Dépannage de la dissociation du point d'accès du contrôleur

Table des matières

Introduction

Ce document décrit des cas d'utilisation pour comprendre la raison de la rupture de tunnel Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) entre les points d'accès (AP) et le contrôleur LAN sans fil (WLC).

Conditions préalables

Exigences

Cisco recommande que vous ayez des connaissances sur la configuration des points d'accès et des contrôleurs, ainsi que des connaissances de base sur le routage et la commutation.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Processus d'enregistrement AP basé sur contrôleur

Les AP passent par le processus mentionné pour s'enregistrer auprès du contrôleur :

1. Demande de message de détection CAPWAP au WLC à partir du point d'accès.
2. Message de réponse de détection du WLC au point d'accès.

3. Le point d'accès choisit le WLC à joindre en fonction de la réponse CAPWAP reçue.
4. Requête de jonction envoyée au WLC à partir du point d'accès.
5. Le contrôleur valide le point d'accès et envoie la réponse de jonction.

Journaux capturés sur AP lors de l'enregistrement avec WLC :

Press RETURN to get started!

Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

%CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY

status of voice_diag_test from WLC is false

%SSH-5-ENABLED: SSH 2.0 has been enabled

Logging LWAPP message to 255.255.255.255.

%CDP_PD-4-POWER_OK: 15.4 W power - NEGOTIATED inline power source

%LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up

%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to up

%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 started - CLI initiated

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up Translating "CISCO-LWAPP-CONTROLLER"...dom

%CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip:

peer_port: 5246

%CAPWAP-5-CHANGED: CAPWAP changed state to

%CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip:

peer_port: 5246

%CAPWAP-5-SENDJOIN: sending Join Request to

%CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

%CAPWAP-5-CHANGED: CAPWAP changed state to CFG

%LWAPP-3-CLIENTERRORLOG: Operator changed mode for 802.11g. Rebooting.

%LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down

%SYS-5-RELOAD: Reload requested by CAPWAP CLIENT. Reload Reason: Operator changed mode for 802.11g.

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down IOS Bootloader - Starting system.

Cas d'utilisation 1

1. Les AP sont dissociés du WLC et une fois vérifiés à partir du commutateur, cela montre que l'AP n'a pas d'IP.

Journaux lorsqu'ils sont connectés au point d'accès :

LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up

%CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!

Solution :

Corrigez les problèmes d'accessibilité à l'adresse IP helper configurée sous le VLAN si le serveur DHCP est situé à distance. Si le DHCP est configuré localement, assurez-vous qu'il n'y a pas de conflit DHCP. Configurez l'adresse IP statique sur le point d'accès :

Connectez-vous au point d'accès et tapez ces commandes :

```
capwap ap ip address <ip> <mask>

capwap ap ip default-gateway <ip>
```

Vous pouvez également spécifier l'adresse IP du contrôleur :

capwap ap controller ip address

2. Notez qu'il existe des points d'accès avec des adresses IP, mais l'échec de la communication avec le WLC peut être une défaillance de résolution de l'IP du contrôleur.

Journaux du point d'accès avec un problème où la résolution DNS (Domain Name System) a

échoué :

```
<Date & time>  %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER.local doamin

Not in Bound state.
```

Solution :

Vérifiez l'accessibilité du serveur DNS interne, si elle est acceptable, assurez-vous que les adresses IP du contrôleur transmises via DHCP sont accessibles.

Break-fix : configurez manuellement le contrôleur sur l'AP.

```
"capwap ap {primary-base | secondary-base | tertiary-base}controller-name controller-ip-address"
```

3. Vous voyez que le point d'accès est enregistré sur le contrôleur et vous ne voyez toujours aucune diffusion de l'identifiant SSID (Service Set Identifier) requis.

```
(4402-d) >config wlan apgroup interface-mapping add <ap group name> <wlandi> <interfacename>
```

Solution :
Ajoutez le réseau local sans fil (WLAN) sous le groupe AP.

Cas d'utilisation 2

Notez que le point d'accès n'est pas visible sur le voisin CDP (Cisco Discovery Protocol) du commutateur, et que le commutateur connecté au point d'accès est dans un état d'erreur désactivée.

Journaux capturés à partir du commutateur :

```
Dec  9 08:42:35.836 UTC: RSTP(10): sending BPDU out Te3/0/47STP: pak->vlan_id: 10

Dec  9 08:42:35.836 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable stateSTP: pak->vlan_id: 1

Dec  9 09:47:32.651 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD

Dec  9 09:47:33.651 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted

Dec  9 09:47:53.545 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state
```

Dec 9 09:48:10.955 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD

Dec 9 09:48:11.955 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted

Dec 9 09:48:32.114 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state

Solution :
Le point d'accès n'envoie pas la protection BPDU (Bridge Protocol Data Unit) en aucun cas, c'est un problème du côté du commutateur. Déplacez le point d'accès vers un autre port libre et répliquez la configuration d'interface avec les vérifications physiques nécessaires.

Cas d'utilisation 3

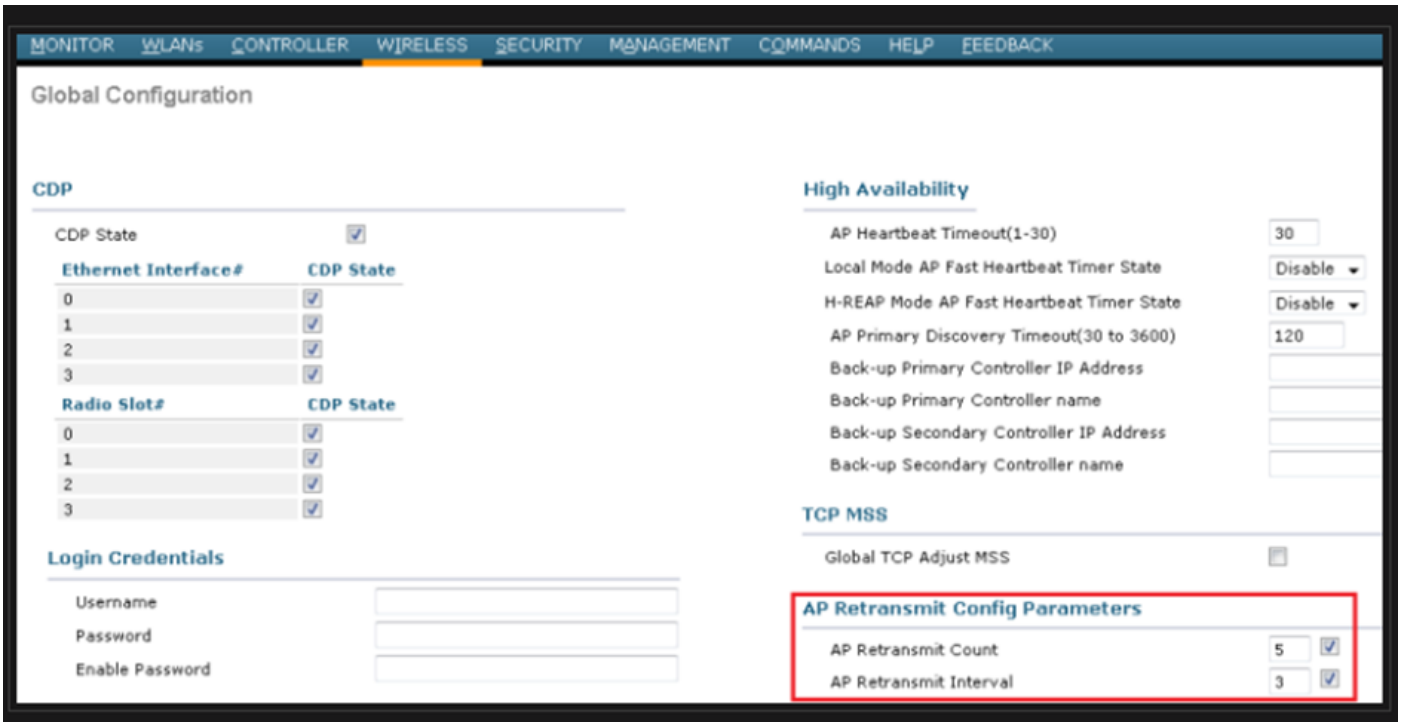
Dans la configuration des bureaux distants, vous voyez souvent le tunnel CAPWAP se démonter de manière aléatoire entre les points d'accès et le contrôleur et les paramètres les plus importants à vérifier sont la retransmission et l'intervalle entre les tentatives.

L'intervalle de retransmission AP et l'intervalle de nouvelle tentative peuvent être configurés à la fois au niveau global et au niveau AP. Une configuration globale applique ces paramètres de configuration à tous les AP. En d'autres termes, l'intervalle de retransmission et le nombre de tentatives sont uniformes pour tous les points d'accès.

Journaux problématiques du WLC :

*spamApTask6: Jun 01 17:17:55.426: %LWAPP-3-AP_DEL: spam_lrad.c:6088 1c:d1:e0:43:1d:20: Entry deleted for AP: 10.209.36.5 (5256) reason : AP

Solution : si le problème concerne tous les sites, augmentez la **Retransmit count** et **Retransmit interval** sous Wireless Global configuration. Option permettant d'augmenter les valeurs lorsque le problème concerne tous les AP.



Option de modification des paramètres de configuration de retransmission AP sous configuration globale

Si le problème est spécifique à un site distant, une augmentation de **Retransmit count** et **Retransmit interval** sur un AP particulier corrige le problème.

Possibilité de modifier le paramètre de configuration de retransmission AP sous un AP spécifique

Cas d'utilisation 4

L'AP est complètement dissocié du WLC et n'est pas en mesure de rejoindre le contrôleur, cela pourrait être lié aux certificats numériques.

Quelques faits rapides sur les certificats de périphérique en termes de WLC et AP Cisco :

- Chaque périphérique qui sort de Cisco est livré avec un certificat par défaut avec une validité de 10 ans.
- Ce certificat est utilisé pour effectuer l'authentification entre le WLC Cisco et le point

d'accès.

- Avec l'aide des certificats, AP et WLC établissent un tunnel DTLS (Datagram Transport Layer Security) sécurisé.

Deux types de problèmes liés aux certificats ont été rencontrés :

Problème 1 : AP plus ancien (ne veut pas rejoindre WLC).

La console vers le point d'accès permet de déterminer le problème et les journaux se présentent comme suit :

```
*Sep 13 18:26:24.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.1.1.1 peer_port: 5246
*Sep 13 18:26:24.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Sep 13 18:26:24.099: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed.
The certificate (SN: XXXXXXXXXXXXXX) has expired.    Validity period ended on 19:56:24 UTC Aug 12 2018
*Sep 13 18:26:24.099: %LWAPP-3-CLIENTERRORLOG: Peer certificate verification failed
*Sep 13 18:26:24.099: %CAPWAP-3-ERRORLOG: Certificate verification failed!
```

Problème 2 : un AP plus récent ne veut pas rejoindre un WLC plus ancien.
La console vers l'AP donne une erreur qui pourrait ressembler à ceci :

```
[*09/09/2019 04:55:26.3299] CAPWAP State: DTLS Teardown
[*09/09/2019 04:55:30.9385] CAPWAP State: Discovery
[*09/09/2019 04:55:30.9385] Did not get log server settings from DHCP.
[*09/09/2019 04:55:41.0000] CAPWAP State: DTLS Setup
[*09/09/2019 04:55:41.3399] Bad certificate alert received from peer.
[*09/09/2019 04:55:41.3399] DTLS: Received packet caused DTLS to close connection
```

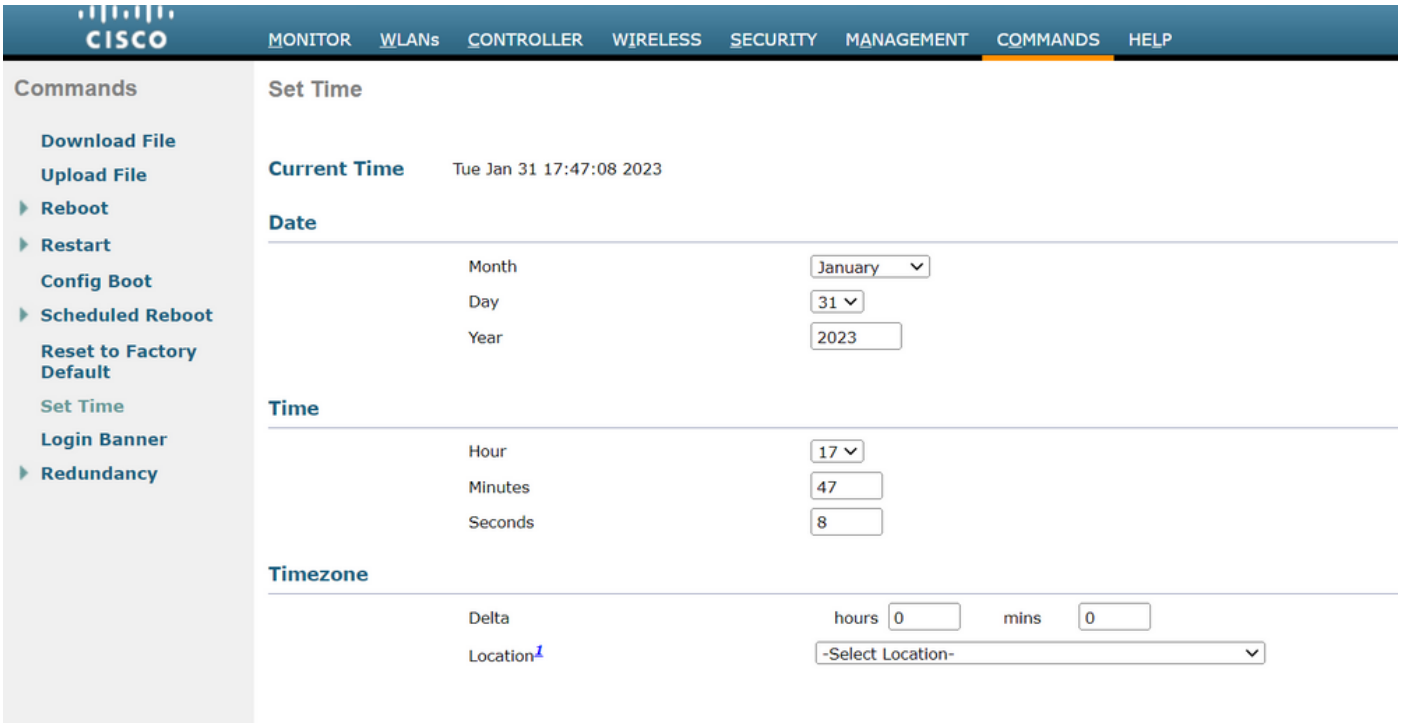
Solution :

1. NTP désactive et définit l'heure manuellement via l'interface de ligne de commande :

```
(Cisco Controller)> config time ntp delete 1
(Cisco Controller)> config time manual 09/30/18 11:30:00
```

2. NTP désactive et définit l'heure manuellement via l'interface utilisateur graphique :

Naviguez jusqu'à **Controller > NTP > Server > Commands > Set Time** afin de supprimer les serveurs NTP répertoriés.



Emplacement de définition manuelle de l'heure sur l'interface utilisateur graphique

2. Désactivez le certificat installé par le fabricant (MIC) sur le contrôleur. Cette commande n'est acceptée que sur les dernières versions.

```
(Cisco Controller)> config ap cert-expiry-ignore mic enable
```

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.