Dépannage d’un point d’accès allégé qui ne parvient pas à se connecter à un WLC

Table des matières

Introduction

Ce document décrit le processus de détection et de jonction du contrôleur LAN sans fil (WLC) AireOS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration des points d'accès légers (LAP) et des WLC Cisco AireOS
- Connaissances de base du protocole CAPWAP (Lightweight Access Point Protocol)

Composants utilisés

Ce document se concentre sur les WLC AireOS et ne couvre pas Catalyst 9800 bien que le processus de jointure soit principalement similaire.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Présentation du processus de détection et de jonction WLC

Dans un réseau sans fil unifié Cisco, les LAP doivent d'abord détecter et joindre un WLC avant de pouvoir prendre en charge des clients sans fil.

Cependant, ceci présente une question : comment les LAP ont-ils trouvé l'adresse IP de gestion du contrôleur quand il est sur un sous-réseau différent ?

Si vous ne dites pas au LAP où se trouve le contrôleur via l'option DHCP 43, la résolution DNS (Domain Name System) de Cisco-capwap-controller.local_domain, ou si vous le configurez statiquement, le LAP ne sait pas où trouver l'interface de gestion du contrôleur sur le réseau.

En plus de ces méthodes, le LAP recherche automatiquement sur le sous-réseau local les contrôleurs ayant la diffusion locale 255.255.255.255. En outre, le LAP se souvient de l'adresse IP de gestion de son contrôleur et des contrôleurs présents en tant qu'homologues de mobilité même lors des redémarrages. Cependant, dès que l'AP rejoint un autre WLC, il ne se souvient que de l'IP de ce nouveau WLC et de ses homologues de mobilité et non des précédents. Par conséquent, si vous placez le LAP en premier sur le sous-réseau local de l'interface de gestion, il trouve l'interface de gestion du contrôleur et se souvient de l'adresse. Cela est appelé « priming ». Cela ne permet pas de trouver le contrôleur si vous remplacez un LAP par la suite. Par conséquent, Cisco recommande l'utilisation de l'option DHCP 43 ou des méthodes DNS.

Les LAP se connectent toujours à l'adresse de l'interface de gestion du contrôleur d'abord avec une demande de détection. Le contrôleur indique ensuite au LAP l'adresse IP de l'interface du gestionnaire AP de couche 3 (qui peut également être la gestion par défaut) afin que le LAP puisse ensuite envoyer une requête de jointure à l'interface du gestionnaire AP.

Le point d'accès suit ce processus au démarrage :

- **Le LAP démarre et applique DHCP à une adresse IP si aucune adresse IP statique ne lui a été précédemment assignée.**

- **Le LAP envoie des demandes de détection aux contrôleurs via les divers algorithmes de détection et établit une liste de contrôleurs. En fait, le LAP apprend autant d'adresses d'interface de gestion que possible pour la liste de contrôleurs via :**

a. **DHCP option 43 (convient aux entreprises internationales dont les bureaux et les contrôleurs se trouvent sur différents continents).**

b. **L'entrée DNS pour** cisco-capwap-controller (bon pour les entreprises locales - peut également être utilisée pour trouver où de nouveaux points d'accès se joignent) Si vous utilisez CAPWAP, assurez-vous qu'il y a une entrée DNS pour cisco-capwap-controller.

- **Les adresses IP de gestion des contrôleurs dont le LAP se souvient précédemment.**
- **Une diffusion de couche 3 sur le sous-réseau.**
- **Les informations configurées statiquement.**
- **Contrôleurs présents dans le groupe de mobilité du WLC auquel l'AP a rejoint pour la dernière fois.**

Dans cette liste, la méthode la plus simple à utiliser pour le déploiement est d'avoir les LAP sur le même sous-réseau que l'interface de gestion du contrôleur et d'autoriser la diffusion de couche 3 des LAP pour trouver le contrôleur. Cette méthode doit être utilisée pour les entreprises disposant d'un petit réseau et ne possédant pas de serveur DNS local.

La méthode la plus facile suivante du déploiement consiste à utiliser une entrée DNS avec DHCP. Vous pouvez avoir plusieurs entrées du même nom DNS. Cela permet au LAP de détecter plusieurs contrôleurs. Cette méthode doit être utilisée par les entreprises qui ont tous leurs contrôleurs dans un emplacement unique et qui possèdent un serveur DNS local. Elle doit être utilisée également si la société a plusieurs suffixes DNS et que les contrôleurs sont isolés par suffixe.

L'option DHCP 43 est utilisée par les grandes entreprises pour localiser les informations par le protocole DHCP. Cette méthode est utilisée par les grandes entreprises qui ont un suffixe DNS unique. Par exemple, Cisco possède des locaux en l'Europe, en Australie et aux États-Unis. Afin de garantir que les LAP joignent les contrôleurs uniquement localement, Cisco ne peut pas utiliser une entrée DNS et doit utiliser les informations de l'option DHCP 43 pour indiquer aux LAP quelle est l'adresse IP de gestion de leur contrôleur local.

Enfin, la configuration statique est utilisée pour un réseau qui n'a pas de serveur DHCP. Vous pouvez configurer statiquement les informations nécessaires pour joindre un contrôleur par le port de console et l'interface de ligne de commande des AP. Pour plus d'informations sur la façon de configurer statiquement les informations du contrôleur à l'aide de l'interface de ligne de commande AP, utilisez cette commande :

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

Pour plus d'informations sur la façon de configurer l'option DHCP 43 sur un serveur DHCP, consultez l'exemple de configuration de l'option DHCP 43

- Envoyez une requête de détection à chaque contrôleur de la liste et attendez la réponse de détection du contrôleur qui contient le nom du système, les adresses IP du gestionnaire AP, le nombre d'AP déjà attachés à chaque interface du gestionnaire AP, et la capacité globale excédentaire pour le contrôleur.

- Consultez la liste de contrôleurs et envoyez une demande de jointure à un contrôleur, dans l'ordre suivant (seulement si l'AP a reçu

une réponse de détection de lui) :

a. Nom du système du contrôleur principal (précédemment configuré sur le LAP).

b. Nom du système du contrôleur secondaire (précédemment configuré sur le LAP).

c. Nom du système du contrôleur tertiaire (précédemment configuré sur le LAP).

d. Contrôleur principal (si le LAP n'a pas été précédemment configuré avec un nom de contrôleur principal, secondaire ou tertiaire). Utilisé pour toujours savoir quel contrôleur est un tout nouveau LAP (joindre).

e. Si aucune des conditions précédentes n'est observée, répartissez la charge entre les contrôleurs en utilisant la valeur de capacité excédentaire dans la réponse de détection.

Si deux contrôleurs ont la même surcapacité, envoyez la demande de jointure au premier contrôleur qui a répondu à la demande de détection avec une réponse de détection. Si un seul contrôleur a plusieurs gestionnaires d'AP sur plusieurs interfaces, choisissez l'interface de gestionnaire d'AP ayant avec le plus petit nombre d'AP.

Le contrôleur répond à toutes les demandes de détection sans vérification de certificat ni informations d'identification d'AP. Cependant, les demandes de jointure doivent avoir un certificat valide pour obtenir une réponse de jointure du contrôleur. Si le LAP ne reçoit pas de réponse de jointure de son choix, le LAP tente le contrôleur suivant dans la liste, sauf si le contrôleur est un contrôleur configuré (principal/secondaire/tertiaire).

- Quand il reçoit la réponse de jointure, l'AP vérifie qu'il a la même image que celle du contrôleur. Si ce n'est pas le cas, l'AP télécharge l'image à partir du contrôleur et redémarre pour charger la nouvelle image, puis recommence tout le processus depuis l'étape 1.

- S'il a la même image logicielle, il demande la configuration à partir du contrôleur et passe dans l'état enregistré sur le contrôleur.

Après avoir téléchargé la configuration, l'AP peut recharger pour appliquer la nouvelle configuration. Par conséquent, un rechargement supplémentaire peut se produire, ce qui constitue un comportement normal.

Déboguer à partir du contrôleur

Il y a quelques **debug** commandes sur le contrôleur que vous pouvez utiliser pour voir l'ensemble de ce processus sur la CLI :

- **debug capwap events enable**: affiche les paquets de détection et les paquets de jonction.

-

debug capwap packet enable: affiche les informations de niveau paquet des paquets de détection et de jointure.

- **debug pm pki enable**: affiche le processus de validation du certificat.

- **debug disable-all**: désactive les débogages.

Avec une application du terminal qui peut capturer la sortie dans un fichier journal, connectez la console à votre contrôleur ou appliquez-lui Secure Shell (SSH)/Telnet, puis entrez les commandes suivantes :

<#root>

config session timeout 120

config serial timeout 120

show run-config

(and spacebar thru to collect all)

debug mac addr <ap-radio-mac-address>

(in xx:xx:xx:xx:xx format)

debug client <ap-mac-address>

debug capwap events enable

debug capwap errors enable

debug pm pki enable

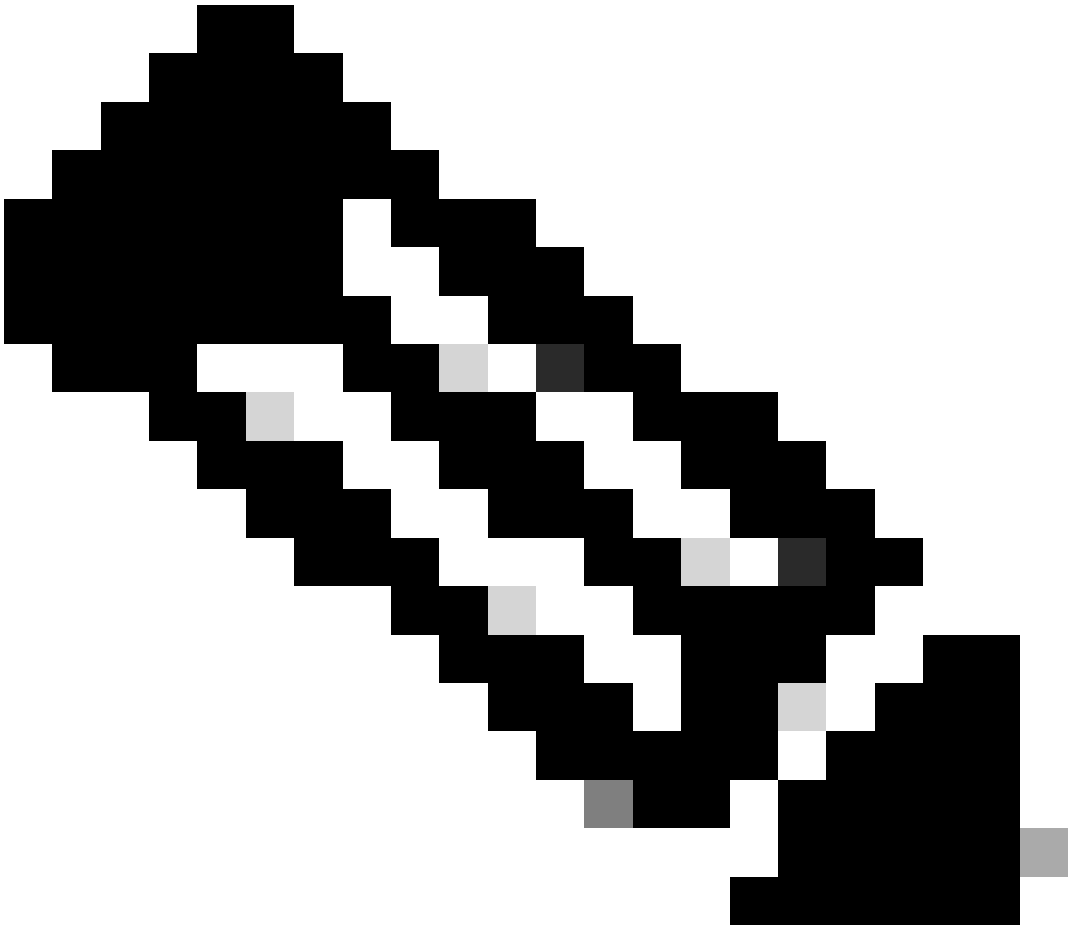
Une fois les débogages capturés, utilisez la commandedebug disable-all pour désactiver tous les débogages.

Les sections suivantes montrent le résultat de ces **debug** commandes lorsque le LAP s'enregistre auprès du contrôleur.

debug capwap events enable

Cette commande fournit des informations sur les événements et les erreurs CAPWAP qui se produisent lors du processus de détection et de jointure CAPWAP.

Voici le résultat de la **debug capwap events enable** commande pour un LAP qui a la même image que le WLC :



Remarque : certaines lignes de la sortie ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

<#root>

debug capwap events enable

*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317

!--- CAPWAP discovery request sent to the WLC by the LAP.

*spamApTask7: Jun 16 12:37:36.039: 00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317

!--- WLC responds to the discovery request from the LAP.

*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

!--- LAP sends a join request to the WLC.

*spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0, Incoming Ap's
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len = 90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join

!--- WLC responds with a join reply to the LAP.

```
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure
```

!--- LAP requests for the configuration information from the WLC.

```
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -- stati
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99 for AP
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload for00:62:ec:6
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to 172:16:17:99
```

!--- WLC responds by providing all the necessary configuration information to the LAP.

```
*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2 cause: 0 d
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to 172.16.17.99:4
.
.
.
.

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP 172.16.17.99:46
.
.
.
.
```

!--- LAP is up and ready to service wireless clients.

```
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmInterferen
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmNeighbourC
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmReceiveCtr
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for CcxRmMeas pay
```

!--- WLC sends all the RRM and other configuration parameters to the LAP.

Comme mentionné dans la section précédente, une fois qu'un LAP s'enregistre auprès du WLC, il vérifie s'il a la même image que le contrôleur. Si les images sur le LAP et le WLC sont différentes, les LAP commencent par télécharger la nouvelle image à partir du WLC. Si le LAP a la même image, il continue à télécharger la configuration et d'autres paramètres à partir du WLC.

Vous voyez ces messages dans le résultat de la **debug capwap events enable** commande si le LAP télécharge une image du contrôleur dans le cadre du processus d'enregistrement :

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and msgLen
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to 172.16.17.201:46318
*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from 172.16.17.201:46318
```

Une fois le téléchargement de l'image terminé, le LAP redémarre et exécute la détection et rejoint à nouveau l'algorithme.

debug pm pki enable

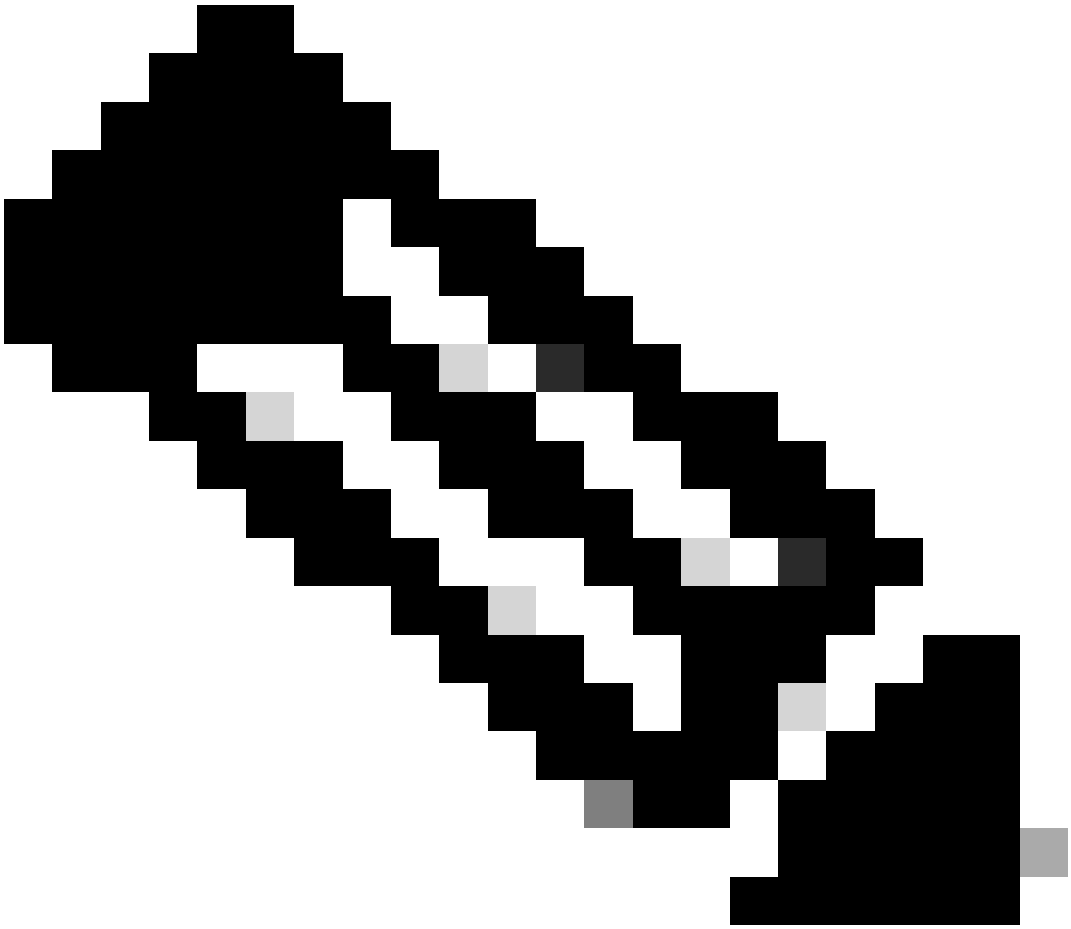
Dans le cadre du processus de jointure, le WLC authentifie chaque LAP en confirmant que son certificat est valide.

Lorsque le point d'accès envoie la requête de jonction CAPWAP au WLC, il intègre son certificat X.509 dans le message CAPWAP. Le point d'accès génère également un ID de session aléatoire qui est également inclus dans la demande de jointure CAPWAP. Lorsque le WLC reçoit la demande de jointure CAPWAP, il valide la signature du certificat X.509 avec la clé publique AP et vérifie que le certificat a été émis par une autorité de certification approuvée.

Il examine également la date et l'heure de début de l'intervalle de validité du certificat AP et compare cette date et cette heure à sa propre date et heure (par conséquent, l'horloge du contrôleur doit être réglée à proximité de la date et de l'heure actuelles). Si le certificat X.509 est validé, le

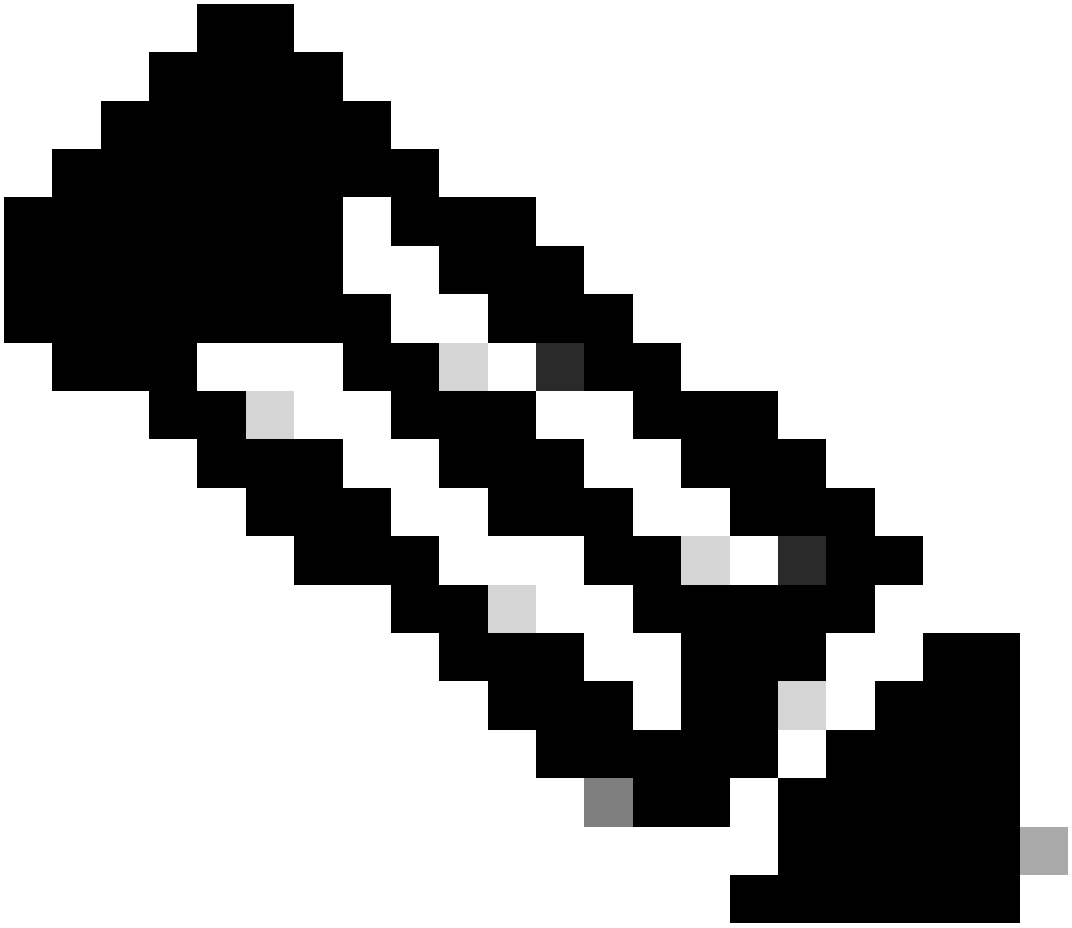
WLC génère une clé de chiffrement AES aléatoire. Le WLC raccorde les clés AES à son moteur de chiffrement afin qu'il puisse chiffrer et déchiffrer les futurs messages de contrôle CAPWAP échangés avec le point d'accès. Notez que les paquets de données sont envoyés en clair dans le tunnel CAPWAP entre le LAP et le contrôleur.

La **debug pm pki enable** commande affiche le processus de validation de certification qui se produit lors de la phase de jointure sur le contrôleur. La **debug pm pki enable** commande affiche également la clé de hachage AP au processus de jointure, si l'AP a un certificat auto-signé (SSC) créé par le programme de conversion LWAPP. Si l'AP a un certificat installé fabriqué (MIC), vous ne voyez pas de clé de hachage.



Remarque : tous les points d'accès fabriqués après juin 2006 sont dotés d'une carte MIC.

Voici le résultat de la **debug pm pki enable** commande quand le LAP avec un MIC rejoint le contrôleur :



Remarque : certaines lignes de la sortie ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

<#root>

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name /C=US/ST=Californ
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

issuer_name /O=Cisco Systems/CN=Cisco Manufacturing CA

```
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is AP3G2-1005c

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from subject


*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

Cert is issued by Cisco Systems.

```
*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in row 5 x

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultNewRootCaCert in

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert in row
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row

*spamApTask4: Mar 20 11:05:15.691: [SA]
```

Verify User Certificate: OPENSSL X509_Verify: AP Cert Verfied Using >cscoDefaultMfgCaCert<

```
*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles:
```

Check cert validity times (allow expired NO)

```
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle:
```

freeing public key

Déboguer à partir du point d'accès

Si les débogages du contrôleur n'indiquent pas de demande de jointure, vous pouvez déboguer le processus à partir de l'AP si l'AP a un port de console. Vous pouvez voir le processus d'amorçage AP avec ces commandes, mais vous devez d'abord passer en mode enable (le mot de passe par défaut est Cisco).

- **debug dhcp detail** : affiche les informations de l'option DHCP 43.
- **debug ip udp**: affiche tous les paquets UDP reçus et transmis par l'AP.
- debug capwap client event : affiche les événements capwap pour l'AP.
- **debug capwap client error**: affiche les erreurs capwap pour le point d'accès.

- **debug dtls client event**: affiche les événements DTLS pour l'AP.

- **debug dtls error enable**: affiche les erreurs DTLS pour l'AP.

- **undebug all**: désactive les débogages sur l'AP.

Voici un exemple de la sortie des debug capwapcommandes. Cette sortie partielle donne une idée des paquets envoyés par le point d'accès au processus de démarrage pour découvrir et joindre un contrôleur.

<#root>

```
AP can discover the WLC via one of these options :
```

!--- AP discovers the WLC via option 43

```
*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery type set
```

!--- capwap Discovery Request using the statically configured controller information.

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery type set
```

!--- Capwap Discovery Request sent using subnet broadcast.

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with discovery type
```

!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

```
*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

Raisons pour lesquelles le LAP ne joint pas le contrôleur

Effectuer tout d'abord les vérifications de base

- L'AP et le WLC peuvent-ils communiquer ?
- Assurez-vous que l'AP obtient une adresse du DHCP (vérifiez que le serveur DHCP loue l'adresse MAC de l'AP).
- Envoyez une requête ping au point d'accès depuis le contrôleur.
- Vérifiez si la configuration STP sur le commutateur est correcte, afin que les paquets vers les VLAN ne soient pas bloqués.
- Si les tests Ping sont effectués avec succès, vérifiez que l'AP a au moins une méthode permettant de détecter au moins une console de WLC ou d'appliquer Telnet/SSH dans le contrôleur pour exécuter les débogages.
-

Chaque fois que l'AP redémarre, il lance la séquence de détection des WLC et essaie de localiser l'AP. Redémarrez l'AP et vérifiez s'il joint le WLC.

Voici certains des problèmes couramment rencontrés en raison de quoi les LAP ne joignent pas le WLC.

Avis sur le terrain : Expirations des certificats - FN63942

Les certificats intégrés dans le matériel sont valides pendant une période de 10 ans après la fabrication. Si vos AP ou WLC ont plus de 10 ans, les certificats expirés peuvent causer des problèmes de jonction AP. Vous trouverez de plus amples renseignements à ce sujet dans le présent avis de secteur : Avis de secteur FN63942.

Problèmes potentiels à rechercher : exemples

Problème 1 : l'heure du contrôleur est en dehors de l'intervalle de validité du certificat

Effectuez les étapes suivantes afin de résoudre ce problème :

- Émettez desdebug dtls client error + debug dtls client event commandes sur le point d'accès :

<#root>

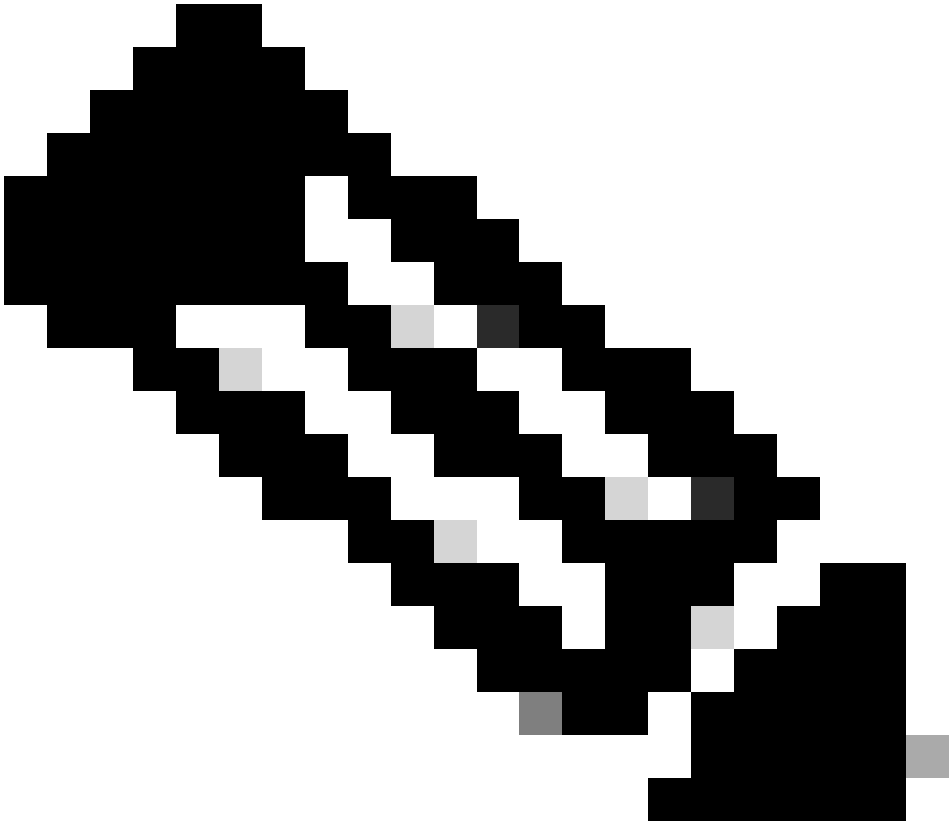
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

Bad certificate Alert

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for Connection 0x8AE
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify Alert
```

Cette information montre clairement que le temps du contrôleur est en dehors de l'intervalle de validité du certificat de l'AP. Par conséquent, AP ne peut pas enregistrer avec le contrôleur. Les certificats installés dans AP ont un intervalle de validité prédéfini. L'heure du contrôleur doit être définie de sorte qu'elle soit comprise dans l'intervalle de validité du certificat AP.

- Émettez la **show time** commande à partir de l'interface de ligne de commande du contrôleur afin de vérifier que la date et l'heure définies sur votre contrôleur tombent dans cet intervalle de validité. Si l'heure du contrôleur est ultérieure ou antérieure à cet intervalle de validité du certificat, modifiez l'heure du contrôleur pour qu'elle soit dans cet intervalle.



Remarque : si l'heure n'est pas définie correctement sur le contrôleur, choisissez Commands > Set Time en mode GUI du contrôleur, ou émettez la commande config time dans l'interface de ligne de commande du contrôleur afin de définir l'heure du contrôleur.

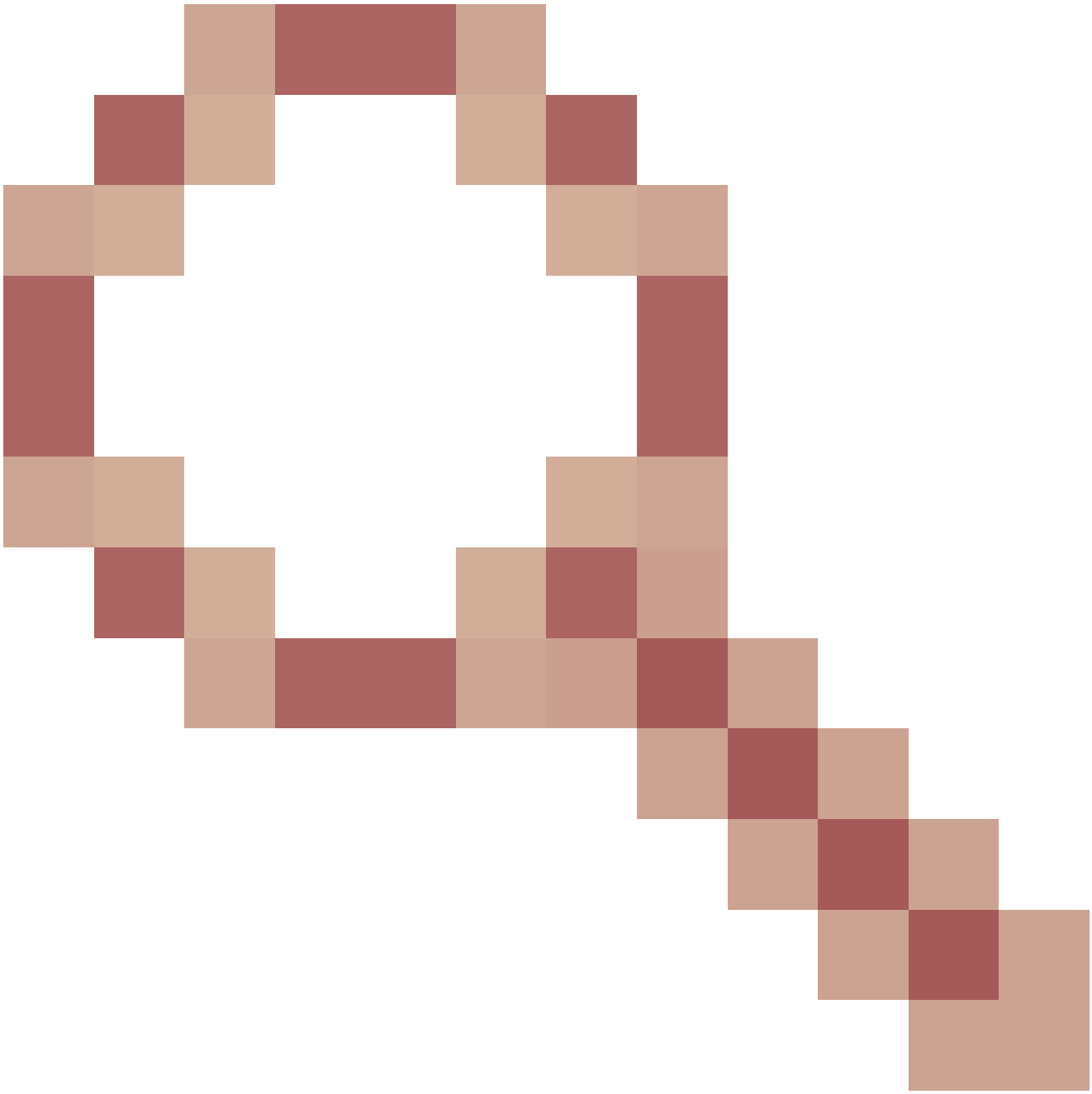
- Sur les AP avec accès CLI, vérifiez les certificats avec la **show crypto ca certificates** commande de l'AP CLI.

Cette commande vous permet de vérifier l'intervalle de validité du certificat défini dans l'AP. Voici un exemple :

```
AP00c1.649a.be5c#show crypto ca cert
.....................................
.....................................
.....................................
.....................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
...............................
...............................
...............................
```

La sortie complète n'est pas répertoriée car de nombreux intervalles de validité peuvent être associés à la sortie de cette commande. Considérez uniquement l'intervalle de validité spécifié par le point de confiance associé : Cisco_IOS_MIC_cert avec le nom AP approprié dans le champ de nom. Dans cet exemple de sortie, il s'agit de `Name : C1200-001563e50c7e`. C'est l'intervalle réel de validité du certificat à considérer.

- Veuillez vous reporter à l'ID de bogue Cisco CSCuq19142



LAP/WLC MIC ou l'expiration de la durée de vie SSC provoque une défaillance DTLS : ID de bogue Cisco CSCuq19142.

Problème 2 : non-concordance dans le domaine réglementaire

Vous voyez ce message dans le résultat de la **debug capwap events enable** commande :

<#root>

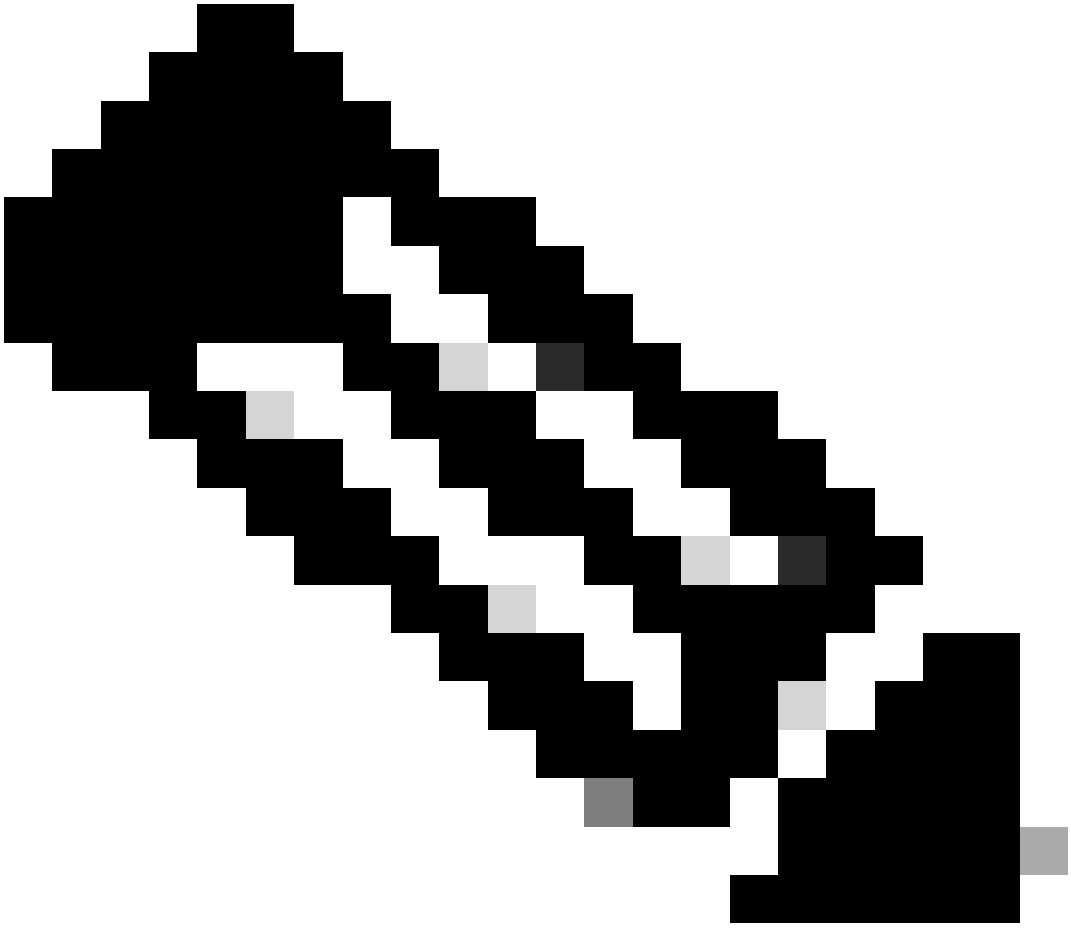
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 no**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:4**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 f**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(603**

WLC msglog show these messages :

*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095 00:cc:fc:13:e5:e0: DT
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch

Le message indique clairement qu'il y a une incompatibilité dans le domaine réglementaire du LAP et du WLC. Le WLC prend en charge plusieurs domaines réglementaires, mais chaque domaine réglementaire doit être sélectionné avant qu'un AP puisse se joindre à partir de ce domaine. Par exemple, le WLC qui utilise le domaine réglementaire -A peut uniquement être utilisé avec les AP qui utilisent le domaine réglementaire -A (etc.). Lorsque vous achetez des points d'accès, assurez-vous qu'ils partagent le même domaine réglementaire. C'est la condition nécessaire pour que l'AP s'enregistre auprès du WLC.



Remarque : les radios 802.1b/g et 802.11a doivent se trouver dans le même domaine réglementaire pour un point d'accès unique.

Problème 3 : liste d'autorisation AP activée sur le WLC ; LAP ne figure pas dans la liste d'autorisation

Dans de tels cas, vous voyez ce message sur le contrôleur dans le résultat de la commandedebug capwap events enable :

<#root>

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
```

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received CAPWAP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 CAPWAP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007:
```

spamRadiusProcessResponse: AP Authorization failure

for 00:0b:85:51:5a:e0

Si vous utilisez un LAP qui a un port de console, vous voyez ce message quand vous émettez la commandedebug capwap client error :

```
<#root>

APO01d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG:
```

No more AP manager IP addresses remain.

Là encore, c'est une indication claire que le LAP ne fait pas partie de la liste d'autorisation AP sur le contrôleur.

Vous pouvez afficher l'état de la liste d'autorisation AP avec cette commande :

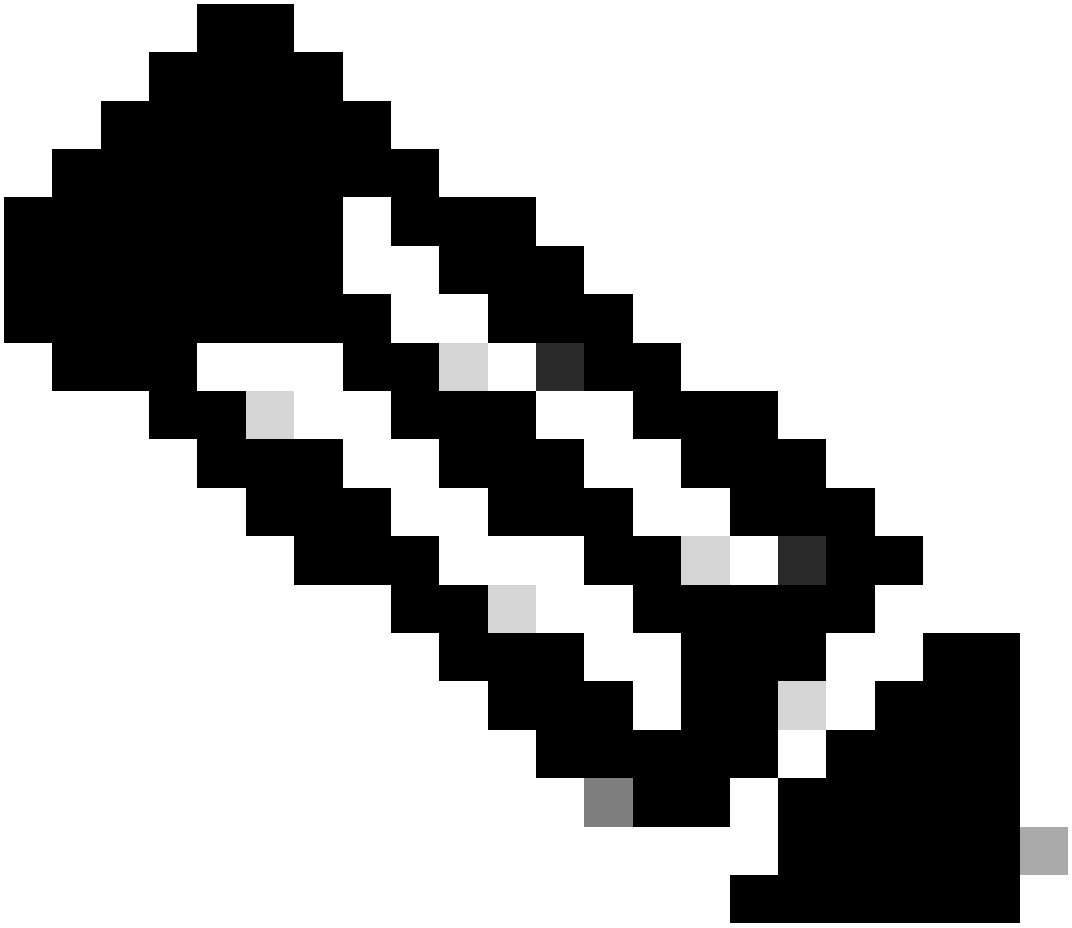
```
<#root>

(Cisco Controller) >

show auth-list

Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Afin d'ajouter un LAP à la liste d'autorisation AP, utilisez la config auth-list add mic <AP MAC Address> commande . Pour plus d'informations sur la façon de configurer l'autorisation d'AP, consultez l'Exemple de configuration de l'autorisation de points d'accès légers (LAP) dans un réseau sans fil unifié Cisco.

Problème 4 : Il y a corruption d'un certificat ou d'une clé publique sur l'AP

Le LAP ne joint pas de contrôleur en raison d'un problème de certificat.

Exécutez les debug capwap errors enable commandes et **debug pm pki enable** . Vous voyez des messages qui indiquent que des certificats ou des clés sont altérés.



Remarque : certaines lignes du résultat ont été déplacées vers les secondes lignes en raison de contraintes d'espace.

<#root>

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 CAPWAP
```

Join Request does not include valid certificate in CERTIFICATE_PAYLOAD
from AP 00:0f:24:a9:52:e0

```
.
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 Deleting and removing AP 00:0f:24:a9:52:e0 from fast path
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free public key for AP
```

Employez l'une de ces deux options afin de résoudre le problème :

- MIC AP - Demande d'autorisation de retour de matériel (RMA).
- LSC AP : remettez en service votre certificat LSC.

Problème 5 : le contrôleur reçoit un message de détection d'AP sur un VLAN incorrect (vous voyez le message de détection debug, mais pas de réponse)

Vous voyez ce message dans le résultat de la commandedebug capwap events enable :

<#root>

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!

Ce message signifie que le contrôleur a reçu une demande de détection par une adresse IP de diffusion avec une adresse IP source qui ne se trouve dans aucun sous-réseau configuré sur le contrôleur. Cela signifie également que le contrôleur est celui qui abandonne le paquet.

Le problème est que l'AP n'est pas ce qui a envoyé la requête de découverte à l'adresse IP de gestion. Le contrôleur signale une demande de détection de diffusion provenant d'un VLAN qui n'est pas configuré sur le contrôleur. Cela se produit généralement lorsque les trunks autorisent les VLAN et ne les limitent pas aux VLAN sans fil.

Complétez les étapes suivantes pour résoudre ce problème :

- Si le contrôleur est sur un autre sous-réseau, les AP doivent être **amorcés** pour l'adresse IP du contrôleur, ou les AP doivent

recevoir l'adresse IP des contrôleurs avec l'utilisation de l'une des méthodes de détection.

- Le commutateur est configuré pour autoriser certains VLAN qui ne se trouvent pas sur le contrôleur. Restreignez les VLAN autorisés sur les agrégations.

Problème 6 : AP incapable de joindre le WLC, pare-feu bloquant les ports nécessaires

Si un pare-feu est utilisé dans le réseau d'entreprise, assurez-vous que ces ports sont activés sur le pare-feu pour que le LAP se connecte et communique avec le contrôleur.

Vous devez activer les ports suivants :

- Activez ces ports UDP pour le trafic CAPWAP :
  - Données - 5247
  - Contrôle - 5246
- Activez les ports UDP suivants pour le trafic de mobilité :
  - 16666 - 16666
  - 16667 - 16667

- Activez les ports UDP 5246 et 5247 pour le trafic CAPWAP.

- TCP 161 et 162 pour SNMP (pour le système de contrôle sans fil [WCS])

Ces ports sont facultatifs (en fonction de vos besoins) :

- UDP 69 pour TFTP

- TCP 80 et/ou 443 pour le HTTP ou HTTPS pour l'accès à la GUI

- TCP 23 et/ou 22 pour Telnet ou SSH pour l'accès à la CLI

Problème 7 : adresse IP dupliquée sur le réseau

C'est un autre problème courant vu quand l'AP essaie de joindre le WLC. Vous pouvez voir ce message d'erreur quand l'AP essaie de joindre le contrôleur.

<#root>

No more AP manager IP addresses remain

Une des raisons pour lesquelles ce message d'erreur apparaît est qu'il y a une adresse IP en double sur le réseau qui correspond à l'adresse IP du gestionnaire d'AP. Dans ce cas, le LAP conserve les initiations de cycle d'alimentation et ne peut pas joindre le contrôleur.

Les débogages montrent que le WLC reçoit des demandes de détection LWAPP des AP et transmet une réponse de détection LWAPP aux AP.

Cependant, les WLC ne reçoivent pas les demandes de jointure LWAPP en provenance des AP.

Afin de résoudre ce problème, effectuez un test Ping sur le gestionnaire d'AP à partir d'un hôte câblé sur le même sous-réseau IP que le gestionnaire d'AP. Vérifiez ensuite le cache ARP. Si une adresse IP dupliquée est trouvée, supprimez le périphérique avec l'adresse IP dupliquée ou modifiez l'adresse IP sur le périphérique afin qu'il ait une adresse IP unique sur le réseau.

L'AP peut alors joindre le WLC.

Problème 8 : les LAP avec une image maillée ne peuvent pas joindre le WLC

Le point d'accès léger ne s'enregistre pas auprès du WLC. Le journal affiche le message d'erreur suivant :

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
     Type: WLAN USER
```

Cela peut se produire si le point d'accès léger a été livré avec une image maillée et est en mode Pont. Si le LAP a été commandé avec un logiciel de maillage, vous devez ajouter le LAP à la liste d'autorisation AP. Choisissez **Security > AP Policies** et ajoutez **AP** à la liste d'autorisation. L'AP doit ensuite se joindre, télécharger l'image à partir du contrôleur, puis s'enregistrer auprès du WLC en mode pont. Ensuite, vous devez changer le point d'accès en mode local. Le LAP télécharge l'image, redémarre et se réenregistre sur le contrôleur en mode local.

Problème 9 : adresse incorrecte Microsoft DHCP

Les points d'accès peuvent renouveler rapidement leurs adresses IP lorsqu'une tentative de connexion à un WLC est effectuée, ce qui peut amener les serveurs DHCP Windows à marquer ces adresses IP comme BAD_ADDRESS, ce qui pourrait rapidement épuiser le pool DHCP. Pour plus d'informations, reportez-vous au chapitre Client Roaming du Guide de configuration du contrôleur sans fil Cisco, version 8.2.

Informations connexes

- **Assistance technique de Cisco et téléchargements**
- **Processus de jonction AP avec Catalyst 9800**

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.