Recette Cuisine : Configuration CLI minimale de démarrage pour Catalyst 9800

Contenu

Introduction
Conditions préalables
Ingrédients
Configuration
Diagramme du réseau
Facultatif: Restauration des paramètres d'usine par défaut du contrôleur - Jour zéro
Ignorer l'assistant de configuration initiale
Modèle Bootstrap - Paramètres de base du périphérique
Configuration initiale du périphérique et connectivité hors bande
Facultatif - Activer CDP
9800-CL - Créer un certificat auto-signé
Créer des VLAN
Configurer les interfaces de données - Appliances
Configurer l'interface de gestion sans fil
Configurer la sincronisation du fuseau horaire et du protocole NTP
Accès VTY et autres services locaux
Configuration RADIUS
Facultatif - Sauvegarde quotidienne de la configuration
Configuration sans fil
Facultatif - Meilleures pratiques
Création de WLAN - WPA2-PSK
Création de WLAN - WPA2-Enterprise
Création de WLAN - Invité avec authentification Web locale
Création de WLAN - Invité avec authentification Web centralisée
Création de stratégies pour les points d'accès en mode local
Création de stratégies pour les points d'accès en mode Flexconnect
Final - Appliquer des balises aux points d'accès
Comment obtenir la liste des adresses MAC AP
Lecture recommandée

Introduction

Ce document décrit plusieurs options disponibles pour « bootstrap » (configuration initiale) pour un contrôleur LAN sans fil (WLC) Catalyst 9800. Certains peuvent nécessiter des processus externes (téléchargement PNP ou TFTP), d'autres peuvent être effectués partiellement via l'interface de ligne de commande, puis les compléter via l'interface utilisateur graphique, etc.

Ce document se concentrera sur un format de « recette de cuisson », avec un ensemble minimal d'actions simplifiées, pour qu'un 9800 soit configuré pour les opérations de base, y compris

l'administration à distance, et les meilleures pratiques, dans les plus brefs délais.

Le modèle fourni contient des commentaires préfacés du caractère « ! » pour expliquer des points spécifiques de la configuration. En outre, toutes les valeurs que vous devez fournir sont indiquées dans le tableau « ingrédients » ci-dessous

Il s'agit des versions 17.3 et ultérieures.

Conditions préalables

- Contrôleur Catalyst 9800 prêt à l'emploi. En gros, sans configuration
- Compréhension de base de la configuration IOS-XE
- Accédez au port de console de votre contrôleur. Il peut s'agir du port physique CON de votre appareil (9800-40, 9800-80, 9800-L) ou de votre client d'accès à distance hyperviseur pour 9800-CL
- Pour l'accès série, toute application client de terminal de votre choix

Ingrédients

Chaque élément majuscule correspond à un paramètre que vous devez modifier avant d'utiliser le modèle de configuration :

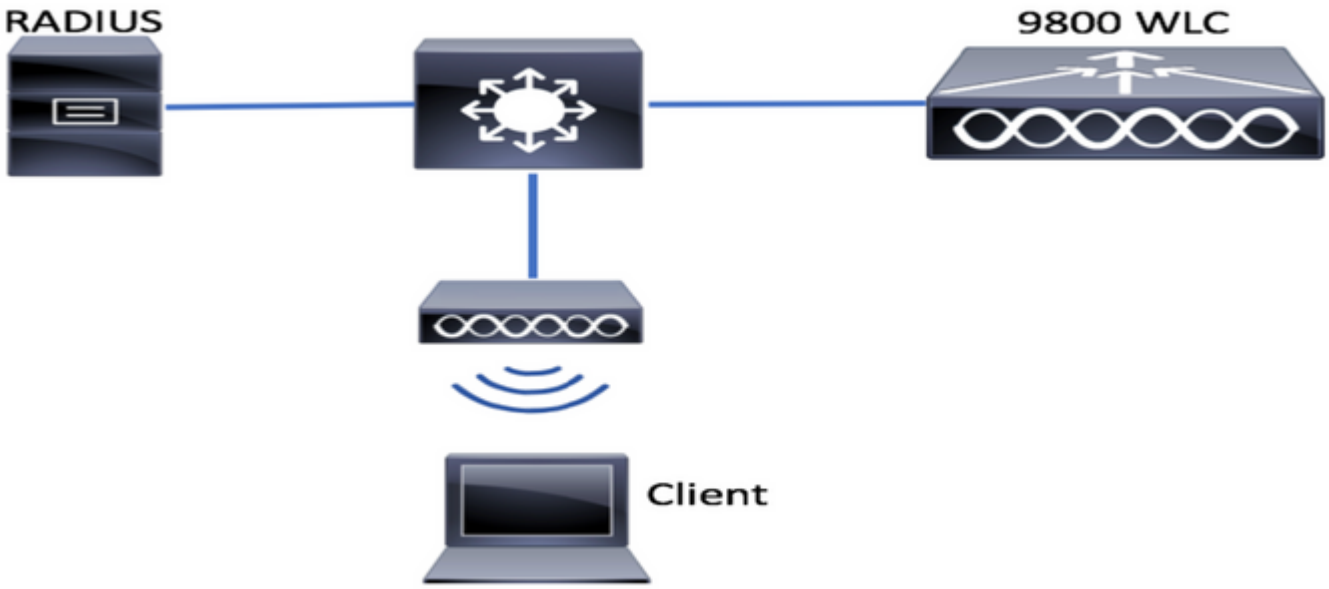
Valeur requise	Nom du modèle	Exemple
IP de gestion hors bande	[OOM_IP]	192.168.0.25
Passerelle par défaut de gestion hors bande	[OOM_GW]	192.168.0.1
Nom d'utilisateur administrateur	[ADMIN]	admin
Mot de passe administrateur	[MOT DE PASSE]	ah1-7k++a1
Nom d'utilisateur de l'administrateur AP	[AP_ADMIN]	admin
Mot de passe CLI AP	[PASSWORD_AP]	alkhb90jlih
AP Enable Secret	[AP_SECRET]	kh20-9yjh
Nom d'hôte du contrôleur	[NOM_WLC]	9800-bcn-1
Nom de domaine de la société	[NOM_DOMAINE]	company.com
ID VLAN du client	[VLAN_CLIENT]	15
Nom du VLAN client	[VLAN_NAME]	vlan_client
VLAN d'interface de gestion sans fil	[WMI_VLAN]	25
IP de l'interface de gestion sans fil	[IP_WMI]	192.168.25.10
Masque d'interface de gestion sans fil	[MASQUE_WMI]	255.255.255.0
GW par défaut de l'interface de gestion sans fil	[WMI_GW]	192.168.25.1
Serveur NTP	[NTP_IP]	192.168.1.2
Adresse IP du serveur Radius	[RADIUS_IP]	192.168.0.98

Clé Radius ou secret partagé	[CLÉ_RADIUS]	ThisIsASharedSecret
WLAN SSID WPA2 Nom de clé prépartagée	[SSID-PSK]	personnel
Authentification WLAN SSID WPA2 802.1x	[SSID-DOT1x]	nom d'entreprise
Authentification Web locale invité SSID WLAN	[SSID-LWA]	invité1
Authentification Web locale invité SSID WLAN	[SSID-CWA	invité2

Configuration

Diagramme du réseau

Ce document suit une topologie très basique, avec un contrôleur Calatyst 9800 connecté à un commutateur, plus un point d'accès sur le même VLAN à des fins de test, avec un serveur Radius en option pour l'authentification



Facultatif: Restauration des paramètres d'usine par défaut du contrôleur - Jour zéro

si votre contrôleur a déjà été configuré et que vous voulez le remettre à un scénario de jour zéro, sans aucune configuration, vous pouvez effectuer la procédure facultative suivante :

```
DAO2#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Sep 7 10:09:31.141: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
DAO2#reload
```

```
System configuration has been modified. Save? [yes/no]: no
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

Sep 7 10:10:55.318: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
Chassis 1 reloading, reason - Reload command
```

Ignorer l'assistant de configuration initiale

Une fois le rechargement terminé, le contrôleur présente un assistant de configuration CLI pour effectuer une configuration initiale de base. Dans ce document, nous contournerons cette option et configurerons toutes les valeurs à l'aide du modèle CLI fourni dans les étapes suivantes.

Attendez que le contrôleur ait terminé son démarrage :

```
Installation mode is INSTALL

No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console

Autoinstall trying DHCPv4 on GigabitEthernet0

Autoinstall trying DHCPv6 on GigabitEthernet0


--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0:
Machine Check: 0 Bank 9: ee2000000003110a
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0
ADDR ff007f00 MISC 228aa040101086
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR
0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0:
Machine Check: 0 Bank 10: ee2000000003110a
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0
ADDR ff007fc0 MISC 228aa040101086
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR
0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0:
Machine Check: 0 Bank 11: ee2000000003110a
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0
ADDR ff007f80 MISC 228aa040101086
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR
0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
Autoinstall trying DHCPv4 on GigabitEthernet0,Vlan1

Autoinstall trying DHCPv6 on GigabitEthernet0,Vlan1

Acquired IPv4 address 192.168.10.105 on Interface GigabitEthernet0
Received following DHCPv4 options:
domain-name : cisco.com
dns-server-ip : 192.168.0.21

OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery
```

```
Guestshell destroyed successfully
```

Appuyez sur la touche Entrée et dites « non » à la boîte de dialogue initiale, et « oui », pour mettre fin au processus d'installation automatique :

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes


Press RETURN to get started!
```

Modèle Bootstrap - Paramètres de base du périphérique

Utilisez les modèles de configuration suivants et modifiez les valeurs indiquées dans le tableau Ingrédients. Ce document est divisé en différentes sections pour faciliter l'examen

Pour toutes les sections, collez toujours le contenu en mode Config, en appuyant sur la touche Entrée pour obtenir l'invite, puis en utilisant les commandes enable et config, par exemple :

```
WLC>enable
WLC#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
WLC(config)#hostname controller-name
```

Configuration initiale du périphérique et connectivité hors bande

Utilisez les commandes suivantes en mode Config. Les commandes finissent par enregistrer la configuration pour s'assurer que SSH est activé, après avoir créé la clé locale

```
hostname [WLC_NAME]

int gi0
ip add [OOM_IP] 255.255.255.0
exit
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 [OOM_GW]

no ip domain lookup

username [ADMIN] privilege 15 password 0 [PASSWORD]

ip domain name [DOMAIN_NAME]

aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
aaa authorization network default local


line con 0
privilege level 15
login authentication CONSOLE
exit
crypto key generate rsa modulus 2048
ip ssh version 2
```

```
end
wr
```

Facultatif - Activer CDP

Passez à nouveau en mode Config et utilisez les commandes suivantes. Pour 9800-CL, remplacez les interfaces Te0/0/0 et Te0/0/1 par Gi1 et Gi2

```
cdp run
int te0/0/0
cdp ena
int te0/0/1
cdp ena
```

9800-CL - Créer un certificat auto-signé

Ceci doit uniquement être effectué sur les contrôleurs 9800-CL, il **n**'est **pas** requis sur les modèles d'appliance (9800-80, 9800-40, 9800-L) pour la jointure CAPWAP AP

```
wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 [CHANGEPASSWORD]
```

Créer des VLAN

Àpartir du mode Config, créez autant de VLAN client que nécessaire et le VLAN correspondant à l'interface de gestion sans fil (WMI).

Dans la plupart des scénarios, il est courant d'avoir au moins 2 réseaux locaux virtuels clients, un pour l'entreprise et un pour l'accès invité. De grands scénarios peuvent couvrir des centaines de réseaux locaux virtuels différents selon les besoins

Le VLAN WMI est le point d'accès au contrôleur pour la plupart des protocoles et des topologies de gestion, et c'est là que les points d'accès créeront leurs tunnels CAPWAP

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

Configurer les interfaces de données - Appliances

Pour 9800-L, 9800-40, 9800-80, à partir du mode de configuration, vous pouvez utiliser les commandes suivantes pour définir les fonctionnalités de base des interfaces de plan de données. Cet exemple propose LACP, avec groupe de canaux créé sur les deux ports.

Il est important de configurer une topologie correspondante du côté du commutateur.

Cette section peut présenter des modifications importantes de l'exemple fourni à ce qui est réellement nécessaire, selon votre topologie et si vous utilisez des canaux de port. Veuillez vérifier attentivement.

```
!!Interfaces. LACP if standalone or static (channel-group 1 mode on) on if HA before 17.1.
interface TenGigabitEthernet0/0/0
description You should put here your switch name and port
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no negotiation auto
channel-group 1 mode active

interface TenGigabitEthernet0/0/1
description You should put here your switch name and port
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no negotiation auto
channel-group 1 mode active
no shut

int po1
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no shut

!!Configure the same in switch and spanning-tree portfast trunk
port-channel load-balance src-dst-mixed-ip-port
```

Configurer l'interface de gestion sans fil

Utilisez les commandes suivantes en mode de configuration pour créer le WMI. Il s'agit d'une étape cruciale

```
int vlan [WMI_VLAN]
ip add [WMI_IP] [WMI_MASK]
no shut

ip route 0.0.0.0 0.0.0.0 [WMI_GW]

!! The interface name will normally be somethng like Vlan25, depending on your WMI VLAN ID
wireless management interface Vlan[WMI_VLAN]
```

Configurer la sincronisation du fuseau horaire et du protocole NTP

Le protocole NTP est essentiel pour plusieurs fonctionnalités sans fil. Pour le configurer, utilisez les commandes suivantes en mode de configuration :

```
ntp server [NTP_IP]
!!This is European Central Time, it should be adjusted to your local time zone
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
```

Accès VTY et autres services locaux

Suivant les meilleures pratiques, cela créera des lignes VTY supplémentaires, pour éviter les problèmes d'accès à l'interface utilisateur graphique et pour permettre aux services de base d'améliorer la gestion des sessions TCP pour les interfaces de gestion

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service tcp-keepalives-in
service tcp-keepalives-out
logging buffered 512000

line vty 0 15
transport input ssh

line vty 16 50
transport input ssh
```

Configuration RADIUS

Cela créera des paramètres de base pour activer les communications RADIUS vers le serveur ISE

```
radius server ISE
address ipv4 [RADIUS_IP] auth-port 1645 acct-port 1646
key [RADIUS_KEY]
automate-tester username dummy probe-on

aaa group server radius ISE_GROUP
server name ISE

aaa authentication dot1x ISE group ISE_GROUP

radius-server dead-criteria time 5 tries 3
radius-server deadtime 5
```

Facultatif - Sauvegarde quotidienne de la configuration

Pour des raisons de sécurité, vous pouvez activer une sauvegarde de configuration quotidienne automatisée sur un serveur TFTP distant :

```
archive
path tftp://TFTP_IP/lab_configurations/9800-config.conf
time-period 1440
```

Configuration sans fil

Cette section présente un exemple de différents types de WLAN, couvrant les combinaisons les plus courantes de WPA2 avec Preshare Key, WPA2 avec 802.1x/radius, Central Webauth et Local Webauth. Il n'est pas prévu que votre déploiement contienne tous ces éléments, vous devez donc les supprimer et les modifier si nécessaire

Il est essentiel de définir la commande country pour s'assurer que le contrôleur marque la configuration comme « complète ». Vous devez modifier la liste des pays pour qu'elle corresponde à votre emplacement de déploiement :

```
ap dot11 24ghz cleanair
ap dot11 5ghz cleanair
no ap dot11 5ghz SI

!!Important: replace country list with to match your location
!!These commands are supported from 17.3 and higher
wireless country ES
wireless country US
```

Facultatif - Meilleures pratiques

Cela garantit que le réseau respecte les meilleures pratiques de base :

- Les points d'accès disposent d'informations d'identification SSH, d'informations d'identification non par défaut et de Syslog, pour améliorer l'expérience de dépannage. Ceci utilise le profil de jointure AP par défaut, si vous ajoutez de nouvelles entrées, vous devez leur appliquer des modifications similaires
- Activer la classification des périphériques pour suivre les types de clients connectés au réseau

```
ap profile default-ap-profile
mgmtuser username [AP_ADMIN] password 0 [AP_PASSWORD] secret 0 [AP_SECRET]
ssh
syslog host [AP_SYSLOG]

device classifier
```

Création de WLAN - WPA2-PSK

Remplacez les variables par les paramètres requis. Ce type de WLAN est principalement utilisé pour les réseaux personnels, les scénarios simples ou pour prendre en charge les périphériques IOT sans fonctionnalités 802.1x

Ceci est facultatif pour la plupart des scénarios Enterprise

```
wlan wlan_psk 1 [SSID-PSK]
security wpa psk set-key ascii 0 [WLANPSK]
no security wpa akm dot1x
security wpa akm psk
no shutdown
```

Création de WLAN - WPA2-Enterprise

Scénario le plus courant de WPA2 WLAN avec authentification Radius. Utilisé dans les environnements d'entreprise

```
wlan wlan_dot1x 2 [SSID-DOT1X]
security dot1x authentication-list ISE
no shutdown
```

Création de WLAN - Invité avec authentification Web locale

Utilisé pour un accès invité simplifié, sans assistance d'invité ISE

Selon la version, il est possible d'obtenir un avertissement lors de la création du premier mappage de paramètres, veuillez répondre oui, pour continuer

```
parameter-map type webauth global
yes ! this may not be needed depending on the version
virtual-ip ipv4 192.0.2.1
virtual-ip ipv6 1001::1
```

```
aaa authentication login WEBAUTH local
aaa authorization network default local

wlan wlan_webauth 3 [SSID-WEBAUTH]
peer-blocking drop
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no security ft
no security wpa wpa2
security web-auth
security web-auth authentication-list WEBAUTH
security web-auth parameter-map global
no shu
```

Création de WLAN - Invité avec authentification Web centralisée

Utilisé pour le support des invités ISE

```
aaa authentication network default local
aaa authorization network MACFILTER group ISE_GROUP
aaa accounting identity ISE start-stop group ISE_GROUP

aaa server radius dynamic-author
client [RADIUS_IP] server-key [RADIUS_KEY]

ip access-list extended REDIRECT
10 deny icmp any any
20 deny udp any any eq bootps
30 deny udp any any eq bootpc
40 deny udp any any eq domain
50 deny ip any host [RADIUS_IP]
55 deny ip host [RADIUS_IP] any
60 permit tcp any any eq www

wlan wlan_cwa 5 [SSID-CWA]
mac-filtering MACFILTER
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no security ft
no security wpa wpa2
no shutdown

!! we will create two policy profiles, to be used later depending if the APs are local or flex
mode
wireless profile policy local_vlanclients_cwa
aaa-override
accounting-list ISE
ipv4 dhcp required
nac
vlan [CLIENT_VLAN]
no shutdown

wireless profile policy policy_flex_cwa
no central association !!Ensure to disable central-assoc for flexconnect APs
no central dhcp
no central switching
aaa-override
accounting-list ISE
ipv4 dhcp required
```

```
nac
vlan [CLIENT_VLAN]
no shutdown
```

Création de stratégies pour les points d'accès en mode local

Les points d'accès en mode local sont ceux qui se trouvent sur le même emplacement physique que le contrôleur Catalyst 9800, généralement sur le même réseau.

Maintenant que nous avons le contrôleur avec la configuration de base des périphériques et les différents profils WLAN créés, il est temps de l'assembler avec les profils de stratégie et de les appliquer via des balises aux points d'accès qui doivent diffuser ces SSID

Pour plus d'informations, consultez Comprendre le modèle de configuration des contrôleurs sans fil Catalyst 9800

```
wireless profile policy policy_local_clients
description local_vlan
dhcp-tlv-caching
http-tlv-caching
radius-profiling
session-timeout 86400 !!Ensure to not use 0 since 0 means no pmk cache
idle-timeout 300
vlan [CLIENT_VLAN]
no shutdown

wireless tag site site_tag_local
description local

wireless tag policy policy_tag_local
description "Tag for APs on local mode"
!! Include here only the WLANs types from previous sections, that you have defined and are
interesting for your organization
!! For guest WLANS (CWA/LWA), it is common to use a different policy profile, to map to a
different VLAN
wlan wlan_psk policy policy policy_local_clients
wlan wlan_dot1x policy policy policy_local_clients
wlan wlan_webauth policy policy policy_local_clients
wlan wlan_cwa policy policy_local_clients
```

Création de stratégies pour les points d'accès en mode Flexconnect

Les points d'accès en mode Flexconnect sont généralement utilisés lorsque la connexion entre le contrôleur et les points d'accès est effectuée sur un WAN (il y a donc un délai de transmission supérieur entre eux), ou lorsque, pour des raisons de topologie, nous avons besoin que le trafic client soit commuté localement au port AP, et non pas amené par CAPWAP pour quitter le réseau aux interfaces du contrôleur

La configuration est similaire au mode local, mais marquée comme étant un côté distant, avec un trafic commuté localement

```
wireless profile flex flex_profile_native
acl-policy REDIRECT
central-webauth
```

```
arp-caching
!! Replace 25 with the VLAN native on your AP L2 topology
native-vlan-id 25
vlan-name [VLAN_NAME]
vlan-id [CLIENT_VLAN]

wireless tag site site_tag_flex
flex-profile flex_profile_native
no local-site

wireless profile policy policy_flex_clients
no central association !!Ensure to disable central-assoc for flexconnect APs
no central dhcp
no central switching
dhcp-tlv-caching
http-tlv-caching
idle-timeout 300
session-timeout 86400 !!Ensure to not use 0 since 0 means no pmk cache
vlan [CLIENT_VLAN]
no shutdown

wireless tag policy policy_tag_flex
description "Profile for Flex mode APs"
!! Include here only the WLANs types from previous sections, that you have defined and are
interesting for your organization
!! For guest WLANS (CWA/LWA), it is common to use a different policy profile, to map to a
different VLAN
wlan wlan_psk policy policy_flex_clients
wlan wlan_dot1x policy policy_flex_clients
wlan wlan_webauth policy policy_flex_clients
wlan wlan_cwa policy policy_flex_cwa
```

Final - Appliquer des balises aux points d'accès

En dernière étape, nous devons appliquer les balises que nous avons définies à chaque point d'accès. Vous devez remplacer l'adresse MAC Ethernet de chaque point d'accès par celle présente sur votre périphérique

```
!!Tag assigment using static method. Replace mac with your device
ap F4DB.E683.74C0
policy-tag policy_tag_local
site-tag site_tag_local
```

Comment obtenir la liste des adresses MAC AP

Vous pouvez obtenir une liste des AP actuellement joints à l'aide de la commande show ap summary

```
Gladius1#sh ap summ
Number of APs: 1

AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address State
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------
9130E-r3-sw2-g1012 3 9130AXE 0c75.bdb6.28c0 0c75.bdb5.7e80 Test123 ES 192.168.25.139 Registered
```

Lecture recommandée

- Meilleures pratiques de configuration de la gamme Cisco Catalyst 9800
- Versions recommandées de Cisco IOS XE pour les contrôleurs LAN sans fil Catalyst 9800
- Outils de dépannage sans fil