Configurer l'affectation de VLAN dynamique avec des WLC basés sur la carte de groupe ISE vers Active Directory

Table des matières

 Introduction

 Conditions préalables

 Exigences

 Composants utilisés

 Conventions

 Affectation de VLAN dynamique avec le serveur RADIUS

 Corrigurer

 Diagramme du réseau

 Configurations

 Intégration et configuration ISE à AD des stratégies d'authentification et d'autorisation pour les utilisateurs sur ISE

 Configuration WLC pour prendre en charge l'authentification dot1x et le remplacement AAA pour le SID 'office hg'

 Vérifier

 Dépannage

Introduction

Ce document décrit le concept d'affectation dynamique de VLAN.

Conditions préalables

Le document décrit comment configurer le contrôleur LAN sans fil (WLC) et le serveur ISE (Identity Services Engine) afin d'attribuer dynamiquement des clients LAN sans fil (WLAN) dans un VLAN spécifique.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base des contrôleurs LAN sans fil (WLC) et des points d'accès légers (LAP)
- Connaissance fonctionnelle d'un serveur d'authentification, d'autorisation et de comptabilité (AAA) tel qu'un ISE

- Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité sans fil
- Connaissance fonctionnelle et configurable de l'attribution dynamique de VLAN
- Compréhension de base des services Microsoft Windows AD, ainsi que des concepts de contrôleur de domaine et DNS
- Connaissance de base du protocole CAPWAP (Control And Provisioning of Access Point Protocol)

Composants utilisés

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

- WLC de la gamme Cisco 5520 qui exécute la version de microprogramme 8.8.11.0
- AP de la gamme Cisco 4800
- Demandeur Windows natif et NAM Anyconnect
- Cisco Secure ISE version 2.3.0.298
- Microsoft Windows 2016 Server configuré comme contrôleur de domaine
- Commutateur de la gamme Cisco 3560-CX qui exécute la version 15.2(4)E1

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Affectation de VLAN dynamique avec le serveur RADIUS

Dans la plupart des systèmes WLAN, chaque WLAN a une stratégie statique qui s'applique à tous les clients associés à un SSID (Service Set Identifier), ou WLAN dans la terminologie du contrôleur. Bien que puissante, cette méthode a des limitations parce qu'elle exige que les clients soient associés à des SSID différents afin d'hériter de QoS et de stratégies de sécurité différentes.

La solution WLAN de Cisco résout cette limitation en prenant en charge la mise en réseau des identités. Cela permet au réseau d'annoncer un SSID unique, mais permet à des utilisateurs spécifiques d'hériter de différentes qualités de service, attributs VLAN et/ou stratégies de sécurité en fonction des informations d'identification de l'utilisateur.

L'affectation de VLAN dynamique est une fonction qui place un utilisateur sans fil dans un VLAN spécifique en fonction des informations fournies par l'utilisateur. Cette tâche d'affectation d'utilisateurs à un VLAN spécifique est gérée par un serveur d'authentification RADIUS, tel que Cisco ISE. Ceci peut être utilisé, par exemple, afin de permettre à l'hôte sans fil de rester sur le même VLAN lorsqu'il se déplace au sein d'un réseau de campus.

Le serveur Cisco ISE authentifie les utilisateurs sans fil par rapport à l'une des bases de données possibles, qui inclut sa base de données interne. Exemple :

- Base de données interne
- Active Directory
- Protocole LDAP (Generic Lightweight Directory Access Protocol)
- Bases de données relationnelles compatibles ODBC (Open Database Connectivity)
- Serveurs à jetons SecurID Rivest, Shamir et Adelman (RSA)
- Serveurs de jetons compatibles RADIUS

Les protocoles d'authentification Cisco ISE et les sources d'identité externes prises en charge répertorient les différents protocoles d'authentification pris en charge par les bases de données internes et externes ISE.

Ce document se concentre sur l'authentification des utilisateurs sans fil qui utilisent la base de données externe Windows Active Directory.

Après une authentification réussie, ISE récupère les informations de groupe de cet utilisateur dans la base de données Windows et associe l'utilisateur au profil d'autorisation correspondant.

Lorsqu'un client tente de s'associer à un LAP enregistré auprès d'un contrôleur, le LAP transmet les informations d'identification de l'utilisateur au WLC à l'aide de la méthode EAP respective.

WLC envoie ces informations d'identification à ISE avec l'utilisation du protocole RADIUS (encapsulation de l'EAP) et ISE transmet les informations d'identification des utilisateurs à AD pour validation avec l'aide du protocole KERBEROS.

AD valide les informations d'identification de l'utilisateur et, après authentification réussie, informe l'ISE.

Une fois l'authentification réussie, le serveur ISE transmet certains attributs IETF (Internet Engineering Task Force) au WLC. Ces attributs RADIUS déterminent l'ID de VLAN qui doit être attribué au client sans fil. Le SSID (WLAN, en termes de WLC) du client n'importe pas parce que l'utilisateur est toujours affecté à cet ID de VLAN prédéterminé.

Les attributs d'utilisateur RADIUS utilisés pour l'affectation de l'ID de VLAN sont :

• IETF 64 (type de tunnel)—Définissez cette valeur sur VLAN

- IETF 65 (Tunnel Medium Type)—Définissez cette valeur sur 802
- IETF 81 (ID de groupe privé de tunnel)—Définissez cette valeur sur ID de VLAN

L'ID de VLAN est de 12 bits et prend une valeur comprise entre 1 et 4094 inclus. Étant donné que l'ID de groupe privé de tunnel est de type chaîne, comme défini dans RFC2868 pour une utilisation avec IEEE 802.1X, la valeur entière de l'ID de VLAN est codée sous la forme d'une chaîne. Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.

Comme indiqué dans la <u>RFC 2868</u>, section 3.1 : le champ Tag a une longueur d'un octet et est destiné à fournir un moyen de regrouper des attributs dans le même paquet qui font référence au même tunnel. Les valeurs valides pour cette zone sont comprises entre 0x01 et 0x1F, inclus. Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00). Référez-vous à <u>RFC 2868</u> pour plus d'informations sur tous les attributs RADIUS.

Configurer

Cette section fournit les informations nécessaires à la configuration des fonctions décrites dans le document.

Diagramme du réseau



Configurations

Voici les détails de configuration des composants utilisés dans ce diagramme :

- L'adresse IP du serveur ISE (RADIUS) est 10.48.39.128.
- L'adresse d'interface de gestion et de gestionnaire AP du WLC est 10.48.71.20.
- Le serveur DHCP réside sur le réseau local et est configuré pour les pools de clients respectifs ; il n'est pas représenté sur le schéma.
- Les VLAN1477 et VLAN1478 sont utilisés tout au long de cette configuration. Les utilisateurs du service Marketing sont configurés pour être placés dans le VLAN1477 et les utilisateurs du service RH sont configurés pour être placés dans le VLAN1478 par le serveur RADIUS Lorsque les deux utilisateurs se connectent au même SSID : office_hq.

VLAN1477 : 192.168.77.0/24. Passerelle : 192.168.77.1 VLAN148 : 192.168.78.0/24. Passerelle : 192.168.78.1

• Ce document utilise 802.1x avecPEAP-mschapv2comme mécanisme de sécurité.



Remarque : Cisco recommande d'utiliser des méthodes d'authentification avancées, telles que l'authentification EAP-FAST et EAP-TLS, afin de sécuriser le WLAN.

Les hypothèses suivantes sont faites avant d'effectuer cette configuration :

- Le LAP est déjà enregistré auprès du WLC
- Une étendue DHCP est attribuée au serveur DHCP
- La connectivité de couche 3 existe entre tous les périphériques du réseau
- Le document traite de la configuration requise du côté sans fil et suppose que le réseau câblé est en place
- Les utilisateurs et les groupes respectifs sont configurés sur Active Directory

Afin d'effectuer l'affectation de VLAN dynamique avec des WLC basés sur le mappage de groupe ISE à AD, ces étapes doivent être effectuées :

- 1. Intégration et configuration ISE à AD des politiques d'authentification et d'autorisation pour les utilisateurs sur ISE.
- 2. Configuration WLC afin de prendre en charge l'authentification dot1x et le remplacement AAA pour SSID 'office_hq'.
- 3. Configuration du demandeur du client final.

Intégration et configuration ISE à AD des stratégies d'authentification et d'autorisation pour les utilisateurs sur ISE

- 1. Connectez-vous à l'interface utilisateur Web ISE à l'aide d'un compte admin.
- $\label{eq:alpha} 2. \ Accédez \ \grave{a} \ Administration > \ Identity \ management > \ External \ Identity \ Sources > \ Active \ directory.$



3. Cliquez sur Ajouter et entrez le nom de domaine et le nom du magasin d'identités à partir des paramètres de nom du point de jonction Active Directory. Dans l'exemple, ISE est enregistré dans le domainewlaaan.comet le point de jointure est spécifié commeAD.wlaaan.comun nom significatif localement pour ISE.

External Identity Sources		Connection		
(= • ₩ •	÷≩.	* Join Point Name		
Certificate Authentication Profile		Join Foint Name	AD.wiaaan.com	U. U
Cive Directory		 Active Directory Domain 	wlaaan.com	()
EDAP LDAP			L	
CDBC				
RADIUS Token		Cubmit Cancel		
RSA SecurID		Submit Cancel		
SAML Id Providers				
Social Login				

4. Une fenêtre contextuelle s'ouvre une foissubmitque vous avez appuyé sur le bouton pour vous demander si vous souhaitez vous connecter immédiatement à ISE et à AD. Appuyez surveset fournissez des informations d'identification d'utilisateur Active Directory avec des droits d'administration pour ajouter un nouvel hôte au domaine.

Connection Whiteliste	d Domains PassiveID	Groups Attributes	Advanced Settings			
Join Point Name AD. Active Directory Domain wla	wlaaan.com aan.com	() ()				
야금 Join 야금 Leave 🤦 Test User 🍯	Diagnostic Tool 🛛 😵 Refresh Table					
ISE Node	▲ ISE Node Role Status	Domain Controller	Site			
rmanchur-ise.wlaaan.com	STANDALONE A Not Joine	d				
Image: manchur-ise.wiaaan.com STANDALONE ▲ Not Joined Join Domain × Please specify the credentials required to Join ISE node(s) to the Active Directory Domain. × * AD User Name ② Administrator * Password • Specify Organizational Unit ③ ● Store Credentials ② ●						

5. Après ce point, vous devez avoir ISE correctement enregistré auprès d'AD.

ernal Identity Sources	Connection Whitelisted Don	ains Passiv	veID Groups	Attributes Advanced	Settings	
Ear Certificate Authentication Profile Active Directory LDAP OnBrc	Join Point Name AD.wlaaan Active Directory Domain wlaaan.c	com		0		
RADIUS Token	9을 Join 9을 Leave 👤 Test User 🕋 Diag	nostic Tool 🛛 🛞 Refre	sh Table			
RSA SecurID	ISE Node	ISE Node Role	Status	Domain Controller	Site	
SAML Id Providers	rmanchur-ise.wlaaan.com	STANDALONE	Operational	WIN-CFA29CSRIL9.wlaaan.com	Default-First-Site-Name	

En cas de problème avec le processus d'enregistrement, vous pouvez utiliser l'Diagnostic

afin d'exécuter les tests requis pour la connectivité AD.

6. Vous devez récupérer les groupes pour les répertoires actifs qui sont utilisés afin d'attribuer des profils d'autorisation respectifs. Accédez àAdministration > Identity management > External Identity Sources

> Active directory >

> Groups

, puis cliquez surAddet choisissezSelect Groups from Active Directory.

→ System Veltertity Management → Network Re	sources	Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
External Identity Sources	Connection Whitelisted Domains PassiveID Groups	Attributes Advanced Settings
	/ Edit Add - X Delete Group Update SID Values	
Certificate Authentication Profile Certificate Authentication Profile Certificate Authentication Profile	Nam Select Groups From Directory Add Group	
🔁 AD.wlaaan.com		No data available
LDAP		
ODBC		
RADIUS Token		
RSA SecurID		
SAML Id Providers		
Social Login		

 Une nouvelle fenêtre contextuelle s'ouvre, dans laquelle vous pouvez spécifier un filtre afin de récupérer des groupes spécifiques ou récupérer tous les groupes à partir d'Active Directory.

Choisissez les groupes respectifs dans la liste des groupes AD et appuyez surok.

Sele	ect Direct	tory Groups					×
THIS	Domair	wlaaan.com	у.	•]		
1	Name Filte	*	SID Filter	*	Type Filter GLOBAL	*	
		Retrieve Groups 13 Groups Retrie	ved.				
	Name			Group SID		Group Type	
	wlaaan.co	om/Users/Cloneable Domain Controlle	ers	S-1-5-21-2222429329-410808516	4-3220345271-522	GLOBAL	
	wlaaan.co	om/Users/DnsUpdateProxy		S-1-5-21-2222429329-410808516	4-3220345271-1102	GLOBAL	
	wlaaan.co	om/Users/Domain Admins		S-1-5-21-2222429329-410808516	4-3220345271-512	GLOBAL	
	wlaaan.co	om/Users/Domain Computers		S-1-5-21-2222429329-410808516	4-3220345271-515	GLOBAL	
	wlaaan.co	om/Users/Domain Controllers		S-1-5-21-2222429329-410808516	4-3220345271-516	GLOBAL	
	wlaaan.co	om/Users/Domain Guests		S-1-5-21-2222429329-410808516	4-3220345271-514	GLOBAL	
	wlaaan.co	om/Users/Domain Users		S-1-5-21-2222429329-410808516	4-3220345271-513	GLOBAL	
	wlaaan.co	om/Users/Group Policy Creator Owne	rs	S-1-5-21-2222429329-410808516	4-3220345271-520	GLOBAL	
\checkmark	wlaaan.co	om/Users/HR		S-1-5-21-2222429329-410808516	4-3220345271-1105	GLOBAL	
	wlaaan.co	om/Users/Key Admins		S-1-5-21-2222429329-410808516	4-3220345271-526	GLOBAL	
\checkmark	wlaaan.co	om/Users/Marketing		S-1-5-21-2222429329-410808516	4-3220345271-1104	GLOBAL	
	wlaaan.co	om/Users/Protected Users		S-1-5-21-2222429329-410808516	4-3220345271-525	GLOBAL	
	wlaaan.co	om/Users/Read-only Domain Control	ers	S-1-5-21-2222429329-410808516	4-3220345271-521	GLOBAL	



8. Les groupes respectifs sont ajoutés à ISE et peuvent être enregistrés. Appuyez sursave.

	Connection	Whitelisted	Domains	PassiveID	Groups	Attributes	Advanced Settings	
/ Edit	Add 🔫	💢 Delete Group	Update SID Values					
	ame			•	SID			
w	laaan.com/Use	ers/HR			S-1-5-21-222242	9329-4108085164-322	0345271-1105	
w	laaan.com/Use	ers/Marketing			S-1-5-21-222242	9329-4108085164-322	0345271-1104	
-	Devet							
Save	Reset							

9. Ajoutez WLC à la liste des périphériques réseau ISE - accédez àAdministration > Network Resources > Network Deviceset appuyez surAdd.

Configuration complète, en fournissant l'adresse IP de gestion WLC et le secret partagé RADIUS entre WLC et ISE.

dentity Service	Bingine Home Context Vability Operations Policy -Administration V Work Centers
F System → Identity N	anagement - Network Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC
Network Devices Network D	twork Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
	0
Network Devices	Network Devices List > New Network Device
Default Device	• Name <u>WIC5520</u>
Device Security Settings	
	IP Address + IP: 10.48.71.20 / 32
	O IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	- Device Prome Eta Lisco + D
	Model Name 📃 👻
	Software Version +
	Network Device Group
	Location LAB S Set To Default
	IPSEC Is IPSEC Device O
	Device Type WLC-tab O Iset To Default
	✓ RADIUS Authentication Settings
	RADIUS UDP Settings
	Protocol RADIUS
	- snareo secret Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings (i)

- 10. Maintenant, après avoir rejoint ISE à AD et ajouté le WLC à la liste des périphériques, vous pouvez commencer la configuration des stratégies d'authentification et d'autorisation pour les utilisateurs.
 - Créez un profil d'autorisation afin d'attribuer des utilisateurs de Marketing à VLAN1477 et du groupe HR à VLAN1478.

Accédez à Policy > Policy Elements > Results > Authorization > Authorization profiles et cliquez sur le boutonAddafin de créer un nouveau profil.

dentity Services Engine H	Iome Context Visibility	Operations	Policy Administration	Work Centers	
Policy Sets Profiling Posture Client	Provisioning Policy Elements				
Dictionaries + Conditions - Results					
G					
Authentication	Standard Authorization	Profiles			
- Authorization	For Policy Export go to Adminis	ration > System > Ba	ickup & Restore > Policy Export	t Page	
Authorization Dealites	/ Edit 🕂 Add 🕞 Duplicat	e 🗙 Delete			
Authorization Profiles	Name		Profile		Description
Downloadable ACLs	Blackhole_Wireless_Acce	55	📸 Cisco 🕀		Default profile used to blacklist wireless de
▶ Profiling	Cisco_IP_Phones		🗰 Cisco 🕀		Default profile used for Cisco Phones.
Posture	Cisco_Temporal_Onboard		🞎 Cisco 🕀		Onboard the device with Cisco temporal ag
	Cisco_WebAuth		📸 Cisco 🕀		Default Profile used to redirect users to the
Client Provisioning	NSP_Onboard		🞎 Cisco 🕀		Onboard the device with Native Supplicant
	Non_Cisco_IP_Phones		諯 Cisco 🕀		Default Profile used for Non Cisco Phones.
	DenyAccess				Default Profile with access type as Access-
	PermitAccess				Default Profile with access type as Access-

 MarketingComplétez la configuration du profil d'autorisation avec les informations VLAN pour le groupe correspondant ; l'exemple montre les paramètres de configuration du groupe.

Dictionaries Conditions Results		
0	Authorization Droffion - Maus Authoritan Reafts	
Authentication	Authorization Profile	
* Authorization	Name Markeung	
Authorization Profiles	Description Marketing	
Downloadable ACLs	* Access Type ACCESS_ACCEPT *	
Profiling	Network Device Profile 🛛 🗰 Cisco 💌 🕀	
▶ Posture	Service Template	
Client Provisioning	Track Movement 🔲 🕧	
-	Passive Identity Tracking 📋 🕡	
	* Common Tacke	
	DACL Name	
	ACL (Filter-ID)	
	SARIHRY CAULA	
	County Gloup	
	VIAN Tao ID 1 Edit Tao ID/Name 1477	
	✓ Advanced Attributes Settings	
	Select an item	
	▼ Attributes Details	
	Access Type = ACCESS_ACCEPT Tunnel-Private-Group-ID = 1:1477	
	Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6	
	Submit Cancel	

Une configuration similaire doit être effectuée pour les autres groupes et les attributs de balise VLAN respectifs doivent être configurés.

 Une fois les profils d'autorisation configurés, vous pouvez définir des stratégies d'authentification pour les utilisateurs sans fil. Pour ce faire, vous pouvez configurerCustomou modifier le jeu de stratégiesDefault. Dans cet exemple, le jeu de stratégies par défaut est modifié. Accédez àPolicy > Policy Sets > Default. dot1xPar défaut pour le type d'authentification, ISE va utiliserAll_User_ID_Stores, bien qu'il fonctionne même avec les paramètres par défaut actuels puisque AD fait partie de la liste de sources d'identité deAll_User_ID_Stores, cet exemple utilise une règle plus spécifiquewLC_labpour ce contrôleur LAB respectif et utilise AD comme seule source pour l'authentification.

						Click here to do wireless setup and visibility setup Do not show th	Nis aga	×.					
cy Sets +	D	efault				Reset		ŝav					
Status	P	olicy Set Name	Descrip	tion	Conditions	Allowed Protocols / Server Sequence	20	HB					
irch													
0	0	lefault	Default p	olicy se		Default Network Access × * +	ł.	0					
Authenticatio	on P	Policy (4)											
+ Statu	5	Rule Name	Condi	tions		Use Hits	Ac	tions					
sarch													
0	0		0.7		Wred_MAB	Internal Endpoints * *		~					
•	_	Weies MA		> Options	_	~							
			ab AND							Wireless_802.1X	AD alaaan.com × *		
/ 0		WLC_lab		F	DEVICE Device Type EQUALS AE Device Types#WLC-lab	Defines 0		۰					
				F	DEVICE Location EQUALS AILLocations#LAB								
0		Denty.			Wred_002.1X	Al_User_ID_Stores * *		~					
			OR		Wireless_802.1X	> Options		~					
0		Data				Al_User_ID_Stores * *		~					
U U		UPINI.				> Options		Ť					
Authorization	n Pa	olicy - Local Exceptions											
Authorization	n Pa	olicy - Global Exceptions											
uthorization	n Po	blicy (12)											

 Vous devez maintenant créer des stratégies d'autorisation pour les utilisateurs qui attribuent des profils d'autorisation respectifs en fonction de l'appartenance au groupe. Accédez à la sectionAuthorization policyet créez des stratégies afin de répondre à cette exigence.

Policy Sea Potling Posture Client Provisioning + Policy Daments						Click here to do wireless setup and visibility setup Do not show this again.				
Policy Sets	→ Default							Reset	Savo	
Statu	as Policy Set Name	Description	Conditions			Allow	ed Protocols / Server S	Sequence	Hits	
Search	Default	Default policy set				Defe	ult Network Access	x.7 +	•	
> Authentica	ation Policy (4)									
> Authorizat	tion Policy - Local Exceptions									
> Authorizat	tion Policy - Global Exceptions									
✓ Authorizat	tion Policy (14)									
• 55	itus Rule Name	Conditions			Results Profiles	Security Groups		Hits	Actions	
Search	Wireless_Marketing	AND E Wreless, Ao	coss om ExternalGroups EQUALS waaan.com/Users/Marketing		× Marketing	Select from list		0	۰	
	Wroless_HR	AND H AD wiseen o	cess com ExternalGroups EQUALS wilaaan.com/Users/HR		(INR)	Select from list	- +	۰	۰	

Configuration WLC pour prendre en charge l'authentification dot1x et le remplacement AAA pour le SSID 'office_hq'

1. Configurez ISE en tant que serveur d'authentification RADIUS sur WLC. Accédez à lasecurity > AAA > RADIUS > Authenticationsection de l'interface utilisateur Web et fournissez l'adresse IP ISE et les informations secrètes partagées.

cisco	MONITOR WLANS CONTRO	ROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication S	Servers > New
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced 	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ISE Default setting Apply Cisco ACA Default setting Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeo Tunnel Proxy PAC Provisioning IPSec Cisco ACA	2 \$ 10.48.39.128 ASCII \$ Image ASCII \$ Image Image (Designed for FIPS customers and requires a key wrap compliant RADIUS server) 1812 Enabled \$ 5 seconds 6 Enable 6 Enable

2. Configurez SSID_{office_hq}sous la sectionwLANssur le WLC ; cet exemple configure SSID avecWPA2/AES+dot1xet AAA override. L'interfaceDummyest choisie pour le WLAN puisque le VLAN approprié est attribué de toute façon via RADIUS. Cette interface fictive doit être créée sur le WLC et recevoir une adresse IP, mais l'adresse IP ne doit pas être valide et le VLAN dans lequel elle est placée ne peut pas être créé dans le commutateur de liaison ascendante de sorte que si aucun VLAN n'est attribué, le client ne peut aller nulle part.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK			
WLANs	WLANs											
VLANs	Current Filter	r: Non	e	[Change Filte	er] [Clear Filter	1				Create	e New 🗘	Go
Advanced	WLAN ID	Туре	Profile Na	me		WLAN SSID		4	Admin Status	Security Policies		
		WLAN	test			test		E	inabled	[WPA2][Auth(802.1X)]		
	□ <u>2</u>	WLAN	AndroidAP			AndroidAP		E	nabled	[WPA2][Auth(PSK)]		
	253	WLAN	BTER-BTwi	fi-public		BTwifi-public		E	nabled	[WPA2][Auth(PSK)]		

cisco	MONITOR	₩LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	ĸ											Home	
WLANs	WLANs >	New																<	Back	`	Apply	
 WLANs WLANs Advanced 	Type Profile Nan SSID ID	ne	office affice 3	an a) a_ha a_ba																		

WL	ANs > Edit 'office_hq	
G	eneral Security Q	oS Policy-Mapping Advanced
	Profile Name Type SSID Status	office_hq WLAN office_hq Imabled
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy Interface/Interface Group(G Multicast Vlan Feature	All dummy Enabled
	Broadcast SSID NAS-ID	Enabled none

WLANs > Edit 'office_hq'

General See	curity QoS	Policy-Map	ping Adva	nced			
Layer 2	ayer 3 AAA Se	ervers					
Layer 2 Secur	rity ⁶ WPA+WPA2 MAC Filtering	÷ +)				
Fast Transition							
Fast Transition Over the DS Reassociation Tin	Ada aneout 20 Seconds	ptive 🕈					
Protected Mana	gement Frame						
PMF	Disa	abled \$					
WPA+WPA2 Pa	rameters						
WPA Policy							
WPA2 Policy	V						
WPA2 Encrypt	tion 🗸 🗹 AES	5 TKIP	CCMP256	GCMP128	GCMP256		
OSEN Policy							
Authentication	Key Management	<u>19</u>					
802.1X	🕑 Enable						

WLANs	WLANs > Edit 'office_hq'	
WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled Authentication Servers EAP Parameters Enabled Prilo.48.39.128, Port:1813 † Server 1 IP:10.48.39.128, Port:1813 † Server 2 None Server 3 None Server 4 None Server 5 None Server 6 None Authorization ACA Server Accounting ACA Server Enabled Enabled	

	Auvancea		
Allow AAA Override	C Enabled	DHCP	
Coverage Hole Detection	Enabled	DHCP Server Override	
Enable Session Timeout 2 1800 Session Aironet IE	Timeout (secs)	DHCP Addr. Assignment CRequired Management Frame Protection (MFP)	
Diagnostic Channel 18	Enabled		
Override Interface ACL	IPv4 None \$ IPv6 None \$	MFP Client Protection 4 Optional \$	
Layer2 Acl	None 🕈	DTIM Period (in beacon intervals)	
IRL ACL	None \$		
P2P Blocking Action	Disabled \$	802.11a/n (1 - 255) 1	
Client Exclusion ²	Enabled I80 Timeout Value (secs)	802.11b/g/n (1 - 255) 1 NAC	
Maximum Allowed Clients ⁸	0	NAC State None +	
Static IP Tunneling 11	Enabled	Load Balancing and Band Select	
Wi-Fi Direct Clients Policy	Disabled \$	Client Load Balancing	
Maximum Allowed Clients Per AP Radio	200	Client Band Select	
Wi-Fi Direct Clients Policy Maximum Allowed Clients Per AP Radio Clear HotSoot Configuration	Disabled \$ 200 Enabled	Client Load Balancing Client Band Select	
		Passive Client	

3. Vous devez également créer des interfaces dynamiques sur le WLC pour les VLAN utilisateur. Accédez au menuController > Interfaces de l'interface utilisateur. Le WLC ne peut honorer l'affectation de VLAN reçue via AAA que s'il a une interface dynamique dans ce VLAN.

DBACK	Ē	HELP	C <u>O</u> MMANDS	M <u>A</u> NAGEMENT	ECURITY	s <u>s</u>	WIRELESS	ROLLER	CONTR	<u>W</u> LANs	MONITOR	ဂျက်၊ cisco	
												ontroller	C
					_				on	nformati	General I	General	
							7	vlan147		Name	Interface	Icons	
							e:e3:5a:1a	00:a3:8		ress	MAC Add	Inventory	
				_						ition	Configura	Interfaces Interface Groups	
										1	Guest La	Multicast	
										e	Quarantir	Network Routes	Þ
									0	ie Vlan Id	Quarantir	Fabric Configuration	Þ
								one	n		NAS-ID	Redundancy	Þ
									ion	informat	Physical	Mobility Management	Þ
								1		ber	Port Num	Ports	
								0		ort	Backup P	NTP	Þ
								1		rt	Active Po	CDP	Þ
)	ient 🗌	1anagem	ynamic AP N	Enable D	PMIPv6	Þ
										Addross	Interface	Tunneling	Þ
					_					Address	Interface	IPv6	Þ
							477	1		ntifier	VLAN Ide	mDNS	Þ
						•	92.168.77.5	1		s	IP Addres	Advanced	Þ
						0	02 169 77 1	2			Cataway	Lawful Interception	
										race	IPv6 Add		
							28	1		ath	Prefix Ler		
							:	:		away	IPv6 Gate		
					:5a1a/64	ff:fee	e80::2a3:8eff	fe	ass	I IPv6 Addre	Link Loca		
									1	ormation	DHCP Inf		
							92.168.77.1	1	r	HCP Server	Primary [
									ver	y DHCP Ser	Secondar		
							Global 🛟			xy Mode	DHCP Pro		
					:5a1a/64	; 0 ff:fee:	477 92.168.77.5 55.255.255.0 92.168.77.1 : 28 : ≥80::2a3:8eff 92.168.77.1 Global ¢	1 0 1 1 1 1 2 1 1 1 5 6	1anagem 255 1 ver	ber prt t (namic AP N Address ntifier s ress ngth way I IPv6 Addre ormation OHCP Server y DHCP Server xy Mode	Port Num Backup P Active Po Enable D Interface VLAN Ide IP Addres Netmask Gateway IPv6 Add Prefix Ler IPv6 Gate Link Loca DHCP Inf Primary I Secondar DHCP Pro	NTP CDP PMIPv6 Tunneling IPv6 mDNS Advanced Lawful Interception	* * * * * * *

Vérifier

Utilisez le demandeur natif Windows 10 et Anyconnect NAM afin de tester les connexions.

Étant donné que vous utilisez l'authentification EAP-PEAP et qu'ISE utilise un certificat auto-signé (SSC), vous devez accepter un avertissement de certificat ou désactiver la validation de certificat. Dans un environnement d'entreprise, vous devez utiliser un certificat signé et approuvé sur ISE et vous assurer que les périphériques des utilisateurs finaux disposent du certificat racine approprié installé sous la liste Autorités de certification approuvées.

Testez la connexion avec Windows 10 et le demandeur natif :

1. OuvrezNetwork & Internet settings > Wi-Fi > Manage known networkset créez un nouveau profil réseau en appuyant sur leAdd new networkbouton ; complétez les informations requises.

← Settings	
命 Wi-Fi	
Manage known networks	
Add a new network	Add a new network
+	Network name
Search this list $ ho$	office_hq
Sort by: Preference $ \smallsetminus $ Filter by: All $ \smallsetminus $	Security type
	WPA2-Enterprise AES V
	EAP method
The second second	Authentication method
	Secured password (EAP-MSCHAP v2) \checkmark
	Connect automatically
The second second	Connect even if this network is not broadcasting
	Save Cancel

2. Vérifiez le journal d'authentification sur ISE et assurez-vous que le profil approprié est sélectionné pour l'utilisateur.

c	Refresh Reset Repeat Counts	Export To •															٣	Filter*	>-
	Time	Status	Details	Repeat	Identity		Endpoint ID	Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Ne	twork Device	Device Port	Identity Group	Posture St	Server	
×					Bob	×	Endpoint ID	Endpoint Profil	Authentication	Authorization Policy	Authorization I	IP Address	 Ne 	twork Device	Device Port	Identity Group	Posture Status	Server	
	Feb 15, 2019 02:16:43:300 PM	•	9	3	Bob		F4.8C 50 62 14 68	Unknown	Default >> W	Default >> Wireless_HR	HR							manchur-is	e
	Feb 15, 2019 02:09:56:389 PM		9		Bob		F4.8C 50.62.14.68	Unknown	Default >> W	Default >> Wireless_HR	HR		WL	C5520		Unknown		manchur-is	•

3. Vérifiez l'entrée du client sur le WLC et assurez-vous qu'il est assigné au bon VLAN et est dans l'état RUN.

	 cısco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK						Saya	Configure	stion <u>P</u> in	g Logou	Befresh
I	Monitor	Clients																Entries 1	- 1 of 1
	Summary Access Points Cisco CleanAir	Current Filter N	lone	19	hanse Filter) (Clear Filter)													
	Statistics CDP	Client MAC Addr <u>14:8c:50:62:14:6b</u>	IP Address/ Joy 192.168.78.36	e4/Iov6)		AP N AP40	ame 277.6D9E.6162			WLAN Profile office_hq	WLAN SSID office_hq	User Name Bob	Protocol 802.11ac(5 GHz)	Status Associated	Auth Yes	Port 1	Slot Id 1	Tunnel No	Fastlane No
	 Rogues Clients 																		
	Sleeping Clients Multicast																		
	Applications																		

4. À partir de l'ILC WLC, l'état du client peut être vérifié avec leshow client dertails

:

show client detail f4:8c:50:62:14:6b
Client MAC Address..... f4:8c:50:62:14:6b
Client Username Bob

Client Webauth Username N/A Hostname: Device Type: Intel-Device AP Name..... AP4C77.6D9E.6162 AP radio slot Id..... 1 Client State..... Associated User Authenticated by RADIUS Server Client User Group..... Bob Client NAC OOB State..... Access Wireless LAN Id..... 3 Wireless LAN Network Name (SSID)..... office_hq Wireless LAN Profile Name..... office_hq Hotspot (802.11u)..... Not Supported Connected For 242 secs IP Address..... 192.168.78.36 Gateway Address..... 192.168.78.1 Policy Manager State..... RUN EAP Type..... PEAP Interface.....vlan1478 Quarantine VLAN......0 Access VLAN..... 1478

Testez la connexion avec Windows 10 et Anyconnect NAM :

1. Choisissez le SSID dans la liste SSID disponibles et le type d'authentification EAP respectif (dans cet exemple PEAP) et le formulaire d'authentification interne.

	🕥 Cisco AnyCo	Connect Secure Mobility Client — 🗆 🗙	
	Web Authenti	VPN: Use a browser to gain access.	
	S	Network: Connected (10.103.150.57) internet	
Cisco AnyConnect		× curity:	
Enter information	n for the connection.	e key.	
Media:	Wi-Fi Hidden Network		
Descriptive Name:	office_hq	Scan:	
SSID:	office_hq	can not required on current Wi-Fi.	
Security:	WPA2 Enterprise AES		
802.1X Configuration			
password ~	PEAP ~	a Formita	
		not currently protected by Umbrella.	
	OK Can	ncel missing.	
A SHARE AND			

2. Fournissez un nom d'utilisateur et un mot de passe pour l'authentification utilisateur.

S Cisco AnyConnect Secure Mobility Client − □ ×	
VPN: Verify your network connection.	
No Network Connectivity	
Network: Authenticating	
office_hq 🖳 🔐 🔛	
Web Security: No License Key.	
System Scan: Limited or no connectivity.	
	 Cisco AnyConnect Secure Mobility Client – × VPI: Verify your network connection. Connect Network Connectivity Network: Authenticating office_hq all image: System Scan: Linited or no connectivity.

3. Étant donné qu'ISE envoie un SSC au client, vous devez choisir manuellement d'approuver le certificat (dans l'environnement de production, il est fortement recommandé d'installer le certificat approuvé sur ISE).

Cisco AnyConnect X		
The server certificate for the network 'office_hq' has failed validation. Do you want to trust it? Certificate Name: rmanchur-ise.wlaaan.com@ Issued To: rmanchur-ise.wlaaan.com Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC Trust Do Not Trust	VPN: Verify your network connection. Connect No Network Connectivity Network: Authenticating office_hq	
	Web Security: No License Key.	

4. Vérifiez les journaux d'authentification sur ISE et assurez-vous que le profil d'autorisation approprié est sélectionné pour l'utilisateur.

C I	Reset Repeat Counts	Z Export To*																	¥ Filter •	۰۰
	Time	Status	Details	Repeat	Identity		Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address		Network Device	Device Port	Identity Group	Posture St	Server	Mdm
×					Alice	×	60	×	Endpoint Prof	Authentication	Authorization Policy	Authorization	IP Address		Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
	Feb 15, 2019 02:51:27.163 PM	٠	0	0	Alice		F4.8C.50.62.14.68		Microsoft-W	Default >>	Default >> Wireless_Marketing	Marketing	192.168.77.32						manchur-ise	
	Feb 15, 2019 02:51:24.837 PM		• •		Alce	*	F4:8C:50:62:14:68	*	Morosoft-W	Default >>	Default >> Wireless_Marketing	Marketing		٠	WLC5520		Workstation �		manchur-ise 💠	

5. Vérifiez l'entrée du client sur le WLC et assurez-vous qu'il est assigné au bon VLAN et est dans l'état RUN.

Clients	Entries 1 - :
Current Filter None (Chappe Filter) (Clear Filter)	
Flient MAF Addr ID Address/Truck/Truck) AD Name WI AN DroFile WI AN SSID ser Name Drohon	I Status Auto Port Slot Id Tunnel
Hard Control Hard Contro	(5 GHz) Associated Yes 1 1 No

6. À partir de l'ILC WLC, l'état du client peut être vérifié avec leshow client dertails

:

Client MAC Address	f4:8c:50:62:14:6b
Client Username	AIICe
Client Webauth Username	N/A
Hostname:	
Device Type:	Intel-Device
AP MAC Address	70:69:5a:51:4e:c0
AP Name	AP4C77.6D9E.6162
AP radio slot Id	1

Client State	Associated
User Authenticated by	RADIUS Server
Client User Group	Alice
Client NAC OOB State	Access
Wireless LAN Id	3
Wireless LAN Network Name (SSID)	office_hq
Wireless LAN Profile Name	office_hq
Hotspot (802.11u)	Not Supported
Connected For	765 secs
BSSID	70:69:5a:51:4e:cd
Channe1	36
IP Address	192.168.77.32
Gateway Address	192.168.77.1
Netmask	255.255.255.0
Policy Manager State	RUN
Policy Type	WPA2
Authentication Key Management	802.1x
Encryption Cipher	CCMP-128 (AES)
Protected Management Frame	No
Management Frame Protection	No
EAP Type	PEAP
Interface	vlan1477
VLAN	1477

Dépannage

1. Utilisez latest aaa radius username

password

wlan-id

afin de tester la connexion RADIUS entre WLC et ISE et latest aaa show radiusafin d'afficher les résultats.

test aaa radius username Alice password <removed> wlan-id 2 Radius Test Request Wlan-id..... 2 ApGroup Name..... none Attributes Values -----_____ User-Name Alice Called-Station-Id 00-00-00-00-00:AndroidAP Calling-Station-Id 00-11-22-33-44-55 Nas-Port 0x0000001 (1)

Nas-Ip-Address	10.48.71.20
NAS-Identifier	0x6e6f (28271)
Airespace / WLAN-Identifier	0x0000002 (2)
User-Password	cisco!123
Service-Type	0x0000008 (8)
Framed-MTU	0x00000514 (1300)
Nas-Port-Type	0x00000013 (19)
Cisco / Audit-Session-Id	1447300a000003041d5665c
Acct-Session-Id	5c66d541/00:11:22:33:44:55/743

test radius auth request successfully sent. Execute 'test aaa show radius' for response (Cisco Controller) >test aaa show radius Radius Test Request Wlan-id..... 2 ApGroup Name..... none Radius Test Response Radius Server Retry Status _____ -----10.48.39.128 1 Success Authentication Response: Result Code: Success Attributes Values _____ _____ User-Name Alice ReauthSession:1447300a000003041d5665c State Class CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59 Tunnel-Type 0x000000d (13) 0x0000006 (6) Tunnel-Medium-Type Tunnel-Group-Id 0x00005c5 (1477)

(Cisco Controller) >

2. Utilisez la debug client

afin de dépanner les problèmes de connectivité du client sans fil.

3. Utilisez ladebug aaa all enableafin de dépanner les problèmes d'authentification et d'autorisation sur le WLC.



Remarque : utilisez cette commande uniquement avec ledebug mac addrafin de limiter la sortie basée sur l'adresse MAC pour laquelle le débogage est effectué.

4. Référez-vous aux journaux en direct ISE et aux journaux de session afin d'identifier les problèmes d'échecs d'authentification et les problèmes de communication AD.

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.