

WLAN FlexConnect avec remplacement AAA 802.1x sur les contrôleurs sans fil Catalyst 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration](#)

[Configuration AAA sur un contrôleur WLC 9800](#)

[Configuration d'un réseau local sans fil \(WLAN\)](#)

[Définir AP comme mode FlexConnect](#)

[Configuration du commutateur](#)

[Configuration du profil des politiques](#)

[Configuration des balises des politiques](#)

[Attribution de balise de stratégie](#)

[Configuration ISE](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer un contrôleur LAN sans fil élastique (WLC 9800) avec des points d'accès (AP) en mode FlexConnect et un réseau local sans fil (WLAN) 802.1x commuté localement avec la priorité AAA (Authentication, Authorization and Accounting) du réseau local virtuel (VLAN).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Mode de configuration WLC 9800
- FlexConnect

Composants utilisés

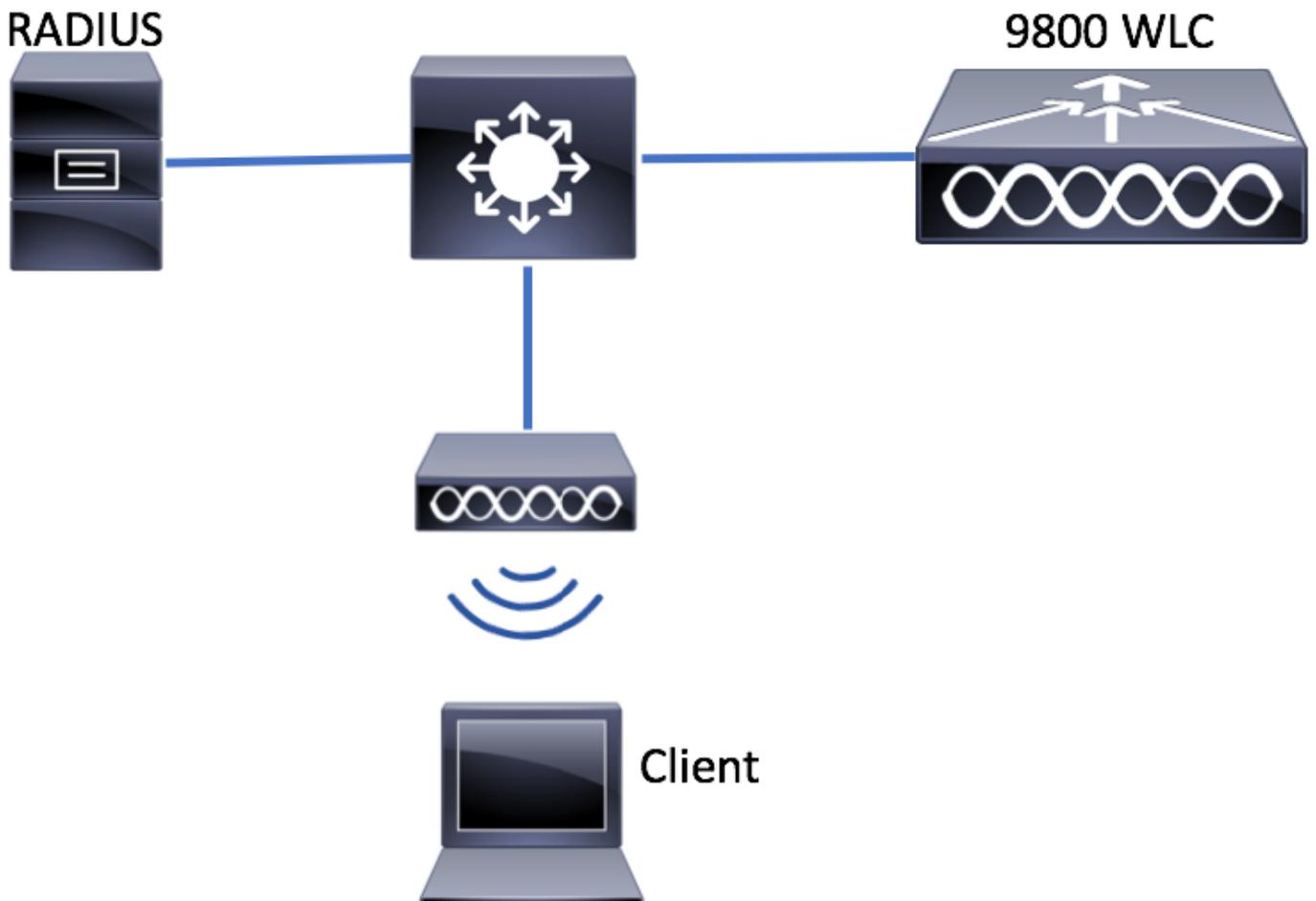
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC 9800 v16.10

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.

Configurer

Diagramme du réseau



Configuration

Configuration AAA sur un contrôleur WLC 9800

Vous pouvez suivre les instructions de ce lien :

[Configuration AAA sur un contrôleur WLC 9800](#)

Configuration d'un réseau local sans fil (WLAN)

Vous pouvez suivre les instructions de ce lien :

[Configuration d'un réseau local sans fil \(WLAN\)](#)

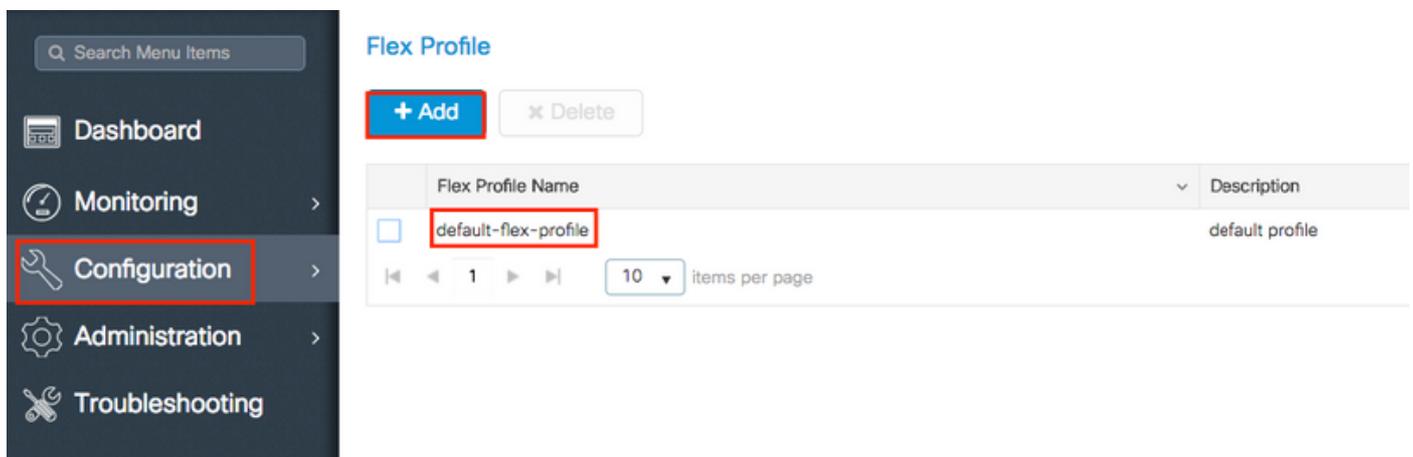
Définir AP comme mode FlexConnect

Contrairement à la configuration AireOS, sur le WLC 9800, il n'est pas possible de configurer le mode AP local ou flexconnect directement à partir du point d'accès. Procédez comme suit pour configurer un point d'accès en mode FlexConnect.

IUG

Étape 1. Configurer un profil flexible.

Naviguez jusqu'à Configuration > Balises et profils > Flex et modifiez le default-flex-profile ou cliquez sur +Add pour en créer un nouveau.

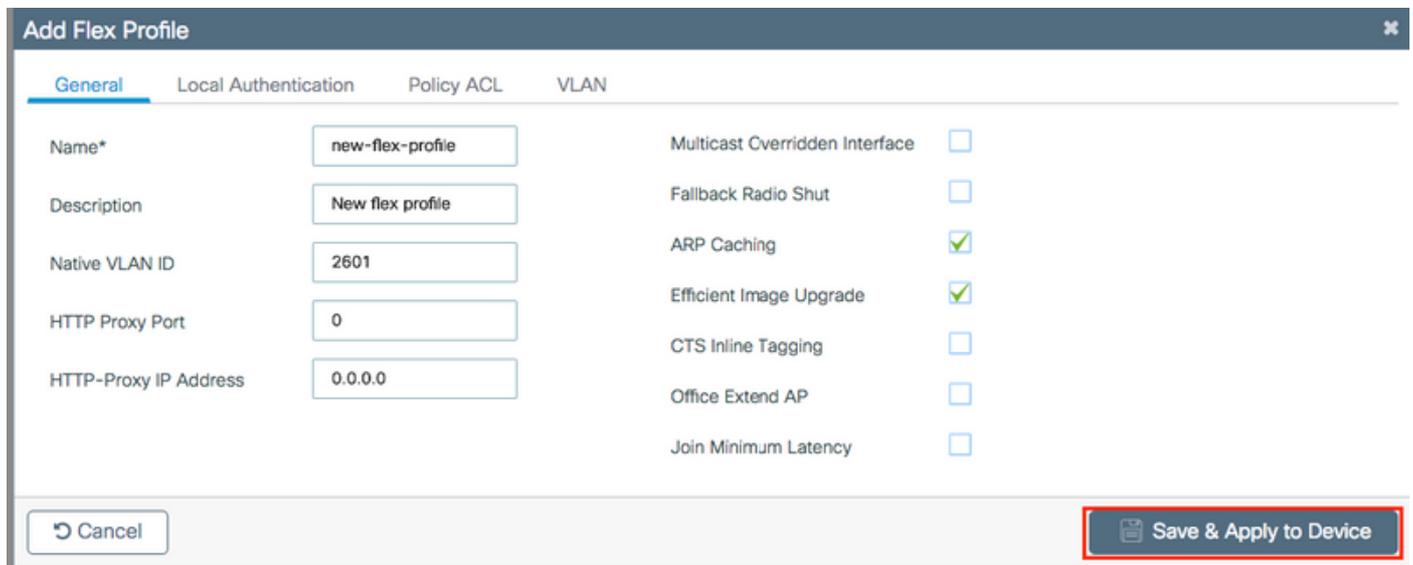


Flex Profile

+ Add × Delete

Flex Profile Name	Description
<input type="checkbox"/> default-flex-profile	default profile

10 items per page



Add Flex Profile

General Local Authentication Policy ACL VLAN

Name* new-flex-profile Multicast Overridden Interface

Description New flex profile Fallback Radio Shut

Native VLAN ID 2601 ARP Caching

HTTP Proxy Port 0 Efficient Image Upgrade

HTTP-Proxy IP Address 0.0.0.0 CTS Inline Tagging

Office Extend AP

Join Minimum Latency

Cancel Save & Apply to Device

Étape 2. Ajoutez les VLAN nécessaires (les VLAN du WLAN par défaut ou les VLAN envoyés depuis ISE).

 Remarque : à l'étape 3 de la section Policy Profile Configuration, vous sélectionnez le VLAN

 par défaut attribué au SSID. Si vous utilisez un nom de VLAN à cette étape, assurez-vous que vous utilisez le même nom de VLAN dans la configuration Flex Profile, sinon les clients ne pourront pas se connecter au WLAN.

Edit Flex Profile

General Local Authentication Policy ACL **VLAN**

+ Add × Delete

VLAN Name	ID	ACL Name
No items to display		

◀ 0 ▶ 10 items per page

Vous pouvez éventuellement ajouter des listes de contrôle d'accès spécifiques par VLAN.

VLAN Name*

VLAN Id*

ACL Name

✓ Save **↺ Cancel**

Affectez éventuellement un groupe de serveurs Radius pour permettre aux points d'accès FlexConnect d'effectuer une authentification locale.

Edit Flex Profile

General **Local Authentication** Policy ACL VLAN

Radius Server Group LEAP

EAP Fast Profile PEAP

TLS

RADIUS

Users

Username

0 items per page

No items to display

Étape 3. Configurez une balise de site.

Accédez à Configuration > Tags & Profiles > Tags > Site. Modifiez la balise default-site-tag (qui est la balise attribuée par défaut à tous les AP) ou créez-en une nouvelle (cliquez sur +Add pour en créer une nouvelle).

Manage Tags

Policy **Site** RF AP

Site Tag Name

default-site-tag

1 items per page

Assurez-vous de désactiver l'option Enable Local Site, sinon l'option Flex Profile n'est pas disponible.

Add Site Tag

Name*

Description

AP Join Profile

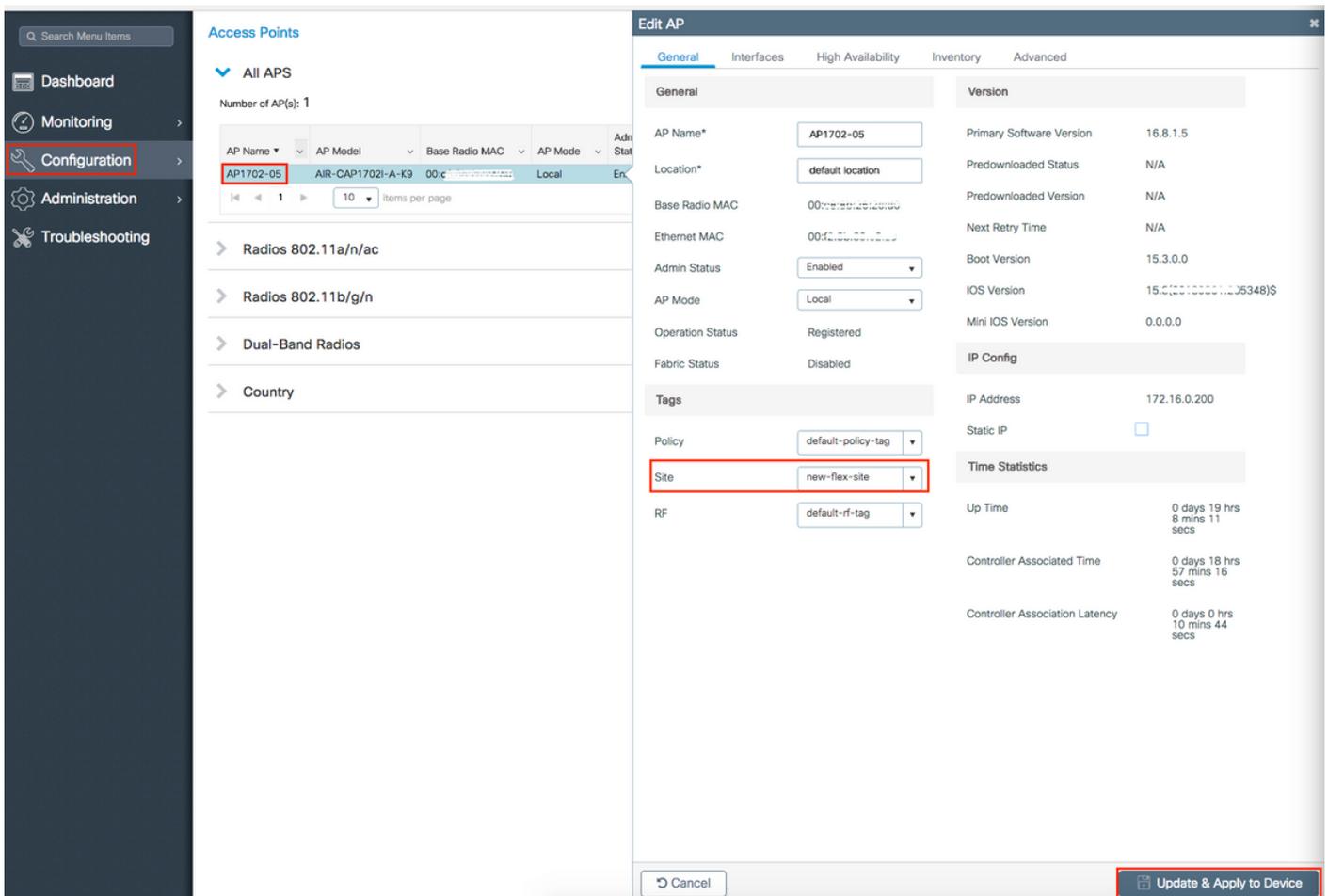
Flex Profile

Enable Local Site

 Remarque : tout point d'accès qui obtient une balise de site avec Activer le site local activé est configuré en mode local. De même, tout AP qui obtient une balise de site avec Enable Local Site désactivé, est configuré en mode flexconnect.

Étape 4. Associez un point d'accès au WLC 9800 et attribuez la balise Site configurée à l'étape 2.

Accédez à Configuration > Wireless > Access Points > AP name et définissez la balise Site. Cliquez ensuite sur Update & Apply to Device pour définir la modification.



The screenshot shows the 'Edit AP' configuration page for AP1702-05. The 'Site' tag is set to 'new-flex-site'. The 'Update & Apply to Device' button is highlighted in red.

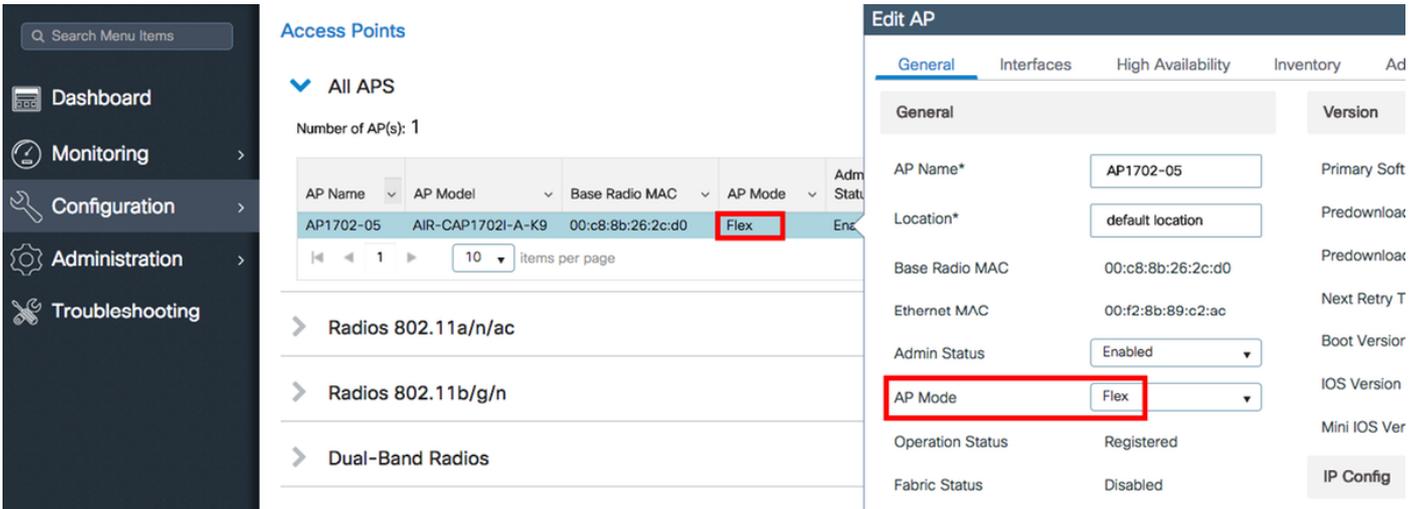
AP Name*	AP Model	Base Radio MAC	AP Mode	Admin Status
AP1702-05	AIR-CAP1702I-A-K9	00:c0:00:00:00:00	Local	Enabled

General	Version
AP Name*	AP1702-05
Location*	default location
Base Radio MAC	00:c0:00:00:00:00
Ethernet MAC	00:f2:00:00:00:00
Admin Status	Enabled
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
Primary Software Version	16.8.1.5
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	15.3.0.0
IOS Version	15.0(201000011.205348)S
Mini IOS Version	0.0.0.0
IP Address	172.16.0.200
Static IP	<input type="checkbox"/>
Up Time	0 days 19 hrs 8 mins 11 secs
Controller Associated Time	0 days 18 hrs 57 mins 16 secs
Controller Association Latency	0 days 0 hrs 10 mins 44 secs

 Remarque : sachez qu'après avoir modifié la balise sur un AP, il perd son association avec

 le WLC 9800 et se reconnecte dans environ 1 minute.

Étape 5. Une fois que le point d'accès se reconnecte, notez que le mode AP est Flex



The screenshot displays the Cisco WLC GUI. On the left is a navigation menu with options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area shows 'Access Points' with a table of APs. The table has columns for AP Name, AP Model, Base Radio MAC, AP Mode, and Admin Status. One AP is listed: AP1702-05, AIR-CAP1702I-A-K9, 00:c8:8b:26:2c:d0, Flex, and Enabled. Below the table are expandable sections for Radios 802.11a/n/ac, Radios 802.11b/g/n, and Dual-Band Radios. On the right, the 'Edit AP' panel is open, showing various configuration fields. The 'AP Mode' dropdown menu is highlighted with a red box and set to 'Flex'.

CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode : FlexConnect
```

Configuration du commutateur

Configurez l'interface du commutateur à laquelle le point d'accès est connecté.

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
```

```
# spanning-tree portfast trunk
# end
```

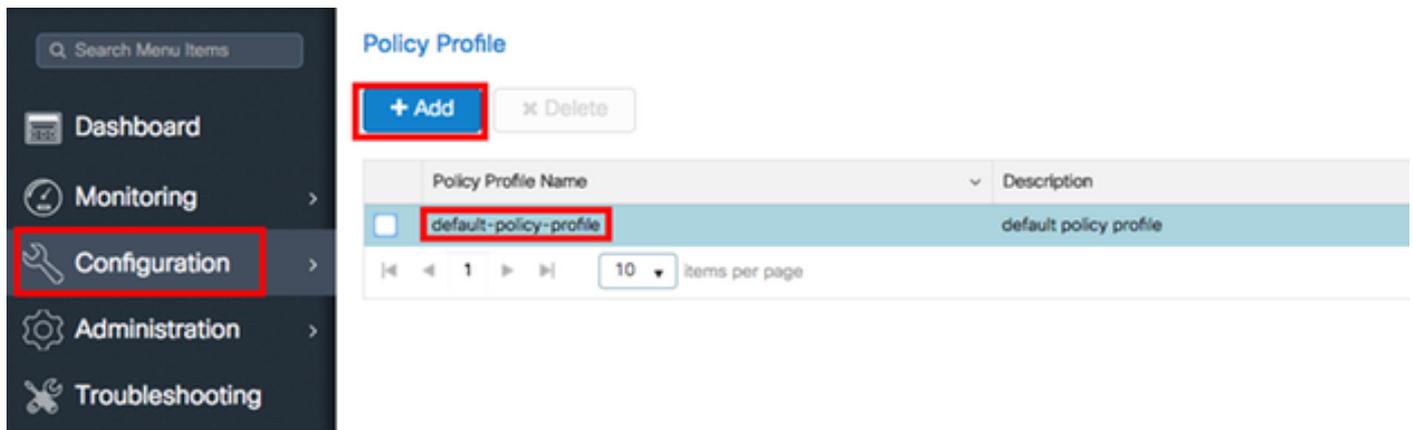
Configuration du profil des politiques

Dans un profil de stratégie, vous pouvez décider à quel VLAN attribuer les clients, entre autres paramètres (comme la liste de contrôle d'accès [ACL], la qualité de service [QoS], l'ancrage de mobilité, les minuteurs, etc.).

IUG

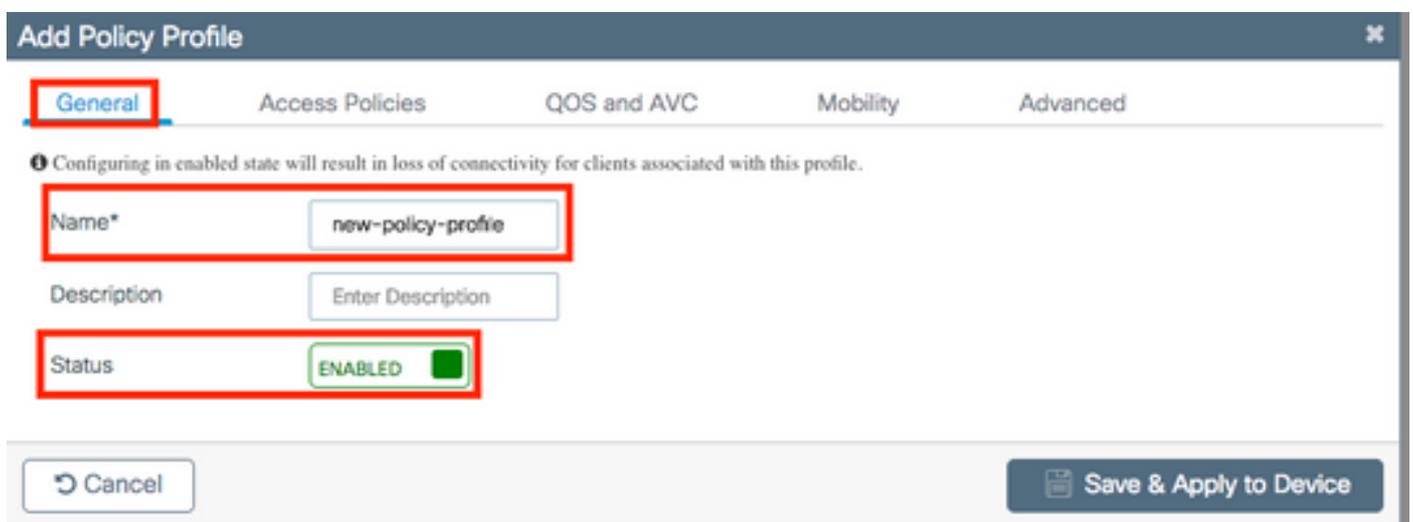
Étape 1. Configurez le profil de stratégie à attribuer au WLAN.

Accédez à Configuration > Tags & Profiles > Policy et créez-en un nouveau ou modifiez le default-policy-profile.



The screenshot shows the 'Policy Profile' configuration page. On the left is a dark sidebar with a search bar and menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area has a title 'Policy Profile' and two buttons: '+ Add' (highlighted with a red box) and 'x Delete'. Below is a table with columns 'Policy Profile Name' and 'Description'. The first row shows 'default-policy-profile' (highlighted with a red box) and 'default policy profile'. At the bottom of the table, there are navigation icons and a dropdown for '10 items per page'.

Étape 2. Dans l'onglet Général, attribuez un nom au profil de stratégie et changez son état en ENABLED.

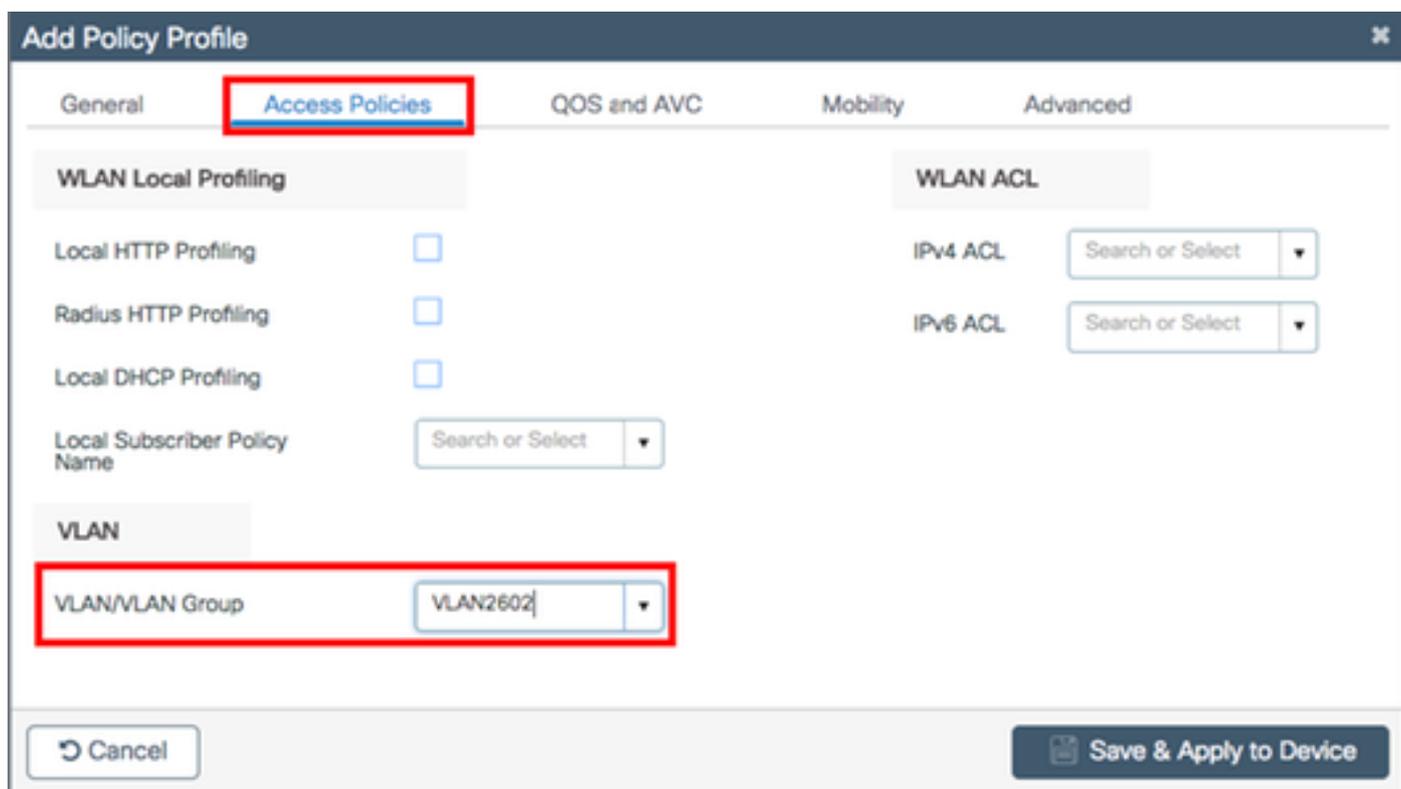


The screenshot shows the 'Add Policy Profile' dialog box with the 'General' tab selected (highlighted with a red box). The dialog has tabs for 'General', 'Access Policies', 'QOS and AVC', 'Mobility', and 'Advanced'. A warning message states: 'Configuring in enabled state will result in loss of connectivity for clients associated with this profile.' The 'Name*' field contains 'new-policy-profile' (highlighted with a red box). The 'Description' field contains 'Enter Description'. The 'Status' field is set to 'ENABLED' with a green toggle switch (highlighted with a red box). At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons.

Étape 3. Dans l'onglet Access Policies, affectez le VLAN auquel les clients sans fil sont affectés lorsqu'ils se connectent à ce WLAN par défaut.

Vous pouvez sélectionner un nom de VLAN dans la liste déroulante ou saisir manuellement un ID de VLAN.

 Remarque : Si vous sélectionnez un nom de VLAN dans la liste déroulante, assurez-vous qu'il correspond au nom de VLAN utilisé à l'étape 2 de la section Définir AP comme mode FlexConnect.



The screenshot shows the 'Add Policy Profile' configuration page with the 'Access Policies' tab selected. The 'VLAN/VLAN Group' field is highlighted with a red box and contains the value 'VLAN2602'. Other fields include 'Local HTTP Profiling', 'Radius HTTP Profiling', 'Local DHCP Profiling', 'Local Subscriber Policy Name', 'WLAN ACL', 'IPv4 ACL', and 'IPv6 ACL'. The 'Cancel' and 'Save & Apply to Device' buttons are visible at the bottom.

General	Access Policies	QOS and AVC	Mobility	Advanced
WLAN Local Profiling		WLAN ACL		
Local HTTP Profiling	<input type="checkbox"/>		IPv4 ACL	<input type="text" value="Search or Select"/>
Radius HTTP Profiling	<input type="checkbox"/>		IPv6 ACL	<input type="text" value="Search or Select"/>
Local DHCP Profiling	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="text" value="Search or Select"/>			
VLAN				
VLAN/VLAN Group	<input type="text" value="VLAN2602"/>			

ou

Edit Policy Profile

General	Access Policies	QOS and AVC	Mobility	Advanced
WLAN Local Profiling		WLAN ACL		
Local HTTP Profiling	<input type="checkbox"/>	IPv4 ACL	Search or Select ▼	
Radius HTTP Profiling	<input type="checkbox"/>	IPv6 ACL	Search or Select ▼	
Local DHCP Profiling	<input type="checkbox"/>			
Local Subscriber Policy Name	Search or Select ▼			
VLAN				
VLAN/VLAN Group	2601 ▼			

Étape 4. Accédez à l'onglet Advanced et activez les options Central Authentication Enable et Allow AAA Overrideoptions. La commutation centrale doit être désactivée.

L'authentification centrale doit être activée si vous voulez que le processus d'authentification soit effectué de manière centralisée par le WLC 9800. Désactivez-la si vous souhaitez que les points d'accès FlexConnect authentifient les clients sans fil.

Edit Policy Profile



General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)*

Idle Timeout (sec)*

Idle Threshold (bytes)*

Client Exclusion Timeout (sec)*

DHCP

DHCP Enable

DHCP Server IP Address

DHCP Opt82 Enable

DHCP Opt82 Ascii

DHCP Opt82 RID

DHCP Opt82 Format

DHCP AP MAC

DHCP SSID

DHCP AP ETH MAC

DHCP AP NAME

DHCP Policy Tag

DHCP AP Location

DHCP VLAN ID

AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

CLI

```
# config t
# wireless profile policy new-policy-profile
# central association
# vlan <vlan-id or vlan-name>
# no shutdown
```

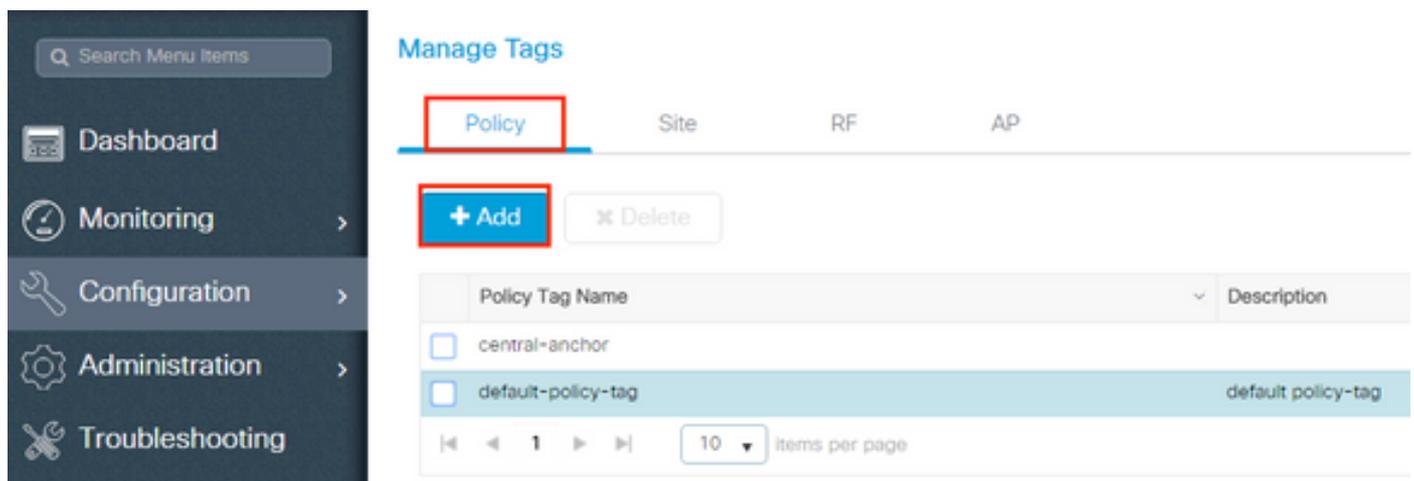
Configuration des balises des politiques

La balise de stratégie est utilisée pour lier le SSID au profil de stratégie. Vous pouvez soit créer une nouvelle balise de politiques, soit utiliser la balise de politique par défaut.

 Remarque : la balise default-policy-tag lie automatiquement tout SSID avec un ID WLAN compris entre 1 et 16 au le profil default-policy-profile. Il ne peut pas être modifié ni supprimé. Si vous disposez d'un WLAN avec l'ID 17 ou supérieur, la balise default-policy-tag ne peut pas être utilisée.

IUG:

Accédez à Configuration > Tags & Profiles > Tags > Policy et ajoutez-en un nouveau si nécessaire.



Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

Liez votre profil de réseau WLAN au profil de politiques souhaité.

Add Policy Tag



Name*

PolicyTagName

Description

Enter Description

+ Add

× Delete

WLAN Profile

Policy Profile

◀ ◁ 0 ▷ ▶ 10 items per page

No items to display

↶ Cancel

📄 Save & Apply to Device

Add Policy Tag



Name*

PolicyTagName

Description

Enter Description

+ Add

× Delete

WLAN Profile

Policy Profile

◀ ◁ 0 ▷ ▶ 10 items per page

No items to display

Map WLAN and Policy

WLAN Profile*

prof-name

Policy Profile*

default-policy-profile



↶ Cancel

📄 Save & Apply to Device

Add Policy Tag ✕

Name*

Description

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile

◀ ◁ 1 ▷ ▶ 10 items per page 1 - 1 of 1 items

CLI :

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Attribution de balise de stratégie

Attribuez la balise Policy au point d'accès

IUG

Pour attribuer la balise à un point d'accès, accédez à Configuration > Wireless > Access Points > AP Name > General Tags, effectuez l'attribution nécessaire, puis cliquez sur Update & Apply to Device.

General

AP Name*	AP1702-00
Location*	default location
Base Radio MAC	00:c0:00:00:00:00
Ethernet MAC	00:c0:00:00:00:00
Admin Status	Enabled
AP Mode	Flex
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	new-policy-tag
Site	new-flex-site
RF	default-rf-tag

Version

Primary Software Version	18.0.0.0
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	18.0.0.0
IOS Version	18.0
Mini IOS Version	0.0.0.0

IP Config

IP Address	172.16.0.200
Static IP	<input type="checkbox"/>

Time Statistics

Up Time	1 days 1 hrs 44 mins 59 secs
Controller Associated Time	0 days 5 hrs 32 mins 0 secs
Controller Association Latency	0 days 20 hrs 11 mins 24 secs

Cancel

Update & Apply to Device



Remarque : sachez qu'après avoir modifié la balise de stratégie sur un AP, il perd son association au WLC 9800 et se reconnecte dans environ 1 minute.

Pour attribuer la même balise de stratégie à plusieurs points d'accès, accédez à Configuration > Wireless > Wireless Setup > Start Now > Apply.

Start

Tags & Profiles

 WLAN Profile  

 Policy Profile  

 Policy Tag   

 AP Join Profile  

Start Now →

 Flex Profile  

 Site Tag   

 RF Profile  

 RF Tag   

Apply

 Tag APs 

Done

 : selon le volume de journaux générés, vous pouvez revenir en arrière de quelques heures à plusieurs jours.

Afin d'afficher les suivis collectés par défaut par le contrôleur WLC 9800, vous pouvez vous connecter par SSH/Telnet au contrôleur WLC 9800 et suivre ces étapes (assurez-vous de consigner la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du contrôleur de sorte que vous puissiez suivre les journaux dans l'heure jusqu'à quand le problème s'est produit.

```
# show clock
```

Étape 2. Effectuez la collecte des journaux du système à partir de la mémoire tampon du contrôleur ou du journal système externe, selon la configuration du système. Cela fournit un aperçu rapide de l'intégrité du système et des erreurs, le cas échéant.

```
# show logging
```

Étape 3. Vérifiez si les conditions de débogage sont activées.

```
# 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 augmenterait le volume de journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque le débogage n'est pas actif.

Étape 4. En supposant que l'adresse MAC testée ne soit pas répertoriée comme condition lors de l'étape 3, collectez les suivis de niveau de notification permanents pour l'adresse MAC.

```
# 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 traçage Radio Active

Si les suivis toujours actifs ne vous fournissent pas suffisamment d'informations pour déterminer ce qui déclenche le problème faisant l'objet de l'enquête, vous pouvez activer le débogage conditionnel et capturer le suivi Radio Active (RA), qui fournira des suivis au niveau du débogage pour tous les processus qui interagissent avec la condition définie (adresse MAC du client dans ce cas). Pour activer la fonction de débogage conditionnel, procédez comme suit.

Étape 5. Assurez-vous 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 plusieurs clients à la fois, exécutez la <aaaa.bbbb.cccc>commande de débogage sans fil mac par adresse MAC.



Remarque : Le résultat de l'activité du client ne s'affiche pas sur la session du terminal, car tout est mis en mémoire tampon interne pour être consulté plus tard.

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

Étape 8. Arrêtez le débogage si le problème est reproduit avant la fin du temps de surveillance par défaut ou configuré.

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

Une fois que le temps de surveillance s'est écoulé ou que le débogage sans fil a été arrêté, le contrôleur WLC 9800 génère un fichier local du nom de :

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 9. Recueillir le fichier de l'activité de l'adresse MAC. Il est possible de copier le fichier de suivi RA .log sur un serveur externe ou d'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 vous ne trouvez toujours pas la cause première, collectez les journaux internes, qui peuvent vous offrir une vue plus détaillée des journaux de niveau de débogage. Vous n'avez pas besoin de déboguer à nouveau le client, car nous examinons seulement 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 : cette sortie de commande retourne des traces pour tous les niveaux de journalisation pour tous les processus et est assez volumineuse. Veuillez faire appel à Cisco TAC pour faciliter l'analyse de ces suivis.

Vous pouvez soit copier le fichier ra-internal-FILENAME.txt sur un serveur externe, soit 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. Supprimez les conditions de débogage.

```
# clear platform condition all
```

 Remarque : assurez-vous de toujours supprimer les conditions de débogage après une session de dépannage.

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.