使用RADIUS伺服器的外部Web驗證

目錄

簡介 必要條件 需求 採用元件 網路圖表 慣例 外部Web驗證 設定WLC 為Cisco Secure ACS配置WLC 在WLC上設定WLAN以進行Web驗證 在WLC上配置Web伺服器資訊 配置Cisco Secure ACS 在Cisco Secure ACS上配置使用者資訊 在Cisco Secure ACS上配置WLC資訊 客戶端身份驗證過程 客戶端配置 使用者端登入程式 驗證 檢驗ACS 驗證WLC 疑難排解 疑難排解指令

<u>相關資訊</u>

<u>簡介</u>

本檔案將說明如何使用外部RADIUS伺服器執行外部Web驗證。

<u>必要條件</u>

<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

- 輕量型存取點(LAP)和Cisco WLC組態的基本知識
- •瞭解如何設定和配置外部Web伺服器
- 瞭解如何配置Cisco Secure ACS

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 運行韌體版本5.0.148.0的無線LAN控制器
- 思科1232系列LAP
- 思科802.11a/b/g無線客戶端介面卡3.6.0.61
- 承載Web驗證登入頁面的外部Web伺服器
- 運行韌體版本4.1.1.24的Cisco Secure ACS版本

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定:



- •WLC使用IP地址10.77.244.206
- •LAP已註冊到IP地址為10.77.244.199的WLC
- •Web伺服器使用IP地址10.77.244.210
- Cisco ACS伺服器使用IP地址10.77.244.196
- 客戶端從對映到WLAN的管理介面接收IP地址 10.77.244.208

<u>慣例</u>

<mark>請參閱<u>思科技術提示慣例以瞭解更多有關文件慣例的資訊。</u></mark>

<u>外部Web驗證</u>

Web驗證是第3層驗證機制,用於對訪客使用者進行網際網路存取的驗證。使用此程式進行身份驗 證的使用者在成功完成身份驗證過程之前將無法訪問Internet。有關外部Web驗證程式的完整資訊 ,請參閱檔案<u>使用無線LAN控制器的外部Web驗證組態範例</u>的<u>外部Web驗證程式</u>一節。

在本檔案中,我們看到一個組態範例,其中使用外部RADIUS伺服器執行外部Web驗證。

<u>設定WLC</u>

在本檔案中,我們假設已設定WLC,且其LAP已註冊到WLC。本檔案進一步假設WLC已設定為基本 操作,且LAP已註冊到WLC。如果您是嘗試將 WLC 設定為搭配 LAP 進行基本操作的新使用者,請 參閱<u>向無線 LAN 控制器 (WLC) 註冊輕量型 AP (LAP)</u>。若要檢視註冊到WLC的LAP,請導覽至 Wireless > All APs。

在WLC設定為基本操作並具有一個或多個LAP註冊到它後,您可以使用外部Web伺服器設定WLC進行外部Web驗證。在我們的示例中,我們使用Cisco Secure ACS版本4.1.1.24作為RADIUS伺服器。首先,我們將為此RADIUS伺服器配置WLC,然後,我們將在Cisco Secure ACS上查詢此設定所需的配置。

為Cisco Secure ACS配置WLC

執行以下步驟以在WLC上新增RADIUS伺服器:

- 1. 在WLC GUI中,按一下「SECURITY」功能表。
- 2. 在AAA功能表下, 導覽至Radius > Authentication子功能表。
- 3. 按一下**New**,然後輸入RADIUS伺服器的IP地址。在本例中,伺服器的IP地址為 10.77.244.196。
- 4. 在WLC中輸入Shared Secret。應在WLC上以相同方式配置共用金鑰。
- 5. 為共用金鑰格式選擇ASCII或十六進位制。在WLC上需要選擇相同的格式。
- 6. 1812是用於RADIUS身份驗證的埠號。
- 7. 確保Server Status選項設定為Enabled。
- 8. 選中Network User Enable框以對網路使用者進行身份驗證。
- 9. 按一下「Apply」。

 cısco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	RADIUS Authenticatio	on Servers > New		(Article) et el este de la ciencie de la		
AAA General RADIUS Authentication Accounting Contents	Server Index (Priority) Server IPAddress	2 V 10.77.244.196				
 TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies 	Shared Secret Confirm Shared Secret	•••••]
AP Policies Local EAP	Key Wrap	(Designed for F	FIPS customer	s and requires a k	ey wrap complia	nt RADIUS server)
 Priority Order Access Control Lists 	Port Number	1812				
Wireless Protection Policies	Server Status	Enabled 💙				
> Web Auth	Support for RFC 3576	Enabled 💌				
P Advanced	Server Timeout	2 seconds				
	Network User	Enable Enable				
	Management	Enable Enable				
	IPSec	Enable				

<u>在WLC上設定WLAN以進行Web驗證</u>

下一步是在WLC上設定WLAN以進行Web驗證。若要在WLC上設定WLAN,請執行以下步驟:

- 1. 從控制器GUI上按一下「WLANs」功能表,然後選擇New。
- 2. 選擇WLAN作為Type。

0

3. 輸入您選擇的Profile Name和WLAN SSID,然後點選Apply。注意:WLAN SSID區分大小寫

ululu cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT
WLANs	WLANs > New				
WLANS	Туре	WLAN	~		
Advanced	Profile Name	WLAN1			
	WLAN SSID	WLAN1			
	HEAT BOLD	TETTA			

4. 在General索引標籤下,確保為Status和Broadcast SSID選中了Enabled選項。WLAN配置

VLANs	WLANs > Edit	
WLANs WLANs	General Security	y QoS Advanced
Advanced	Profile Name	WLANI
	Туре	WLAN
	SSID	WLAN1
	Status	C Enabled
	Padia Policy	(Modifications done under security tab will appear after applying the changes.)
	Radio Policy	All
	Interface	management 💌
	Broadcast SSID	Enabled
	Foot Notes	

- 5. 為WLAN選擇介面。通常,在唯一VLAN中配置的介面會對映到WLAN,以便客戶端接收該 VLAN中的IP地址。在本例中,我們將*management*用於介面。
- 6. 選擇**Security**頁籤。
- 7. 在Layer 2選單下,為Layer 2 Security選擇None。
- 8. 在Layer 3選單下,為Layer 3 Security選擇None。勾選「Web Policy」覈取方塊,然後選擇「 Authentication」。

WLANS	WLANs > Edit
WLANS	General Security QoS Advanced
WLANS	Layer 2 Layer 3 AAA Servers
Advanced	
	Layer 3 Security None
	Web Policy 2
	Authentication
	O Basethermah
	C Passanrougn
	Conditional Web Redirect
	Splash Page Web Redirect
	Preauthentication ACL None 👻
	Over-ride Global Config 🔲 Enable
	L
	Foot Notes

9. 在「AAA servers」功能表下,對於「驗證伺服器」,選擇在此WLC上設定的RADIUS伺服器 。其他選單應保留預設值。

CISCO WLANs WLANs WLANs HAlvanced	MONITOR WLANS CONTROLLER WRELESS SECURITY MANAGEMENT COMMS WLANS > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers	WIDS HELP		
	Select AAA servers below to override use of default servers on this WLAN Radius Servers	LDAP Server	rs .	
	Authentication Servers Accounting Servers	Server 1	None	¥
	C Enabled	Server 2	None	¥
	Server 1 None V Server 2 JP:10.77.204.196, Port:1812 None V Server 3 None V Local EAP Authentication	Server 3	None	
	Local EAP Authentication Enabled Authentication priority order for web-auth user			
	Faat Notes 2 CKIP is not supported by 20xx model APs 2 Web Policy cannot be used in combination with IPsec. 3 H-REAP Local Switching is not supported with IPsec. CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require adminis	trative override to reset e	voluded clients)	

在WLC上配置Web伺服器資訊

應在WLC上配置承載Web身份驗證頁面的Web伺服器。執行以下步驟配置Web伺服器:

- 1. 按一下Security頁籤。前往Web Auth > Web Login Page。
- 2. 將Web驗證型別設定為External。
- 3. 在「Web伺服器IP地址」欄位中,輸入託管「Web身份驗證」頁的伺服器的IP地址,然後按一 下**新增Web伺服器**。在本例中,IP地址為*10.77.244.196*,該地址顯示在External Web Servers下。
- 4. 在URL欄位中輸入Web Authentication頁面的URL(在本例中為 *http://10.77.244.196/login.html*)。

cisco	MONITOR WLANS CO	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Security	Web Login Page				
General	Web Authentication T	уре	External (Redirect to ext	ternal server) 🔽
Authentication	URL http://10.77.244.196	/login.html			
Fallback	External Web Servers				
LDAP	10.77.244.196 <u>Remove</u>				
Local Net Users MAC Filtering Disabled Clients User Login Policies	Web Server IP Addres	s]	
AP Policies		A	dd Web Ser	ver	
Local EAP					
Priority Order					
Access Control Lists					
 Wireless Protection Policies 					
 Web Auth Web Login Page Certificate 					
Advanced					

配置Cisco Secure ACS

在本文檔中,我們假設Cisco Secure ACS伺服器已經安裝並在電腦上運行。有關如何設定Cisco Secure ACS的詳細資訊,請參閱<u>Cisco Secure ACS 4.2配置指南</u>。

在Cisco Secure ACS上配置使用者資訊

要在Cisco Secure ACS上配置使用者,請執行以下步驟:

1. 從Cisco Secure ACS GUI中選擇**User Setup**,輸入使用者名稱,然後按一下**Add/Edit**。在本示 例中,使用者為*user1*。

CISCO SYSTEMS	User Setup
	Select
User Setup	User: user1
Shared Profile Components	List users beginning with letter/number:
System Configuration	ABCDEFGHIJKLM NOPQRSTUVUXYZ 0123456789
Administration Control	Remove Dynamic Users
Validation	Back to Help
Contine Documentation	

2. 預設情況下,PAP用於驗證客戶端。使用者的密碼在User Setup > Password Authentication > Cisco Secure PAP下輸入。確保選擇ACS Internal Database進行密碼身份驗證。

STATEMS	User Setup				
ser etup	Edit				
roup		User: us	eri (New C	Jser)	
ared Profile mponents		A 🗆	ccount Disabled		
work figuration		Supplem	entary User Info)	?
tem	Real Name	User1			
erface figuration	Description	-			
ministration itrel					-
ernal User abases		Us	ser Setup		?
ture	Password Aut	hentication:			_
work Access			AC	S Internal Database	•
les	CiscoSec	ure PAP (Also used	d for CHAP/MS-C	HAP/ARAP, if the Separa field is not checker	te j.)
orts and ivity	Pas	sword			
neumentation	Confirm Pas	sword			
	🗆 Separate	(CHAP/MS-CHAP/	ARAP)		
	Pas	sword			
	Confirm Pas	sword			
	When a token CHAP passwo especially use	server is used for rd for a token care ful when token ca	r authentication, d user allows CHA ching is enabled.	supplying a separate P authentication. This is	5
		Group to whi	ch the user is as	signed:	
		Default Group		•	

- 3. 需要為使用者分配使用者所屬的組。選擇Default Group。
- 4. 按一下「Submit」。

在Cisco Secure ACS上配置WLC資訊

要在Cisco Secure ACS上配置WLC資訊,請執行以下步驟:

- 1. 在ACS GUI中,按一下Network Configuration頁籤,然後按一下Add Entry。
- 2. 系統將顯示Add AAA client螢幕。
- 3. 輸入客戶端的名稱。在本範例中,我們使用WLC。
- 4. 輸入客戶端的IP地址。WLC的IP地址是10.77.244.206。
- 5. 輸入共用金鑰和金鑰格式。此專案應與WLC的「Security」功能表中建立的專案相符。
- 6. 選擇ASCII作為按鍵輸入格式,在WLC上應該相同。
- 7. 選擇**RADIUS(Cisco Airespace)**以使用Authenticate,以設定WLC和RADIUS伺服器之間使用的 通訊協定。
- 8. 按一下「Submit + Apply」。

	Add AAA Client
AAA Client Hostname	WLC
AAA Client IP Address	10.77.244.206
n Shared Secret	abc 123
RADIUS Key Wrap	
Key Encryption Key	
Key Input Format	∉ ASCII C Hexadecimal
Authenticate Using	RADIUS (Cisco Airespace)
Single Connect TACACS+	AAA Client (Record stop in accounting on failure)
Log Update/Watchdog Pa	ckets from this AAA Client
Log RADIUS Tunneling Part	skets from this AAA Client
Match Framed-IP-Address	s with user IP address for accounting packets from this AAA Client
	Submit Submit + Apply Cancel

<u>客戶端身份驗證過程</u>

<u>客戶端配置</u>

在本示例中,我們使用Cisco Aironet案頭實用程式執行Web身份驗證。執行以下步驟以配置 Aironet案頭實用程式。

- 1. 從開始>Cisco Aironet > Aironet Desktop Utility 開啟Aironet案頭實用程式。
- 2. 點選Profile Management選項卡。

Cisco Aironet Desktop Utility - Current Profile: Default ion Options Help	t ?
urrent Status Profile Management Diagnostics	
Default	<u>N</u> ew
	Modify
	Remo <u>v</u> e
	Activate
Details	
Network Type:	Import
Security Mode:	
Network Name 1 (SSID1):	<u>Export</u>
Network Name 2 (SSID2):	Scan
Network Name 3 (SSID3):	- Ogana
Auto Select Profiles	Order Profiles

3. 選擇**Default**配置檔案,然後按一下**Modify**。按一下**General**頁籤。配置配置檔名稱。在此範例 中,使用*Default*。在Network Names下配置SSID。在本範例中,使用*WLAN*1。

Profile Management	
General Security Advanc	red
Profile Settings	
Profile Name:	Default
Client Name:	Client1
Network Names	
SSID1:	WLAN1
SSID2:	
SSID3:	
-	
	OK Cancel

注意:SSID區分大小寫,並且應該與WLC上配置的WLAN匹配。按一下**Security**頁籤。為 Web驗證選擇**None**作為Security。

Profile Management	? 🔀
General Security Advanced	
Set Security Options	
O WPA/WPA2/CCKM WPA/WPA2/CCKM EAP Type: LEAP ✓	
○ WPA/WPA2 Passphrase	
0 802.1x 802.1x EAP Type: LEAP	
Pre-Shared Key (Static WEP)	
None	
Configure Allow Association to Mixed Cells Locked Profile	
Group Policy Delay: 0 😂 sec	
	ancel

按一下Advanced頁籤。在「Wireless Mode」選單下,選擇無線客戶端與LAP通訊的頻率。在 Transmit Power Level下,選擇WLC上設定的電源。保留「Power Save Mode(節能模式)」 的預設值。選擇Infrastructure作為Network Type。將802.11b前導碼設定為Short & Long以獲 得更好的相容性。按一下「OK」(確定)。

Transmit Power Level	Power Save Mode:	CAM (Constantly A	wake Mode) 🛛 💙							
802.11b/g: 100 mW	Network Type:	× Infrastructure								
802.11a: 40 mW	802.11b Preamble:	Short & Long	O Long Only							
Wireless Mode	Wireless Mode When Starting	g Ad Hoc Network								
🗹 5 GHz 54 Mbps										
🗹 2.4 GHz 54 Mbps	🔿 5 GHz 54 Mbps	◯ 5 GHz 54 Mbps								
2.4 GHz 11 Mbps	O 2.4 GHz 11 Mbps									
	2.4 GHz 54 Mbps	Channe	l. Auto 👻							
	802.11 Authentication Mode	802.11 Authentication Mode								
	O Auto 💿 O	ipen () Shared							

4. 在客戶端軟體上配置配置檔案後,客戶端將成功關聯並從為管理介面配置的VLAN池接收IP地 址。

使用者端登入程式

本節說明如何進行使用者端登入。

- 開啟瀏覽器視窗並輸入任何URL或IP地址。這會將Web驗證頁面導向使用者端。如果控制器執行的是低於3.0的任何版本,使用者必須輸入*https://1.1.1.1/login.html*以開啟Web驗證頁面。此時將顯示一個安全警報視窗。
- 2. 按一下「Yes」以繼續。
- 3. 出現「Login(登入)」視窗時,輸入在RADIUS伺服器上配置的使用者名稱和密碼。如果登入 成功,您將看到兩個瀏覽器視窗。較大的視窗表示登入成功,您可以使用此視窗瀏覽

Web Authentication
Login Successful I
You can now use all regular network services over the wireless network.
Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page: <u>https://l.1.1Apgout.html</u>

Internet。使用較小的視窗,以便在使用完訪客網路後註銷。



要成功進行Web身份驗證,您需要檢查裝置是否以適當的方式配置。本節介紹如何驗證過程中使用 的裝置。

<u>檢驗ACS</u>

1. 在ACS GUI上按一下**User Setup**,然後按一下**List All Users**。

CISCO SYSTEMS	User Setup
and the and the second	Select
User Setup	
Group Setup	User:
Shared Profile Components	Find Add/Edit
Network Configuration	List users beginning with letter/number:
System Configuration	<u>A B C D E F G H I J K L M</u> N O P Q R S T U V W X Y Z
Configuration	
Administration Control	List all users
Databases	Remove Dynamic Users
name Nation	
Network Access Profiles	P Back to Help
Reports and Activity	
Documentation	

確保Status of the User為Enabled, 並且Default組對映到使用者。

er List			
User	Status	Group	Network Access Profile
user1	Enabled	Default Group (2 users)	(Default)

2. 按一下Network Configuration索引標籤,然後檢視AAA Clients表,以驗證WLC是否已設定為 AAA使用者端。

and the second second	and the						
ab No	% Q	AAA Clients					
ed Profile posents	AAA Client Hostname	AAA Client IP Address	Authen	ticate Using			
	wici	10.77.244.206	RADIUS (C	isco Airespace)			
-		Add Fotry Search					
		How Entry Goardin					
tion							
in l	\$	AAA Servers					
	AAA Server Name	AAA Server IP Address	AAA Server IP Address AA				
	TS-Web	10.77.244.196	Cis	coSecure ACS			
		Add Entry Search					
60 N							
		Proxy Distribution Table					
	Character String	AAA Servers	Strip	Account			
	(Default)	TS-Web	No	Local			
		Add Entry Sort Entries					

<u>驗證WLC</u>

1. 在WLC GUI上按一下**WLANs**選單。確保頁面中列出了用於Web身份驗證的WLAN。確保 WLAN的Admin Status為*Enabled*。確保WLAN的安全策略顯示*Web-Auth*。

cisco	MONITOR WLANS		SS SECURITY MANAGEN	MENT COMMANDS	: HELP	
WLANS	WLANs Profile Name	Туре У	VLAN SSID	Admin Status	Security Policies	
Advanced	WLAN1	WLAN W	WLAN1	Enabled	Web-Auth	

2. 在WLC GUI上按一下「SECURITY」選單。確保頁面上列出了Cisco Secure ACS(10.77.244.196)。確保選中「Network User(網路使用者)」框。確認連線埠為 *1812*,且管理狀態為*Enabled*。

cisco	MONITOR	<u>W</u> LANS <u>C</u> O	ONTROLLER	WIRELESS S	ECURITY N	MANAGEMENT CO	MMANDS HELP	
Security	RADIUS	Authenticati	ion Serve	rs				
 AAA General RADIUS Authentication Accounting Fallback TACACS+ 	Call Stati	ion ID Type [Key Wrap	IP Address	ed for FIPS custome	ers and require	es a key wrap compli	ant RADIUS server)	
	Network	Management	Server Index	Server Address	Port	IPSec	Admin Status	
LDAP Local Net Users		V	1	10.77.244.196	1812	Disabled	Enabled	
Disabled Clients User Login Policies AP Policies								
Priority Order								
Priority Order Access Control Lists								
Priority Order Access Control Lists Wireless Protection Policies								
 Priority Order Access Control Lists Wireless Protection Policies Web Auth 								

<u>疑難排解</u>

Web驗證不成功的原因有很多,<u>對無線LAN控制器(WLC)上的Web驗證進行排解疑難</u>檔案清楚說明 這些原因。

<u>疑難排解指令</u>

注意:使用這些<u>debug命令之前,請先參</u>閱有關Debug命令**的重要**資訊。

Telnet至WLC並發出以下命令對驗證進行疑難排解:

• debug aaa all enable

Fri	Sep	24	13:59:52	2010:	00:4	0:96:	ac:	dd:(05 ;	Suco	ces	sful	l tı	ans	miss	sion	n of	ΕAι	ithe	enti	ic
atic	on Pa	acke	et (id 1)	to 10	.77.2	44.19	6:18	812	, p:	roxy	/ st	tate	e 00):40	:96	ac	:dd	:05-	-00:	:01	
Fri	Sep	24	13:59:52	2010:	0000	:0000	01	01	00	73	00	00	00	00	00	00	00	00	00	00	0
0 00).	s																			
Fri	Sep	24	13:59:52	2010:	0000	0010:	00	00	00	00	01	07	75	73	65	72	31	02	12	93	С
3 66	5.		user1	f																	
Fri	Sep	24	13:59:52	2010:	0000	0030:	75	73	65	72	31										
	us	seri	1																		
Fri	Sep	24	13:59:52	2010:	****]	Enter	pro	oces	ssI	ncor	ning	gMes	ssag	ges:	res	spoi	nse	cod	le=2	2	
Fri	Sep	24	13:59:52	2010:	****]	Enter	pro	oces	ssRa	adiı	ısRe	espo	onse	e: r	espo	onse	e co	ode=	=2		
Fri	Sep	24	13:59:52	2010:	00:4	0:96:	ac:	dd:(05 2	Acce	ess	-Aco	cept	re	ceiv	zed	fro	om I	RAD	IUS	s
erve	er 10	0.77	7.244.196	for mo	obile	00:4	0:9	6:a0	c:do	d:05	5 re	ece	lve	[d =	0						
Fri	Sep	24	13:59:52	2010:	Auth	oriza	tio	nRes	spoi	nse	: 0:	x122	2380	lb0							
Fri	Sep	24	13:59:52	2010:		str	ucti	ure	Siz	e										. 89	Э
Fri	Sep	24	13:59:52	2010:		res	ult	Code	e											0	
Fri	Sep	24	13:59:52	2010:		pro	toc	olUs	sed											. 03	x0
0000	001																				
Fri	Sep	24	13:59:52	2010:		pro	xyS	tate	e											00):
40:9	6:A0	C:DI	0:05-00:0	0																	
Fri	Sep	24	13:59:52	2010:		Pac	ket	COI	nta	ins	2 2	AVP	5:								
Fri	Sep	24	13:59:52	2010:			AV	P[01	1] 1	Frar	ned	-IP	-Ado	lres	s						
	.0x1	Effi	Effff (-1) (4 by	ytes)																
Fri	Sep	24	13:59:52	2010:			AV	P[02	2] (Clas	ss.										
	.CAC	CS:()/5183/a4	df4ce/u	lser1	(25	byt	es)													
Fri	Sep	24	13:59:52	2010:	Auth	entic	ati	on :	fai	led	fo	r us	serí	L, S	erv	ice	Тур	pe:	0		

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio n 00:40:96:ac:dd:05 Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96 :ac:dd:05 source: 48, valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s tation 00:40:96:ac:dd:05 Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c Fri Sep 24 13:59:52 2010: Packet contains 12 AVPs: AVP[01] User-Name..... Fri Sep 24 13:59:52 2010:user1 (5 bytes) Fri Sep 24 13:59:52 2010: AVP[02] Nas-Port.....0x00000002 (2) (4 bytes) Fri Sep 24 13:59:52 2010: AVP[03] Nas-Ip-Address.....0x0a4df4ce (172881102) (4 bytes) AVP[04] Framed-IP-Address..... Fri Sep 24 13:59:52 2010:0x0a4df4c7 (172881095) (4 bytes)

debug aaa detail enable

失敗的身份驗證嘗試列在Reports and Activity > Failed Attempts處的選單中。

相關資訊

- 無線 LAN 控制器 Web 驗證組態範例
- 對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 在無線LAN控制器(WLC)上使用LDAP的Web驗證組態範例
- 技術支援與文件 Cisco Systems

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)。