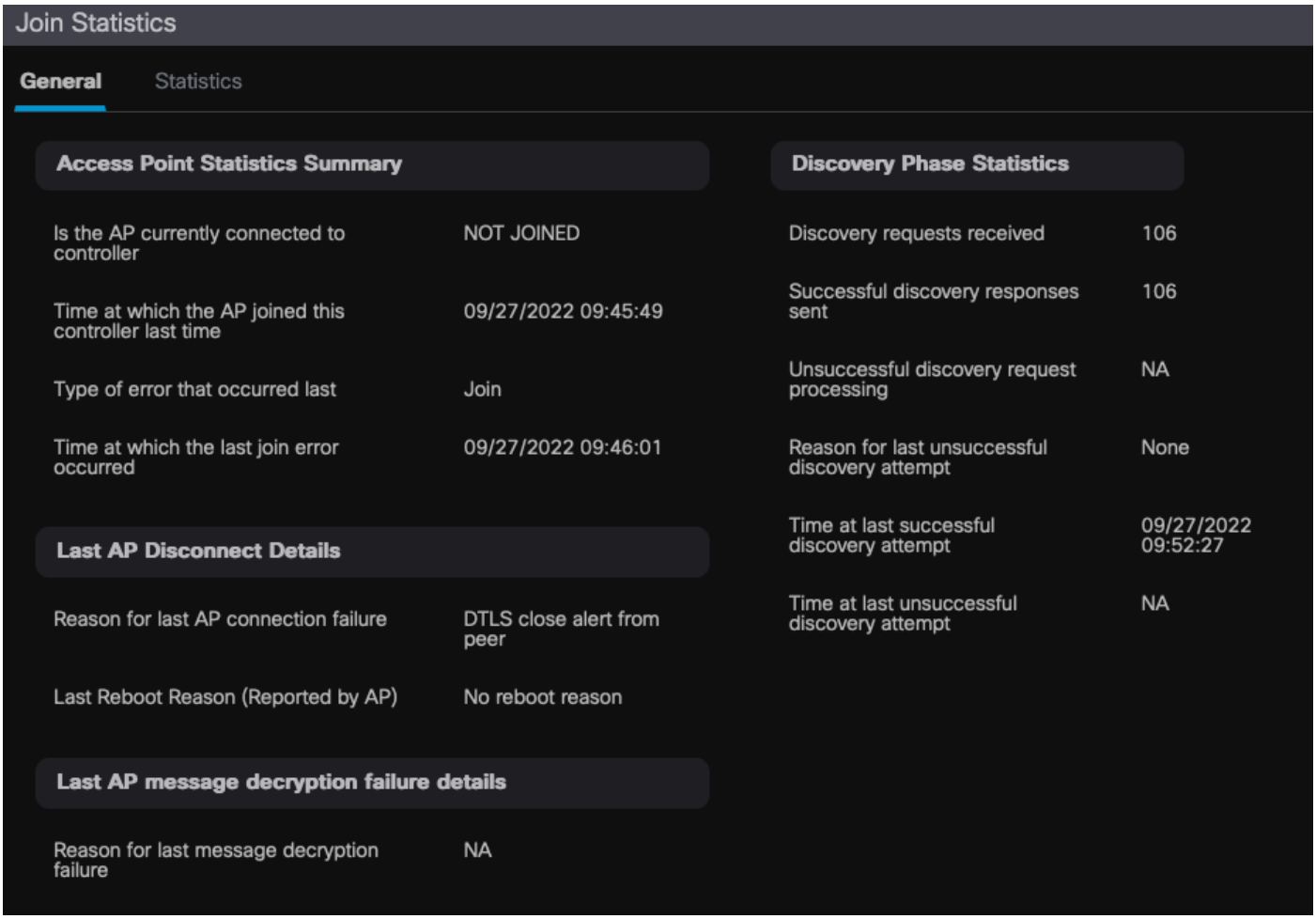
Sur votre WLC, accédez à Monitoring > Wireless > AP Statistics > Join Statistics vous pouvez voir

la Dernière raison de redémarrage signalée par n'importe quel AP et la Dernière raison de déconnexion enregistrée par le WLC.



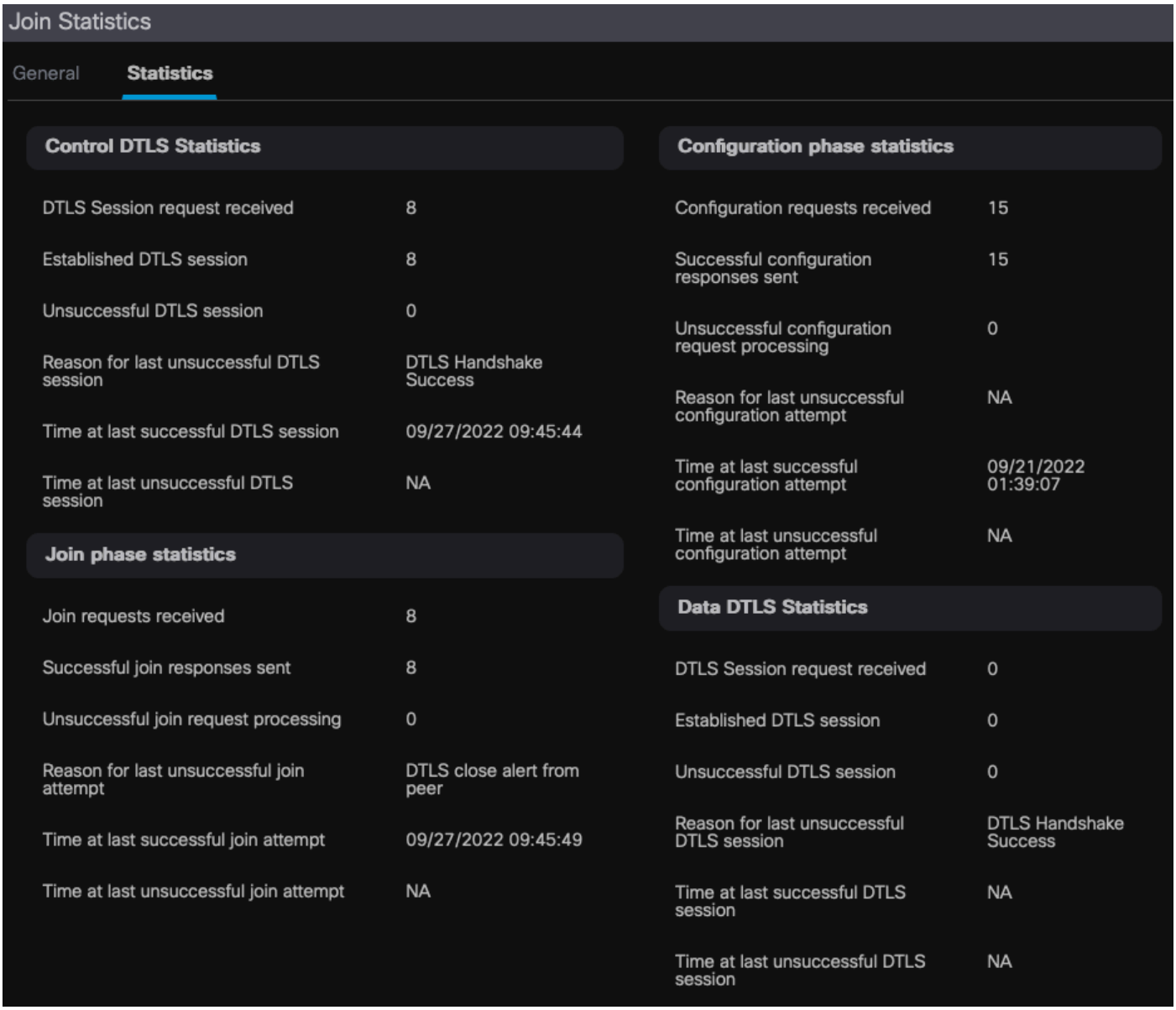
Page AP Join Statistics sur le WLC

Vous pouvez cliquer sur n'importe quel point d'accès et vérifier les détails des statistiques de jonction AP. Ici, vous pouvez voir des informations plus détaillées, comme l'heure et la date à laquelle l'AP s'est joint pour la dernière fois et a tenté de découvrir le WLC.



Statistiques générales de jointure AP

Pour plus d'informations, accédez à l'onglet Statistiques de la même fenêtre. Vous pouvez ici comparer le nombre de réponses de jointure envoyées avec le nombre de demandes de jointure reçues, ainsi que le nombre de réponses de configuration envoyées par rapport au nombre de demandes de configuration reçues.



Statistiques détaillées de jointure AP

Commandes

Ces commandes sont utiles pour dépanner les problèmes de jointure AP :

À partir du WLC

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

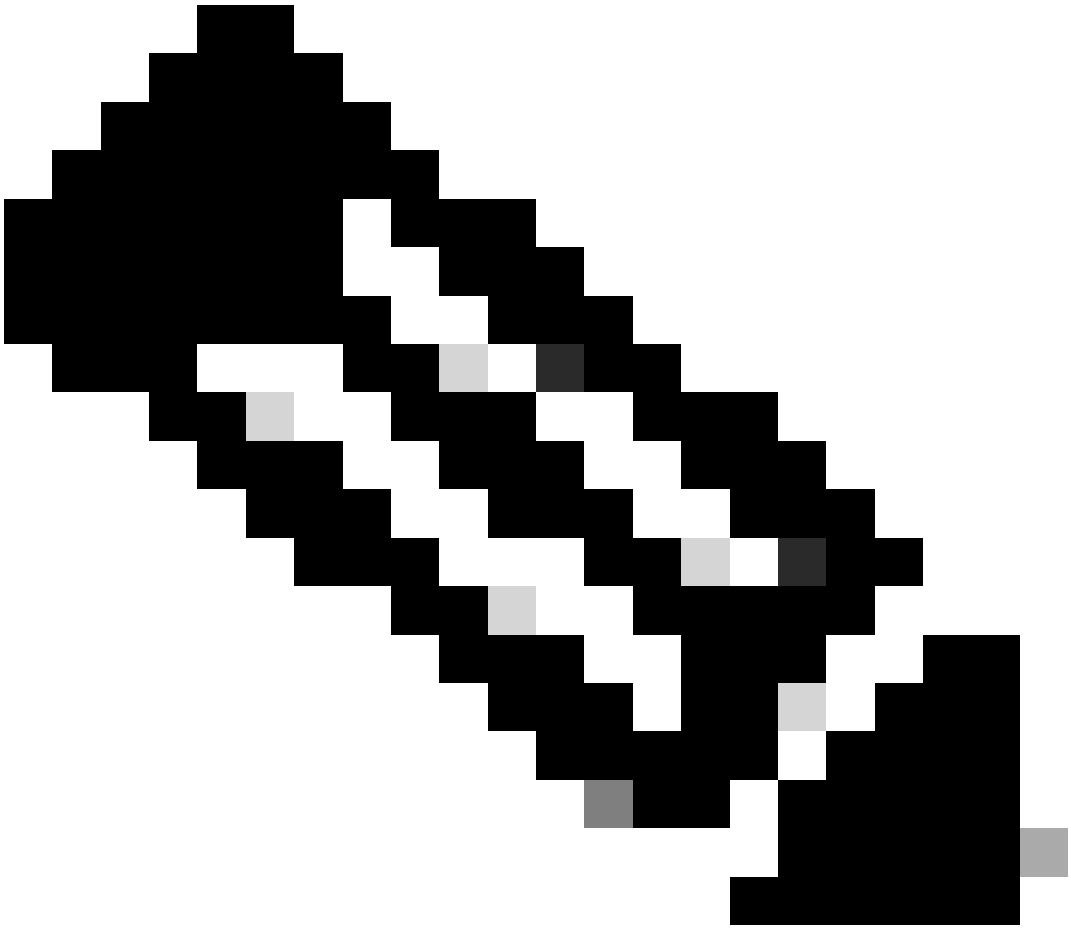
Depuis les points d'accès Wave 2 et Catalyst 11ax

- debug capwap client events (débogage des événements clients capwap)
- debug capwap client error
- debug dtls client error
- debug dtls client event

- debug capwap client keepalive
- redémarrage du capwap de test
- capwap ap erase all

À partir des points d'accès Wave 1

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



> Remarque : Lorsque vous vous connectez aux AP via Telnet/SSH pour dépanner, émettez toujours la commande terminal monitor tout en reproduisant le problème après l'activation des débogages sur les AP. Sinon, vous ne pouvez pas voir les résultats des débogages.

Traces radioactives

Un bon point de départ lors du dépannage des problèmes de jonction d'AP est de prendre des traces radioactives des adresses MAC radio et Ethernet d'un AP qui a des problèmes de jonction. Référez-vous à la collection Debug & Log sur le document WLC Catalyst 9800 pour plus de détails sur la génération de ces journaux.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.