Dépannage des problèmes courants de connectivité des clients sans fil des contrôleurs sans fil Catalyst 9800

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Collecter les journaux
  - Scénarios dans lesquels le client ne peut pas se connecter
    - Les identifiants d'authentification Web ne fonctionnent pas
    - Aucun VLAN valide défini sur le profil de stratégie
    - Mot de passe incorrect
    - La liste de contrôle d'accès envoyée par RADIUS n'existe pas sur le WLC 9800
    - Le VLAN envoyé par RADIUS n'existe pas sur le WLC 9800
    - Déconnecté en raison de modifications apportées au WLAN ou au profil de stratégie
    - Le client est supprimé manuellement du réseau
    - Déconnecté en raison du délai EAP
    - Déconnecté en raison de la réinitialisation radio AP
    - Déconnecté en raison du délai d'authentification Web
    - Déconnecté en raison du délai d'expiration de la session
    - Déconnecté en raison du délai d'inactivité
    - Le client a changé de SSID

Introduction

Ce document décrit les scénarios de problèmes de connectivité des clients sans fil les plus courants et comment les résoudre sur les contrôleurs sans fil Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleurs sans fil Cisco Catalyst 9800
- Accès aux contrôleurs sans fil via l'interface de ligne de commande (CLI)

Composants utilisés

Les informations contenues dans ce document sont basées sur la plate-forme logicielle et

matérielle Cisco IOS® XE Gibraltar 16.10 ou version ultérieure.

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.

Collecter les journaux

Le contrôleur WLC 9800 offre des fonctionnalités de traçage TOUJOURS ACTIVES. Cela garantit que toutes les erreurs, avertissements et messages de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une défaillance après qu'il se soit produit.


Remarque : Selon le volume de journaux générés, vous pouvez revenir de quelques heures à plusieurs jours.

Afin d'afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter via SSH/Telnet au WLC 9800 et suivre ces étapes (assurez-vous que votre session est enregistrée dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du contrôleur afin de pouvoir suivre les journaux dans le temps jusqu'à quand le problème s'est produit.

```
# show clock
```

Étape 2. Collectez les syslogs à partir de la mémoire tampon du contrôleur ou du syslog externe, comme dicté par la configuration du système. Cela permet d'avoir un aperçu rapide de l'état et des erreurs du système, le cas échéant.

```
# show logging
```

Étape 3 : vérification de l’activation des conditions de débogage

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

Remarque : Si une condition est répertoriée, cela signifie que les traces sont enregistrées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmente le volume des journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque vous ne procédez pas activement au débogage.

Étape 4. En supposant que l'adresse MAC testée n'était pas répertoriée comme condition à l'étape 3., collectez les suivis de niveau de notification toujours actif pour l'adresse MAC spécifique.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Débogage conditionnel et suivi actif radio :

Si les traces toujours actives ne vous donnent pas suffisamment d'informations pour déterminer le déclencheur du problème en cours d'investigation, vous pouvez activer le débogage conditionnel et capturer la trace Radio Active (RA), qui fournit des traces au niveau du débogage pour tous les processus qui interagissent avec la condition spécifiée (l'adresse MAC du client dans ce cas). Afin d'activer le débogage conditionnel, vérifiez ces étapes.

Étape 5. Vérifiez qu’aucune condition de débogage n’est activée.

```
# clear platform condition all
```

Étape 6. Activez la condition de débogage pour l’adresse MAC du client sans fil que vous souhaitez surveiller.

Cette commande commence à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez aussi augmenter ce délai pour qu’il atteigne jusqu’à 2085978494 secondes.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Remarque : afin de surveiller plus d'un client à la fois, exécutez la commande debug wireless mac
par adresse mac.

Remarque : vous ne voyez pas le résultat de l'activité du client sur la session du terminal, car tout est mis en mémoire tampon en interne pour être visualisé ultérieurement.

Étape 7. Reproduisez le problème ou le comportement que vous souhaitez surveiller.

Étape 8. Arrêtez les débogages si le problème est reproduit avant que le temps de surveillance par défaut ou configuré ne soit écoulé.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Une fois le temps de surveillance écoulé ou le débogage sans fil arrêté, le WLC 9800 génère un fichier local avec le nom :

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Étape 9. Collectez le fichier de l'activité d'adresse MAC. Vous pouvez copier le fichier ra trace .log sur un serveur externe ou afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA.

```
# dir bootflash: | inc ra_trace
```

Copiez le fichier sur un serveur externe :

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Affichez-en le contenu :

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 10. Si la cause première n'est toujours pas évidente, collectez les journaux internes qui sont une vue plus détaillée des journaux de niveau débogage. Vous n'avez pas besoin de déboguer à nouveau le client, car cela ne sert qu'à examiner plus en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

Remarque : Ce résultat de commande renvoie des suivis pour tous les niveaux de journalisation pour tous les processus et est assez volumineux. Contactez le TAC Cisco pour vous aider à analyser ces traces.

Vous pouvez copier le fichier ra-internal-FILENAME.txt sur un serveur externe ou afficher le résultat directement à l'écran.

Copiez le fichier sur un serveur externe :

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Affichez-en le contenu :

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Étape 11. Supprimer les conditions de débogage

```
# clear platform condition all
```

Remarque : Veillez à toujours supprimer les conditions de débogage après une session de dépannage.

Scénarios dans lesquels le client ne peut pas se connecter

Les identifiants d'authentification Web ne fonctionnent pas

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [27915]: UUID: 100000000015b, ra: 15, (info): [e4b
```

Motif :

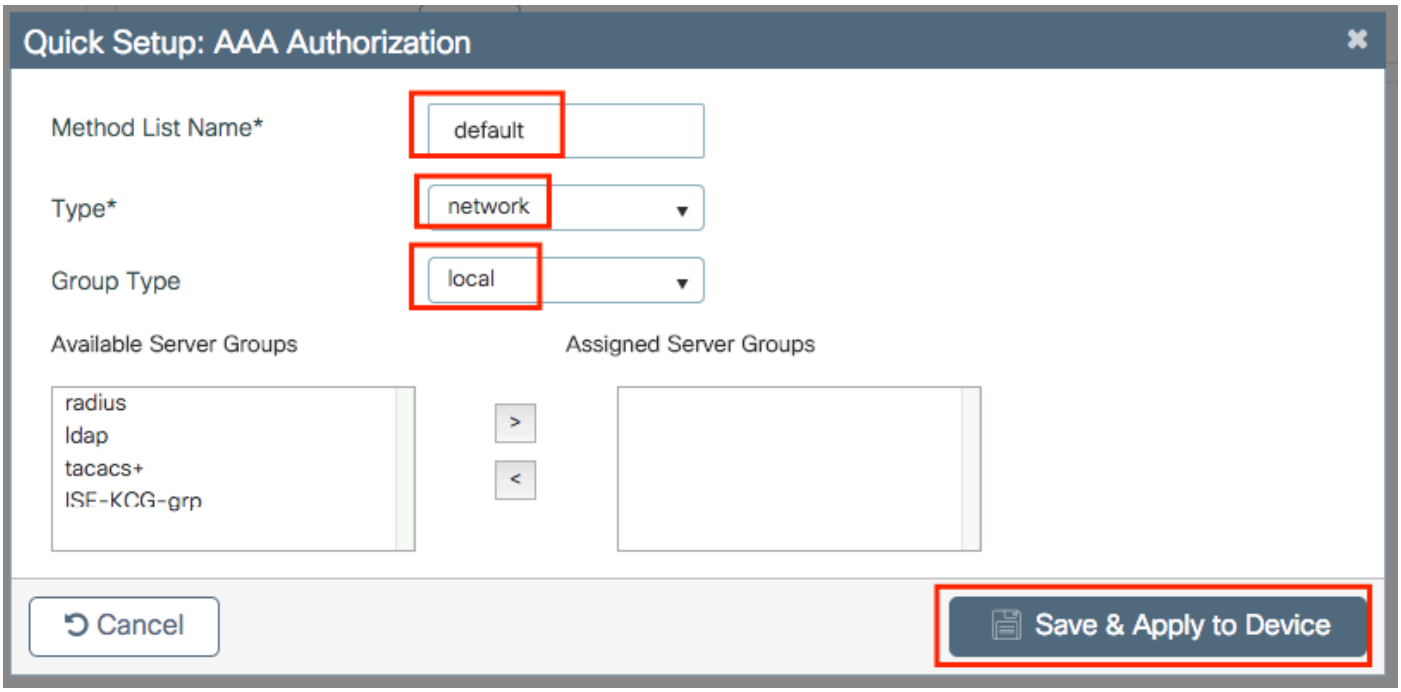
- Le client n'utilise pas d'informations d'identification valides
- Aucun réseau d'autorisation par défaut n'est défini sur le WLC 9800

Solutions possibles :

- Vérifiez que le client utilise des informations d'identification valides
- Ajouter une méthode de réseau d’autorisation par défaut

IUG:

Accédez àConfiguration > Security > AAA > AAA Method List > Authorization > + Addet créez une nouvelle méthode d'autorisation avec ces paramètres.



CLI :

```
# config t
# aaa authorization network default local
```

Aucun VLAN valide défini sur le profil de stratégie

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm] [25054]: UUID: 1000000000019, ra: 15, (ERR): EPM_PLUGIN
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [25054]: UUID: 1000000000019, ra:
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [25054]: UUID: 1000000000019, ra:
```

Motif :

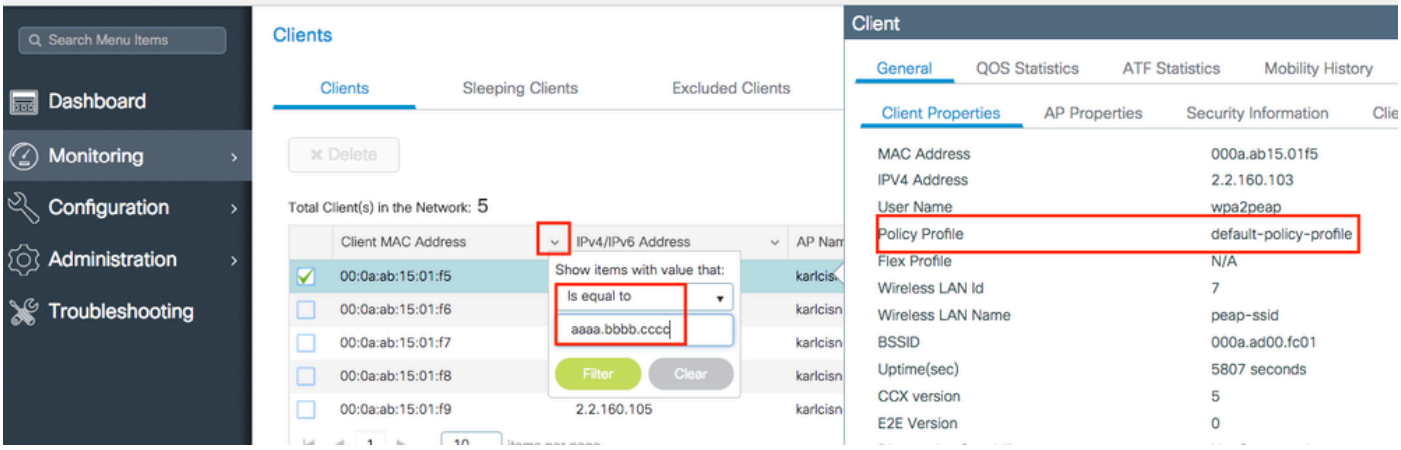
Aucun VLAN valide n'est défini sur le profil de stratégie attribué au WLAN.

Solution :

1. Vérifiez quel profil de stratégie est utilisé par le client.

IUG:

Accédez àMonitoring > Wireless > Clients > Client row > Client Properties(recherche facultative d'un client spécifique à l'aide de son adresse MAC).



CLI :

<#root>

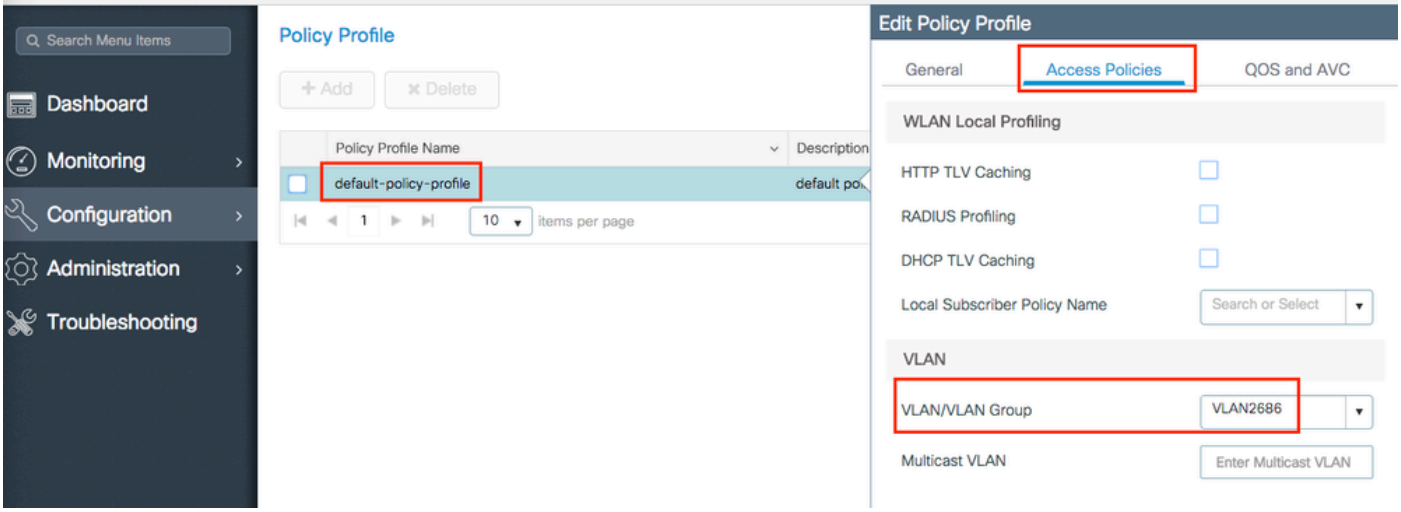
```
# show wireless client mac-address <aaaa.bbbb.cccc> detail | inc Policy Profile
Policy Profile :
```

default-policy-profile

2. Vérifiez quel VLAN est affecté à ce profil de stratégie.

IUG:

Accédez à Configuration > Tags & Profiles > Policy > Policy Profile row > Access Policies.



CLI :

<#root>

```
# show wireless profile policy detailed
```

default-policy-profile

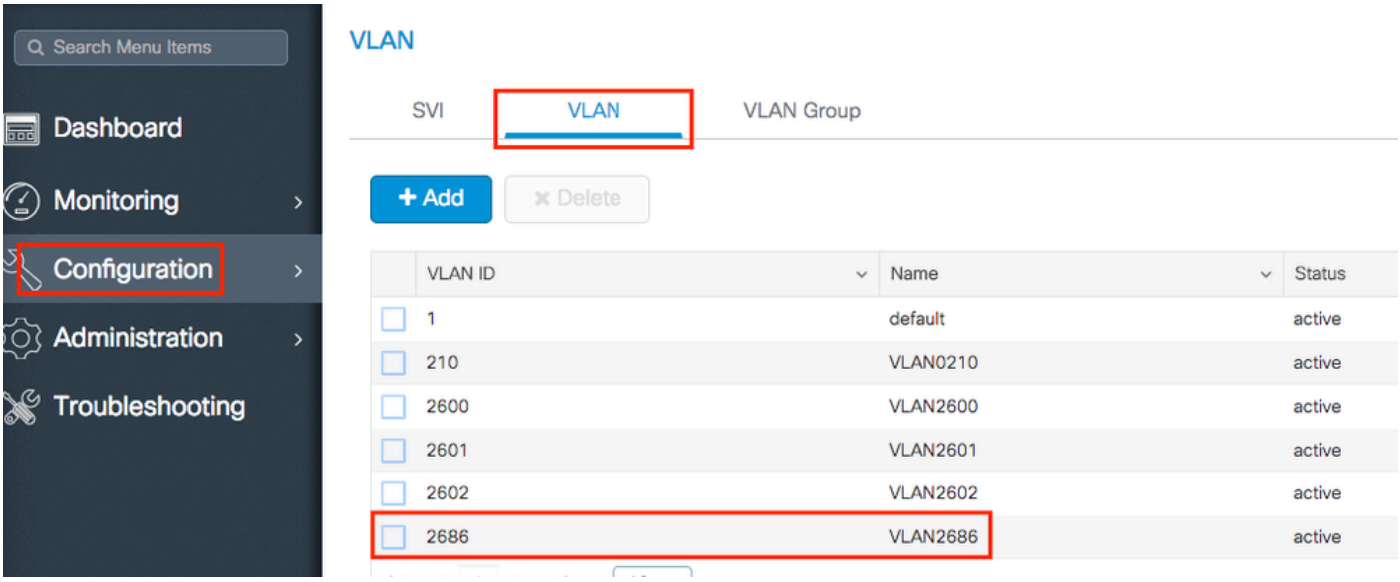
```
 | inc VLAN
VLAN                            :
```

VLAN2686

3. Assurez-vous que le paramètre VLAN a un nom ou un ID de VLAN valide et actif.

IUG:

Accédez à Configuration > Layer2 > VLAN > VLAN.



CLI :

<#root>

```
# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Te0/0/2, Te0/0/3
210  VLAN0210                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2600 VLAN2600                         active
2601 VLAN2601                         active
2602 VLAN2602                         active
2686
```

VLAN2686

```
                          active
```

Remarque : si un nom de VLAN est utilisé, il est sensible à la casse, donc assurez-vous qu'il est exactement le même que celui vu sur la show vlan briefcommande.

---

4. Corrigez le VLAN selon les besoins.

IUG:

Revenez au VLANConfiguration > Tags & Profiles > Policy > Policy Profile row > Access Policieset corrigez-le.

CLI :

```
# config t
# wireless profile policy default-policy-profile
# shutdown
# vlan <vlan-# or vlan-name>
# no shutdown
```

Mot de passe incorrect

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-keymgmt] [27782]: UUID: 1000000000088, ra: 15, (ERR):
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-keymgmt] [27782]: UUID: 1000000000088, ra: 15, (ERR):
```

Motif :

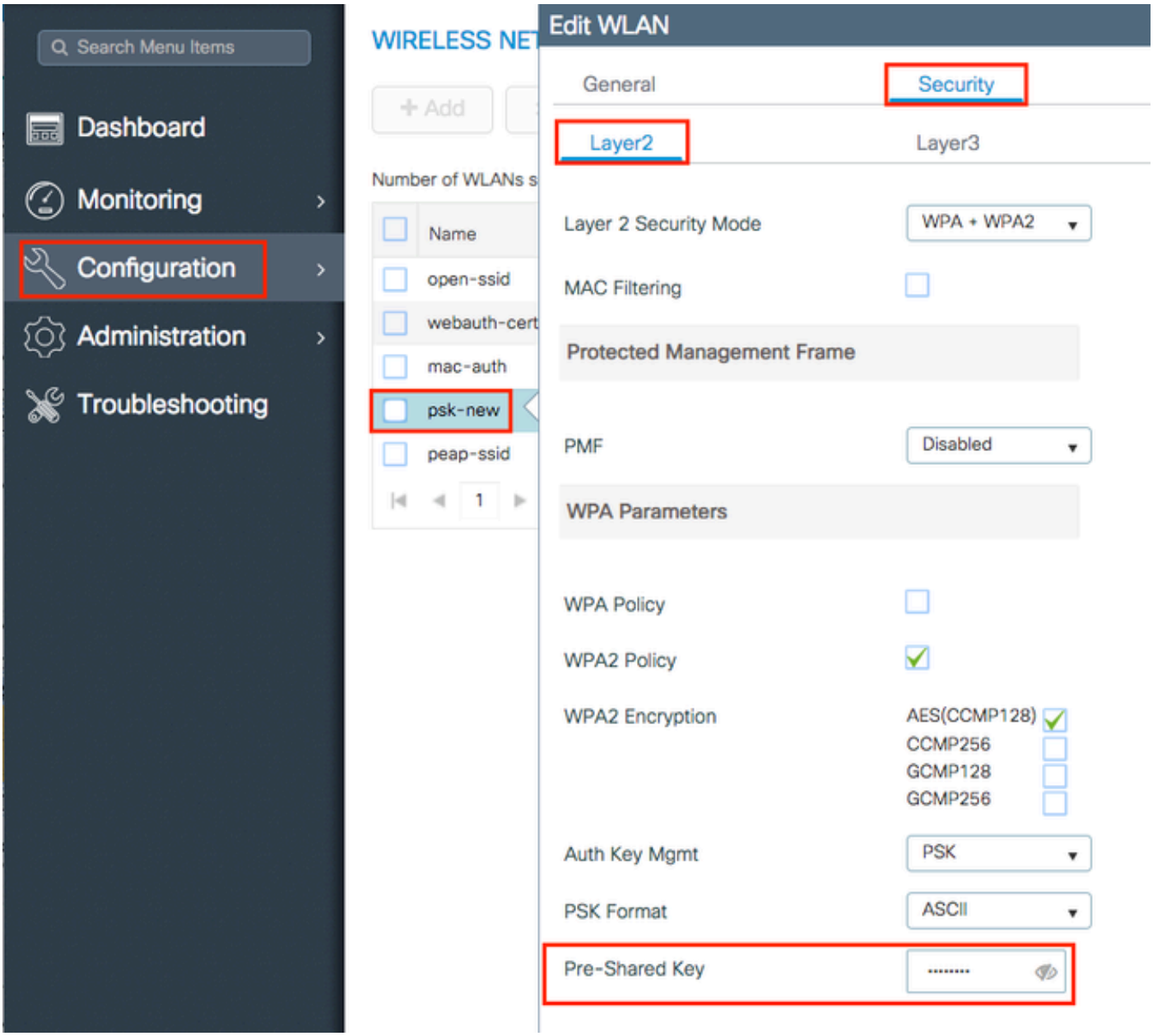
Le client entre un mot de passe incorrect.

Solutions possibles :

- Corriger le mot de passe dans le périphérique terminal
- Corriger le mot de passe sur le SSID

IUG:

Accédez à Configuration > Wireless > WLANs > WLAN name > Security > Layer2, et corrigez le mot de passe.



CLI :

```
# config t
# wlan <wlan-name>
# shut
# security wpa psk set-key ascii 0 <clear-text-password>
# no shut
```

La liste de contrôle d'accès envoyée par RADIUS n'existe pas sur le WLC 9800

Exemple de journal :

<#root>

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm-acl] [8104]: (ERR): ACL
```

acl-sent-by-ise

```
 is missing in configuration for mac e4b3.187c.3058
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm-acl] [8104]: (ERR): Unable to parse EPM attributes
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_PLUGIN_CONF
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm] [8104]: (ERR): Error in activating feature (EPM ACL PLU
.
.
.
EPM Data Base:
 Number of Authz_info: 2
 Authz info 1 details
 Number of feat info: 2, State: Success, Priority: 254
 EPM Vlan PLUG-IN Status: Success
 VLAN Group: VLAN2602
 VLAN-ID: 2602
 SM Reauth PLUG-IN Status: Success
 Authz info 2 details
 Number of feat info: 4, State: Fail, Priority: 100
 EPM MISC PLUG-IN Status: Success
 Anchor Vlan: 0
```

EPM ACL PLUG-IN Status: Activate Failure

```
 SM ACCOUNTING PLUG-IN Status: Success
 linksec Status: Success
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-infra-evq-lib] [8104]: (note): already started radi
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_SVM_APPLY_UP_FAIL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] SM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] Un
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet eventQ: AUTH_MGR_MQ, message:3
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8104]: (ERR): MAC: e4b3.187c.3058 client authz
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-exclusion] [8104]: (info): MAC: e4b3.187c.3058  Add c
```

Motif :

La liste de contrôle d'accès envoyée par le serveur RADIUS n'existe pas sur le WLC 9800.

Solutions possibles :

- Corrigez la configuration du serveur RADIUS pour envoyer le bon nom de liste de contrôle d'accès
- Ajoutez la liste de contrôle d'accès manquante au WLC 9800

Le VLAN envoyé par RADIUS n'existe pas sur le WLC 9800

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm] [8104]: (ERR): Error in activating feature (EPM Vlan PL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_START_CALL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-infra-evq] [8104]: (ERR):
EPM Data Base:
 Number of Authz_info: 2
 Authz info 1 details
 Number of feat info: 2, State: Success, Priority: 254
 EPM Vlan PLUG-IN Status: Conflict
 SM Reauth PLUG-IN Status: Success
 Authz info 2 details
 Number of feat info: 4, State: Activate, Priority: 100
 EPM MISC PLUG-IN Status: Success
 Anchor Vlan: 0
 SM ACCOUNTING PLUG-IN Status: Success
 EPM Vlan PLUG-IN Status: Activate Failure
 VLAN Group: vlan-sent-by-ise
 VLAN-ID: 0
 linksec Status: Success
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_SVM_APPLY_UP_FAIL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] SM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] Un
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet eventQ: AUTH_MGR_MQ, message:3
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8104]: (ERR): MAC: e4b3.187c.3058 client authz
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-exclusion] [8104]: (info): MAC: e4b3.187c.3058 Add cl
```

Motif :

Le VLAN envoyé par le serveur RADIUS n'existe pas sur le WLC 9800.

Solutions possibles :

- Corrigez la configuration du serveur RADIUS pour envoyer le bon nom/ID de VLAN
- Ajoutez le VLAN manquant au WLC 9800

Déconnecté en raison de modifications apportées au WLAN ou au profil de stratégie

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-infra-evq] [8522]: (note): Mcast: Sent L2 MGID 2602
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [apmgr-bssid] [8522]: (ERR): 00c8.8b26.d790 Radio:0 BSSID:1 -
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [8522]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [8522]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [multicast-main] [8522]: (info): MAC: e4b3.187c.3058 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-iplearn] [8522]: (info): MAC: e4b3.187c.3058 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [8522]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-transition] [8522]: (info): MAC: e4b3.187c.3058 MMIF FSM
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [8522]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8522]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8522]: (info): [e4b3.187c.3058:capwap_90000003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute :bsn-vlan-
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute : timeout
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8522]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 DOT11 state trans
```

Motif :

Des modifications ont été effectuées dans l'interface utilisateur graphique ou le SSID ou le profil de stratégie a été désactivé manuellement.

Solution :

Il s'agit d'un comportement normal. Évitez de modifier les SSID ou les profils de stratégie pendant les heures de production.

Le client est supprimé manuellement du réseau

Exemple de journal :

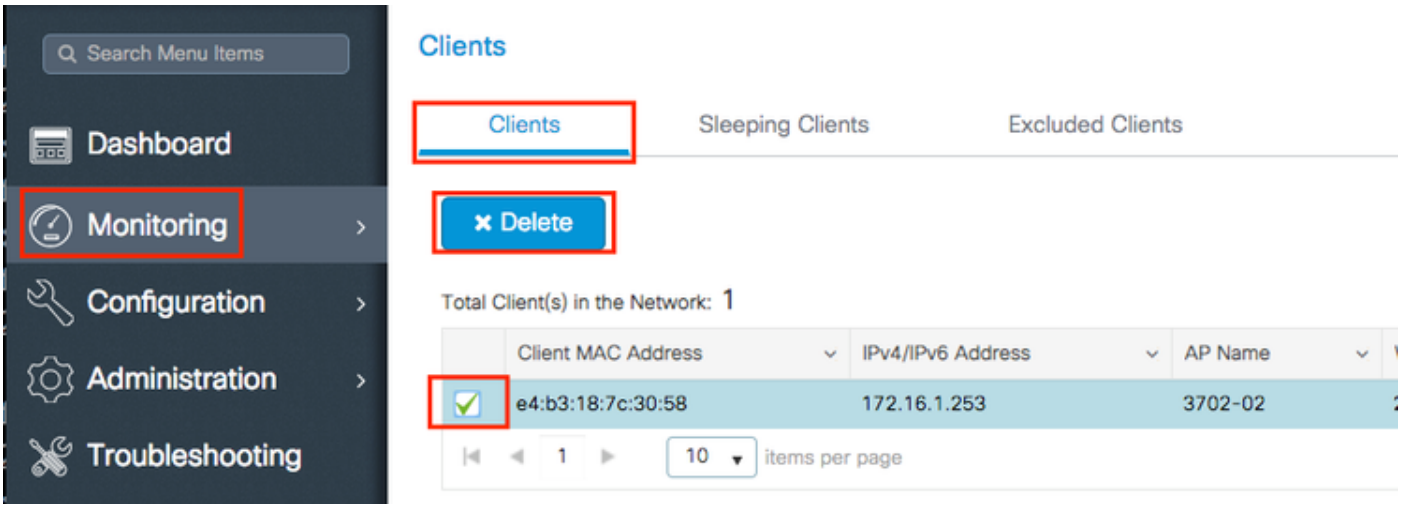
```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [8522]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [8522]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [multicast-main] [8522]: (info): MAC: e4b3.187c.3058 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-iplearn] [8522]: (info): MAC: e4b3.187c.3058 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [8522]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-transition] [8522]: (info): MAC: e4b3.187c.3058 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [8522]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8522]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8522]: (info): [e4b3.187c.3058:capwap_90000003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute :bsn-vlan-
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute : timeout
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8522]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 DOT11 state trans
```

Motif :

Le client a été manuellement supprimé du réseau par l'interface de ligne de commande :

```
# wireless client mac-address aaaa.bbbb.cccc deauthenticate
```

Ou par interface utilisateur graphique :



Solution :

Aucun, comportement normal initié par l'utilisateur.

Déconnecté en raison du délai EAP

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [errmsg] [8681]: (note): %DOT1X-5-FAIL: Authentication failed
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] (
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] R
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (info): MAC: 0874.0277.1345 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (note): MAC: 0874.0277.1345 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-state] [8681]: (note): MAC: 0874.0277.1345 Clien
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-transition] [8681]: (info): MAC: 0874.0277.1345 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-client] [8681]: (ERR): MAC: 0874.0277.1345 Client not pre
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dot11] [8681]: (info): MAC: 0874.0277.1345 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dot11] [8681]: (info): MAC: 0874.0277.1345 DOT11 state trans
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet eventQ: EAP_CORE_MQ, message:2
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-state] [8681]: (note): MAC: 0874.0277.1345 Client
```

Motif :

Le client ne répond pas au paquet EAP (Extensible Authentication Protocol) envoyé par le WLC 9800 dans l'intervalle EAP-Request Timeout ni dans les délais EAP-Request Max Retries.

Solutions possibles :

- Mettre à jour les pilotes client sans fil vers le dernier
- Assurez-vous que le client sans fil approuve le certificat RADIUS
- Augmenter le délai d'attente de la demande EAP et/ou le nombre maximal de tentatives de la demande EAP

CLI :

```
# config t
# wireless security dot1x request retries <0-20>
# wireless security dot1x timeout <1-120 seconds>
```

IUG:

Accédez aux paramètres requisConfiguration > Security > Advanced EAPet personnalisez-les.

Déconnecté en raison de la réinitialisation radio AP

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [apmgr-capwap-config] [8621]: (info): f07f.06ee.f590 Radio: 1
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [apmgr-db] [8621]: (note): MAC: f07f.06ee.f590 Radio 1 is dis
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [radio-history-reset] [8621]: (info): Radio reset of the AP f
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8621]: (note): MAC: e4b3.187c.3058 Client
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dpath_svc] [8621]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-transition] [8621]: (info): MAC: e4b3.187c.3058 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-client] [8621]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [wncd_1] [8621]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [auth-mgr] [8621]: (info): [e4b3.187c.3058:capwap_90400003] D
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-auth] [8621]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 DOT11 state trans
```

Motif :

Le point d'accès auquel le client était associé a modifié le canal ou l'alimentation, provoquant une réinitialisation radio.

Solutions possibles :

- C'est un comportement normal
- Vous pouvez configurer la fréquence à laquelle le WLC 9800 est autorisé à effectuer des modifications de canal

CLI :

```
# config t
# ap dot11 { 5ghz | 24ghz } rrm channel dca interval <0-24>

Valid values 1,2,3,4,6,8,12 and 24 hours, 0 = 10 minutes (default)
```

IUG:

Accédez à **Configuration > Radio Configurations > RRM > 5 GHz Band/2.4 GHz Band > DCA > Increase Interval Setting.**

Déconnecté en raison du délai d'authentification Web

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet eventQ: AUTH_MGR_MQ, message:6
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_AUTHC_FAI
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [9800 WLC-infra-evq] [8681]: (ERR): Authc failure for mac 087
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] S
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [errmsg] [8681]: (note): %SESSION_MGR-5-FAIL: Authorization f
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_AUTHZ_FAI
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (ERR): MAC: 0874.0277.1345 L3 Authentic
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [9800 WLC-infra-evq] [8681]: (ERR): WLAN profile = prof-name,
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (info): MAC: 0874.0277.1345 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (note): MAC: 0874.0277.1345 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-state] [8681]: (note): MAC: 0874.0277.1345 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [9800 WLC-qos-client] [8681]: (ERR): MAC: 0874.0277.1345 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [multicast-main] [8681]: (info): MAC: 0874.0277.1345 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-iplearn] [8681]: (info): MAC: 0874.0277.1345 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dpath_svc] [8681]: (note): MAC: 0874.0277.1345 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-transition] [8681]: (info): MAC: 0874.0277.1345 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-client] [8681]: (ERR): MAC: 0874.0277.1345 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [aaa-attr-inf] [8681]: (info): [ Applied attribute :bsn-vlan-
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [aaa-attr-inf] [8681]: (info): [ Applied attribute : timeout
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: 0874.0277.1345 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dot11] [8681]: (info): MAC: 0874.0277.1345 DOT11 state trans
```

Motif :

Le client n'a pas terminé l'authentification Web dans le délai imparti (environ 120 secondes).

Solution :
Assurez-vous que les clients effectuent l'authentification Web dans les 120 secondes.

Déconnecté en raison du délai d'expiration de la session

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-auth] [8621]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8621]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [9800 WLC-qos-client] [8621]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [multicast-main] [8621]: (info): MAC: e4b3.187c.3058 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-iplearn] [8621]: (info): MAC: e4b3.187c.3058 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dpath_svc] [8621]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-transition] [8621]: (info): MAC: e4b3.187c.3058 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-client] [8621]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-auth] [8621]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 DOT11 state trans
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8621]: (note): MAC: e4b3.187c.3058 Clien
```

Motif :

Le client a atteint son délai d'expiration de session.

Solutions possibles :

- C'est un comportement normal
- Augmenter le délai d'expiration de session de profil de stratégie associé au SSID

CLI :

```
# config t
# wireless profile policy <policy-profile-name>
# shutdow
# session-timeout <20-86400 seconds>
# no shutdown
```

IUG:

Accédez aux compteursConfiguration > Tags & Profiles > Policy > Policy Profile Name > Advanced > WLAN Timeoutet personnalisez-les si nécessaire.

Déconnecté en raison du délai d'inactivité

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [7807]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [7807]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [7807]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Clien
```

Motif :

Le client n'a pas envoyé de trafic (ou suffisamment de trafic) dans l'intervalle de délai d'inactivité configuré.

Solutions possibles :

- C'est un comportement normal
- Personnaliser les paramètres d'inactivité du profil de stratégie associés au SSID

CLI :

```
# config t
# wireless profile policy <policy-profile-name>
# shutdow
# idle-timeout <15-100000 seconds>
# idle-threshold  <0-4294967295 bytes>
# no shutdown
```

IUG:

Accédez aux paramètres d'inactivitéConfiguration > Tags & Profiles > Policy > Policy Profile Name > Advanced > WLAN Timeoutet personnalisez-les si nécessaire.

Remarque : si vous ne configurez pas le seuil d'inactivité, le client doit envoyer n'importe quelle quantité de trafic dans le délai d'inactivité pour ne pas être déconnecté. Si vous configurez le seuil d'inactivité, le client doit envoyer cette quantité d'octets dans le délai d'inactivité pour ne pas être déconnecté (c'est-à-dire, si vous configurez un seuil d'inactivité de 10 octets et un délai d'inactivité de 30 secondes, les clients sans fil doivent envoyer au moins 10 octets de trafic toutes les 30 secondes pour ne pas être déconnectés du réseau).

Le client a changé de SSID

Exemple de journal :

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (note): MAC: e4b3.187c.3058 Associat
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (ERR): MAC: e4b3.187c.3058 Failed to
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Client
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (note): MAC: e4b3.187c.3058 Client de
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Client
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [7807]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {fman_fp_F0-0}{1}: [wireless-client] [10254]: UUID: 1000000006930, ra: 5 (note)
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [7807]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [7807]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Client
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8009]: (note): MAC: e4b3.187c.3058 Associat
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8009]: (note): MAC: e4b3.187c.3058 Client
```

Motif :

Le client a été connecté à un SSID et déplacé vers un autre.

Solutions possibles :

- comportement normal ;
- Supprimez le 2e SSID du client

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.