Exemple de configuration du portail captif DNA Spaces avec contrôleur AireOS

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Configurer Diagramme du réseau Configurations Connectez le WLC à Cisco DNA Spaces Créer le SSID sur les espaces DNA Configuration ACL sur le contrôleur Portail captif sans serveur RADIUS sur les espaces DNA Portail captif avec serveur RADIUS sur les espaces DNA Créez le portail sur DNA Spaces Configuration des règles du portail captif sur les espaces DNA Vérifier Dépannage

Introduction

Ce document décrit comment configurer des portails captifs à l'aide de Cisco DNA Spaces avec un contrôleur AireOS.

Contribution de Andres Silva Ingénieur du centre d'assistance technique Cisco

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès aux contrôleurs sans fil via l'interface de ligne de commande ou l'interface utilisateur graphique
- Espaces Cisco DNA

Composants utilisés

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

Contrôleur LAN sans fil 5520 version 8.10.12.0

Configurer

Diagramme du réseau



Configurations

Connectez le WLC à Cisco DNA Spaces

Le contrôleur doit être connecté à DNA Spaces à l'aide de l'une des configurations disponibles, Direct Connect, via DNA Spaces Connector ou à l'aide de CMX Tethering.

Dans cet exemple, l'option Connexion directe est utilisée, bien que les portails captifs soient configurés de la même manière pour toutes les configurations.

Pour connecter le contrôleur à Cisco DNA Spaces, il doit pouvoir accéder au cloud Cisco DNA Spaces via HTTPS. Pour plus d'informations sur la façon de connecter le contrôleur à des espaces DNA, référez-vous à ce lien : <u>Exemple de configuration de connexion directe des espaces DNA</u>

Étape 1. Cliquez sur Captive Portals dans le tableau de bord de DNA Spaces :



Étape 2. Ouvrez le menu du portail captif en cliquant sur l'icône des trois lignes dans le coin supérieur gauche de la page, puis cliquez sur **SSID** :

⊕ + 0 e	C A Hard And And And And And And And And And An	- U d i i
Cisco DNA Sp	paces	C sure
D Partiel		
🐨 Caption Portal Ru 🕈 55654	200 2010	ImpartiConfigure 550
A therefore		

Étape 3. Cliquez sur **Import/Configure SSID**, sélectionnez **CUWN (CMX/WLC)** comme type de « réseau sans fil » et entrez le nom SSID :



Configuration ACL sur le contrôleur

Une ACL de pré-authentification est requise car il s'agit d'un SSID d'authentification Web, et dès que le périphérique sans fil se connecte au SSID et reçoit une adresse IP, l'état du gestionnaire de politiques du périphérique passe à l'état **Webauth_Reqd** et l'ACL est appliquée à la session client pour restreindre les ressources que le périphérique peut atteindre.

Étape 1. Accédez à **Security > Access Control Lists > Access Control Lists**, cliquez sur **New** et configurez les règles pour autoriser la communication entre les clients sans fil et les espaces DNA comme suit. Remplacez les adresses IP par celles fournies par les espaces DNA pour le compte utilisé :

Gen	eral									
Acces	s List Name	DNASpec	es-ACL							
Deny	Counters	٥								
Seq	Action	Source IP/Hask	Destination IP/Mask	Protocol	Source Port	Deat Port	OSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 /	34.235.248.212	TCP	Any	HTTPS	Any	Any	0	•
2	Permit	34.235.248.212 /	0.0.0.0	TCP	HTTPS	Any	Any	Any	0	
1	Permit	0.0.0.0 /	52.55.235.39 /	Any	Any	Any	Any	Any	0	•
4	Permit	\$2.55.235.39 / 255.255.255.255	0.0.0.0	TCP	HTTPS	Any	Any	Any	0	•

Remarque : pour obtenir les adresses IP des espaces DNA autorisés dans la liste de contrôle d'accès, cliquez sur l'option **Configure Manually (Configurer manuellement)** du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces (Créer le SSID sur les espaces DNA)** sous la section ACL configuration.

Le SSID peut être configuré pour utiliser un serveur RADIUS ou non. Si la durée de session, la limite de bande passante ou la configuration transparente d'Internet est configurée dans la section **Actions** de la configuration de la règle du portail captif, le SSID doit être configuré avec un serveur RADIUS, sinon, il n'est pas nécessaire d'utiliser le serveur RADIUS. Tous les types de portails sur les espaces ADN sont pris en charge sur les deux configurations.

Portail captif sans serveur RADIUS sur les espaces DNA

Configuration SSID sur le contrôleur

Étape 1. Accédez à WLAN > WLANs. Créez un nouveau WLAN. Configurez le nom de profil et le SSID. Assurez-vous que le nom SSID est le même que celui configuré à l'étape 3 de la section **Créer le SSID sur des espaces d'ADN.**

cisco	HONETON	WLANG C	CATROLIZE WORDLESS	SECURITY HANAGEMENT	COMMANDS HELP	TEDBACK	
WLANs	WLANs						
WLANA WLANA	Correct Filte	n None	(Change Filter)	(Dear Filter)		Create New	
> Advanced	O WLAN 20	Type	Profile Name	WLAN SSOD	Admin Status	Security Policies	
	01	WUM	.440	.AND	Brabled	[MPA2][Auth(P9A]]	

Étape 2. Configurer la sécurité de couche 2 Accédez à l'onglet **Security > Layer 2** dans l'onglet WLAN configuration et sélectionnez **None** dans le menu déroulant de Layer 2 Security. Vérifiez que le filtrage MAC est désactivé.

uludu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 🐔 None 🖸
	MAC Filtering 2
	OWE Transition Mode
	Fast Transition Adaptive
	Over the DS
	Reassociation Timeout 20 Seconds

Étape 3. Configurer la sécurité de couche 3 Accédez à l'onglet Security > Layer 3 dans l'onglet WLAN configuration, configure Web **Policy as the Layer 3 security method, Enable Passthrough, configure the preauthentication ACL, enable Override Global Config as set the Web Auth Type as External,** configure the Redirect URL.

cisco	MONITOR MERRY CONTROLLER WORKLISS SECURITY HANAGEMENT COMMANDS HELP REEDMACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANS WLANS	General Security QeS Policy-Mapping Advanced
> Advanced	Laser 3 fecunity web Pairsy Captive Relevant Topers Inc. Captive Relevant Topers Inc. Captive Relevant Captive Relev
	Or Cade Sources Redirect URL https://vplash.dooppoorci.ls/pl/meenant3 Email Input Seeping Cleat Enable Seeping Cleat Enable Overmite Source Config ²¹ Enable Web-Auth type External (Re-direct to external server)

Remarque : pour obtenir l'URL de redirection, cliquez sur l'option **Configure Manually**, à partir du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces**, sous la section SSID configuration.

Portail captif avec serveur RADIUS sur les espaces DNA

Remarque : le serveur RADIUS DNA Spaces prend uniquement en charge l'authentification PAP provenant du contrôleur.

Configuration des serveurs RADIUS sur le contrôleur

Étape 1. Accédez à **Security > AAA > RADIUS > Authentication,** cliquez sur **New** et entrez les informations du serveur RADIUS. Cisco DNA Spaces joue le rôle de serveur RADIUS pour

l'authentification des utilisateurs et peut répondre sur deux adresses IP. Configurez les deux serveurs RADIUS :

cisco	BONITOR	HEARS (ONTROLL	IR WORKLESS	SECURITY IN	INAGEMENT	COMMUNICS	ни	REDMOX			
Security	RADIUS	Authentica	tion Ser	vers								
General • RADIO/S	Auto Cal	led Station 10 Key Wrap	her (d	P MAC Address 5 Designed for F2PS	ISID	ires a key write	compliant Audit	US serve	n			
Accounting Auth Cachad Users Fallback DNS	MAC Dwi Pramed	imitar MTU		typhan 100	1							
Downloaded AVP + TACACE+	Natiwork User	Management	Tunnel Prony	Server Index Be	erver Address(3pv4	(Tavel)		Part	1Pfec	Admin 9	latus	
LOAP		0		1 34	1.197.146.105			1812	Disabled	Enabled		
Locar Net Users				2 34	228.1.95			1812	Disabled	Enabled	1	

Remarque : pour obtenir l'adresse IP et la clé secrète RADIUS pour les serveurs principal et secondaire, cliquez sur l'option **Configure Manually** du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces** et accédez à la section **RADIUS Server Configuration**.

Étape 2. Configurez le serveur RADIUS de gestion des comptes. Accédez à **Security > AAA > RADIUS > Accounting** et cliquez sur **New**. Configurez les deux mêmes serveurs RADIUS :

cisco	HONETON	WLANS O	ONTROLL	ER WJRELESS	SECURITY MANA	аемент	COMMANDS	HE /	TEDMAX		
Security	RADIUS	Accounting	Server	8							
• AAA General • RADUIS Authentication Accounting Authorithed Users	Ant Cal MAC De AP Even	ind Station ID Ty Instar In Accounting	en 13 13 0	lystem MAC Addr typhen Enable	•••						
Palback Deck	Network Unar	Management	Tunnel Prezy	Server Index	Server Address(Spr4	(/tpv6)	- г	Port	1Pliec	Admin Status	1
Downloaded #179				1	34.107.146.105			1813	Orabled	Enabled	
TREACE+ LOAP				2	34.228.1.95	_	L	1813	Oxabled	Drabled	•

Configuration SSID sur le contrôleur

Important : avant de commencer la configuration SSID, assurez-vous que l'**authentification Web Radius** est définie sur « PAP » sous Controller > General.

Étape 1. Accédez à WLAN > WLANs. Créez un nouveau WLAN. Configurez le nom de profil et le SSID. Assurez-vous que le nom SSID est le même que celui configuré à l'étape 3 de la section **Créer le SSID sur des espaces d'ADN.**

cisco	HONETON	elans o	ONTROLLER WIRELESS	SECURITY HEMAGEMENT	COMMANDS HELP	TEDBACK	
WLANs	WLANs						
WLANS WLANS	Correct Filter	n Nore	(Change Filter)	(Coar filter)		Crante Now	
> Advanced	O WLAN DO	Type	Profile Name	WLAN SSO	Admin Status	Security Policies	
	01	WSAN	JAND	.440	tratied	[MPA2][Autr(P9A]]	

Étape 2. Configurer la sécurité de couche 2 Accédez à l'onglet **Security > Layer 2** dans l'onglet WLAN configuration. Configurez la sécurité de couche 2 sur **Aucun**. Activez le filtrage Mac.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 4 None C MAC Filtering 2 C
	OWE Transition Mode
	Fast Transition Adaptive Over the DS Image: Comparison of the second se

Étape 3. Configurer la sécurité de couche 3 Accédez à l'onglet Security > Layer 3 dans l'onglet WLAN configuration, configure Web **Policy as the Layer 3 security method, Enable On Mac Filter failure, configure the preauthentication ACL, enable Override Global Config as set the Web Auth Type as External, configure the Redirect URL.**

cisco	MONITOR MLANI CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANOS HELP (REDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANs MUNNs F Advanced	General Security QoS Policy-Happing Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security vectoris
	Capitha Nataarik Aasiatani Bypans Piere B Authonitication Peanthrough Canditional Web Redirect Splanh Page Web Rodirect
	Presedimentication ACL IP+4 DIARSpectre ACL I IP+4 Term II WebAuth Flex IP+4 Ad Norm II WebAuth Flex IP+5 Ad Norm II Redirect UAL Https://spicol.dnospects.in/p3/movemt3 Simping Client Auto Authenticate III Enable Simping Client Auto Authenticate III Enable
	Override Global ConfigM 2 Endle Web Auth type External(Re-direct to external server)

Étape 4. Configurer des serveurs AAA Accédez à l'onglet **Security > AAA Servers** dans l'onglet WLAN configuration, activez **Authentication Servers** and **Accounting Servers** et dans le menu déroulant choisissez les deux serveurs RADIUS :

cisco	HONITOR MLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEBAA	×
WLANs	WLANs > Edit 'AireOS-DNASpaces'	
WLANS	General Security QoS Policy-Mapping Advanced	
+ Advanced	Layer 2 Layer 3 AAA Servers	
	RADIUS Servers RADIUS Server Overante Interface Enabled Apply Cisco 19E Default Settings Enabled Authentication Servers Accounting Servers	
	C Enabled C Enabled	
	Server 1 IP:34.197.146.105, Port:1812 DP:34.197.146.105, Port:1813	
	Server 2 19:34.228.1.95, Port:1812 🚦 19:34.228.1.95, Port:1813 🔒	
	Server 3 None O None O	
	Server 4 None 📴 None 📴	
	Server 5 None 0	
	Server 6 None 0	

Étape 6. Configurez l'ordre de priorité d'authentification pour les utilisateurs Web-auth. Accédez à l'onglet Security > AAA Servers dans l'onglet WLAN configuration, et définissez RADIUS en premier dans l'ordre.

MONITOR MI	ANS CON	TROLLER	wpetess	SECURITY	MANAGEMEN	T COMMANDS	HELP	TEEDBACK
WLANs > Ed	it 'AireO	S-DNASp	aces'					
General PADEUS Aut Authentic LDAP Server Server 1 Server 2 Server 3 Lecal EAP A Lecal EAP	Security Anntication ation Survival re None C None C None C None C Authentication Authentication ation prior Not Used	QoS Sarvivabili biity in Endbi ity order	Policy-Hap; hy	th user	Vanced	Used For Author RADUS	tication	Up
	WLANS > Ed General RADOUS Ant Authentic Server 1 Server 2 Server 3 Lecal EAP A Local EAP Authentic	WLANS > Edit 'AireO WLANS > Edit 'AireO General Security EADCUS Authentication Authentication Survival LDAP Servers Server 1 None S Server 2 None S Server 3 None S Local EAP Authentication Local EAP Authentication Local EAP Authentication Not Used	Solition WDAs Connector WLANs > Edit 'AireOS-DNASp General Security QoS RADCUS Authentication Survivability LDAP Servers Server 1 None Server 2 None Server 3 None Local EAP Authentication Local EAP Authentication Local EAP Authentication Enable Authentication priority order Net Used	Solution WLANS > Edit 'AlreOS-DNASpaces' General Security QoS Policy-Map; BADEUS Authentication Survivability Image: Control of the security Banyor 1 None Survivability Server 2 None Survivability Server 3 None Survivability Local EAP Authentication Enabled Authentication priority order for web-authentication Net Used	Solverow MUANS Contraction Speciality WLANS > Edit 'AlreOS-DNASpaces' General Security QoS Policy-Mapping Ad BADEUS Authentication Survivability Authentication Ad Authentication Survivability BADEUS Addentication Server 1 None Server 3 Server 3 Server 3 None Server 4 Server 5 Local EAP Authentication Enabled Authentication priority order for web-auth user Net Used 2 Server 5 Server 6	Soletok MARS Connocitek Marcels WLANs > Edit 'AlreOS-DNASpaces' General Security QoS Policy-Mapping Advanced Authentication Servirability	Solariok BLANS Connection Package WLANs > Edit 'AireOS-DNASpaces' General Security QoS Policy-Mapping Advanced MADEUS Authentication Servivability	Solariok MUAS Control Link Policy-Mapping Advanced WLANs > Edit 'AlreOS-DNASpaces' General Security QoS Policy-Mapping Advanced MUDUS Authentication Survivability

Étape 7. Accédez à l'onglet **Advanced** dans l'onglet WLAN configuration et activez **Allow AAA Override.**

altalta cisco	MONITOR MLANI CONTROLLER WIRELESS SECURITY MANAGEMEN	NT COMMANDS HELP (TEDBACK
WLANs	WLANs > Edit 'AireOS-ONASpaces'	
* WLANs MLANs	General Security QoS Policy-Mapping Advanced	
> Advanced	Allow AAA Overvide 🛛 Enabled	DIRCP
	Coverage Hele Detection 👩 Enabled	DRCP Server Override
	Enable Session Timesut Session Timeout (secc)	DRCP Addr. Ansignment C Required
	Aronet II Clinabled	Management Frame Protection (MFP)
	Diagnostic Charvel 4 Citabled Override Interface IIC; 2Pvt None 2 2Pv6 None 2 Larve? Ad None 2	MIP Cleat Protection f Optional B
	URL ACL None C P2P Backing Attion Deated Claret Exclusion 7 Claret Section (1997)	803.114(h (1 - 255) 3 803.155(y/n (1 - 255) 1 NAC
	Maximum Allowed Clients	NHC State None
	Static P Turneling 44 Enabled W-H Orwalt Clants Policy Disabled	Olert Load Balancing Olert Band Select

Étape 1. Cliquez sur Captive Portals dans le tableau de bord de DNA Spaces :

ACT - Leverage Digitization toolkits t	o Act on Insights.
Captive Portals	Engagements 1
Onboard and acquire visitors at your properties	Delver contextual multi-channel notifications
1	0

Étape 2. Cliquez sur **Create New**, entrez le nom du portail et sélectionnez les emplacements qui peuvent utiliser le portail :

	0			
	Portal Information	Authentication	Data Dapture	User Agreement
PORTAL NAME				
AirwOS-ONASpaces				
 Enable this portal for all location 	ions .			
Enable this portal for all locals	kes .		Faircin	Al ocations
Endle this portal for all local Location Hierarchy	ion		Selecto	d Locations
Endle this potal for all local Location Herarchy MEX-EAST-1	ion		Selecter	d Locations
	ken		Selecter	d Locations Inclument X
	brs Dr		Selecter Hazo-14	dilucations (sections) ×
	br br		Stiector	dilocations becaused x

Étape 3. Sélectionnez le type d'authentification, choisissez si vous souhaitez afficher la capture de données et les accords utilisateur sur la page d'accueil du portail et si les utilisateurs sont autorisés à s'inscrire pour recevoir un message. Cliquez sur **Suivant** :

o	<u> </u>		•	
Panal Internation	Autoritation	Own-Captern	the Apendonia	
BLC TE ATHRONOL 195		-		
Enal		4		
Approximative solution that analog access the internet.		-		
Display Authentication and User Agreements on partial home page				
Allow-users to Opt in to receive message				
	500	Day Next 1		

Étape 4. Configurez les éléments de capture de données. Si vous voulez capturer des données des utilisateurs, cochez la case **Enable Data Capture** et cliquez sur **+Add Field Element** pour

ajouter les champs désirés. Cliquez sur Suivant :

	Paral Internation	Alternation	-O Inclusion	4 See Aparters	×
E Ender Date Cartore					_
Furn Falls				+ Add Field Dement	
A Lathers					:
		500	6 Page 1		

Étape 5. Cochez la case Enable Terms & Conditions et cliquez sur Save & Configure Portal :

	0			o)
	Paral Internation	Automiculary	Date Capture	the spectrum	
To portion place any to english and portform To	mail Condition and Princip and	to Taxanto			
Inderferte Landton					
CARD & LEND YOR MESSAGE					() English
0.0.0.0.11.0.0.0.0	9.0.8				
8 J 8 6 6 8 K [L D 1 1	in sin a set	이 아이는 것 같아요. 한 것 같아요.	000		
System - + Format - + Fort + 8	In 1.1 (A) (B) [H [H])				
M.F. Sensor Line, Last-antided Stationary 17, 1	10.1.				
Taxa M.J. Serie & Southers (Miles the Mill)	here a subsection with the William (1)	the man and used in Mall an	nim.		
Description of the Description	and designed as a result.	and been loss and a second			
	in the second				
or posted using the literature is annum that users on	nyiy with it was the fit of the sampler it	to be, as a contrary process, posed	kola mi	and the fit beings is seening of all the to	and over any president recorded, record
		See Etw	Sava & Contigues Parial		

Étape 6. Modifiez le portail si nécessaire, cliquez sur Enregistrer :

Partial - AlreoD-DBMAgeness / concess Taxable / Beat / Beat /	nn indiana Philipping	0 2 Superstant N. 199
Constant of the second of configure Constant of the second of configure Constant of the second of the		Normal Prevalue Ciscos Systemas Wotome-to-Splorations Graphic the true bases to connect to internet (maint) Difference D
AM Make		
	Corr Carve	

Configuration des règles du portail captif sur les espaces DNA

Étape 1. Ouvrez le menu du portail captif et cliquez sur Règles du portail captif :

⊖ → ♂ ☆	A https://dnaspaces.io/captiveportal/hules/captive-portal	
Cisco DNA Space	5	
D Portal		
E Captive Portal Rules		Created
ङ \$\$D\$		Feb 24, 2020
A Reports	>	○ 8.02 PM

Étape 2. Cliquez sur + Créer une règle. Entrez le nom de la règle, choisissez le SSID précédemment configuré et sélectionnez les emplacements pour lesquels cette règle de portail est disponible :

Onara Captue Ponal Rule III.1 (Auto Dialityeen	
seen wil os es os per observa per Mich a fera con pessa.	
	DUMMANY
Milen a user is on VIII - and connected to Awd0-dfWdpacer -	211 Mar
	stw01-Oatlgaren
UDC/FIDHS - When do you want the rule to fin?	NAME.
	When your is an INFL and summaried to firm?
At any of the following locations	1004004
+ detri analizza	For all locations under
	1000-1 Own/Gammer
Hate + development ×	wateria
	ID-HDail
Plan by Middale Artise the over location and by including or evaluating locations by metalogs	
	4C101
	Draw Capition Partial

Étape 3. Sélectionnez l'action du portail captif. Dans ce cas, lorsque la règle est activée, le portail s'affiche. Cliquez sur **Enregistrer et publier.**

C1045	A19976
Show Daprise Partial Decise a Partial to dispuped to Users when they connectify the with	50404.E
AtreCS-DRADpains -	ADDN
Section Duration	Pertal : An/OS-ON/Opecies
Swowdhittee	
Searchearly Providen Internet Directly providen internet without allowing any suff writedate	
Carry Internet Stay area from anomaling the Internet	
Tage there uses as	
(+ Ani hup)	
C Toger AT	
Seen & Publich Seen	

Vérifier

Pour confirmer l'état d'un client connecté au SSID, accédez à **Monitor > Clients**, cliquez sur l'adresse MAC et recherchez Policy Manager State :

BONILLOW M.	LAN	CONTROLLER	WPIELESS	SECORITY	HANAGEMENT	COMMANDS	HELP.	EEDBACK	
Clients > Detail									< Back
Max Number o	f Record	Is 10 * CB	ar AVC Stats	1					
General	AVC S	tatistics							
						AP radio alo	e 1d	1	
Client Type		Regular				WLAN Profil		AireOS-OMASpaces	
Client Tunne	el Type	Simple IP				WLAN SSID		AireOS-ONASpeces	
User Name						Status		Associated	
Webauth Us	er Name	None				Association	10	1	
Port Numbe	e	1				802.11 Aut	hentication	Open System	
Diterface		management				Reason Cod	e .	1	
VLAN ID		20				Status Code		0	
Quarantine	VLAN ID	0				CF Pollable		Not Implemented	
CCX Version		Not Supported				CF Pull Reg.	rest.	Not Implemented	
E2E Version		Not Supported				Short Pream	-ble	Not Emplemented	
Mobility Rol		Local				PBCC		Not Emplemented	
Hobility Pee	er IP	N/A				Chernel Age	iky	Not Implemented	
Mobility Mo	ve Count	0				Timeout		0	
Pelicy Hara	Q67	RUN				WEP State		WEP Disable	

Dépannage

La commande suivante peut être activée dans le contrôleur avant le test pour confirmer le processus d'association et d'authentification du client.

```
(5520-Andressi) >debug client
```

(5520-Andressi) >debug web-auth redirect enable mac

Voici le résultat d'une tentative réussie d'identification de chacune des phases au cours du processus d'association/d'authentification lors de la connexion à un SSID sans serveur RADIUS :

Association/authentification 802.11 :

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

Authentification DHCP et de couche 3 :

*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68

user_agent = AnyConnect Agent 4.7.04056 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to configured Web-Auth type *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual IP, using virtual IP =192.0.2.1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN ID:1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using URL:https://splash.dnaspaces.io/p2/mexeast1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio), redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"</pre> content="no-cache"><META http-equiv="Pragma" content="</pre> *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is HTTP/1.1 200 OK Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34: *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-Url:https://splash.dnaspaces.io/p2/mexeast1 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send Authentification de couche 3 réussie, déplacez le client à l'état d'exécution :

*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255, URL ACL ID 255, URL ACL
Action 0)

*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user

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.