# Démonstration du profilage client sur le contrôleur LAN sans fil 9800

# Table des matières

Introduction Composants utilisés Processus de profilage Profilage OUI d'adresse MAC Problèmes liés aux adresses MAC administrées localement Profilage DHCP Profilage HTTP **Profilage RADIUS** Profilage RADIUS DHCP **Profilage RADIUS HTTP** Configuration du profilage sur le WLC 9800 Configuration du profilage local Configuration du profilage RADIUS Profilage des cas d'utilisation Application de stratégies locales basées sur la classification de profil local Profilage Radius pour les ensembles de politiques avancés dans Cisco ISE Profilage dans les déploiements FlexConnect Authentification centrale, Commutation locale Authentification locale, Commutation locale Dépannage **Traces radioactives** Captures de paquets

# Introduction

Ce document décrit le fonctionnement de la classification et du profilage des périphériques sur les contrôleurs LAN sans fil Cisco Catalyst 9800.

## Composants utilisés

- 9800 CL WLC exécutant l'image 17.2.1
- Point d'accès 1815i
- Client sans fil Windows 10 Pro
- Cisco ISE 2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Processus de profilage

Cet article présente en détail le fonctionnement de la classification et du profilage des périphériques sur les contrôleurs LAN sans fil Cisco Catalyst 9800, décrit des cas d'utilisation potentiels, des exemples de configuration et les étapes nécessaires pour le dépanner.

Le profilage de périphérique est une fonctionnalité qui permet de trouver des informations supplémentaires sur un client sans fil qui a rejoint l'infrastructure sans fil.

Une fois le profilage de périphérique effectué, il peut être utilisé pour appliquer différentes stratégies locales ou pour correspondre à des règles de serveur RADIUS spécifiques.

Les WLC Cisco 9800 peuvent effectuer trois (3) types de profilage de périphérique :

- 1. Adresse MAC OUI
- 2. DHCP
- 3. HTTP

## Profilage OUI d'adresse MAC

L'adresse MAC est un identificateur unique de chaque interface réseau sans fil (et filaire). Il s'agit d'un nombre de 48 bits généralement écrit au format hexadécimal MM:MM:SS:SS:SS.

Les 24 premiers bits (ou 3 octets) sont appelés OUI (Organizationally Unique Identifier) et ils identifient de manière unique un fournisseur ou un fabricant.

Ils sont achetés auprès de l'IEEE et attribués par celui-ci. Un fournisseur ou un fabricant peut acheter plusieurs OUI.

Exemple :

00:0D:4B - owned by Roku, LLC 90:78:B2 - owned by Xiaomi Communications Co Ltd

Une fois qu'un client sans fil s'associe au point d'accès, le WLC effectue la recherche OUI pour déterminer le fabricant.

Dans les déploiements de commutation locale Flexconnect, le point d'accès relaie toujours les informations pertinentes du client au WLC (comme les paquets DHCP et l'adresse MAC du client).

Le profilage basé uniquement sur l'OUI est extrêmement limité et il est possible de classer l'appareil comme une marque spécifique, mais il ne permet pas de faire la différence entre un ordinateur portable et un smartphone.

#### Problèmes liés aux adresses MAC administrées localement

Pour des raisons de confidentialité, de nombreux fabricants ont commencé à implémenter des fonctionnalités de randomisation mac dans leurs appareils.

Les adresses MAC administrées localement sont générées aléatoirement et ont un second bit de poids faible du premier octet de l'adresse défini sur 1.

Ce bit agit comme un indicateur qui annonce que l'adresse MAC est en fait une adresse générée

aléatoirement.

Il existe quatre formats possibles d'adresses MAC gérées localement (x peut être n'importe quelle valeur hexadécimale) :

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

Par défaut, les périphériques Android 10 utilisent une adresse MAC gérée localement et générée de manière aléatoire chaque fois qu'ils se connectent à un nouveau réseau SSID.

Cette fonctionnalité annule complètement la classification de périphérique basée sur l'OUI car le contrôleur reconnaît que l'adresse a été randomisée et n'effectue aucune recherche.

## **Profilage DHCP**

Le profilage DHCP est effectué par le WLC par l'examen des paquets DHCP que le client sans fil envoie.

Si le profilage DHCP a été utilisé pour classer le périphérique, le résultat de la commande **show wireless client mac-address [MAC\_ADDR] detailed** contient :

Device Type	:	Microsoft-Workstation
Device Name	:	MSFT 5.0
Protocol Map	:	0x000009 (OUI, DHCP)
Protocol	:	DHCP

Le WLC inspecte plusieurs champs d'option DHCP dans les paquets envoyés par les clients sans fil :

#### 1. Option 12 - Nom d'hôte

Cette option représente le nom d'hôte des clients et se trouve dans les paquets DHCP Discover et DHCP Request :



2. Option 60 - Identifiant de la classe du fournisseur

Cette option se trouve également dans les paquets DHCP Discover et Request.

Avec cette option, les clients peuvent s'identifier auprès du serveur DHCP et les serveurs peuvent alors être configurés pour répondre uniquement aux clients avec un identifiant de classe de fournisseur spécifique.

Cette option est le plus souvent utilisée pour identifier les points d'accès dans le réseau et y répondre uniquement avec l'option 43.

Exemples d'identificateurs de classe fournisseur

- « MSFT 5.0 » pour tous les clients Windows 2000 (et versions ultérieures)
- « MSFT 98 » pour tous les clients Windows 98 et Me
- «MSFT» pour tous les clients Windows 98, Me et 2000

Les périphériques Apple MacBook n'envoient pas l'option 60 par défaut.

Exemple de capture de paquets à partir du client Windows 10 :

```
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: MSFT 5.0
```

#### 3. Option 55 - Liste des demandes de paramètres

L'option DHCP Parameter Request List contient les paramètres de configuration (codes d'option) que le client DHCP demande au serveur DHCP. Il s'agit d'une chaîne écrite en notation séparée par des virgules (par exemple 1,15,43).

Ce n'est pas une solution parfaite, car les données qu'elle génère dépendent du fournisseur et peuvent être dupliquées par plusieurs types de périphériques.

Par exemple, les périphériques Windows 10 demandent toujours par défaut une liste de paramètres spécifique. Les iPhones et iPads d'Apple utilisent différents ensembles de paramètres sur lesquels il est possible de les classer.

Exemple de capture à partir du client Windows 10 :

```
Option: (55) Parameter Request List
  Length: 14
  Parameter Request List Item: (1) Subnet Mask
  Parameter Request List Item: (3) Router
  Parameter Request List Item: (6) Domain Name Server
  Parameter Request List Item: (15) Domain Name
  Parameter Request List Item: (31) Perform Router Discover
  Parameter Request List Item: (33) Static Route
  Parameter Request List Item: (43) Vendor-Specific Information
  Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
  Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
  Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
  Parameter Request List Item: (119) Domain Search
  Parameter Request List Item: (121) Classless Static Route
  Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
  Parameter Request List Item: (252) Private/Proxy autodiscovery
```

La classe d'utilisateur est une option qui n'est généralement pas utilisée par défaut et qui nécessite une configuration manuelle du client. Par exemple, cette option peut être configurée sur un ordinateur Windows à l'aide de la commande suivante :

ipconfig /setclassid "ADAPTER\_NAME" "USER\_CLASS\_STRING"

Le nom de l'adaptateur se trouve dans le Centre Réseau et partage du Panneau de configuration :



Configurez l'option DHCP 66 pour le client Windows 10 dans CMD (nécessite des droits d'administrateur) :



En raison de l'implémentation de l'option 66 par Windows, Wireshark n'est pas en mesure de décoder cette option et une partie du paquet suivant l'option 66 apparaît comme malformée :



## **Profilage HTTP**

Le profilage HTTP est la méthode la plus avancée de profilage prise en charge par le WLC 9800 et offre la classification de périphérique la plus détaillée.

Pour qu'un client soit profilé HTTP, il doit être à l'état « Exécuter » et exécuter une requête HTTP GET.

WLC intercepte la requête et examine le champ « User-Agent » dans l'en-tête HTTP du paquet.

Ce champ contient des informations supplémentaires sur le client sans fil qui peuvent être utilisées pour le classer.

Par défaut, presque tous les fabricants ont mis en oeuvre une fonctionnalité permettant à un client sans fil de vérifier la connectivité Internet.

Cette vérification est également utilisée pour la détection automatique du portail invité. Si un périphérique reçoit une réponse HTTP avec le code d'état 200 (OK), cela signifie que le WLAN n'est pas sécurisé avec webauth.

Si c'est le cas, le WLC effectue alors l'interception nécessaire pour effectuer le reste de l'authentification. Ce HTTP GET initial n'est pas le seul que le WLC peut utiliser pour profiler le périphérique.

Chaque requête HTTP suivante est inspectée par le WLC et il en résulte peut-être une classification encore plus détaillée.

Les périphériques Windows 10 utilisent le domaine **msftconnecttest.com** pour effectuer ce test. Les appareils Apple utilisent **captive.apple.com**, tandis que les appareils Android utilisent généralement **connectivitycheck.gstatic.com**.

Les captures de paquets du client Windows 10 effectuant cette vérification sont disponibles cidessous. Le champ User Agent est renseigné avec **Microsoft NCSI**, ce qui a pour résultat que le client est profilé sur le WLC comme **Microsoft-Workstation** :

No.	Title	Source	Destination	Protocol	Leigh 3rfs
	32 11.230352	10.48.39.235	64.182.6.247	DNS	83 Standard query 0x66e8 AAAA www.msftconnecttest.com
	48 11.344857	64.182.6.247	28.48.39.235	DNS	249 Standard query response Build16 A www.msftconnecttest.com CMAPE v4nc
-	55 11.354877	10.48.39.235	13.187.4.52	HTTP	165 GET /connecttest.txt HTTP/1.1
	70 11.378809	13.107.4.52	28.48.39.235	HTTP	624 HTTP/1.1 200 OK (text/plain)
3	Frame SS: 165 byte	s on wire (1320 bits	), 165 bytes capture	d (1320 bit	s) on interface \Device\APF_{95ADD082-D827-4F85-8918-98A8466839A8}, id 0
2	Ethernet II, Src:	Edimente_f6:76:f0 ()	4:da:38:f6:76:f0), D	st: Cisco_B	9:41:e1 (24:7e:12:19:41:e1)
>	Internet Protocol	Version 4, Srci 10.4	48.39.235, Dst: 13.18	7.4.52	
3	Transmission Contr	ol Protocol, Src Por	t: 56815, Dat Port: i	80, Seq: 1,	Ack: 1, Len: 111
¥	Hypertext Transfer	Protocol			
	OFT /connecttes	t.txt HTTP/1.1\//a			
	> [Expert Info	(Chat/Sequence): 68	T /connecttest.txt H	TP/1.1\r\n	]
	Request Reth	INF GET			
	Request URI:	/connecttest.txt			
	Request Versi	ion: HTTP/1.1			
	Connection: Clo	selvia			
	User-Agent: MSc	resoft MCSI\r\n			
	Nost: www.mafte	onnecttest.com/r\n			
	1/ha				
	[full request U	E: http://www.mofte	connecttest.com/connecttest.com/connect	(ttest.txt]	
	(HTTP request 1	/11			
	Descente in fr	and had			

Exemple de sortie de **show wireless client mac-address [MAC\_ADDR] détaillé** pour un client qui est profilé via HTTP :

Device Type	:	Microsoft-Workstation
Device Name	:	MSFT 5.0
Protocol Map	:	0x000029 (OUI, DHCP, HTTP)
Device OS	:	Windows NT 10.0; Win64; x64; rv:76.0
Protocol	:	НТТР

# **Profilage RADIUS**

En ce qui concerne les méthodes utilisées pour classer le périphérique, il n'y a aucune différence entre le profilage local et le profilage RADIUS.

Si le profilage RADIUS est activé, le WLC transfère les informations qu'il a apprises sur le périphérique via un ensemble spécifique d'attributs RADIUS spécifiques au fournisseur au serveur RADIUS.

## Profilage RADIUS DHCP

Les informations obtenues via le profilage DHCP sont envoyées au serveur RADIUS dans la demande de comptabilisation en tant que RADIUS AVPair spécifique au fournisseur **cisco-av-pair** 

#### : dhcp-option=<option DHCP>

Exemple d'un paquet de demande de comptabilisation montrant des paires AVP pour les options DHCP 12, 60 et 55, respectivement envoyées du WLC au serveur RADIUS (la valeur de l'option 55 peut apparaître comme corrompue en raison du décodage Wireshark) :

No.	Title	Source	Destination	Protocol	Langt	SourcePart	Destination Port	2-6	
14	829 9,290998	18.48.39.252	38,48,73,92	8400/5	78	64389	1413	Accounting-Request	14-342
τ.	840 9.198995	10.48.71.92	18.48.39.212	BADDUS	6.	1813	64189	Accounting Response	Ld=282
L.	858 9.298995	10.48.71.92	18.48.39.212	RADIDUS	6	1813	64189	Accounting-Response	1d-282, Duplicate Response
<									
-	Frank Rith, 783 hrs	ter on when fitted b	(a). 783 below control	of COMPANY NAMES					
0	Ethernel 17, Sec.	AD	(an an an an an an) a	A					
0	Seneroet Bostorel	Maralian & Social Int	48 30 222 047. 18 48	71.50	terre for				
	liner Batancas Box	naral. for Burts 64	186 Aut Burt, 1813						
6	Ballin, Protocol	were, are rerer of	tarry unt rent: 2013						
	Code: Accounts	(A) forward (A)							
	Parket Linet14	Lett dute (367)							
	Length: 343	the state (state)							
	Authent Leaters	20120345454545991716	8582c+362576c5						
	CThe response	to this request is	in frame \$491						
	w attribute value	e Pairs	and the second						
	) JUP: tollend	or-descific(36) last	5 underlagedustees(3)						
	) JUP: Ervlenk	or-Specific(26) bab	a under Dereitunteen (9)						
	) AVP: Ervenk	er-Specific(26) bet	a under Darafunteen (9)						
	> auto beyond	er-teeclific(26) b-b	e und-classifystees(b)						
	ANP: D-Vend	or-Specific(26) 1-5	# und-classifystees(#)						
	) ANP: S-Vend	or-Specific(26) 1-2	5 vnd-clacelystees(9)						
	W ANP: Evilendi	or-Specific(36) 1+3	9 undeclassiustees(9)						
	Type: 26								
	Longth	39							
	Vendor 22	Di cloudystees (9)							
	> VSAL CHO	Lace-mittabr(1) 1+03	val-dhop-option-1888/1	VANA-WERE ADDRESS TOP-	41.82894				
	W AVP: DeVend	or-Specific(26) 1+5	2 vnd-clacsdystees(9)						
	Type: 26								
	Longth:	32							
	Vendor 22	Di classifystems (9)							
	<ul> <li>VSA: 4-41</li> </ul>	Contemporate (S) 2424	second second convictions	ANN INSPECT 5.4					
	* AVP: Ervende	or-Specific(26) 2+3	8 vnd+clacstystees(9)						
	Type: 26								
	Longth:	38							
	Vendor 1	It clocedystems (9)					-		
	> VSA: two	ince-www.in(1) 1-92	val-dup-option-later	A0010125-00010000	000101212-00	Place Weeks	•		

## Profilage RADIUS HTTP

Les informations obtenues via le profilage HTTP (champ User-Agent de l'en-tête de la requête HTTP GET) sont envoyées au serveur RADIUS à l'intérieur de la requête de comptabilisation en tant que RADIUS AVPair spécifique au fournisseur **cisco-av-pair : http-tlv=User-Agent=<user-agent>** 

La vérification de connectivité initiale du paquet HTTP GET ne contient pas beaucoup d'informations dans le champ User-Agent, seulement « Microsoft NCSI ». Exemple d'un paquet de gestion des comptes transférant cette valeur simple au serveur RADIUS :

4847 3583,868996	38.48.39.252	10.48.71.92	8400V5	708 57397	1813	Accounting-Request 58-385
4854 3583,875888	38.48.71.92	10.48.39.212	RA03V5	62 1813	\$739P	Accounting-Response id-105
4855 3583,875988	38.48.71.92	10.48.39.212	R403V5	62 1813	\$7397	Accounting-Response id-105, Duplicate Response
User Datagram Proto	cel, Sec Port: 579	97, Dot Port: 1813				
MODUS Protocol						
Code: Accounting Packet Identifie Length: 058 Authenticator: 0 [The response to	-Request (4) r: 0x00 (305) 006atc0f36(4346a5a 1565 request is 2	NENI7M6124d				
· Attribute value	Palins					
<ul> <li>JUP: Erkendor</li> </ul>	-SpecLPLx(24) 2+84 -SpecLPLx(24) 2+97 -SpecLPLx(24) 2+97 -SpecLPLx(24) 2+29 -SpecLPLx(24) 2+29 -SpecLPLx(24) 2+29 -SpecLPLx(24) 2+29 -SpecLPLx(24) 2+29	under(Locallystees(3) under(Locallystees(3) under(Locallystees(3) under(Locallystees(3) under(Locallystees(3) under(Locallystees(3) under(Locallystees(3)				
Type: 26 Length: 35 Vendor ID: > VSA: t=CLs	classigatema (9) co-dummir(1) 1-20 v	al-http-tlo-\0001001	and an element			

Une fois que l'utilisateur a commencé à naviguer sur Internet et qu'il a créé des requêtes HTTP GET supplémentaires, il est possible d'obtenir plus d'informations à ce sujet.

WLC envoie un paquet de comptabilisation supplémentaire à l'ISE s'il détecte de nouvelles valeurs User-Agent pour ce client.

Dans cet exemple, il est possible de voir que le client utilise Windows 10 64 bits et Firefox 76 :

-4	44 3595.102000	38.48.39.252	38.48.71.92	RADOV5	765 57397	1813	Accounting-Request id=106
-4	49 3595.111994	38.48.71.92	38.48.39.232	RADOV5	62 1815	\$739P	Accounting-Response 1d+386
4	758 3595.111994	38.48.71.92	28.48.39.212	RADOUS	62 1813	57397	Accounting-Response id=386, Duplicate Response
	· Colorian Books	und. See Burts \$71	NT. Dot Burt: 1813				
-	Dif. Protocol	the second second	not and positionally				
	Code: Accounting Packet identifie Length: 723 Authenticator: 4	-Request (4) r: Rx6a (106) dbd5c3d8b0exae7d62	45807798444727				
1	atter Duty Malor	Pales	A TORNE ADAD				
	> JUP: tolender	Same Office (245) Taski	under ExcelorAppa/40				
	> #VP: toVendor	Specific(26) 1+37	vndweliaceSystems(H)				
	> #VP: toVendor	-Specific(26) 1+68	vnd-claceSystems(90)				
	> #VP: t+Vendor	-Specific(26) 1+29	vnd+cEsceSystems(90				
	> #VP: t+Vendor	-Specific(26) 1+30	vnd+cEsceSystems(9)				
	> #VP: t+Vendor	-Specific(26) 1+26	vnd-claceSystems(9)				
1	V AVP: t-Vendor Type: 26	-Specific(26) 1+99	vnd+cEscoSystems(9)				
	Length: 99						
	Vendor 101	clacofystems (9)					
	> WEAR THERE	co-Authair(1) 1+05	valuette the last and	And Starting and American Starting	windows NT 18-81 M	India: while my	The set of a stand between a stand set of the set

# Configuration du profilage sur le WLC 9800

## Configuration du profilage local

Pour que le profilage local fonctionne, activez simplement Device Classification sous Configuration > Wireless > Wireless Global. Cette option active simultanément les profils MAC OUI, HTTP et DHCP :

(	Configuration * >	Wireless * >	Wireless Global
	Default Mobility Domain *	default	±.
	RF Group Name*	default	
	Maximum Login Sessions Per User*	0	
	Management Via Wireless		
	Device Classification		
	AP LAG Mode		

En outre, sous Policy configuration, vous pouvez activer HTTP TLV Caching et DHCP TLV Caching. Le WLC effectue le profilage même sans eux.

Lorsque ces options sont activées, le WLC met alors en cache les informations précédemment

apprises sur ce client et évite d'avoir à inspecter des paquets supplémentaires générés par ce périphérique.

Edit Policy	/ Profile			
General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS F	Profiling			
HTTP TL	/ Caching			
DHCP TU	V Caching			
WLAN L	ocal Profiling			
Global St Classifica	ate of Device tion	Enabled (		
Local Sub	oscriber Policy Name	BlockPoli	cy x v	

## Configuration du profilage RADIUS

Pour que le profilage RADIUS fonctionne, outre l'activation globale de la classification des périphériques (comme mentionné dans la configuration du profilage local), il est nécessaire de :

1. Configurez la méthode de comptabilité AAA avec le type «identité» pointant vers le serveur RADIUS :

Configuration * >	Security* > AAA						
+ AAA Wated							
Servers / Groups	AAA Method List	AAA Advanced					
Authentication							
Authorization	+ Add	× Delete					
Accounting	Name	< Type	< Group1	< Group2	< Group3	< Group4	~
	AccMetho	5 Identity	15622	N/A.	NA	NA	
	H - 4 - 1	× × 20 •	terns per page			1 - 1 of 1	herra

2. La méthode de comptabilisation doit être ajoutée sous Configuration > Tags & Profiles > Policy > [Policy\_Name] > Advanced :

licies QOS and AVC	Mobility	Advanced	
		Fabric Profile	Search or Select
1800		mDNS Service Policy	default-mdns-servic +
300			Cause and a second
0		Hotspot Server	Search or Select
at (sec)	_	User Private Netwo	rk
wout		Status	
		Drop Unicast	
		Umbrella	
а		Umbrella Parameter Map	Not Configured  Clear
		Flex DHCP Option for DNS	ENABLED
		DNS Traffic Redirect	KINORE
		WLAN Flex Policy	
		VLAN Central Switchi	ng 🗌
RADIUS	•	Solt MAC ACL	Search or Select
default-aaa-policy	× •	oper moto more	· · · · · · · · · · · · · · · · · · ·
AcctMethod	× •	Air Time Fairness P	olicies
	Nicles QOS and AVC  1800  1800  0  0  0  0  0  0  0  0  0  0  0  0	Nicles QOS and AVC Mobility  1800  1800  0  0  4 (sec)   60  10  1  10  10  10  10  10  10  10	Alicies QOS and AVC Mobility Advanced Fabric Profile 1800 1800 300 0 4 (sec) © 60 Hotspot Server 0 User Private Networ Status Drop Unicast Umbrella Parameter Map Fiex DHCP Option for DNS Fiex DHCP Option for DNS Fiex DHCP Option for DNS NS Traffic Redirect WLAN Fiex Policy VLAN Central Switchi Split MAC ACL default-aaa-policy x • AcctMethod x •

3. Enfin, la case à cocher Profilage RADIUS doit être cochée sous Configuration > Tags & Profiles > Policy Cette case à cocher active à la fois le profilage RADIUS HTTP et DHCP (les anciens WLC AireOS avaient 2 cases à cocher distinctes) :

Edit Policy Profile			
General Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Profiling			
HTTP TLV Caching			
DHCP TLV Caching			
WLAN Local Profiling			
Global State of Device Classification	Enabled (	)	
Local Subscriber Policy Name	BlockPoli	cy x v	]

## Profilage des cas d'utilisation

## Application de stratégies locales basées sur la classification de profil local

Cet exemple de configuration illustre la configuration de la stratégie locale avec un profil QoS bloquant l'accès à YouTube et à Facebook qui est appliqué uniquement aux périphériques profilés comme Windows-Workstation.

Avec de légères modifications, cette configuration peut être modifiée pour, par exemple, définir un marquage DSCP spécifique pour les téléphones sans fil uniquement.

Créez un profil QoS en accédant à **Configuration > Services > QoS**. Cliquez sur Ajouter pour créer une nouvelle stratégie :



Spécifiez le nom de la stratégie et ajoutez une nouvelle carte de classe. Parmi les protocoles disponibles, sélectionnez ceux qui doivent être bloqués, marqués DSCP ou limités en bande passante.

Dans cet exemple, youtube et facebook sont bloqués. Veillez <u>à ne pas</u> appliquer ce profil QoS aux profils de stratégie situés au bas de la fenêtre QoS :

Auto QOS	DISABLED					
Policy Name*	block					
Description						
Match v Match Type Value	< Mark − < Type	Mark v Value	Police Value	Drop ~	AVC/User v Defined	Actions ~
H 4 0 F H	20 🔹 items per	page			No iten	ns to display
	× Delete					
AVC/User Defined	AVC					
		<u> </u>				
Match	Any O At	·				
Match Drop	®Any OA∎					
Match Drop Match Type	Any O All     protocol					
Match Drop Match Type	Any     All     protocol     Available Protocol(s)	•	elected Protocol(s)			

Available (8)		Selected (0)		
Profiles		Profiles	Ingress	Egress
🛜 vasa	÷			
🛜 33nps	÷			
🛜 webauth	+			
11webauth	+			
😭 11mobility	+			
🛜 11override	+			
	×		_	
Cancel				🗄 Apply to De

Accédez à Configuration > Security > Local Policy et créez un nouveau modèle de service :

Configuration * > Security * > Local Policy		
Service Template Policy Map		
+ Add X Delete		
Service Template Name	< Source	~
webauth-global-inactive		
DEFAULT_CRITICAL_DATA_TEMPLATE		
DEFAULT_ORTICAL_VOICE_TEMPLATE		
DEFAULT_LINKSEC_POLICY_MUST_SECURE		
DEFAULT_LINKSEC_POUCY_SHOULD_SECURE		
H 4 1 H 20  amma per page		1 - 5 of 5 items

Spécifiez le profil QoS d'entrée et de sortie créé à l'étape précédente. Une liste d'accès peut également être appliquée à cette étape. Si aucune modification de VLAN n'est nécessaire, laissez le champ vlan vide :

Create Service Template	1	×
Service Template Name*	BlockTemplate	
VLAN ID	1-4094	
Session Timeout (secs)	1-65535	
Access Control List	None 🔻	
Ingress QOS	block x v	
Egress QOS	block x v	
mDNS Service Policy	Search or Select	Ŷ
Cancel		Apply to Device

Accédez à l'onglet Carte de stratégie et cliquez sur Ajouter :



Définissez le nom du mappage de stratégie et ajoutez de nouveaux critères. Spécifiez le modèle de service créé à l'étape précédente et sélectionnez le type de périphérique auquel ce modèle est appliqué.

Dans ce cas, Microsoft-Workstation est utilisé. Si plusieurs stratégies sont définies, la première correspondance est utilisée.

Un autre cas d'utilisation courant serait de spécifier des critères de correspondance basés sur l'OUI. Si un déploiement comporte un grand nombre de scanners ou d'imprimantes du même modèle, ils ont généralement le même OUI MAC.

Cela peut être utilisé pour appliquer un marquage QoS DSCP spécifique ou une liste de contrôle d'accès :

olicy Map Name *	BlockPolicy						
Aatch Criteria List							
+ Add X Deb	te Move To 🔶	Move Up 🛛 🔶 Move	lown				
Device Type(Match Criteria)	V User Role(Match Criteria)	- User Name(Match Criteria)	- OUI(Match Criteria)	×	MAC Address(Match Criteria)	×	Service Template 🗸
udd Match Criteria	20 • Items per page	]	-				No herrs to display
udd Match Criteria	20 • Items per page	Mcrosoft - Workstatic	]				No herre to display
udd Match Criteria iervice Template * Ievice Type Iser Role	20 • terms per page BlockTemplate • eq • Select Fiber Type •	Microsoft Workstatic					No herrs to display
Add Match Criteria Service Template * Nevice Type Joer Role Joer Name	20 • terms per page BlockTemplate • • Geq • Select Filter Type • Select Filter Type •	Microsoft - Workstatic Enter User Role Enter User Name					No items to display
Add Match Criteria Service Template * Nevice Type Iser Role Iser Name	20 • terms per page BlockTemplate • • Geq • Select Filter Type • Select Filter Type •	Microsoft-Workstatic Enter User Role Enter User Name XX, yy.22					No Items to display

Pour que le WLC puisse reconnaître le trafic de youtube et de facebook, la visibilité de l'application doit être activée.

Naviguez jusqu'à **Configuration > Services > Application Visibility** eActivez la visibilité pour le profil de stratégie de votre WLAN :

and a second sec	pplication Visibility				
Enable AVC O Dutied	olicy				
Img and Drop, double click or click o	on the button from Selev	cted Profiles to addimensive Profi	les	Q. Search	Ei Acoly
			10.00	destruction distances	
Profiles		Profiles	Visibility	Collector Address	
Profiles 111welbauth	+ 1	Profiles	Vability	Local 🖉 Edemai	+
Profiles IlliveDouth IlliveDouth IlliveDouth IlliveDouth	*	Profiles	Vabilty	Local / Edemai	+
Profiles  11webauth  11mobility  11profiling	* * *	Profiles 11ovende	visibility	Local 🖉 Ditemal	*
Profiles  11webauth  11mobility  11profiling  33nps	* * *	Profiles           11override	Visibility	Local 🖉 Ditemai	•
Profiles   11webauth  11mobility  33nps  Capwap1	+ + + +	Profiles  11override	Visibility	Local 🖉 Desmal	*

Vérifiez que, sous le profil de stratégie, la mise en cache TLV HTTP, la mise en cache TLV DHCP et la classification globale des périphériques sont activées et que la stratégie d'abonné local pointe vers la carte de stratégie locale créée au cours de l'une des étapes précédentes :

dit Polic	y Profile						
ieneral	Access Policies	QOS and AVC	Mobility	Advanced			
RADIUS	Profiling				WLAN ACL		
HTTP TL	V Caching	2			IPv4 ACL	Search or Select	•
DHCP TL	V Caching				IPv6 ACL	Search or Select	•
WLANI	ocal Profiling				URL Filters		
Global S Classifica	tate of Device ation	Enabled (	D		Pre Auth	Search or Select	•
Local Su	bscriber Policy Name	BlockPol	icy x •	]	Post Auth	Search or Select	•
VLAN							
VLAN/VL	AN Group	VLAN00	39 •	)			
Multicast	VLAN	Enter M	ulticast VLAN	]			

Une fois le client connecté, il est possible de vérifier si la stratégie locale a été appliquée et de tester si youtube et facebook sont réellement bloqués.

Le résultat de la commande show wireless client mac-address [MAC\_ADDR] detailed contient :

```
Input Policy Name : block
Input Policy State : Installed
Input Policy Source : Native Profile Policy
Output Policy Name : block
Output Policy State : Installed
Output Policy Source : Native Profile Policy
Local Policies:
   Service Template : BlockTemplate (priority 150)
   Input QOS : block
```

```
Output QOS: blockService Template: wlan_svc_lloverride_local (priority 254)VLAN: VLAN0039Absolute-Timer: 1800Device Type: Microsoft-WorkstationDevice Name: MSFT 5.0Protocol Map: 0x000029 (OUI, DHCP, HTTP)Protocol: HTTP
```

## Profilage Radius pour les ensembles de politiques avancés dans Cisco ISE

Lorsque le profilage RADIUS est activé, le WLC transfère les informations de profilage à l'ISE. Sur la base de ces informations, il est possible de créer des règles d'authentification et d'autorisation avancées.

Cet article ne couvre pas la configuration ISE. Pour plus d'informations, reportez-vous au <u>Guide</u> <u>de conception de profilage Cisco ISE</u>.

Ce flux de travail nécessite généralement l'utilisation de CoA, donc assurez-vous qu'il est activé sur le WLC 9800.

## Profilage dans les déploiements FlexConnect

## Authentification centrale, Commutation locale

Dans cette configuration, le profilage local et le profilage RADIUS continuent de fonctionner exactement comme décrit dans les chapitres précédents. Si le point d'accès passe en mode autonome (le point d'accès perd la connexion au WLC), le profilage de périphérique cesse de fonctionner et aucun nouveau client ne peut se connecter.

#### Authentification locale, Commutation locale

Si AP est en mode connecté (AP joint au WLC), le profilage continue à fonctionner (AP envoie une copie des paquets DHCP client au WLC pour effectuer le processus de profilage).

Bien que le profilage fonctionne, étant donné que l'authentification est effectuée localement sur le point d'accès, les informations de profilage ne peuvent pas être utilisées pour une configuration de stratégie locale ou des règles de profilage RADIUS.

## Dépannage

#### **Traces radioactives**

La façon la plus simple de dépanner le profilage client sur le WLC est via des traces radioactives. Accédez à **Troubleshooting > Radioactive Trace**, entrez l'adresse MAC de la carte sans fil cliente et cliquez sur Start :

#### Troubleshooting \* > Radioactive Trace

Co	nditional Debug Global Stat	te: Started	
+	Add × Delete	Start	
	MAC/IP Address	Trace file	
	74da.38f6.76f0	debugTrace_74da.38f6.76f0.txt 📥	► Generate
н	< 1 ⊨ ⊨ 20	<ul> <li>items per page</li> </ul>	1 - 1 of 1 items

Connectez le client au réseau et attendez qu'il atteigne l'état d'exécution. Arrêtez les traces et cliquez sur **Generate**. Assurez-vous que les journaux internes sont activés (cette option n'existe que dans les versions 17.1.1 et ultérieures) :

Enter time interval		×
Enable Internal Logs		
Generate logs for last	10 minutes	
	O 30 minutes	
	O 1 hour	
	O since last boot	
	O 0-4294967295 seconds •	
	<u></u>	
Cancel	Apply to Device	

Des extraits pertinents de la trace radioactive sont disponibles ci-dessous :

Client profilé par WLC comme Microsoft-Workstation :

```
2020/06/18 10:46:41.052366 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (info):
[74da.38f6.76f0:capwap_9000004] Device type for the session is detected as Microsoft-
Workstation and old device-type not classified earlier &Device name for the session is detected
as MSFT 5.0 and old device-name not classified earlier & Old protocol map 0 and new is 41
2020/06/18 10:46:41.052367 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (debug):
[74da.38f6.76f0:capwap_9000004] updating device type Microsoft-Workstation, device name MSFT
5.0
```

Mise en cache WLC de la classification du périphérique :

(debug): [74da.38f6.76f0:unknown] Updating cache for mac [74da.38f6.76f0] device\_type: Microsoft-Workstation, device\_name: MSFT 5.0 user\_role: NULL protocol\_map: 41 WLC recherchant la classification de périphérique dans le cache :

(info): [74da.38f6.76f0:capwap\_90000004] Device type found in cache Microsoft-Workstation WLC appliquant une politique locale basée sur la classification :

(info): device-type filter: Microsoft-Workstation required, Microsoft-Workstation set - match for 74da.38f6.76f0 / 0x9700001A (info): device-type Filter evaluation succeeded (debug): match device-type eq "Microsoft-Workstation" :success WLC envoyant des paquets de comptabilité contenant l'attribut de profilage DHCP et HTTP :

[caaa-acct] [21168]: (debug): [CAAA:ACCT:c9000021] Accounting session created [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap\_90000004] Getting active filter list [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap\_90000004] Found http [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap\_90000004] Found dhcp [aaa-attr-inf] [21168]: (debug): Filter list http-tlv 0 [aaa-attr-inf] [21168]: (debug): Filter list dhcp-option 0

[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-profile-name 0 "Microsoft-Workstation" [aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-name 0 "MSFT 5.0" [aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-class-tag 0 "Workstation:Microsoft-Workstation" [aaa-attr-inf] [21168]: (debug): Get acct attrs dc-certainty-metric 0 10 (0xa) [aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 0c 00 0f 44 45 53 4b 54 4f 50 2d 4b 4c 52 45 30 4d 41 [aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 3c 00 08 4d 53 46 54 20 35 2e 30 [aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 37 00 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 fc

### http profiling sent in a separate accounting packet
[aaa-attr-inf] [21168]: (debug): Get acct attrs http-tlv 0 00 01 00 0e 4d 69 63 72 6f 73 6f 66
74 20 4e 43 53 49

#### Captures de paquets

Dans un déploiement à commutation centrale, les captures de paquets peuvent être effectuées sur le WLC lui-même. Accédez à **Troubleshooting > Packet Capture** et créez un nouveau point de capture sur l'une des interfaces qui sont utilisées par ce client.

Il est nécessaire d'avoir une interface SVI sur le VLAN afin d'effectuer la capture sur celui-ci, sinon prendre la capture sur le port physique lui-même

Troubleshooting * > Packet Capture	
AAT NOT DOOR	
Capture - Name Piterface - Monitor Control Plane - Buffer Size - Filter by - Limit 5	tatus - Action
x x 0 x x 20 + here per page	
Create Packet Capture	*
Capture Name* Cepture	
Filter <sup>4</sup> My +	
Monitor Control Plane 😡	
Buffer Sze (M8)* 10	
Limit by* Duration • 5600 secs -+ 1.00 hour	
Available (4) Selected (1)	
Gigabitithemet1 + Gi Van39	•
C Ggebittmened +	
Gigabit(memet)	
e Vari +	
D Cancel	te l

### 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.