配置基於ISE的WLC到Active Directory組對映的 動態VLAN分配

目錄
<u>簡介</u>
<u>必要條件</u>
採用元件
<u>慣例</u>
<u>使用RADIUS伺服器進行動態VLAN分配</u>
<u>設定</u>
<u>網路圖表</u>
<u>ISE到AD整合和配置ISE上使用者的身份驗證和授權策略</u>
WLC配置支援SSID 'office hq'的DOT1x身份驗證和AAA覆蓋
<u>驗證</u>
<u>疑難排解</u>

簡介

本檔案介紹動態VLAN指派的概念。

必要條件

本文說明如何設定無線LAN控制器(WLC)和身分辨識服務引擎(ISE)伺服器,以便動態地將無線LAN (WLAN)使用者端指派到特定VLAN。

需求

思科建議您瞭解以下主題:

- 無線區域網路控制器(WLC)和輕量存取點(LAP)的基本知識
- 身份驗證、授權和記帳(AAA)伺服器(例如ISE)的功能知識
- 全面瞭解無線網路和無線安全問題
- 動態VLAN分配的功能和配置知識
- 基本瞭解Microsoft Windows AD服務,以及域控制器和DNS概念
- 具備存取點通訊協定(CAPWAP)控制與布建的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco 5520系列WLC(執行韌體版本8.8.111.0)
- Cisco 4800系列AP
- 本地Windows請求方和Anyconnect NAM
- 思科安全ISE版本2.3.0.298
- Microsoft Windows 2016 Server 配置為域控制器
- 執行版本15.2(4)E1的Cisco 3560-CX系列交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

使用RADIUS伺服器進行動態VLAN分配

在大多數WLAN系統中,每個WLAN都有一個靜態策略,該策略適用於與服務集識別符號(SSID)或 控制器術語中的WLAN相關聯的所有客戶端。此方法雖然功能強大,但有一定的侷限性,因為它要 求客戶端與不同的SSID關聯以繼承不同的QoS和安全策略。

Cisco WLAN解決方案透過支援身份網路解決了這一限制。 這允許網路通告單個SSID,但允許特定 使用者根據使用者憑證繼承不同的QoS、VLAN屬性和/或安全策略。

動態VLAN分配是一種功能,可根據使用者提供的憑證將無線使用者置於特定VLAN中。將使用者分 配到特定VLAN的任務由RADIUS身份驗證伺服器(如Cisco ISE)處理。例如,這可用於允許無線 主機在園區網路中移動時保持在相同的VLAN上。

思科ISE伺服器根據多個可能的資料庫之一(包括其內部資料庫)對無線使用者進行身份驗證。舉例來說:

- 內部DB
- Active Directory
- 通用輕量型目錄存取通訊協定(LDAP)
- 開放資料庫連線(ODBC)相容關聯式資料庫
- Rivest、Shamir和Adelman (RSA) SecurID令牌伺服器
- 與RADIUS相容的權杖伺服器

Cisco ISE身份驗證協定和支援的外部身份源列出了ISE內部和外部資料庫支援的各種身份驗證協定

o

本文檔重點介紹如何對使用Windows Active Directory外部資料庫的無線使用者進行身份驗證。

身份驗證成功後,ISE從Windows資料庫中檢索該使用者的組資訊,並將該使用者關聯到相應的授 權配置檔案。

當客戶端嘗試與註冊到控制器的LAP關聯時,LAP會藉助相應的EAP方法將使用者的憑證傳遞到 WLC。

WLC使用RADIUS協定(封裝EAP)將這些憑證傳送到ISE,ISE將使用者的憑證傳遞到AD以在 KERBEROS協定的幫助下進行驗證。

AD驗證使用者憑證,並在身份驗證成功後通知ISE。

身份驗證成功後,ISE伺服器會將某些Internet工程任務組(IETF)屬性傳遞到WLC。這些RADIUS屬 性決定了必須分配給無線客戶端的VLAN ID。使用者端的SSID (WLAN,從WLC的角度而言)並 不重要,因為系統一律會將使用者指定給這個預先設定的VLAN ID。

用於VLAN ID分配的RADIUS使用者屬性包括:

- IETF 64(隧道型別)—將其設定為VLAN
- IETF 65(隧道介質型別)—將此值設定為802
- IETF 81(隧道專用組ID)—將其設定為VLAN ID

VLAN ID為12位,取值範圍為1至4094(含)。由於Tunnel-Private-Group-ID屬於字串型別(如 RFC2868中所定義,用於IEEE 802.1X),因此VLAN ID整數值被編碼為字串。傳送這些隧道屬性 時,需要填寫標籤欄位。

如<u>RFC 2868</u>第3.1部分中所述:標籤欄位的長度為一個八位組,用於提供在同一資料包中分組參考 同一隧道的屬性的方法。此欄位的有效值為0x01到0x1F (含)。如果「標籤」欄位未使用,它必 須是零(0x00)。有關所有RADIUS屬性的詳細資訊,請參閱<u>RFC 2868</u>。

設定

本節提供設定檔案中所述功能所需的資訊。

網路圖表



組態

以下是此圖中所用元件的配置詳細資訊:

- ISE (RADIUS)伺服器的IP地址是10.48.39.128。
- WLC的管理和AP管理器介面地址為10.48.71.20。
- DHCP伺服器駐留在LAN網路中,並且針對各個客戶端池進行了配置;圖中未顯示它。
- VLAN1477和VLAN1478用於此配置。市場行銷部門的使用者配置為置於VLAN1477中,而HR 部門的使用者配置為由RADIUS伺服器置於VLAN1478中 當兩個使用者都連線到同一個 SSID時— office_hq.

VLAN1477:192.168.77.0/24。網關: 192.168.77.1 VLAN1478:192.168.78.0/24。網關: 192.168.78.1

• 本文檔使用帶PEAP-mschapv2的802.1x作為安全機制。



注意:Cisco建議您使用高級身份驗證方法,如EAP-FAST和EAP-TLS身份驗證,以便保護WLAN。

這些假設是在您執行此組態之前做出的:

- LAP已註冊到WLC
- 為DHCP伺服器分配了DHCP作用域
- 網路中所有裝置之間存在第3層連線
- 本文檔討論無線端所需的配置,並假設有線網路已就緒
- 在AD上配置了各自的使用者和組

要根據ISE到AD組對映透過WLC完成動態VLAN分配,必須執行以下步驟:

- 1. ISE到AD整合和配置ISE上使用者的身份驗證和授權策略。
- 2. 配置WLC,以支援SSID 'office_hq'的dot1x身份驗證和AAA覆蓋。
- 3. 最終客戶端請求方配置。

ISE到AD整合和配置ISE上使用者的身份驗證和授權策略

- 1. 使用admin帳戶登入ISE Web UI介面。
- 2. 導航到Administration > Identity management > External Identity Sources > Active directory。

titude Identity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers	
System Identity Management Network R	esources	ent pxGrid Service	
Identities Groups External Identity Sources	Identity Source Sequences	ngs	
External Identity Sources	Active Directory		
	/ Edit 👷 Add 🗙 Delete	Node View 🔂 Advanced Tools 👻 Scope Mode	
Certificate Authentication Profile	Join Point Name	 Active Directory Domain 	
Active Directory			No data available
EDAP LDAP			
ODBC			
RADIUS Token			
SAML Id Providers			
Social Login			

3. 按一下Add, 然後從Active Directory加入點名稱設定輸入域名和身份庫名稱。在本例中, ISE註冊到域wlaaan.com, 連線點指定為AD.wlaaan.com -對於ISE為本地重要名稱。

External Identity Sources		Connection		
* E *	ŵ. -	* Join Point Name	AD wlaaan com	
 Certificate Authentication Profile 		our on that	Abtmiddent.com	
Calify Active Directory		* Active Directory Domain	wlaaan.com	1
EDAP LDAP			·	
CDBC				
RADIUS Token		Cubanita Connect		
RSA SecurID		Submit Cancel		
SAML Id Providers				
Social Login				

4. 按Submit下按鈕後,彈出窗口打開,詢問您是否要立即將ISE加入AD。按Yes,並提供具有管理 員許可權的Active Directory使用者憑據以向域中增加新主機。

Connection Whitelisted	Domains Passiv	veID Groups	Attributes	Advanced Settings			
* Join Point Name AD.w	aaan.com						
* Active Directory Domain wlaa	an.com		۲				
Join 淫 Leave 🧕 Test User 音	Diagnostic Tool 🛛 😵 Refre	sh Table					
ISE Node	▲ ISE Node Role	Status	Domain Controller	Site			
rmanchur-ise.wlaaan.com	STANDALONE	A Not Joined					
Join Domain × Please specify the credentials required to Join ISE node(s) to the Active Directory Domain. × • AD User Name () Administrator • Password • • Specify Organizational Unit () •							
	C Store C	redentials (j)		OK Cancel			

5. 在此之後,您必須將ISE成功註冊到AD。

I Identity Sources	Connection Whitelisted Doma	ains PassiveID Groups	Attributes Advanced	Settings
E v @v Certificate Authentication Profile Active Directory DAP	Join Point Name AD.wlaaan.co Active Directory Domain wlaaan.co	com m	Ū.	
RADIUS Token	👷 Join 🛛 👷 Leave 👤 Test User 🛛 🔓 Diagn	ostic Tool 🛛 🛞 Refresh 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

如果註冊過程有任何問題,您可以使用Diagnostic Tool 來運行AD連線所需的測試。 您必須檢查用於公配相應採購配置檔案的活動且偽得。道院到,以此,以下以下。

6. 您必須檢索用於分配相應授權配置檔案的活動目錄組。導航到Administration > Identity management >

External Identity Sources > Active directory >

>Groups ,然後點選Add並選擇Select Groups from Active Directory。



7. 新的彈出窗口隨即打開,您可以在其中指定過濾器以檢索特定組或從AD檢索所有組。 從AD組清單中選擇相應的組,然後按OK。

Select Direc	tory Groups					×
This dialog is u	used to select groups from the Directo	ory.				
Domai	n wlaaan.com		*			
Name Filte	۲ ۲ *	SID Filter	*	Type Filter GLOBAL	•	
	Retrieve Groups 13 Groups Retrie	eved.				
Name			Group SID		Group Type	
wlaaan.c	om/Users/Cloneable Domain Control	ers	S-1-5-21-2222429329-410808516	4-3220345271-522	GLOBAL	
wlaaan.c	om/Users/DnsUpdateProxy		S-1-5-21-2222429329-410808516	4-3220345271-1102	GLOBAL	
wlaaan.c	om/Users/Domain Admins		S-1-5-21-2222429329-410808516	4-3220345271-512	GLOBAL	
wlaaan.c	om/Users/Domain Computers		S-1-5-21-2222429329-410808516	4-3220345271-515	GLOBAL	
wlaaan.c	om/Users/Domain Controllers		S-1-5-21-2222429329-410808516	4-3220345271-516	GLOBAL	
wlaaan.c	om/Users/Domain Guests		S-1-5-21-2222429329-410808516	4-3220345271-514	GLOBAL	
wlaaan.c	om/Users/Domain Users		S-1-5-21-2222429329-410808516	4-3220345271-513	GLOBAL	
wlaaan.c	om/Users/Group Policy Creator Own	ers	S-1-5-21-2222429329-410808516	4-3220345271-520	GLOBAL	
vlaaan.c	om/Users/HR		S-1-5-21-2222429329-410808516	4-3220345271-1105	GLOBAL	
wlaaan.c	om/Users/Key Admins		S-1-5-21-2222429329-410808516	4-3220345271-526	GLOBAL	
vlaaan.c	om/Users/Marketing		S-1-5-21-2222429329-410808516	4-3220345271-1104	GLOBAL	
wlaaan.c	om/Users/Protected Users		S-1-5-21-2222429329-410808516	4-3220345271-525	GLOBAL	
wlaaan.c	om/Users/Read-only Domain Control	lers	S-1-5-21-2222429329-410808516	4-3220345271-521	GLOBAL	



8. 相應的組將增加到ISE並可儲存。按Save。

	C	onnectio	on		Whiteliste	d Domains	PassiveID	Groups	Attributes	Advanced Settings	
1	Edit	م ك	id -	X Del	ete Group	Undate SID Valu	es				
_	hla	T.w	.u •	~ 00	ctc oroup			CID			
	INa	ime					-	510			
	wla	aaan.co	m/Use	ers/HR				S-1-5-21-222	2429329-4108085164-3	220345271-1105	
	wla	aaan.co	m/Use	ers/Marl	eting			S-1-5-21-222	2429329-4108085164-3	220345271-1104	
Sa	ve	Reset									

9. 將WLC增加到ISE網路裝置清單-導航到Administration > Network Resources > Network Devices,然後按Add。 在WLC和ISE之間提供WLC管理IP地址和RADIUS共用金鑰,從而完成配置。

tituliti Identity Services Engine	Home + Context Visibility + Operations + Policy Administration + Work Centers
System Hentity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Network Devices Network Device G	roups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM → Location Services
0	
Network Devices	Notwork Devices List > New Network Device
Default Device	• Name 140,75520
Device Security Settings	
	Providence
	IP Address + IP: 10.48.71.20 / 32
	IPVe is supported only for IAUAUS, At least one IPVe must be defined when RAUJUS is selected
	Device Profile data Cisco v
	Model Name
	Software Version
	Network Device Group
	Location TAR C Set To Default
	Device Trace Device
	Vertex type WLC-tab
	RADUIS INP Sattings
	Protoci PADIIS
	· Share Secret
	CoA Port
	Contract [1/00] Set to besture
	KADIUS DTLS Settings ()

10. 現在,當您將ISE加入AD並將WLC增加到裝置清單後,您可以開始為使用者配置身份驗證和 授權策略。 • 建立授權配置檔案,以將來自Marketing 的使用者分配到VLAN1477,將來自HR 組的使 用者分配到VLAN1478。

導航到Policy > Policy Elements > Results > Authorization > Authorization profiles, 然後按一下Add按鈕以建立 新配置檔案。

cisco Identity Services Engine Ho	me Context Visibility Operations Policy	Administration Work Centers	
Policy Sets Profiling Posture Client F	Provisioning Policy Elements		
Dictionaries + Conditions - Results			
0			
Authentication	Standard Authorization Profiles		
- Authorization	For Policy Export go to Administration > System > Backup &	Restore > Policy Export Page	
	/ Edit + Add Duplicate X Delete		
Authorization Profiles	□ Name	Profile	Description
Downloadable ACLs	Blackhole_Wireless_Access	🚓 Cisco 🕀	Default profile used to blacklist wireless dev
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	就 Cisco 🕀	Default Profile used to redirect users to the
Client Provisioning	NSP_Onboard	👬 Cisco 🕀	Onboard the device with Native Supplicant
	Non_Cisco_IP_Phones	就 Cisco 🕀	Default Profile used for Non Cisco Phones.
	DenyAccess		Default Profile with access type as Access-
	PermitAccess		Default Profile with access type as Access-

• 使用相應組的VLAN資訊完成授權配置檔案配置;該示例顯示Marketing組配置設定。

Dictionaries + Conditions - Results	s
G	A desirable Profiles - Marchaelen Bardin
Authentication	Authorization Profile
▼ Authorization	* Name Marketing
	Description Marketing
Authorization Profiles	* ACCOSS TVD0 ACCESS ACCENT
Downloadable ACLs	ACCESS ACCEPT
 Profiling 	Network Device Profile 🛛 🎰 🕀
Posture	Service Template
Client Provisioning	Track Movement 🔲 🕡
	Passive Identity Tracking y 👔
	Common Tasks
	DACL Name
	ACL (Filter-ID)
	Security Group
	V VLAN Tag ID 1 Edit Tag 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

必須為其他組執行類似的配置,並且必須配置相應的VLAN標籤屬性。

• 配置授權配置檔案後,您可以為無線使用者定義身份驗證策略。這可以透過配置Custom或

修改Default Policy set來完成。在本示例中,預設策略集被修改。導航到Policy > Policy Sets > Default。預設情況下,對於dot1x身份驗證型別,ISE將使用All_User_ID_Stores,儘管它可以在 當前預設設定下使用,因為AD是All_User_ID_Stores的身份源清單的一部分,此示例針對相應 的LAB控制器使用更具體的規則wLC_lab,並使用AD作為唯一的身份驗證源。

ets → Default			Resot Se	
Status Policy Set Name	Descript	Conditions	Allowed Protocols / Server Sequence H	
Default	Default pr	sot.	Default Network Access × * +	
ntication Policy (4)				
Status Rule Name	Condit	1	Use Hits Actio	
⊙ MAB	OR	Wred_MA8	Internal Endpoints × * 0	
	U.I.	Wreless_MAB	> Options	
		Wireless_602.1X		
WLC_lab	AND	DEVICE Device Type EQUALS All Device Types#WLC-lab	Aci wissan.com v o O	
	E DEVICEL	Location EQUALS AI Locations#LA8	> Options	
0 0011	07	Wired_802.1X	Wired_802.1X	Al_User_ID_Stores
O DAIX	OR	Windess_802.1X	> Options	
(P) Default			Al_User_ID_Stores * *	
0 000			> Options	
rization Policy - Local Exceptions				
rization Policy - Global Exceptions				
rization Policy (12)				

• 現在,您必須為根據組成員身份分配相應授權配置檔案的使用者建立授權策略。導航到 Authorization policy部分並建立策略以滿足此要求。

Policy Sets Pr	Policy Sea. Policy Pature Clerc/Provisioning + Policy Dements						ess setup and visibility setup Do	not show th	is again. X
Policy Sets +	Default							Reset	Savo
Status	Policy Set Name	Description	Conditions				Allowed Protocols / Server	Sequence	e Hits
Search	Default	Default policy set					Default Network Access	** *	•
> Authenticatio	on Policy (4)								
> Authorization	n Policy - Local Exceptions								
> Authorization	n Policy - Global Exceptions								
✓ Authorization	n Policy (14)								
(+) Statu	s Rule Name	Conditions			Results Profiles	Security 0	Groups	Hits	Actions
Search						_			
/ 0	Wireless_Marketing	AND E AD.wissan.c	cess om ExternalGroups EQUALS wlasan.com/Users/Marketing		Marketing	+ Select from	• •	0	۰
	Wreless_HR	AND H AD wisean o	cess om ExternalGroups EQUALS wilaean.com/Users/HR		INR	+ Select from	nist y	۰	۰

支援SSID 'office_hq'的dot1x身份驗證和AAA覆蓋的WLC配置

1. 將ISE配置為WLC上的RADIUS身份驗證伺服器。導航到Web UI介面中的Security > AAA > RADIUS > Authentication部分,提供ISE IP地址和共用金鑰資訊。

cisco	MONITOR WLANS CONTROLLER	R WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Serve	ers > 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 settings Apply Cisco ACA Default settings Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeout Tunnel Proxy PAC Provisioning IPSec Cisco ACA	<pre>ers > New 2 2 10.48.39.128 ASCII ASC</pre>

2. 在WLC上的wLANs部分下配置SSIDoffice_hq;本示例使用wPA2/AES+dot1x和AAA override配置 SSID。已為WLAN選擇InterfaceDummy,因為還是透過RADIUS分配了正確的VLAN。必須在 WLC上建立此虛擬介面並給予IP地址,但IP地址不必有效,並且不能在上行鏈路交換機中建 立放置該虛擬介面的VLAN,因此,如果未分配VLAN,則客戶端無法前往任何地方。

cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK			
WLANs	WLANs											
VLANs	Current Filte	r: Nor	ne	[Change Filte	er] [Clear Filter	1				[Create New	\$ Go
Advanced	WLAN ID	Туре	Profile Na	ime		WLAN SSID		A	dmin Status	Security Policies		
		WLAN	test			test		E	inabled	[WPA2][Auth(802.1X)]	
	2	WLAN	AndroidAP			AndroidAP		E	nabled	[WPA2][Auth(PSK)]		
	253	WLAN	BTER-BTwi	ifi-public		BTwifi-public		E	nabled	[WPA2][Auth(PSK)]		

cisco	MONITOR WLANS	CONTROLLER W	IRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	ĸ							A Home	
WLANs	WLANs > New													< Back	Apply	
	Type Profile Name SSID ID	WLAN office_hq office_ha 3 t	1													

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_h	q'		
WLANs	General Security	QoS Policy-Mapping	Advanced	
Advanced	Layer 2 Layer 3	AAA Servers		
	Select AAA servers below RADIUS Servers RADIUS Server Overwrite Apply Cisco ISE Default S Authentication Server 2 None Server 3 None Server 4 None Server 5 None Server 6 None Server 6 None Server 7 None 2 Server 7 None	to override use of default serv e interface Enabled settings Enabled DN Servers Accounting Set 128, Port: 1812 ¢ None ¢ None ¢ None	rvers EAP Pau 28, Port:1813 ¢	rameters le

ANs > Edit 'office_hq'		
eneral Security QoS Pol	icy-Mapping Advanced	
Allow AAA Override	Enabled	DHCP
Coverage Hole Detection	Enabled	DHCP Server Override
Enable Session Timeout 21800 Aironet IE	Timeout (secs)	DHCP Addr. Assignment Required Management Frame Protection (MFP)
Override Interface ACL	IPv4 None \$ IPv6	None MFP Client Protection Optional
Layer2 Acl	None \$	DTIM Period (in beacon intervals)
URL ACL P2P Blocking Action	None ¢ Disabled ¢	802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1
Maximum Allowed Clients ⁸	Cenabled Timeout Value (secs)	NAC State None 1
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
Clear HotSpot Configuration	Enabled	Passive Client
Client user idle timeout(15-100000)		Descha Client

3. 您還必須在WLC上為使用者VLAN建立動態介面。導航到Controller > InterfacesUI選單。如果WLC在 該VLAN中具有動態介面,則它只能支援透過AAA接收的VLAN分配。

	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller								
General	General Informati							
Icons	Interface Name	vlan14	77					
Inventory	MAC Address	00:a3:	8e:e3:5a:1a					
Interfaces Interface Groups	Configuration				_			
Multicast	Guest Lan							
Network Routes	Quarantine							
Fabric Configuration	Quarantine Vlan Id	0						
Redundancy	NAS-ID	none						
Mobility Management	Physical Informati	ion						
Ports	Port Number		1					
► NTP	Backup Port		0					
► CDP	Active Port		1					
▶ PMIPv6	Enable Dynamic AP M	lanagement						
Tunneling								
▶ IPv6	Interface Address							
▶ mDNS	VLAN Identifier		1477					
Advanced	IP Address		192.168.77.5					
Lawful Interception	Netmask		255.255.255.0					
	Gateway		192.168.77.1					
	IPv6 Address		::					
	Prefix Length		128					
	IPv6 Gateway							
	Link Local IPv6 Addre	ess	fe80::2a3:8eff:f	ee3:5a1a/64				
	DHCP Information							
	Primary DHCP Server		192.168.77.1					
	Secondary DHCP Ser	ver						
	DHCP Proxy Mode	(Global 🛟					

驗證

使用Windows 10本機請求方和Anyconnect NAM來測試連線。

由於您使用EAP-PEAP身份驗證且ISE使用自簽名證書(SSC),您必須同意證書警告或停用證書驗證 。在企業環境中,您必須在ISE上使用簽名和受信任的證書,並確保終端使用者裝置在受信任CA清 單下安裝了適當的根證書。

測試與Windows 10和本地請求方的連線:

1. 按Network & Internet settings > Wi-Fi > Manage known networksAdd new network按鈕打開並建立新網路配置檔案 ;填寫所需資訊。

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

2. 檢查ISE上的身份驗證日誌並確保為使用者選擇了正確的配置檔案。

c	Refresh O Reset Repeat Counts	Export To •																Filter	۰.
	Time	Status	Details	Repeat	Identity		Endpoint ID	Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Neb	work Device	Device Port	Identity Group	Posture St	Server	
×					Bob	×	Endpoint ID	Endpoint Profi	Authentication	Authorization Policy	Authorization I	IP Address	Net	work Device	Device Port	Identity Group	Posture Statue	Server	
	Feb 15, 2019 02:16:43:300 PM	0	à	3	Bob		F4.8C 50 62 14 68	Unknown	Default >> W	Default >> Wireless_HR	HR							manchu	ise
	Feb 15, 2019 02:09:56.389 PM		0		Bob		F4/8C/50/62/14/68	Unknown	Default >> W	Default >> Wireless_HR	HR		WLC	:5520		Unknown		manchu	ise

3. 檢查WLC上的客戶端條目,確保已將其分配給正確的VLAN並處於RUN狀態。

،، ،،، ،، cısco	MONITOR WLANS	CONTROLLER V	WIRELESS SECURIT	Y MANAGEMENT	COMMANDS	HELP	FEEDBACK						Saya C	onfiguration	Bing Log	out Befresh
Monitor	Clients														Entries	1 - 1 of 1
Summary Access Points Cisco CleanAir	Current Filter N	one	[Charge_Eits	er] [Clear.Filter]												
Statistics CDP	Client MAC Addr (4:8c:50:62:14:6b	IP Address(Jov4 192.168.78.36	(lav6)	AP N AP4C	ame 77.6D9E.6162			WLAN Profile office_hq	WLAN SSID office_hq	User Name Bob	Protocol 802.11ac(5 GHz)	Status Associated	Auth Yes	Port Slot	Id Tunne No	No No
Rogues Clients																
Sleeping Clients Multicast																
Applications																

4. 從WLC CLI中,可以使用show client dertails 檢查客戶端狀態:

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 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	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
BSSID	70:69:5a:51:4e:cd
Channel	36
IP Address	192.168.78.36
Gateway Address	192.168.78.1
Netmask	255.255.255.0
••••	
Policy Manager State	RUN
EAP Type	PEAP
Interface	vlan1478
VLAN	1478
Quarantine VLAN	0
Access VLAN	1478

測試與Windows 10和Anyconnect NAM的連線:

1. 從可用的SSID清單和相應的EAP驗證型別(在本例中為PEAP)以及內部驗證表單中選擇 SSID。

	Cisco AnyConnect Secure Mobility Client – X VPN: Use a browser to gain access. Connect Web Authentication Required
	Network: Connected (10.103.150.57) internet all v image:
Cisco AnyConnect	× curity:
Enter info	rmation for the connection.
Media:	Wi-Fi Hidden Network
Descriptive Name:	office_hq
SSID:	office_hq can not required on current Wi-Fi.
Security:	WPA2 Enterprise AES
802. 1X Configuration	✓ PEAP ✓ g Security:
	tot currently protected by Umbrella.
	OK Cancel

2. 提供使用者驗證的使用者名稱和密碼。



3. 由於ISE向客戶端傳送SSC,您必須手動選擇信任證書(在生產環境中,強烈建議在ISE上安 裝受信任的證書)。

The server certificate for the network 'office_hq' has failed validation. Do you want to trust it? Certificate Name: manchur-ise.wlaaan.com@ Issued To: 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 Office_hq Issued To: Trust No Network: Authenticating office_hq Issued To: Trust Do Not Trust VPN: Venty your network connection. Issued By: Trust Do Not Trust Otable Bartific Bartific Bart Bart Bart BartBart BartBart BartB	Cisco AnyConnect X		
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 No Network: Authenticating office_hq	The server certificate for the network 'office_hq' has failed validation. Do you want to trust it?	VPN: Verify your network connection.	
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 No Network: Authenticating office_hq ull _ important	Certificate Name: rmanchur-ise.wlaaan.com@		
Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC Trust Do Not Trust Network: Authenticating office_hq ::!! ::!	Issued To: rmanchur-ise.wlaaan.com	No Network Connectivity	
Trust Do Not Trust	Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC	Network: Authenticating	
	Trust Do Not Trust	office_hq 🔒 📶 🗸 📰	
No License Key.		Web Security: No License Key.	

4. 檢查ISE上的身份驗證日誌並確保為使用者選擇了正確的授權配置檔案。

c	Refresh O Reset Repeat Counts	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	×	65	×	Endpoint Prof	Authentication	Authorization Policy	Authorization	IP Address		Network Device	Device Port	Identity Group	Posture Statu	Server	Mpm
	Feb 15, 2019 02:51:27.163 PM	٠	ò	0	Alce		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		à +		Alce	٠	F4:8C:50:62:14:68	*	Morosoft-W	Default >>	Default >> Wireless_Marketing	Marketing		*	WLC5520		Workstation 💠		manchur-ise 4	·

5. 檢查WLC上的客戶端條目,確保已將其分配給正確的VLAN並處於RUN狀態。

Clients											Entries 1 - :
Current Filter Nor	ne [Change Filter] [Clear Filte	z]									
Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel
f4:8c:50:62:14:6b	192.168.77.32	AP4C77.6D9E.6162	office_hq	office_hq	Alice	802.11ac(5 GHz)	Associated	Yes	1	1	No

6. 從WLC CLI中,可以使用show client dertails 檢查客戶端狀態:

Client MAC Address Client Username Client Webauth Username Hostname:	f4:8c:50:62:14:6b Alice N/A
Device Type: AP MAC Address AP Name AP radio slot Id Client State User Authenticated by Client User Group	Intel-Device 70:69:5a:51:4e:c0 AP4C77.6D9E.6162 1 Associated RADIUS Server Alice
Client NAC OOB State Wireless LAN Id Wireless LAN Network Name (SSID) Wireless LAN Profile Name Hotspot (802.11u) Connected For BSSID Channel IP Address Gateway Address Netmask	Access 3 office_hq office_hq Not Supported 765 secs 70:69:5a:51:4e:cd 36 192.168.77.32 192.168.77.1 255.255.255.0
 Policy Manager State	RUN
Policy Type. Authentication Key Management. Encryption Cipher. Protected Management Frame Management Frame Protection. EAP Type. Interface. VLAN.	WPA2 802.1x CCMP-128 (AES) No PEAP vlan1477 1477

疑難排解

1. 使用test aaa radius username

password

wlan-id

來測試WLC和ISE之間的RADIUS連線,使用test aaa show radius來顯示結果。

test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request Wlan-id..... 2 ApGroup Name..... none Values Attributes -----_____ 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 0x6e6f (28271) NAS-Identifier Airespace / WLAN-Identifier 0x0000002 (2) User-Password cisco!123 Service-Type 0x0000008 (8) 0x00000514 (1300) Framed-MTU Nas-Port-Type 0x0000013 (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

Raulus Selvei	Retry	Status
10.48.39.128	1	Success

Authentication Response: Result Code: Success

Attributes	Values
User-Name	Alice
State	ReauthSession:1447300a000003041d5665c
Class	CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59

Tunnel-Type Tunnel-Medium-Type Tunnel-Group-Id 0x000000d (13) 0x0000006 (6) 0x00005c5 (1477)

(Cisco Controller) >

2. 使用debug client 對無線客戶端連線問題進行故障排除。

3. 使用debug aaa all enable對WLC上的身份驗證和授權問題進行故障排除。



注意:請僅對debug mac addr使用此命令,以便根據進行調試的MAC地址限制輸出。

4. 請參閱ISE即時日誌和會話日誌,以確定問題身份驗證失敗和AD通訊問題。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。