[Date]

Cisco Catalyst 9800-CL Wireless Controller for Cloud

Migration Contrôleur WiFi Cisco WLC AirOS

Mamadou CAMARA BTS SIO, SISR

SOMMAIRE :

1. CONTEXTE	3
2. OBJECTIF	3
3. FONCTIONNEMENT DU CISCO WLC (CAPWAP)	3
4. L'ARCHITECTURE	4
5. PRE-INSTALLATION	5
6. DEPLOIEMENT ET CONFIGURATION DU CONTROLEUR VIRTUEL SANS FIL CISCO CATA	<u>ALYST 9800 CL 7</u>
A. À PARTIR DU CLIENT VSPHERE, DEPLOYEZ LE MODELE OVA 9800-CL.	7
ETAPE 1 : DEPLOIEMENT DU CONTROLEUR CISCO CATALYST 9800 SUR L'HYPERVISEUR VMWARE	7
ETAPE 2 : CONFIGURATION DU CONTROLEUR CISCO CATALYST 9800 DEPUIS L'INTERFACE GRAPHIQUE HT	TPS:// <ip-< td=""></ip-<>
CONTROLEUR>	13
A. CONFIGURATION DU CONTROLEUR	16
CREATION DE VLANS	17
SERVEUR RADIUS :	19
WLANs (SSID)	21
ATTRIBUTION DE BALISE DE STRATEGIE	31
PARAMETRES DE JONCTION AP (AP JOIN PROFILE) SUR LES WLC 9800	31
B. MIGRATION DES APS (AIR-AP1832I-E-K9) VERS CISCO CATALYST 9800 CL	35
B.1 PROBLEME RENCONTRE : IMPOSSIBLE DE DEPLACER LES APS DU CONTROLEUR AIREOS VERS LE NOUV	EAU CONTROLEUR
CATALYST 9800-CL	35
B.2 SOLUTIONS :	35
1 ^{MC} OPTION : REINITIALISER LES APS	35
2 ^{cm} OPTION : POUR UNE MIGRATION MASSIVE	37
<u>7.</u> <u>TEST</u>	38
8. CONFIGURATION FINALE :	39
9. SUPERVISION (ZABBIX & NAGIOS)	39
A. AGENT SNMP (CONTROLEUR CATALYST 9800 CL)	39
CONFIGURATION DE L'AGENT SNMP SUR LE CONTROLEUR CISCO CATALYST 9800 CL	39
B. ZABBIX	42
ETAPE 1 : INTEGRATION DU CONTROLEUR CATALYST SUR ZABBIX	42

Etape 2 : creer une carte dans Zabbix afin de visualiser l'etat des points d'acces (APs)	43
ETAPE 2 : CONFIGURATION D'UNE CARTE POUR LES APS	44

1. CONTEXTE

Le Contrôleur Cisco WLC AireOS Cisco Virtual Wireless Controller n'est plus compatible avec certaines AP (Point d'accès). La DSI du CH Esquirol veut migrer vers une nouvelle version Cisco Catalyst 9800-CL Wireless Controller for Cloud.

2. OBJECTIF

Mise en place d'un contrôleur virtuel WLC Cisco Catalyst Wireless Controleur 9800.

Cette solution devra s'adapter au portail captif déjà en place (Utopia) et à une authentification 802.1X NPS Windows Server 2012 (Radius).

3. FONCTIONNEMENT DU CISCO WLC (CAPWAP)

La méthode de communication entre les AP et le contrôleur WLC.

Les bornes Wi-Fi et le contrôleur WLC (Wireless LAN Controleur) communiquent généralement via un protocole appelé **CAPWAP (**Control and Provisioning of Wireless Access Points).

Fonctionnement entre les bornes Wi-Fi et le contrôleur WLC via CAPWAP :

Lors du démarrage, l'AP contacte le serveur DHCP qui à son tour envoie une configuration IP complète avec notamment l'adresse du Contrôleur WLC en **option 43** (adresse en hexadécimale sous forme de **hex f1.04.[adresse IP du Contrôleur en hexa]**.

- Association initiale : Lorsque l'AP démarre, il effectue une découverte du contrôleur WLC sur le réseau. Une fois le contrôleur identifié, l'AP établit une association initiale avec le contrôleur pour établir une connexion de découverte.
- Tunnel CAPWAP : Une fois l'association établie, l'AP établie un tunnel CAPWAP avec le contrôleur WLC servant un transport des données de contrôle, les informations de configuration et les commandes de gestion entre l'AP et le contrôleur.
- Echange de données de contrôle : Une fois le tunnel CAPWAP établi, l'AP envoie périodiquement des informations de surveillance.
- **Configuration et mise à jour** : Le contrôleur WLC envoie les paramètres de configuration à l'AP via le tunnel CAPWAP, tels que les paramètres sécurités, les SSID, les VLANS etc...
- Gestion du trafic : Le contrôleur est responsable de la gestion et du contrôle du trafic des AP.

Port de communication : UDP (5246 pour le contrôle de communication et 5247 pour les échanges de données)



4. L'ARCHITECTURE

L'architecture est basée sur un vlan par SSID avec :

- Le réseau WiFi_PATIENT avec uniquement en niveau 2 jusqu'au portail captif Ucopia,

- Le réseau WiFi_PRO avec une authentification 802.1x, l'authentification est assurée par un serveur 802.1X NPS Windows Server 2012 (Serveur Radius).

- Le réseau WiFi PHARMATIE avec une authentification WiFi WPA 2 PSK + Filtrage et adresse mac



5. Pré-installation

1. Etape 1

Prise de connaissance de la documentation technique de l'ancien Contrôleur Cisco WLC AirOS

- 2. Prise de connaissance de la configuration de l'ancien contrôleur Cisco **WLC AirOs** depuis l'interface graphique.
- Sauvegarde de la configuration
- Exportation de la configuration

ululu cisco	MONITOR WLANS CONTROLL	er w <u>i</u> reless <u>s</u> ecurit	MANAGEMENT	C <u>O</u> MMANDS	HELP			Sa <u>v</u> e Configuration <u>F</u> User:mcamara
Monitor	Summary							
Summary Access Points Cisco CleanAir Statistics	Controller Summary	313 Cisco Virtual ۱	Access Points Suppo	rted Ier		Rogue Summary		
 CDP Rogues Clients 	Management IP Address Service Port IP Address Software Version Emergency Image Version					Active Rogue APs Active Rogue Clients Adhoc Rogues Rogues on Wired Network	180 32 0	<u>Detail</u> Detail Detail
Sleeping Clients Multicast Applications Local Profiling	System Name Up Time System Time Redundancy Mode					Session Timeout	0	
Cloud Services	802.11a Network State 802.11b/g Network State Local Mobility Group					Top WLANs Profile Name WiFi PRO	# of Clients	s Detail
	CPU(s) Usage Individual CPU Usage Memory Usage vWLC Config					WIFLPATIENT PHARMACIE BIOMEDICAL	82 7 1	Detail Detail Detail
	Access Point Summary					Most Recent Traps SNMP Authentication Failure: IP Addre		
	802.11a/n/ac/ax Radios 802.11b/g/n/ax Radios Dual-Band Radios Dual-SG Radios			Detai Detai Detai Detai	1 1 1	SNMP Authentication Failure: IP Addre SNMP Authentication Failure: IP Addre SNMP Authentication Failure: IP Addre SNMP Authentication Failure: IP Addre		
	All APs Client Summary			Detai	1	View All Top Flex Applications Application Name Packet Count Byte Cou	nt	
	Current Clients Excluded Clients Disabled Clients	190 10 0		<u>Detail</u> Detail Detail		View All This page refreshes every 30 seconds.		

- Conversion de la configuration de Cisco WLC en Catalyst 9800-CL via le site Cisco TAC Tool Config Converter : https://cway.cisco.com/wlc-config-converter/

		1. Constructions Frontier
b IAC lool - WLC Contig Converter		Informatique Esquiro
Minration de contrôleure cans filuere ou denuie l'une des plates formes suivantes : contrôleure 2500/5500/7500/8500/MISM2/3650//29	50/4500 S9E/5760/Catalvet 9	800
Migration de controleurs sans in vers ou depuis rune des places-ronnes suivances , controleurs 2500/5500/7500/8500/wiswi2/5000/565	50/4500 362/5700/Catalyst 9	800
Veuillez telecharger ce qui suit : AireOS : sortie « show run-config startup-commands » ou sauvegarde de la configuration TFTP		
Accès convergé : sortie « show running-config »		
Détails		`
Sauvegarde de la configuration TFTP ou sortie 'show run-config startup-commands' d'AireOS WLC.		
/		
ث.		
Cirquez ici où deposez le richier pour le telecharger		
l late-forme AireOS>Catalvst 9800		(2)
Courir		
Courir	🕁 Télécharge	r CSV 👌 Télécharger CFG tra
Courtr	순 Télécharge	rr CSV 🕁 Télécharger CFG tra
Courte Lignes de configuration converties	ڻ, Télécharge	r CSV 👌 Télécharger CFG tra
Courie Lignes de configuration converties Configuration traduite	는 Télécharge	ir CSV టి, Télécharger CFG tra
Courir Lignes de configuration converties Configuration traduite Configuration non prise en charge	는 Télécharge	r CSV 👌 Télécharger CFG tra

3. Etape 3

Téléchargement de l'image en format OVA du nouveau contrôleur Wi-Fi **Catalyst 9800-CL Wireless Controller for Cloud** depuis le site **Cisco** 4. Etape 4

Vérification de la compatibilité entre la nouvelle version et l'ancienne :

6. Déploiement et configuration du contrôleur Virtuel sans fil Cisco Catalyst 9800 CL

a. À partir du client vSphere, déployez le modèle OVA 9800-CL.

Etape 1 : Déploiement du contrôleur Cisco Catalyst 9800 sur l'hyperviseur VMware

Déployer un modèle OVF	Sélectionner un nom et un dossier X
1 Sélectionner un modèle OVF	Nom de la machine virtuelle : CTRLWIFI
2 Sélectionner un nom et un dossier	Sélectionnez un emplacement pour la machine virtuelle.
Sélectionner une ressource de calcul	 Esquirol CAM
4 Vérifier les informations	 Discovered virtual machine FORMATION
5 Sélectionner un stockage	 CITRIX ORACLE
6 Prêt à terminer	 Machine virtuelle détectée Templates VM_ETEINTES_avant_suppression
	ANNULER PRÉCÉDENT SUIVANT

Déployer un modèle OVA/OVF depuis l'hyperviseur VMware (Client vSphere)

• On sélectionne ensuite une ressource de calcul dans /Esquirol/Production/



Déployer un modèle OVF



Vérifier les informations

Vérifiez les détails du modèle.

Éditeur	Aucun certificat présent
Produit	Cisco C9800-CL Wireless Lan Controller
Version	17.12.04
Fournisseur	Cisco Systems, Inc.
Taille du téléchargement	1,2 Go
Taille sur le disque	1,5 Go (provisionnement dynamique) 17,2 Go (à provisionnement statique)

ANNULER PRÉCÉDENT

T SUIVANT

Х

• Le profil du contrôleur choisi étant « **Small** » (Le nombre des APs ne dépasse pas 1000), on choisit 1k APs, 10k Clients pour la configuration de déploiement.

Déployer un modèle OVF	Configuration	×
1	Sélectionner une configuration de déploiement	
1 Sélectionner un modèle OVF	O 100 APs, 1K Clients	Description
2 Sélectionner un nom et un dossier	⑧ 1K APs, 10K Clients	Disk
Sélectionner une ressource de	() 1K APs, 10K Clients, High Throughput	
3 calcul) 3K APs, 32K Clients	
4 Vérifier les informations) 3K APs, 32K Clients, High Throughput	
E. Configuration	O 6K APs, 64K Clients	
) 6K APs, 64K Clients, High Throughput	
6 Sélectionner un stockage		
7 Sélectionner les réseaux		
8 Personnaliser un modèle		
9 Prêt à terminer	A	NNULER PRÉCÉDENT SUIVANT

Ensuite créez un mot de passe pour le mode privilégié (Enable password) afin de sécuriser la configuration du contrôleur via le consol.

Déployer un modèle OVF

1 Sélectionner un modèle OVF

Sélectionner un nom et un 2 dossier

Sélectionner une ressource de 3 calcul

- 4 Vérifier les informations
- 5 Configuration
- 6 Sélectionner un stockage
- 7 Sélectionner les réseaux
- 8 Personnaliser un modèle
- Déployer un modèle OVF 1 Sélectionner un modèle OVF Sélectionner un nom et un 2
 - Sélectionner une ressource de 3 calcul
 - 4 Vérifier les informations
 - 5 Configuration

dossier

- 6 Sélectionner un stockage
- 8 Personnaliser un modèle

Personnaliser un modèle

✓ 1. Basic Management Setup	2 paramètres	
1.1 Hostname	Hostname of this wire CTRLWIFI	eless lan controller
1.2 Enable Password	Password for privileg WARNING: While this the plain-text passwo file.	ed (enable) access. s password will be stored securely within IOS, ord will be recoverable from the OVF descriptor
	Mot de passe	······ ©
	Confirmer le mot de passe	©
		ANNULER PRÉCÉDENT SUIVANT

Sélectionner un stockage Х Compatibilité Nom Capacité Provisionné 🝸 Libre Ŧ Ŧ T Y de stockage 0 FOR_UNITY_VW_PROD-2 1,08 To 4 To 2,97 To ---FOR_UNITY_VW_PROD-3 4 To 2,64 To 1,43 To Gérer Les Colonnes Éléments par page 10 \vee 7 élément(s) Compatibilité ✓ Contrôles de compatibilité effectués avec succès.

PRÉCÉDENT ANNULER

SUIVANT

Х

À partir de la liste déroulante de mappage du réseau, attribuez 3 cartes d'interface réseau virtuelle (vNIC) au réseau de destination. Connectez chaque carte à une interface unique.

- **GigabitEthernet 1** à l'interface de gestion des dispositifs et mappée sur le réseau de gestion hors bande (INFRASTRUCTURE).
- **GigabitEthernet 2** à l'interface de gestion sans fil et mappée sur le réseau permettant d'atteindre les points d'accès (AP) et les services. Habituellement, il s'agit d'un **Trunk** pour transporter plusieurs VLAN (WIFI_INFRA).
- **GigabitEthernet 3** à l'interface de haute disponibilité et mappée sur un réseau séparé pour la communication peer-to-peer pour le SSO (Ici, on mappe sur l'interface pour le teste, la haute disponibilité n'étant pas envisagée).

Déployer un modèle OVF	Sélectionner les réseaux Sélectionnez un réseau de destination pour cha	aque réseau source.
1 Sélectionner un modèle OVF	Réseau source	Réseau de destination
Sélectionner un nom et un	GigabitEthernet1	INFRASTRUCTURE V
2 dossier	GigabitEthernet2	WIFL_INFRA v
Sélectionner une ressource de 3 calcul	GigabitEthernet3	TEST v
4 Vérifier les informations	Gérer Les Colonnes	3 élément(s)
E. Castinumtian	Paramètres d'allocation d'IP	
5 Configuration	Allocation d'IP :	Statique - Manuel
6 Sélectionner un stockage	Protocole IP :	IPv4
7 Sélectionner les réseaux		
8 Personnaliser un modèle		ANNULER PRÉCÉDENT SUIVANT

• On indique ensuite l'adresse de l'interface de gestion (pour accéder à l'interface graphique du contrôleur via https://<ip-adresse-contrôleur>)

Déployer un modèle	Personnaliser un modèle	Х
OVF	2.1 Device Management/Service Interface	Management interface (such as "GigabitEthernet1") GigabitEthernet1
1 Sélectionner un modèle OVF	2.2 Device Management/Service Interface	IPv4 address and mask for management interface (such as
2 Sélectionner un nom et un dossier	IPv4 Address/Netmask	"192.0.2.100/24" or "192.0.2.100 255.255.255.0"), or "dhcp" to configure via DHCP
Sélectionner une ressource de 3 calcul	2.3 Device Management/Service Interface	IPv4 gateway address (such as "192.0.2.1") for management
4 Vérifier les informations	IPv4 Gateway	interface, or "dhcp" to configure via DHCP
5 Configuration	2.4 Remote Device Management/Service	This will add a route to the remote network where you want to
6 Sélectionner un stockage	Network Route/Netmask	manage your device from (Hint: To add the default route enter 0.0.0.0) 0.0.0.0
7 Sélectionner les réseaux		
8 Personnaliser un modèle		ANNULER PRÉCÉDENT SUIVANT

• On Crée un utilisateur admin pour accéder à l'interface graphique du contrôleur WiFi.

_

Déployer un modèle	Personnaliser un modèle			
JVF	✓ 3. User login Configuration	4 paramètres		
1 Sélectionner un modèle OVF	3.1 Login Username	Username for remote admin	login	
2 dossier	3.2 Login Password	Password for remote	login.	securely within IOS
3 Sélectionner une ressource de calcul		the plain-text passwo	rd will be recoverable fro	om the OVF descriptor
4 Vérifier les informations		Mot de passe	•••••	0
5 Configuration				
6 Sélectionner un stockage		Confirmer le mot de passe	•••••	<u></u>
7 Sélectionner les réseaux				
8 Personnaliser un modèle			ANNULER PRÉC	CÉDENT



Etape 2 : Configuration du contrôleur Cisco Catalyst 9800 depuis l'interface graphique https://<ip-controleur>

Indiquer le nom du contrôleur, le pays (FR), et l'adresse IP du serveur NTP pour synchroniser l'heure.

1. General Settings		
Deployment Mode	Standalone	T
Host Name*	CTRLWIFI	
Country	US	•
Date	15 Jan 2025	t) I
Time / Timezone	11:36:12 (D heure •
NTP Servers	Enter NTP Server	€
	Added NTP servers	

• On complétera l'adresse du serveur radius ultérieurement

1. General Settings			
AAA Servers	Enter Radius Server IP Enter Key Added AAA servers	ø 🗘	
Wireless Management Settings		Static Route Settings	
Port Number Wireless Management VLAN*	GigabitEthernet2 v	Click here to view currently configured routes	
IPv4 Wireless Management IP*		IPv6 Route	
Subnet Mask*			
IPv6			
			Next

• On complètera cette partie ultérieurement. Cliquer sur Next

2. Wireless Network Settings		
+ Add X Delete		
Network Name	Network Type	Security
id d ▶ ⊨ 10 v		No items to display
		Previous Next

• Ensuite, indiquer le **groupe RF** (Radio Frequency Group) pour la gestion des paramètres RF, le **type du trafic** (Data). Laisser l'adresse IP virtuelle du contrôleur par défaut (192.0.2.1).

. Advanced Settings				
Client Density	•	•	(•	
RF Group Name*	RF-CETRA	Typical	High	
Traffic Type	Data 💌			
/irtual IP Address	192.0.2.1			
AP Certificate				
Generate Certificate	YES			
RSA Key-Size	4096			
ignature Algorithm	sha256 🔻			
Password*	•••••••••			
Create New AP Management User				
New AP Management User*				
				Previc

Etape 3 : déploiement de la configuration de l'ancien contrôleur Cisco WLC AireOS

On déploie la configuration depuis **Configuration>Services.**

Ce service permet de transformer la configuration du contrôleur Cisco WLC **AireOS** (ancien contrôleur) en une configuration adapter au contrôleur **Cisco Catalyst 9800-CL**.

Cisco	Cisco Cat	talyst 9800-CL V	/ireless Controller		Welcome mcamara	*	A	1 0 C	Search APs and Clients Q	Feedback
Q Search Menu	Items	Configuration *	Services > AireC	DS Config Translator						
📻 Dashboard		1 Select and	Upload the AireOS Co	onfig file (i)						
() Monitoring										
🔏 Configurat										
(O) Administra	tion >									
C Licensing										
💥 Troublesho	ooting									
Walk Me Thro	ugh >									

Une fois le fichier de configuration importé, on ajuste la configuration :

- Adresse IP des interfaces à modifier notamment pour celles de management,
- On indique les mots de passe des utilisateurs crées sur l'ancien contrôleur puisque les mots de passe contenant dans le fichier de configuration de Cisco AireOS ne peuvent pas être importés.
- Les clés du serveur Radius ...



- Problèmes rencontrés : impossible de déployer la configuration de l'ancien contrôleur Cisco WLC AirOS. Problème d'incompatibilité au niveau de certains éléments notamment les balises entre les deux systèmes.
- **Solutions** : Configuration parallèle à l'ancien contrôleur (SVI, VLAN, WLAN, SSID, Policy & Tag, Flex Groupe, Groupe WLAN...)
 - a. Configuration du Contrôleur
- Création des SVI pour les VLANs 3, 5, 24, 87 et 89

Cisco	Cisco Cata	alyst 980	00-CL V	Wireless C	Control	ler		Welcom	ne <i>mcam</i>	ara 🕋 🐔	•	8 ¢	1	0	Search	APs and C	Clients C	2	Feedback	e (*
Q. Search Menu Item	ns	Configu	ration * >	Layer2 • >	VLAN															
Dashboard		SVI	VLAN	VLAN Grou	p															
	,	+	Add	× Delete	_		_	-	_		_					_				-
			Name		•	Admin Status	Υ.	Operational Status	Υ.	IPv4 Address	Ť	IPv6 Add	lress			T	Descriptio	n		T
			Vlan1			0		0		unassigned		Unassign	əd							
	۰ ۱		Vlan3			•		o				Unassign	ed			v	vifi_patien	t		
			Vlan5			0		0				Unassigne	ed			b	iomedical			
C Licensing			Vlan24			o		0				Unassign	ed			v	vifi_pro			
💥 Troubleshootin	ng		Vlan87			0		o				Unassigne	ed							
			< 1	> > 1	0 🗸														1 - 5 of 5	items

Le contrôleur a une interface dans chaque vlan (89, 87, 3, 5 et 24), de façon à pouvoir orienter le trafic (PRO/Patient) en fonction du SSID :

Description	wifi_pro	(1-200 Characters)
Admin Status		
VRF	None 🔻	
MTU (bytes)	1500	
IP Options	✓ IPV4 IPV6	
	IPv4 Type	Static 🔻
	IP Address *	
	Subnet Mask *	255.255.0.0
	Secondary IP	

• Création de VLANs On crée un VLAN pour chaque SVI

Configuration - Lay	er2 · > VLAN							
SVI VLAN VLA	AN Group							
+ Add × De	elete							
VLAN ID	T	Name	T	Status	T	Ports		T
1		default		active		Gi3		
3		wifi_patient		active				
5		biomedical		active				
24		wifi_pro		active				
87		VLAN0087		active				
⊨ ⊲ 1 ⊨ ⊨	10 🔻						1 - 5 of 5 item	IS

Déclarer les VLAN clients :

Avant de commencer la configuration, vous devez ajouter les VLAN nécessaires (VLAN auxquels les clients sans fil sont affectés).

Étape 1. Accédez à **Configuration > Layer2 > VLAN > VLAN > + Add**.

Étape 2. Saisissez le	s informations	requises.
-----------------------	----------------	-----------

Edit VLAN: wifi_pro			×
VLAN ID*	24		
Name	wifi_pro	i	
State	ACTIVATED		
IGMP Snooping	DISABLED		
ARP Broadcast	DISABLED		
Port Members		Q Search	
	Available (1)	Associated (0)	
	Gi3 >		
		No Associated Members	

Répétez les étapes 1 et 2 pour tous les VLAN nécessaires. Une fois terminé, vous pouvez passer à l'étape 3.

Étape 3. Vérifiez que les VLAN sont autorisés dans vos interfaces de données.

Accédez à **Configuration > Interface > Ethernet > Nom d'interface > General**. Si vous le voyez configuré comme Allowed Vlan = All, vous avez terminé la configuration. Si vous voyez les ID VLAN autorisés = VLAN, ajoutez les VLAN nécessaires et ensuite cliquez sur **Update & Apply to Device**. Aucune modification requise :

General Advanced	Ichemelz	
Interface	GigabitEthernet2	
Description	(1-200 Characters)	
Admin Status		
Enable Layer 3 Address	DISABLED	
Switchport Mode	trunk 🔻	
Allowed VLAN	O All O VLAN IDs	
VLAN IDs	3,5,24,87 (e.g. 1,2,4,6-10)	
Native VLAN	1	

• Serveur Radius :

Pour l'installation des WLC Catalyst 9800, vous pouvez utiliser les assistants de configuration disponibles pour vous guider tout au long du processus de configuration.

Si vous devez utiliser des serveurs RADIUS sur votre déploiement, vous pouvez d'abord utiliser l'Assistant AAA, puis choisir entre la configuration sans fil de base ou avancée.

Si vous n'utilisez pas de serveurs RADIUS sur votre déploiement, vous pouvez accéder directement à la configuration sans fil de base ou avancée.

Assistant AAA

Étape 1. Accédez à Configuration > Security > AAA > + AAA Wizard.

Q Search Menu Items	Authentication Authorizatio	n and Accounting
	AAA Method List	Servers / Groups AAA Ac
(Monitoring >		
Configuration	General	Dot1x System Auth Control
() Administration	Authentication	Local Authentication
💥 Troubleshooting	Authorization	Local Authorization
	Accounting	Radius Server Load Balance
		Show Advanced Settings >>>

Étape 2 : Activez le type de serveurs requis et entrez un nom de serveur (il peut s'agir de l'adresse IP ou de toute autre chaîne), l'adresse IP du serveur et le secret partagé. Après cela, cliquez sur **Next**.

Add Wizard				3
				Basic O Advanced
	0			
	SERVER		SERVER GROUP ASSOCIATION	MAP AAA
RADIUS 🗹	TACACS+	LDAP		
RADIUS				
Name*	server-name			
Server Address*				
Shared Secret*	-			
Confirm Shared Secret*				

Étape 3. Entrez les informations nécessaires à la création d'un groupe de serveurs. Assurez-vous d'ajouter le serveur spécifié à l'étape précédente aux **serveurs affectés**.

Edit AAA Radius Server	Group
Name*	Server_Radius
Group Type	RADIUS
MAC-Delimiter	none 🔻
MAC-Filtering	none 🔻
Dead-Time (mins)	5
e Load Balance	DISABLED
Source Interface VLAN ID	1 🔹 🔽
Available Servers	Assigned Servers
Server_Radius_2	Radius_Server
	<
	»
	«
	«

Étape 4 : Activez l'authentification et créez une méthode d'authentification.

Accédez à l'onglet **Authentification** et saisissez les informations nécessaires. Une fois terminé, cliquez sur **Save & Apply to Device**

Quick Setup: AAA Authentication									
Method List Name*	authList_WiFi_PRO	0_2							
Туре*	dot1x	• (i)							
Group Type	group	v (i)							
Fallback to local									
Available Server Groups		Assigned Server Groups							
ldap tacacs+	> Se rau > (erver_Radius							

• WLANs (SSID)

WLAN sur les WLC 9800

Flux de configuration :

1. Création des SSID

Créez votre SSID

Étape 1. Accédez à Configuration > Wireless > WLANs > + Add.

Cisco Cata	alyst 9800-C	Welcome m	ncamara 🛛 🕋 🕏	A 🖪								
Q Search Menu Items Configuration > Tags & Profiles > WLANS												
Dashboard	+ Add	× Delete	Enable WLAN	Disable WLAN								
Monitoring >	Selected WLAN	s:0										
	Status Y	Name	▼ ID	Ŧ	SSID							
		WiFi_PATIENT	2		WiFi_PATIENT							
Administration	•	WiFi_PRO	۶ (WiFi_PRO							
A Licensing	•	biomedical	% 4		biomedical							
	•	PHARMACIE	\$ 5		PHARMACIE							
X Troubleshooting		▶ ► 10 -										

 Création de WLAN pour WiFi_PRO
 Le SSID WiFi_PRO est configuré avec une authentification 802.1X alors que WiFi_PATIENT n'a pas de sécurité pour pouvoir se connecter, c'est le portail captif ucopia qui remplit ce rôle.

Dans l'onglet *General,* Entrez toutes les informations nécessaires (nom SSID, type de sécurité, etc.) et une fois terminé, cliquez sur **Save & Apply to Device**.

Edit WLAN			×
A Changing	g WLAN parameters while it is enabled	d will result in loss of connectivity for clients connected to it.	
General Security	Advanced Add To Policy T	lags	
Profile Name*	WiFi_PRO	Radio Policy (i)	
SSID*	WiFi_PRO	Show slot configuration	
WLAN ID*	3	Status DISABLED	
Status	ENABLED	5 GHz	
Broadcast SSID	ENABLED		
		2.4 GHz Status ENABLED	
		802.11b/ 802.11b/g 🔻	

Dans l'onglet Security, on précise le type d'authentification.

Ce SSID est affecté à l'interface wifi_pro correspondant au vlan 24. L'authentification utilisé est le 802.1x.

Par mesure de sécurité la diffusion du SSID est caché.

Edit WLAN		×
A Changing WLAN parameters while it is enabled will r	esult in loss of connectivity for clier	nts connected to it.
General Security Advanced Add To Policy Tags		
Layer2 Layer3 AAA		
WPA + WPA2 O WPA2 + WPA3 O W	O Static WEP	O None
MAC Filtering		
Lobby Admin Access		
WPA Parameters	Fast Transition	
WPA Policy 🗌 WPA2 Policy 🔽	Status	Disabled 🔻
GTK OSEN Policy Randomize	Over the DS	
WPA2 Encryption	Reassociation Timeout *	20
AES(CCMP128)		
GCMP128 GCMP256	Auth Key Mgmt	
Protected Management Frame	802.1X	PSK
	Easy-PSK	
PMF Disabled v	802.1X-	PSK-SHA256
	SHA256	
	MPSK Configuration -	'
	Enable MPSK	
Cancel	[Update & Apply to Device

Ensuite, on précise la méthode d'authentification dans la liste déroulante de Authentification list

Edit WLAN		
	A Changir	ng WLAN parameters while it is enabled will result in loss of connectiv
General	Security	Advanced Add To Policy Tags
Layer2	Layer3	
Authentica	ation List	
Local EAP	Authenticati	on 🗌

On précise le policy Tags (Stratégie de police) qui permet de gérer finement le comportement, l'accès des utilisateurs et des dispositifs sur le réseau sans fil.

Edit WLAN	×
A Changing WLAN parameters while it is enabled will result in loss o	f connectivity for clients connected to it.
General Security Advanced Add To Policy Tags	
Policy Tag	Policy Tag New-policy-tag 🗸 Z
New-policy-tag wifi-pro-policy-profil ⋈ ▲ ▲ ▲ 10 - 1 of 1 items	Policy Profile wifi-pro-policy-pr
	✓ Save

- Création de WLAN PHARMACIE avec filtrage des adresses MAC

Le réseau **wifi Pharmacie** est spécifique et diffusé que dans le bâtiment pharmacie. L'authentification se fait avec une clé **WPA** et déclaration des adresses **MAC** sur le contrôleur wifi.

Etape 1 : Accéder dans Configuration>Policy&Tags>WLANs , puis click sur +Ajouter On saisit les information nécessaire (SSID, le nom du profil ..)

Edit WLAN			×
A Changin	g WLAN parameters while it is e	enabled will result in loss of connectivity for clients connected to it.	
General Security	Advanced Add To Pe	olicy Tags	
Profile Name*	PHARMACIE	Radio Policy (i)	
SSID*	PHARMACIE	Show slot configuration	
WLAN ID*	5	Status DISABLED	
Status	ENABLED	5 GHz	
Broadcast SSID	ENABLED		
		Status ENABLED	
		802.11b/ 802.11b/g 🔻	

Dans l'onglet **Security**, activez **MAC Filtering**. Dans la liste déroulante de **Authorization List**, sélectionnez la méthode d'autorisation **Mac-Filter** qui sera créée à l'étape suivante (étape 2), ensuite Cliquez sur **Save & Apply to Device.**

Edit WLAN	×
General Security Advanced Add To Policy Tags	
• WPA + WPA2 • WPA2 + WPA3 • WPA3	PA3 O Static WEP O None
MAC Filtering Authorization Li	st* Mac-Filter v
WPA Parameters WPA Policy GTK Randomize OSEN Policy	Fast Transition Status Over the DS
WPA2 Encryption AES(CCMP128) GCMP128 GCMP256	Reassociation Timeout * 20 Auth Key Mgmt
PMF Disabled	802.1X PSK Easy-PSK CCKM A FT + 802.1X FT + PSK 802.1X- PSK-SHA256 SHA256
	PSK Format ASCII PSK Type Unencrypted Pre-Shared Key* ••••••••••••••••••••••••••••••••••••
Cancel	Update & Apply to Device

Au final, 4 SSID sont crées

Cisco Cat	alyst 9	9800-Cl	Wireless C	ontroller		Welcon	ne <i>m</i> a	amara 🖌 🎢	\$ 0	A 🖪	¢	1	0 0	Search APs	and Clients	Q	Feed	back 🖌	•
Q, Search Menu Items Configuration -> Tags & Profiles -> WLANs																			
Dashboard	+	Add	× Delete	Clone Enab	le WLAN	Disable WLAN											V	WLAN Wiza	ird
Monitoring >	Sele	cted WLAN	s : 0																
Configuration		Status Y	Name	T	ID		T	SSID			Y 2	.4/5 G	Hz Secur	ity	T	6 GHz Secur	ity		\mathbf{T}
		ο	WiFi_PATIENT	•	2			WIFI_PATIENT			[0	pen]							
() Administration		O	WiFi_PRO	•	3			WiFi_PRO			[V	VPA2][302.1x][A	ES]					
C Licensing		O	biomedical	•	4			biomedical-2			[V	VPA2][302.1x][A	ES]					
		ο	PHARMACIE	•	5			PHARMACIE			[V	VPA2][I	PSK [[AES]	,MAC Filtering					
X Troubleshooting	н	← 1	▶ ▶ 10	•													1	- 4 of 4 iter	ms

Etape 2 : Créez une méthode de réseau d'autorisation (Filtrage Mac).

Naviguez jusqu'à Configuration > Security > AAA > AAA Method List > Authorization > + Add et créez-le.

Configuration • >	Security • >	AAA												
+ AAA Wizard														
Servers / Groups	AAA Methoo	d List	AAA Advanced											
Authentication		_	_											
Authorization		+	Add × Delete											
Accounting			Name	Туре	T	Group Type	r (Group1	T	Group2	•	Group3	Group4	•
			default	network		local	S	Server_Radius		N/A	Ν	N/A	N/A	
			authList_WiFi_PATIE	network		local	n	radius		N/A	N	N/A	N/A	
			Mac-Filter	network		local	N	N/A		N/A	N	N/A	N/A	
		м	< 1 ▷ ▷	10 🔻									1 - 3 of 3 ite	ems

Indiquer le nom de la méthode (Mac-Filter), le type (network) et le groupe en local.

Quick Setup: AAA Authoriza	tion	×
Method List Name*	Mac-Filter	
Type*	network T	
Group Type	local v (i	
Authenticated		
Available Server Groups	Assigned Server Groups	
radius Idap tacacs+ Server_Radius	 > ><	

Ensuite on crée une attribue dans laquelle on indique le SSID qui nous concerne (**PHARMACIE**). Accéder à **Configuration > Security > AAA >Attribute Liste Name> + Add**

Configuration • > Security • >	AAA
+ AAA Wizard	
Servers / Groups AAA Metho	od List AAA Advanced
Global Config	+ Add × Delete
RADIUS Fallback	Attribute List Name
Attribute List Name	ATTR_LIST_PHARMACIE
Device Authentication	Attr-Mac-PHAR
AP Policy	⊌ ◀ 1 ▷ ▷ 10 ▼
Password Policy	
AAA Interface	
Configuration * > Security * > AAA Edit Attribute	List
+ AAA Wizard	Ime ATTR_LIST_PHARMACI
Servers / Groups AAA Method List AAA Advanced Attribute Ty	ype Y Attribute Value Y
Global Config + Add × Delete SSID	PHARMACIE
RADIUS Fallback H 4 1	Attribute Type* SSID V
Attribute List Name ATTR_LIST_PHARK	Attribute Value* PHARMACIE
Device Authentication Attr-Mac-PHAR	
AP Policy	
Password Policy	
AAA Interface	

Enregistrez les adresses MAC autorisées.

Enregistrez localement les adresses MAC sur le WLC pour l'authentification locale.

Accédez à **Configuration > Security > AAA > AAA Advanced > Device Authentication >** + Add

Configuration • > Security • >	AAA				
+ AAA Wizard					
Servers / Groups AAA Meth	od List AAA Advanced				
Global Config	MAC Address Serial Number				
RADIUS Fallback		Ph. Colored Fi			
Attribute List Name					-
Device Authentication		ATTR_LIST_PHARMACIE	Portable Pharmacie	PHARMACIE	Ţ
AP Policy		ATTR_LIST_PHARMACIE		PHARMACIE	
Password Policy		ATTR_LIST_PHARMACIE		PHARMACIE	
,		ATTR_LIST_PHARMACIE		PHARMACIE	
AAA Interface		ATTR LIST PHARMACIE		PHARMACIE	

Indiquer l'adresse MAC de la carte Wi-Fi des appareilles que l'on veut autoriser. Dans la liste déroulante de *Attribute List Name*, choisie celle crée précédemment (ATTR_LIST_PHARMACIE) et indiquer le WLAN auquel on veut appliquer la méthode (PHARMACIE).

Edit MAC Filtering		×
MAC Address*		
Attribute List Name	ATTR_LIST_PHAR	
Description	Portable Pharmacie	
WLAN Profile Name	PHARMACIE 🗸 🛛	

2. Créer/modifier un profil de stratégie

Étape 1 : Accédez à **Configuration > Tags & Profiles > Policy** Cliquez sur **+ Ajouter** pour en ajouter un nouveau. Assurez-vous qu'il est activé, définissez le VLAN nécessaire et tout autre paramètre que vous souhaitez personnaliser.

Edit Policy Profile		
A Disabling a Police	cy or configuring it in 'Enabled' state, will result in loss of (connectivity for clients associated with this Policy profile.
General Access Policies	s QOS and AVC Mobility Advanced	
RADIUS Profiling		WLAN ACL
HTTP TLV Caching		IPv4 ACL Search or Select 🗸
DHCP TLV Caching		IPv6 ACL Search or Select 👻 🛛
WLAN Local Profiling		URL Filters (i)
Global State of Device Classification	Disabled (i)	
Local Subscriber Policy Nam	e Search or Select 🔻 💈	Pre Auth Search or Select V
VLAN		Post Auth Search or Select V
VLAN/VLAN Group	wifi_pro v	
Multicast VLAN	Enter Multicast VLAN	

Étape 2. Une fois terminé, cliquez sur **Enregistrer et appliquer au périphérique**. Créer en un pour chaque vlan

Confi	Configuration > Tags & Profiles > Policy						
+	Add	C Delete	Clone				
	Admin Y Status	Associated 1 Y Policy Tags	Policy Profile Name	Description			
	0	•	default-policy-profile	default policy profile			
	0	•	wifi-pro-policy-profil				
	0	•	biomedical-policy-profil				
	0	•	wifi-patient-policy-profil				
м	← 1 →	▶ 10 🔻					

3. Créer/Modifier une balise de stratégie (Lier le SSID au profil de stratégie souhaité)

La balise Policy est le paramètre qui vous permet de spécifier quel SSID est lié à quel profil de stratégie.

Étape 1 : Accédez à **Configuration > Tags & Profiles > Tags > Policy**. Sélectionnez le nom d'une balise établie ou cliquez sur **+ Ajouter** pour en ajouter une nouvelle.

Cisco Cisco Ca	atalyst 9800-CL Wireless Controller	Welcome mcamara 🛛 🛠 🕏 🏝 🏟	Search APs and Clients Q
Q Search Menu Items	Configuration > Tags & Profiles > Tags		
Bashboard	Policy Site RF AP		
Monitoring >	Add. × Delete		
	Policy Tag Name	T Description	T
Configuration	New-policy-tag	Esquirol-policy-tag	
() Administration	default-policy-tag	default policy-tag	
© Licensing	H 4 1 F F 10 V		1 - 2 of 2 items
- Troubleshooting			

Étape 2 : Dans la balise de stratégie (WLAN-POLICY Maps), cliquez sur +Add, dans la liste déroulante, sélectionnez le nom du profil WLAN que vous souhaitez ajouter à la balise de stratégie et au profil de stratégie auxquels vous souhaitez établir une liaison. Ensuite, cliquez sur la coche.

Edit Policy Tag				×
A Changes may r	esult in loss of connectivity	for some clients	that are associated to A	APs with this Policy Tag.
Name* Description	New-policy-tag Esquirol-policy-tag			
VIAN-POLICY	Maps: 4			
+ Add × Delet	e			
WLAN Profile		T	Policy Profile	Ŧ
WiFi_PRO			wifi-pro-policy-profil	
PHARMACIE			wifi-pro-policy-profil	
biomedical			biomedical-policy-pro-	fil
WiFi_PATIENT			wifi-patient-policy-pro	ĥl
⊌ ∢ 1 ⊨ ⊨	10 🔻			1 - 4 of 4 items
Map WLAN and Polic	су			
WLAN Profile*	WiFi_PRO v		Policy Profile*	wifi-pro-policy-pr 🔻 🛛
> RLAN-POLICY	Maps: 0			T Update & Apply to Device

• Attribution de balise de stratégie

Vous pouvez attribuer une balise de stratégie directement à un point d'accès ou attribuer la même balise de stratégie à un groupe de points d'accès en même temps. Choisissez celui qui vous convient.

Cisco Cat	alyst 9800-CL Wireless Controller	Welcome mcamara	* • • •	Search APs and Clier	The seedback of the seedback o
Q. Search Menu Items	Configuration >> Wireless >> Access Points	Edit AP			×
	All Access Points	General Interfaces	High Availability Inventory	Geolocation ICap	Advanced Support Bundle
Cashboard		General		Tags	
Monitoring >	Total APs : 1	AP Name*	1.47D2.35A8	Policy	New-policy-tag
Configuration	Ada	Location*	default location	Site	new-site-tag
Administration	AP Name : AP Model : Slots : Stat	Base Radio MAC	84f1.47d3.1fc0	RF	default-rf-tag 🗸 🗸
C Licensing	-7D2.35A8 🚠 🔟 🛑 Е-К9 2 🧭	Ethernet MAC	d2.35a8	Write Tag Config to AP	i
X Troubleshooting	4 4 1 ⊨ ⊨ 10 ▼	Admin Status		Version	
••	> 6 GHz Radios	AP Mode	Flex •	Primary Software Version	17.12.4.22
		Operation Status	Registered	Predownloaded Status	N/A
	> 5 GHz Radios	Fabric Status	Disabled	Predownloaded Version	N/A
	> 2.4 GHz Radios	CleanAir <u>NSI Key</u>		Next Retry Time	N/A
		LED State		Boot Version	1.1.2.4
	Dual-Band Radios	Brightness Level		IOS Version	.4.22
	> Country			Mini IOS Version	0.0.0.0
	SC Provision	Flash State	DISABLED	IP Config	
			2 Apply	CAPWAP Preferred Mode	IPv4
	> AP Certificate Policy			DHCP IPv4 Address	
		Cancel			Update & Apply to Device

• Paramètres de jonction AP (AP Join Profile) sur les WLC 9800

Le **profil de jonction (AP Join Profile)** est un profil de configuration qui définit les paramètres qu'un point d'accès (AP) utilisera lorsqu'il rejoindra le réseau sans fil. Ce profil spécifie des paramètres comme le mode de fonctionnement de l'AP.

Flux de configuration :

1. Créer/modifier un profil de jointure AP

Étape 1. Accédez à **Configuration > Tags & Profiles > AP Join**.

Sélectionnez le nom d'un profil établi ou cliquez sur + Ajouter pour en ajouter un nouveau.

¢	cisco Catalyst 9800-CL Wireless Controller				Welcome mcamara	*	6	٥	1	0	C	
	Search Menu Items	Cont	iguration ▼ > Tags & P Add × Delete	rofiles > AP Join								
			AP Join Profile Name			▼ Description						
	Monitoring	`	GRP-AP-MAS									
2	Configuration	、	GRP-AP-MDA									
ŝ	Administration		GRP-AP-TEST									
	Administration		GRP-AP-USIS									
C	Licensing		GRP-AP-MAGNAC									
S.	Troubleshooting		GRP-AP-BOBILLOT									
6789			GRP-AP-ESQUIROL									
			GRP-AP-STJUNIEN									
			GRP-AP-PHARMACIE									
			GRP-AP-SERVCTECH									
		н	4 1 2 ▶ ₩	10 🔻								

Étape 2 : Modifiez le profil comme vous le souhaitez. Une fois terminé, cliquez sur Enregistrer et appliquer au périphérique.

Edit AP Join Profile						×
General Client	CAPWAP AP	Management	Security ICap	QoS	Geolocation	
Name*	GRP-AP-ESQUIRC	DL	OfficeExtend	d AP Config	juration	
Description	Enter Description		Local Access			
Country Code	FR	• 🔺 i	Link Encryptio	n		
Time Zone	Not Configured		Rogue Detecti	on		
	Use-Controller		Provisioning S	SID		
	Delta from WLC		Antenna Mo	nitoring		
LED State			Antenna Monit	toring		
LAG Mode			DSSI Foil Through	abold(dP)*	40	
NTP Server	0.0.0		ROOF Pair Three	shold(db)"	40	
GAS AP Rate Limit			Weak RSSI(dE	im)*	-60	
USB Enable			Detection Time	e(min)*	12	
Apphost						
Fallback to DHCP						

2. Créer/modifier un profil flexible (si AP en mode flexible)

Étape 1. Accédez à **Configuration > Tags & Profiles > Flex**.

Sélectionnez le nom d'un profil établi ou cliquez sur + Ajouter pour en ajouter un nouveau.

Cisco Cisco Cata	alyst 9800-CL Wireless Controller	Welcome mcamara 🛛 🏘 隊 🛕 🖺 🏟 👰 📿	
Q Search Menu Items	Configuration • > Tags & Profiles • > Flex + Add × Delete Clone		
	Flex Profile Name	Y Description	
(Monitoring >	GRP-FLEX-MDA		
Configuration	GRP-FLEX-USIS		
	GRP-FLEX-MAGNAC		
CCS Administration >	GRP-FLEX-ESQUIROL		
C Licensing	GRP-FLEX-STJUNIEN		
Troubleshooting	GRP-FLEX-ESQUIROL2		
©169	GRP-FLEX-ESQUIROL3		
	GRP-FLEX-AIGUEPERSE		
	default-flex-profile	default flex profile	
	GRP-FEX-SITES-DISTANTS		

Étape 2. Modifiez ou créer le profil comme vous le souhaitez en y ajouter les VLANs crées. Une fois terminé, cliquez sur **Enregistrer et appliquer au périphérique**.

Cisco Cisco Ca	atalyst 9800-CL Wireless Controller	Welcome mcamara 🛛 🐐 📽 🛕 🖹 🏟 🔞 🤣 🎜 Search APs and Cleres 🔍 🗍 🕿 Feedback 🖍 🗭
Q Search Menu Items	Configuration > Tags & Profiles > Fl	Edit Flex Profile ×
	+ Add × Delete	General Local Authentication Policy ACL VLAN DNS Layer Security
Dashboard	Flex Profile Name	+ Add × Delete
Monitoring >	GRP-FLEX-MDA	VLAN Name Y ID Y Ingress ACL Y Egress ACL Y
Configuration	GRP-FLEX-USIS	
Administration .	GRP-FLEX-MAGNAC	VLAN0087
Administration	GRP-FLEX-ESQUIROL	wifi_pro
C Licensing	GRP-FLEX-STJUNIEN	biomedical
	GRP-FLEX-ESQUIROL2	wifi_patient
6769 ·····	GRP-FLEX-ESQUIROL3	H 4 1 P H 10 V 1 - 5 of 5 Items
	GRP-FLEX-AIGUEPERSE	
	default-flex-profile	
	GRP-FEX-SITES-DISTANTS	
	H 4 1 ⊨ H 10 ▼	

3. Créer/modifier une balise de site

La balise Site est le paramètre qui vous permet de spécifier quelle jointure AP et/ou quel profil Flex est attribué aux AP. **Étape 1 :** Accédez à **Configuration > Tags & Profiles > Tags > Site**. Sélectionnez le nom d'un profil établi ou cliquez sur **+ Ajouter** pour en ajouter un nouveau.

Cisco Cat	alyst 9800-CL Wireless Controller	Welcome mcamara	* * A B * Ø	8 2 Sear				
Q. Search Menu Items	Configuration * > Tags & Profiles * > Tags							
📻 Dashboard	Policy Site RF AP							
Monitoring >	+ Add × Delete Clone Reset APs							
2	Site Tag Name	Tescription						
Configuration	new-site-tag		mode flexible					
(O) Administration	default-site-tag		default site tag					
C Licensing								
X Troubleshooting								

Étape 2 : Dans la balise de site, sélectionnez le **profil de jonction AP** que vous voulez ajouter à la balise de site.

Si vous souhaitez convertir les AP (mode de fonctionnement en mode **flexconnect**), désactivez l'option **Enable Local Site (mode Local)**.

Une fois désactivé, vous pouvez également sélectionner un **profil flexible**. Après cela, cliquez sur **Enregistrer et appliquer au périphérique**.

	Edit Site Tag	
	Name*	new-site-tag
д	Description	mode flexible
	AP Join Profile	GRP-AP-ESQUIROL 🔻
	Flex Profile	GRP-FLEX-ESQUI ▼
	Fabric Control Plane Name	default-control-pl .x 🔻
	Enable Local Site	
	Load* (i)	0

N'oubliez pas de maintenir l'option Activer le site local activée si les points d'accès sont prévus pour être utilisés en mode local.

b. Migration des APs (AIR-AP1832I-E-K9) vers Cisco Catalyst 9800 CL

DHCP Option 43 :

Une plage d'adresse IP est activé sur le cœur de réseau pour le vlan 87, afin que les nouveaux points d'accès récupèrent une adresse IP de façon à ce qu'il remonte sur le contrôleur. Une fois le point d'accès récupéré, son IP est figée.

b.1 Problème rencontré : Impossible de déplacer les APs du contrôleur AireOS vers le nouveau contrôleur Catalyst 9800-CL

Le nouveau contrôleur n'accepte pas les AP initialement connectés à l'ancien contrôleur WLC AirOS.

- Échec de la vérification du certificat

] display_verify_cert_statu	s: Verify Cert: FAILED at 1 depth: self signed certificate in certificate chain
[*02/10/2025 12:48:06.1299]	X509 OpenSSL Errors
[*02/10/2025 12:48:06.1299]	
[*02/10/2025 12:48:06.1299]	NONE
[*02/10/2025 12:48:06.1299]	
[*02/10/2025 12:48:06.1299]	
[*02/10/2025 12:48:06.1299]	dtls_verify_con_cert: Controller certificate verification error
[*02/10/2025 12:48:06.1299]	dtls_process_packet: Controller certificate verification failed
[*02/10/2025 12:48:06.1399]	sendPacketToDtls: DTLS: Closing connection 0x2b1cca00.
[*02/10/2025 12:48:06.1399]	
[*02/10/2025 12:48:06.1399]	Going to restart CAPWAP (reason : dtls_rc_connection_closed)
[*02/10/2025 12:48:06.1399]	
[*02/10/2025 12:48:06.1399]	DTLS: Error while processing DTLS packet 0x2b23f000.
[*02/10/2025 12:48:06.1399]	Restarting CAPWAP State Machine.

b.2 Solutions : 1^{ère} Option : Réinitialiser les APs

Etape 1 :

- Alimenter le point d'accès via un câble Rj45 (POE)
- Connexion au point d'accès via un câble console
- Connexion au point d'accès via le logiciel PuTTY

alegory:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP 	Basic options for your PuTT Specify the destination you want to co Serial line COM3 Connection type: SSH Serial Other: 1 Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: Always Never Only of the setting of the section of the setting of the section of th	Y session onnect to Speed 9600 Felnet V Load Save Delete on clean exit

Etape 2 :

- Une fois connecté à l'AP, réinitialiser le avec la commande capwap ap erase all

[*01/22/2025 12:35:45.1299]	
[*01/22/2025 12:35:45.1499]	dtls_verify_server_cert: vWLC is using SSC, returning l
[*01/22/2025 12:35:45.2399]	
[*01/22/2025 12:35:45.2399]	CAPWAP State: Join
[*01/22/2025 12:35:45.4299]	Sending Join request to through port 5256, packet size 1376
[*01/22/2025 12:35:50.3683]	Sending Join request the second through port 5256, packet size 1376
[*01/22/2025 12:35:50.3783]	Join Response from ., packet size 1397
[*01/22/2025 12:35:50.3783]	AC accepted previous sent request with result code: 0
[*01/22/2025 12:35:50.3783]	Received wlcType 0, timer 30
[*01/22/2025 12:35:50.5683]	nss_capwapmgr_enable_tunnel[1682]:ef30b800: tunnel 0 is already enabled
[*01/22/2025 12:35:50.6082]	
[*01/22/2025 12:35:50.6082]	CAPWAP State: Image_Data
[*01/22/2025 12:35:50.6082]	AP image version 2.4.22 backup 8.10.185.0, Controller 17.12.4.22
[*01/22/2025 12:35:50.6082]	Version is the same, do not need update.
[*01/22/2025 12:35:50.7382]	status 'upgrade.sh: Script called with args:[NO_UPGRADE]'
[*01/22/2025 12:35:50.7882]	do NO_UPGRADE, partl is active part

¢	cisco	Cisco (Cataly	st 9800-Cl	Wireless	Controller			We	lcome mcama	ara	* *	A [a 🌣 🕸	0	C Search APs	s and Clients Q	Feedback	₽ 🕒
Q	Search Menu	Items		Monitoring • >	Wireless * >	AP Statistics													
			-	General Jo	oin Statistics	AFC Statistic:	6									Misconfigur	ed APs		
C			Total APs : 1					Only 'Cor	tains' i	is supported whil	e filterir	ng two or more	column	Tag : 0	Country Code : 0	LSC Fallback : 0 m Bulk AP Provisionin	g feature		
Ľ	Configuratio		>	Operation State	us «Is equal to»	Registered x	7												
ত্যি			>	AP Name	:	AP Model	: :	Admin : Status	Up Time	IP Address	:	AP Radio MAC	:	Ethernet MAC	:	Operation : Status	Configuration Status	Power Derate Capable	: Pc
C					ф ф	AIR-AP1832I-E	-K9	0	0 days 1 hrs 42 mins 39 secs			84f1.47d3.1fc0	F	.47d2.35a	a8 🎤	Registered	Healthy	No	Ne
×				⊨ - 1	▶ H	10 🔻												1 - 1 of 1 item	5 Č

2^{ème} Option : pour une migration massive

Pour résoudre le problème lié aux certificats entre les deux contrôleurs :

Configurez le même token d'authentification sur AireOS et 9800 WLC.

- Assurez-vous que tous les bornes sont associées au WLC AireOS.
- Entrez la commande suivante sur le 9800 CL certificate ssc hash validation disable
- Entrez la commande suivante sur le AireOS config certificate ssc auth-token « mot-de-passe »
- Entrez la commande suivante sur le **9800** CL wireless management certificate ssc auth-token 0 « motde-passe »
- Commencez ensuite à migrer les points d'accès.



7. Test

Vérification des SSID

• Pour le WiFi_PATIENT et WiFi_PRO

RLWIFI#sh w	ireless client vlan s							
IRLWIFI#sh w	ents: 11							
	encs. II							
AC Address	AP Name	Type	ID	State	Method	Role	VLAN	VLAN name
		WLAN	2	Run	None	Local		wifi_patient
	AP-CINCIPALITY	WLAN		Run	Dot1x	Local	24	wifi_pro
	AP-	WLAN		Run	None	Local		wifi_patient
	AP-	WLAN		Run	Dot1x	Local	24	wifi_pro
		WLAN	3	Run	Dot1x	Local	24	wifi pro
		WLAN	2	Run	None	Local	3	wifi patient
	AP	WLAN	2	Run	None	Local	3	wifi patient
	AP- CONTRACTOR 2.	WLAN	2	Run	None	Local	3	wifi patient
		WLAN	3	Run	Dot1x	Local	24	wifi pro
	AP- CONTRACTOR	WLAN	3	Run	Dot1x	Local	24	wifi pro
	AD DESIGNATION	LU AN	>	Run	Dot1x	Local	24	wifi nro

Top WLANs × Last Updated: 2/13/2025, 1:26:49 PM ×									
Sort by: WLANs With High	est Client Co	•	6 0						
WLAN Name	ID	Clients	Data Usage						
WiFi_PRO	3	11 警	26 GB						
WiFi_PATIENT	2	7 誓	72 GB						
biomedical	4	1 🚢	3.2 MB						

8. Configuration finale :



9. Supervision (Zabbix & Nagios)

Objectif : Obtenir une vue d'ensemble instantanée sur la disponibilité et l'état de chaque point d'accès du réseau (Esquirol). Cela inclut la connectivité (en ligne/hors ligne) et l'état de chaque AP.

A. Agent SNMP (Contrôleur Catalyst 9800 CL)

Configuration de l'agent SNMP sur le contrôleur Cisco Catalyst 9800 CL

Aller dans Administration>SNMP



Ensuite dans la section Community Strings, on ajoute le deux communautés (Privée et Public)

Cisco Cata	alyst 9800-CL Wireless	Controller		Welcome mc	amara	*	1 0	A 🖪	٥		0 (3
Q Search Menu Items	Administration - > Manage	ement > SNMP										
	SNMP Mode	ENABLED										
bashboard	General SNMP Views	Community Strings	V3 User Groups	V3 Users	Hosts	Wir	eless T	raps				
Monitoring >	+ Add × Delete											
Configuration >												
Administration		Community Name							▼ Ac	cess M	lode	
		Prive							Re	ad Only		
C Licensing		Public							Re	ad Only		
X Troubleshooting	₩ 4 1 ► ₩	10 🔻										

Dans la section Hosts, on indique l'adresse IP de Zabbix + le port 162

Cisco Cata	lyst 9800-CL Wireless Controller	Welcome mcamara	* * A B * 0 0 0
Q Search Menu Items	Administration -> Management -> SNMP	1	
Dashboard	General SNMP Views Community Strin	J gs V3 User Groups V3 Users Hosts	Wireless Traps
Monitoring Configuration	+ Add × Delete		
Administration >	IP Addr Hosts		×
C Licensing	IPv4/IPv6 Address*		
₩ Troubleshooting	Version Community String*	V1 V	
	Port	162	
	Туре	traps 🔻	
	"Cancel		Apply to Device

Enfin, dans la partie Wireless Traps, on active les informations que l'on veut collecter

eneral	SNMP Views	Community Strings	V3 User Groups	V3 Users	Hosts	Wireless T	raps		
Enable	All Disable All								🖺 Apply
Me V	Abate SNR Child Moved Excessive Hopc Parent Change	C ount (Authentication Fi Excessive Childre Onset SNR	AABLED		Wir	eless Client Association Fail Authentication Fail Disassociate Authenticate	ENABLED Associate Deauthenticate Excluded Maximum Threshold Wa	Irrning elect All
RF	Tx Power Coverage Load		Channels Interference Noise	DISABLED		Rog	ue Rogue Client	Rogue AP	BLED elect All
Wir RRI Ger	eless Mobility Anchor Client En M Group neral Controller	abled	(DISABLED DISABLED DISABLED			ess Point Crash IP Address Fallback No Radio Cards MFP Dual-band Radio Role Change Authorization	ENABLED Interface Up Mode Register Broken Antenna Dual-band Radio Band I AP Stats	Change
								□ s	elect All

B. Zabbix

Etape 1 : Intégration du contrôleur Catalyst sur Zabbix

	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	A DECEMBER OF	1.1		3			• •
ZABBIX « ป zabbix	Hôtes < ⊽						?	run hôte 💽 👯
Tableaux de bord	Nom Groupos sthétos	CTRLWIFI	Sáloctionnar	État Tous	Activé Désactivé			
Surveillance	Croupes anotes		Coloculoniner	lago Loo	Cont	lient M volour	Supprimar	
Problèmes	DNS			Ajouter	Com	Valeur	Suppriner	
Hôles	Port			Afficher les hôtes en maintenance 🔽	Afficher les problèmes s	supprimés		
Dernières données								
Cartes	Sevente	Non classe Avertissement	- Haut					
Découverte								
🖧 Services 🗸 🗸			Enregi	strer sous Appliquer Réinitialiser]			
🕎 Inventaire -	Nom Interface	Disponibilité	Tags État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
🕂 Rapports -	CTRLWIFI	SNMP	Activé	Dernières données 186	4	Graphiques 15	Tableaux de bord	Web
Collecte de données 🗸							Affichage de	1 sur 1 trouvés
de donneed								

Aller dans Surveillance>Hôtes et clique sur créer un hôte

Ensuite, dans la section Hôte, indiquez l'adresse IP du Contrôleur Wi-Fi Catalyst 9800 CL

Hôte								? >
Hôte IPMI Tag	s Macros	3 1 Inventaire • Chiffreme	ent Table de correspondance					
* Nom de l'hôte	CTRLWIFI							
Nom visible	CTRLWIFI							
Modèles	Nom		Action					
	Network_Ci	sco_WiFi_WLC	Supprimer lien Supprimer lien et nettoyer					
	taper ici po	our rechercher		Sélection	ner			
* Groupes d'hôtes	Linux serv	ers ×		Sélection	iner			
	taper ici po							
Interfaces	Туре	adresse IP	Nom DNS	Connex	ion a	Port		
	✓ SNMP			IP	DNS	161	Supprimer	
	Ajouter							
Description								
			1					
Surveillé par	Serveur	Proxy Groupe de proxy]					
Activé	~							
						Actualise	Clone Supprimer	Annuler

Dans la section Macro, on indique la communauté (Public)

Hôte				? >	ζ
Hôte IPMI Tags Macros 1 Inventaire	Chiffrement Table de correspondance				
Macros d'hôte Macros héritées et de l'hô	le				
Macro	Valeur	Description			
{\$SNMP_COMMUNITY}	Public	T ∽ description		Supprimer	
Ajouter					
			Actualiser Clone	Supprimer Annuler]

Etape 2 : créer une carte dans Zabbix afin de visualiser l'état des points d'accès (APs)

Aller dans l'onglet "Administration>Général>Images"
 On importe une image cartographique (plan du lieu où se trouve les APs) dans un premier temps.





Images ~

* Nom	
* Télécharger	Choisir un fichier Aucun fichier n'a été sélectionné
	Ajouter Annuler

Etape 2 : configuration d'une carte pour les APs

Avant de commencer la configuration de vos cartes sur Zabbix montrant tous les points d'accès (AP), il vous faut d'abord vous assurer que tous les points d'accès y sont bien intégrés avec leurs données de surveillance collectées (comme la disponibilité, la performance, etc.).

Une fois que les données sont collectées, vous pouvez créer une **carte** pour visualiser l'état de tous les APs. Voici les étapes générales pour réaliser cela :

ZABBIX « 🛛	Cartes				? Créer une carte Importer
zabbix					▽ Filtre
		Nom			
Surveillance		Appliquer	Réinitialiser		
Problèmes	Nom 🔺	Largeur	Hauteur	Actions	
Hôtes	Cafetariat	747	328	Propriétés Édition	
Dernières données	DE NERVAL	1142	544	Propriétés Édition	
Cartes	ESQUIROL_WIFI	1600	900	Propriétés Édition	
Découverte	Formation_NV1	1445	737	Propriétés Édition	
🚠 Services	Formation_NV2	1525	739	Propriétés Édition	
Inventaire	Formation_RDC	1576	724	Propriétés Édition	
C Provente	Local network	680	200	Propriétés Édition	
Hi Rappons					Affichage de 7 sur 7 trouvés
Collecte de données	0 sélectionné Exporter 🗸 Supprimer				

1. Aller dans Surveillance/Cartes + Créer une carte

Ensuite indiquer le nom de la carte (Bâtiment où se trouve les APs), + l'image cartographique importée précédemment (Formation_RDC)

Cartes réseau			
Carte Partage			
* Propriétaire	mcamara (Mamadou CAMARA) × Sélectionner		
* Nom	Formation_RDC		
* Largeur	1576		
* Hauteur	724		
Image de fond	Formation_RDC V		
Correspondance d'icône automatique	<manuel></manuel>		
Icône surlignée			
Marquer les éléments lors de changement de l'état du déclencheur			
Afficher les problèmes	Détailler problème unique Nombre de problèmes Nombre de problèmes et détailler le plus critique		
Étiquettes avancées			
Type d'étiquette de l'élément de carte	Étiquette ~		
Emplacement de l'étiquette de l'élément de carte	Bas V		
Affichage des problèmes	Tous		
Sévérité minimale	Non classé Information Avertissement Moyen Haut Désastre		
Afficher les problèmes supprimés			
URLs	Nom URL	Élément	Action
	Ajouter	nute	Supprinter
Actualiser Clone	Supprimer Annuler		

Une fois la carte créée, on clique sur Editer

Cartes			
	Nom		
	Appliquer	Réinitialiser	
□ Nom ▲	Largeur	Hauteur	Actions
Cafetariat	747	328	Propriétés Édition
DE NERVAL	1142	544	Propriétés Édition
ESQUIROL_WIFI	1600	900	Propriétés Édition
Formation_NV1	1445	737	Propriétés Édition
Formation_NV2	1525	739	Propriétés Édition
Formation_RDC	1576	724	Propriétés Édition
Local network	680	200	Propriétés Édition

0 sélectionné Exporter 🗸 Supprimer

- Créez une carte avec des icônes représentant vos APs.
- Ajoutez un **déclencheur** qui suit l'état de la connectivité pour chaque AP (par exemple, si l'AP est en ligne ou hors ligne).
- Utiliser les icones représentant l'état (Disponibilité de l'AP (ping ou autre vérification)) pour refléter l'état actuel de chaque AP.





On fais pareil pour les autres lieux (Aps)



2. Carte pour tous les APs du CH Esquirol (Satellite)

Cartes réseau	?
Carte Partage	
* Propriétaire	valbert (Vincent ALEBRT) × Sélectionner
* Nom	ESQUIROL_WIFI
* Largeur	1600
* Hauteur	900
Image de fond	WIFL_ESQUIROL_GLOBAL ~
Correspondance d'icône automatique	<manuel> v afficher les correspondances d'icônes</manuel>
Icône surlignée	
Marquer les éléments lors de changement de l'état du déciencheur	
Afficher les problèmes	Détailler problème unique Nombre de problèmes Nombre de problèmes et détailler le plus critique
Étiquettes avancées	
Type d'étiquette de l'élément de carte	Étiquette v
Emplacement de l'étiquette de l'élément de carte	Bas v
Affichage des problèmes	Tous 🗸
Sévérité minimale	Non classé Information Avertissement Moyen Haut Désastre
Afficher les problèmes supprimés	
URLs	Nom URL Élément Action
	Hôte V Supprimer
	Ajouer
Actualiser Clone	Supprimer Annuler

Aller dans Surveillance>Cartes + Créer une carte

Ensuite indiquer le nom de la carte (Esquirol_WiFi), l'image cartographique du site de CH Esquirol (Satellite).

Une fois la carte créée, on clique sur Editer, + Ajouter (Elément de la carte).

Ensuite on indique le type (Carte), l'étiquette (Le nom du bâtiment où se trouves les APs)



On peut vérifier l'état de tous les APs (Bâtiment par bâtiment) depuis la carte (ESQUIROL_WIFI)



DENERVAL

