Cisco整合無線網路TACACS+組態

目錄

簡介 必要條件 需求 採用元件 慣例 控制器中的TACACS+實作 驗證 **Authorization** 會計 WLC中的TACACS+組態 新增TACACS+身份驗證伺服器 新增TACACS+授權伺服器 新增TACACS+記帳伺服器 配置身份驗證順序 驗證設定 配置Cisco Secure ACS伺服器 網路設定 介面組態 使用者/組設定 Cisco Secure ACS中的記帳記錄 WCS中的TACACS+配置 使用虛擬域的WCS 配置Cisco Secure ACS以使用WCS 網路設定 介面組態 使用者/組設定 調試 從WLC為role1=ALL調試 從WLC調試多個角色 從WLC調試授權失敗 相關資訊

<u>簡介</u>

本檔案將提供思科無線LAN控制器(WLC)和思科整合無線網路的思科無線控制系統(WCS)中的終端 存取控制器存取控制系統Plus(TACACS+)組態範例。本文還提供一些基本的故障排除提示。

TACACS+是一種使用者端/伺服器通訊協定,可為嘗試取得路由器或網路存取伺服器管理存取的使

用者提供集中式安全。TACACS+提供以下AAA服務:

- 嘗試登入網路裝置的使用者的身份驗證
- 確定使用者應具有何種訪問級別的授權
- •用於跟蹤使用者所做的所有更改的記帳

有關AAA服務和TACACS+功能的詳細資訊,請參閱<u>配置TACACS+</u>。

請參閱<u>TACACS+和RADIUS比較</u>,以比較TACACS+和RADIUS。

<u>必要條件</u>

<u>需求</u>

思科建議您瞭解以下主題:

- •瞭解如何配置WLC和輕量型存取點(LAP)以進行基本操作
- •輕量型存取點通訊協定(LWAPP)和無線安全方法知識
- •基本知識RADIUS和TACACS+
- Cisco ACS配置基礎知識

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 適用於Windows的Cisco安全ACS版本4.0
- 執行版本4.1.171.0的Cisco無線LAN控制器。軟體版本4.1.171.0或更新版本支援WLC上的 TACACS+功能。
- 運行版本4.1.83.0的Cisco無線控制系統。4.1.83.0或更高版本的軟體支援WCS上的 TACACS+功能。

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。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

控制器中的TACACS+實作

<u> 驗證</u>

可以使用使用使用者名稱和密碼的本地資料庫、RADIUS或TACACS+伺服器執行身份驗證。實施沒 有完全模組化。身份驗證和授權服務相互關聯。例如,如果使用RADIUS/本機資料庫執行驗證,則 不會使用TACACS+執行授權。它將使用與本地或RADIUS資料庫中的使用者關聯的許可權,例如只 讀或讀取/寫入,而使用TACACS+執行身份驗證時,授權與TACACS+關聯。

在配置了多個資料庫的情況下,會提供CLI以指定後端資料庫的引用順序。

Authorization

授權是基於任務的,而不是基於每個命令的實際授權。這些任務將對映到多個頁籤,這些頁籤對應 於當前在Web GUI上的七個選單欄專案。以下是選單欄專案:

- 監視
- WLAN
- 控制器
- 無線
- 安全性
- 管理
- 指令

此對映的原因是因為大多數客戶使用Web介面而不是CLI來配置控制器。

大廳管理員管理(LOBBY)的附加角色可供僅需要具有大廳管理員許可權的使用者使用。

使用者享有的任務是在TACACS+(ACS)伺服器中使用自訂屬性值(AV)配對進行設定。使用者可以獲 得執行一項或多項任務的授權。最小授權僅監控,最大授權為ALL(授權執行所有七個頁籤)。 如 果使用者無權執行特定任務,則仍允許使用者以只讀模式訪問該任務。如果啟用了身份驗證,且身 份驗證伺服器無法訪問或無法授權,則使用者無法登入到控制器。

注意:若要使通過TACACS+的基本管理身份驗證成功,必須在WLC上配置身份驗證和授權伺服器 。記帳配置是可選的。

會計

每當成功執行特定使用者啟動的操作時,都會發生記帳。變更的屬性將連同以下內容一起記錄在 TACACS+記帳伺服器上:

- 進行更改的個人的使用者ID
- 使用者從其登入的遠端主機
- 執行命令的日期和時間
- 使用者的授權級別
- 一個字串,提供有關執行的操作和提供的值的資訊

如果計費伺服器無法訪問,使用者仍可以繼續會話。

注意:在軟體版本4.1或更早版本中,不會從WCS生成會計記錄。

WLC中的TACACS+組態

WLC軟體版本4.1.171.0和更新版本引入新的CLI和網路GUI變更,以便在WLC上啟用TACACS+功能 。本節列出了介紹的CLI以供參考。Web GUI的相應更改將新增到「安全」頁籤下。

本檔案假設WLC的基本組態已完成。

若要在WLC控制器中設定TACACS+,需要完成以下步驟:

- 1. <u>新增TACACS+身份驗證伺服器</u>
- 2. <u>新增TACACS+授權伺服器</u>

3. <u>新增TACACS+記帳伺服器</u>

4. 配置身份驗證順序

新增TACACS+身份驗證伺服器

完成以下步驟即可新增TACACS+驗證伺服器:

1. 使用GUI,然後前往Security > TACACS+ > Authentication。

uluulu cisco	MONITOR MLANS	CONTROLLER WIPELES	S SECURITY	M&N4GEMENT	COMMANDS	HELP	Sage Configuration Eng Logout Befreu
Security	TACACS+ Auther	ntication Servers					New
AAA General e RADIUS Authentication Accounting TACACS+ Authentication Accounting Authentication Accounting Authentication	Server Index	Server Address	For	L Admin Sta	lus		

2. 新增TACACS+伺服器的IP地址並輸入共用金鑰。如果需要,請更改TCP/49的預設埠。

cisco	MONITOR MLANS CONTRO	LLER WIRELESS SECURIT	Y MANAGEMENT	сомнилоз	Herb	Sage Configuration Eng Logaut Bafresh
Security	TACACS+ Authentication	Servers > New				< Back Apply
- AAA General	Server Index (Priority)	1 🛩				
RADOJS Authentication Accounting	Server IPAddress	10.3.1.12				
TACACS+ Aythentication	Shared Secret Format	ASCII 🛩				
Accounting Authorization	Shared Secret]	
Local Net Users MAC Filtering	Confirm Shared Secret]	
Disabled Clients User Login Policies AP Policies	Port Number	49				
+ Local EAP	Server Status	Enabled 💌				
Priority Order Access Control Lists	Retransmit Timoout	2 seconds				

3. 按一下「**Apply**」。您可以使用**config tacacs auth add** <Server Index> <IP addr> <port> [ascii/hex] <secret>指令,從CLI完成**此操**作:

(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123

新增TACACS+授權伺服器

完成以下步驟即可新增TACACS+授權伺服器:

- 1. 在GUI上,前往Security > TACACS+ > Authorization。
- 2. 新增TACACS+伺服器的IP地址並輸入共用金鑰。如果需要,請更改TCP/49的預設埠。

սիսիս cisco	MONITOR WLANS CONTR	OLLER WIPELESS	SECURITY MOUNCEMENT	соммалов не	Sage Configuration	i Eng i Logout Befreih
Security	TACACS+ Authorization	Servers > New			< 8	ack Apply
T AAA General	Server Index (Priority)	1 💌				
RADGUS Authentication	Server IPAddress	10.1.1.12				
Accounting TACACS+ Authentication	Shared Secret Format	4500 💌				
Accounting Authorization	Shared Secret	*****				
LDAP Local Net Users MAC Filtering	Confirm Shared Secret					
Disabled Cherks User Login Policies AP Policies	Port Number	49				
+ Local EAP	Server Status	Enabled 💌				
Priority Order Access Control Lists	Retransmit Timeout	2 seconds				

3. 按一下「Apply」。您可以使用config tacacs atr add <Server Index> <IP addr> <port> [ascii/hex] <secret>指令,從CLI完成此操作:

(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123

新增TACACS+記帳伺服器

完成以下步驟即可新增TACACS+記帳伺服器:

- 1. 使用GUI,然後前往Security > TACACS+ > Accounting。
- 2. 新增伺服器的IP地址並輸入共用金鑰。如果需要,請更改TCP/49的預設埠。

alialia cisco	MONITOR MUNIC	ONTROLLER WIRELESS	SECURITY	MUNICEMENT	сомилоз	Rh	Sage Configuration Eing Logaut Befresh
Security	TACACS+ Accountin	ng Servers > New					< Back Apply
Ceneral	Server Index (Priority)	1 🛩					
Authentication	Server IPAddress	10.1.1.12					
TACACS+ Authentication	Shared Secret Format	ASCII 🛩					
Authorization	Shared Secret						
Local Net Users MAC Filtering Disabled Clents	Confirm Shared Secret						
User Login Publies AP Policies	Port Number	49					
Local EAP	Server Status	Enabled 💌					
Priority Order	Bakaran b Taranak						
Access Control Lists	Petransmit Timeout	seconds					

3. 按一下「Apply」。您可以使用config tacacs acct add <Server Index> <IP addr> <port> [ascii/hex] <secret>命令,在CLI中完成以下操作:

(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123

<u>配置身份驗證順序</u>

此步驟說明當配置了多個資料庫時,如何配置AAA身份驗證順序。驗證順序可以是**local和** RADIUS,或者local和TACACS。驗證順序的預設控制器組態為*本機和RADIUS*。

完成以下步驟以設定驗證順序:

- 1. 在GUI中,轉至Security > Priority Order > Management User。
- 2. 選擇身份驗證優先順序。在本範例中,已選擇TACACS+。
- 3. 按一下Apply即可進行選擇。

cisco	MONITOR WLANS	CONTROLLER	WPELESS	SECURITY	MANAGEMENT	соммира	HEID	Sage Configuration Bing Logaut Befresh
Security	Priority Order > N	lanagement U	ser					Apply
LICA General FADDUS Authentication Accounting TACACS+ Authentication Accounting Authentication LDAP Local Net Users NAC Filtering Disabled Cleants User Login Policies AP Policies	Authentication Prior	ty as the first server	O Redus @	TACACS+				
Local EAP Priority Order Management User								

您可以使用config aaa auth mgmt <server1> <server2>指令,在CLI中完成以下操作:

(Cisco Controller) >config aaa auth mgmt tacacs local

驗證設定

本節介紹用於驗證WLC上的TACACS+組態的命令。以下是一些有用的**show**命令,可幫助確定配置 是否正確:

```
• show aaa auth — 提供有關驗證順序的資訊。
 (Cisco Controller) >show aaa auth
Management authentication server order:
   1.....local
   2..... Tacacs

    show tacacs summary — 顯示TACACS+服務和統計資訊的摘要。

 (Cisco Controller) >show tacacs summary
Authentication Servers
Idx Server Address Port State Tout
 ____ _____
               ____
                    _____
                           ____
   10.1.1.12 49 Enabled 2
1
Authorization Servers
Idx Server Address Port
                    State
                          Tout
   _____ ____
                           ____
1 10.1.1.12
              49
                   Enabled 2
Accounting Servers
Idx Server Address Port State Tout
   ----- -----
____
    10.1.1.12 49 Enabled
                           2
• show tacacs auth stats — 顯示TACACS+驗證伺服器統計資訊。
 (Cisco Controller) >show tacacs auth statistics
Authentication Servers:
Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests.....
                                 7
Retry Requests..... 3
```

Accept Responses. Reject Responses. Error Responses. Restart Responses. Follow Responses. GetData Responses. Encrypt no secret Responses.	3 0 0 0 0 0 0
Challenge Responses	0 0 12 0 0 哭体計姿司
• SHOW LACAUS ALLER SLALS — 顯小TACAUS+投催问版	命机計具剤。
(Cisco Controller) >snow tacacs athr statistics	
Server Index. Server Address. Msg Round Trip Time. First Requests. Retry Requests. Received Responses. Authorization Success. Authorization Failure. Challenge Responses. Malformed Msgs. Bad Athrenticator Msgs. Timeout Requests. Unknowntype Msgs. Other Drops. • Show facacs acct stats — 顯示TACACS+記帳伺脈 (Cisco Controller) >show tacacs acct statistics Accounting Servers:	1 10.1.1.12 0 (1/100 second) 3 3 3 0 0 0 0 0 0 0 0 0 0 8 器統計資訊。
Server Index Server Address. Msg Round Trip Time. First Requests. Retry Requests. Accounting Response. Accounting Request Success. Accounting Request Failure. Malformed Msgs. Bad Authenticator Msgs. Timeout Requests. Unknowntype Msgs. Other Drops.	1 10.1.1.12 0 (1/100 second) 133 0 0 0 0 0 0 0 0 399 0 0 0

配置Cisco Secure ACS伺服器

本節提供TACACS+ACS伺服器中用於建立服務和自定義屬性以及將角色分配給使用者或組的步驟。

本節不介紹使用者和組的建立。假定根據需要建立使用者和組。有關如何建立使用者和使用者組的 資訊,請參閱<u>適用於Windows Server 4.0的Cisco Secure ACS使用手冊</u>。 完成以下步驟:

將控制器管理IP地址新增為AAA客戶端,身份驗證機製為TACACS+(Cisco IOS)。



<u>介面組態</u>

請完成以下步驟:

- 1. 在Interface Configuration選單中,選擇TACACS+(Cisco IOS)連結。
- 2. 啟用New Services。
- 3. 選中User和Group覈取方塊。
- 4. 輸入ciscowlc作為「服務」,輸入common作為「協定」。
- 5. 啟用Advanced TACACS+功能。

User Group Image: PPP IP PPP IP Image: PPP IPX PPP IPX Image: PPP Multilink PPP Apple Talk Image: PPP Apple Talk PPP Apple Talk Image: PPP VPDN PPP LCP Image: PPP LCP Image: ARAP Image: PIX Shell (exec) Image: PIX Shell (pixshell) Image: Protocol Image: Service Image: Protocol Image: Protocol Image: Protocol Image: Protocol			TACACS+ Serv	ices	3
Image: PPP IP Image: PPP IPX Image: PPP IPX Image: PPP Multilink Image: PPP Multilink Image: PPP Apple Talk Image: PPP VPDN Ima	User	Group			
□ □ PPP IPX □ □ PPP Multilink □ □ PPP Apple Talk □ □ PPP VPDN □ □ PPP LCP □ □ ARAP □ □ ARAP □ □ PIX Shell (exec) □ □ SLIP		•	PPP IP		
PPP Multilink PPP Apple Talk PPP VPDN PPP LCP ARAP Shell (exec) PIX Shell (pixshell) SLIP			PPP IPX		
Image: PPP Apple Talk Image: PPP VPDN Image: PPP LCP Image: ARAP Image: PIX Shell (exec) Image: PIX Shell (pixshell) Image: PIX Shell (pi			PPP Multilink		
□ PPP VPDN □ PPP LCP □ ARAP □ Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Service Protocol			PPP Apple Talk		
□ PPP LCP □ ARAP □ Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Service Protocol			PPP VPDN		
□ ARAP □ Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Service Protocol ☑ ☑ ☑ ☑ □ □ □ □ □ □ □ □ □ □			PPP LCP		
□ I Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Service Service Protocol I Iciscowlc □ Iciscowlc □ Iciscowlc			ARAP		
□ PIX Shell (pixshell) □ SLIP New Services Service Protocol ☑ ☑ ☑ ☑ □ □		1	Shell (exec)		
SLIP New Services Service Protocol Image: Common Image: Common Image: Common			PIX Shell (pixshell)		
New Services Service Protocol Common			SLIP		
Service Protocol Image: Service Im	New S	ervices			
Image: Second control Image: Control Image: Control			Service	Protocol	
		1	ciscowlc	common	
			•		
Advanced Configuration Options			Advanced Configurati	ion Options	3

6. 按一下「Submit」以應用變更。

使用者/組設定

請完成以下步驟:

- 1. 選擇以前建立的使用者/組。
- 2. 前往TACACS+設定。
- 3. 勾選與「介面配置」部分中建立的ciscowlc服務對應的覈取方塊。
- 4. 選中Custom attributes覈取方塊。

Cisco Systems	Group Setup	
يحتا التسحيا التس	Jump To Access Restrictions	
User Setup	Shell Command Authorization Set	
Setup Shared Profile Components	Assign a Shell Command Authorization Set for any network device	
Network Configuration	C Per Group Command Authorization Unmatched Cisco IOS commands	
System Configuration	© Deny	
Administration	Anuments:	
Del External User Databases	Arguments:	
Posture Validation	Unlisted arouments	
Reports and Activity	C Permit © Deny	
Documentation	✓ ciscowic common	
	✓ Custom attributes	
	role1=ALL	
	Custom attributes	
	IETF RADIUS Attributes	
	Callback NAS Promot	
	Submit Submit + Restart Cancel	

- 5. 如果建立的使用者只需要訪問WLAN、SECURITY和CONTROLLER,請在Custom attributes下方的文本框中輸入此文本:role1=WLAN role2=SECURITY role3=CONTROLLER。如果使用者僅需要訪問SECURITY頁籤,請輸入以下文本:role1=安 全。此角色對應控制器網路GUI中的七個功能表欄專案。選單欄專案包括MONITOR、 WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT和COMMAND。
- 6. 輸入使用者需要的role1、role2等角色。如果使用者需要所有角色,則應使用關鍵字ALL。大 廳管理員角色應使用關鍵字LOBBY。

<u>Cisco Secure ACS中的記帳記錄</u>

WLC的TACACS+記帳記錄可在Cisco Secure ACS的「TACACS+報告和活動管理」中獲得:

Carofecure ACS - No	crosoft Internet Explorer											X
File Edit View Favo	rites Tools melp											
4-8ad + 17 - Q	3 3 QSeath (Branner Steda 3)	ù-@										_
Address (a) http://127.0-1	8.1.40877											• 12 Co Units *
Google C+	🛨 Ga 🕂 💭 🕈 🦙 😭 Backmarks = 👰	I blocked 🚏 Owsk = 🦄	ANNA - DAVID	Sedtor 🖉								 Settingire
Case Status	Reports and Activity											×
- A. A.	Select	Select										
SHITTER.		Tecoca+ Administrati	on active.csv	infrash 🕅 Gam	micad							
Cogramp 1	Reports	Regular Expression		Start Date	5 Time	End Date & Time		Pows per	Fage			
Bell Seller				nm/88/007	y Minimum as	mm/88/yyyyy,24c-mm	55	50				
S Paretterte	E TAGACE+ Accounts	Apply Filter Ce	ar Filter									
- Internet	A TACACS+ Admostration	Filtering is not applied.										
Carliardia	EADIL/S Accounting	Date 4 Time	User-Name On	sa-Name		cmd	aris b	d service	NAS-Portname	task id	NAS-12-Add	ess reason
Zhibin.	D Yor Accounts	02/22/2007 36:26:52	ac Tacacs	Group for WLC	wian enable 1		249	shell		224	10.10.80.3	
Consideration	E Faled attended	02/22/2007 14-26-52	ac Tacacs	Group for WLC	wian idap delete	1 position 2	249	shell		223	10.10.00.3	
Configuration	Logged-in Users	02/22/2007 14:26:52	ac Tacace	Group for WLC	wian Idap déléte	1 position 1	249	1040		222	10.10.00.3	
- St Laterature	Detabled accounts	02/22/2007 16:26:52	ac Tacaca	Group for WLC	wian Idap delete	1 position 0	249	shell		221	10.10.80.3	
and Cashed	Bill acts backup and Pestore	02/22/2007 16:26:52	ad Tacads	Group for WLC	wian timeout 1.0		249	shell		220	10.10.80.3	
1 Drivenal Uper	PD total and total at	02/22/2007 16:26:52	ac Tacacs	Group for WLC	wian reac-filterin	g disable 1	249	shell		229	10.10.80.3	
P.Z. DOBUG	EL DECEDERE PRENCECON	02/22/2007 36:26:52	ac Tacace	Group for WLC	wan security is t	NONE for wian-id 1	249	shell		238	10.10.80.3	- C - 1
TITLE Participan	Administration, Audit	02/22/2007 14:26:52	ac Tacaca	Group for WLC	wian security wa	N(WPA/RSN) disable 1	249	12740		417	10.10.80.9	100
Concession Access	User Reservord Charges	02/22/2007 14:26:52	ac Tacaca	Group for WLC	wian aaa-overtid	e disable 1	249	1540		236	10.10.00.3	
Troller	ACS Service Monitoring	10/20/20/1 30/20/52 1	HIC THOMOS	Group for WLC	wan gos 1 plater	um .	1000	straps		235	10.10.00.5	
C Assertant	-	100/00/00/1110/00/00 1	ini Tecece	Group for WLC	was show a at	r 1 0 0 0 0 mm inst	249	steel		2010	10.10.00.0	
C. Lagrange		02/22/2007 116:26:52	lat Tatata	Group for WLC	wian broadcast-s	usid enable 1	249	shell		212	10.10.80.3	- C
B Prometation		02/22/2007 16:26:52	ac Tacaca	Group for WLC	wiat exclusionist	10	249	shell	1	711	10.10.00.3	- C - 1
	P Ball to Welp	02/22/2007 16 26 52	ac Tacaca	Group for WLC	when enclusionist	1 disable	249	shell	2	230	10.10.80.9	
		02/22/2007 16:26:52	IN TACACS	Group for WLC	wian act 1		249	shell	-	209	10.10.80.3	
		02/22/2007 36:26:52	ac Tacacs	Group for WLC	wian interface 1	100	249	shell		208	10.10.00.3	
		02/22/2007 36:26:52	ac Tacace	Group for WLC	wian disable 1		249	shell		207	10.10.00.3	
•		10		1.0				1		1		erset.
Martine 🛄 🏶 🖓	Chooleoure ACS Lop	TCS - Netteped		The state by Ph.	Averal	itta enecitada	-Parend.	 Class 	Arpydan(2),	Jeco - Morosol	1944-1 S.C	10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

<u>WCS中的TACACS+配置</u>

請完成以下步驟:

- 1. 從GUI使用根帳戶登入WCS。
- 2. 新增TACACS+伺服器。前往Administration > AAA > TACACS+ > Add TACACS+ Server。

ahaha	Wireless Control System	Username: root Logout Refresh Print View 🖄
cisco	Bonitor • Beports • Configure • Location • Administration • Belo •	
AAA	TACACS+	Select a command 👻 640
Change Password	No TACACS+ Servers found in the system	
AAA Node		
Users		
Groups		
Active Sessions		
TACACS+		
RADIUS		

3. 新增TACACS+伺服器詳細資訊,例如IP地址、埠號(49為預設值)和共用金鑰。

ababa	Wireless Control S	ystem	Username: root Logaut Refresh Print View 🔡
cisco	Monitor • Beports • Cor	ifigure = Location = Administration = Help =	
AAA	TACACS+		
Change Password	Server Address	10.1.1.12	
AAA Node	Port	49	
liters	Shared Secret Format	ASCII 🛩	
CHILD .	Shared Secret		
Groups	Confirm Shared Secret	••••	
Active Sessions	Retransmit Timeout	5 seconds	
TACACS+	Retries	1	
	Authentication Type	PAP 💌	
AADIOS	Submit Cancel		

4. 在WCS中啟用TACACS+身份驗證以進行管理。前往Administration > AAA > AAA Mode > Select TACACS+。

abab	Wireless Control System Usemane: root Logout Refresh Print View	
cisco	Bonitor + Beports + Configure + Location + Administration + Belo +	
AAA	AAA Mode Settings	
Change Password	AAA Mede O Local O RADIUS @ TACACS+	
AAA Node	Falback on Local 🗹	
Users	0x	
Groups	locally irrespective of the AAA Mode Settings.	
Active Sessions		
TACACS+		
RADIUS		

使用虛擬域的WCS

虛擬域是WCS版本5.1中引入的一項新功能。WCS虛擬域由一組裝置和對映組成,並將使用者檢視 限製為與這些裝置和對映相關的資訊。通過虛擬域,管理員可以確保使用者只能檢視他們負責的裝 置和對映。此外,由於虛擬域的篩選器,使用者只能配置、檢視警報和生成其分配的網路部分的報 告。管理員為每個使用者指定一組允許的虛擬域。只有其中一個可以在登入時對該使用者啟用。使 用者可以通過從螢幕頂部的Virtual Domain下拉選單中選擇其他允許的虛擬域來更改當前虛擬域。現 在,所有報告、警報和其他功能都按該虛擬域進行過濾。

如果系統中僅定義了一個虛擬域(根),且使用者在TACACS+/RADIUS伺服器的自定義屬性欄位 中沒有任何虛擬域,則預設情況下會為使用者分配根虛擬域。

如果有多個虛擬域,且使用者沒有任何指定的屬性,則阻止使用者登入。為了允許使用者登入,虛 擬域自定義屬性必須匯出到Radius/TACACS+伺服器。

「虛擬域自定義屬性」視窗允許您為每個虛擬域指定相應的協定特定資料。虛擬域層次結構邊欄上 的「匯出」按鈕會預先格式化虛擬域的RADIUS和TACACS+屬性。您可以將這些屬性複製並貼上到 ACS伺服器。這允許您僅將適用的虛擬域複製到ACS伺服器螢幕,並確保使用者僅有權訪問這些虛 擬域。

若要將預先格式化的RADIUS和TACACS+屬性套用到ACS伺服器,請完成<u>虛擬網域RADIUS和</u> <u>TACACS+屬性</u>一節中說明的步驟。

配置Cisco Secure ACS以使用WCS

本節提供TACACS+ ACS伺服器中用於建立服務和自定義屬性以及將角色分配給使用者或組的步驟。

本節不介紹使用者和組的建立。假定根據需要建立使用者和組。

網路設定

完成以下步驟:

將WCS IP地址新增為AAA客戶端,身份驗證機製為TACACS+(Cisco IOS)。

CISCO SYSTEMS	Network Configuration		
tillitutillitu	Edit		
User Setup			
Group Setup	AAA Client Setup For		
Shared Profile Components	WCS		
Network Configuration	192.168.60.5		
System Configuration	AAA Client IP Address		
Configuration	Key cisco		
Administration Control	Authenticate Using TACACS+ (Cisco IOS)		
External User Databases	Single Connect TACACS+ AAA Client (Record stop in accounting on failure).		
Posture Validation	Log Update/Watchdog Packets from this AAA Client		
Network Access Profiles	Log RADIUS Tunneling Packets from this AAA Client		
Reports and Activity	Replace RADIUS Port info with Username from this AAA Client		
Online Documentation	Submit Submit + Apply Delete Delete + Apply Cancel		
	Pack to Help		

<u>介面組態</u>

請完成以下步驟:

- 1. 在Interface Configuration選單中,選擇TACACS+(Cisco IOS)連結。
- 2. 啟用New Services。
- 3. 選中User和Group覈取方塊。
- 4. 輸入Wireless-WCS(適用於服務)和HTTP(適用於協定)。注意:HTTP必須採用CAPS格式。
- 5. 啟用Advanced TACACS+功能。

Cisco Systems	Inte	rface	Configuration	
			PPP IP	
User			PPP IPX	
[백월 Setup			PPP Multilink	
Group Setup			PPP Apple Talk	
🛞 Shared Profile			PPP VPDN	
📽 Components			PPP LCP	
Network Configuration			ARAP	
Sustem		\checkmark	Shell (exec)	
Configuration			PIX Shell (pixshell)	
Interface Configuration			SLIP	
Administration	New	Servic	es	
			Service	Protocol
Databases		\checkmark	ciscowlc	common
Posture Validation		•	Wireless-WCS	НТТР
Network Access Profiles				
Reports and Activity		Ac	Ivanced Configuratio	on Options 🤶
Documentation	I A	dvance	d TACACS+ Features	

6. 按一下「Submit」以應用變更。

使用者/組設定

請完成以下步驟:

1. 在WCS GUI中,導航到**Administration > AAA > Groups**以選擇任何預配置的使用者組,例如 WCS中的SuperUsers。

ababa	Wireless Control System			Joanname: root Lagout Rafresh Print View			
CISCO	Bontor + Beants + Configure + Location + demonstration + Belp +						
AAA	All Groups						
Change Password	Group Name	headars	Audit Trad	Freed			
Local Password Policy	Admin		20	Task List			
AAA Nede	Conflictionecers		20	Tank List			
Users	Seatern Manifacing		2	Tank sist			
Groups	Users Assistant		20	Task List			
Active Seasons	Lobbs Ambassador	bilder	20	Twok List			
TACACS	Manifest Liter		2	Task List			
	North Bound AFI	-	20	Tank List			
RADUUS	Superlines	-	28	Task List			
	test	aut	201 C	Task List			
	User, Defined 1		20	Tank.Lint			
	User Defined 2	_	20 C	Task List			
	User.Defined.3		20	Task List			
	User Defined 4		20	Tank List			

2. 為預配置的使用者組選擇Task List(任務清單),然後複製貼上到ACS。

ababa	Wireless Control System	Coername: root Logout Refrech Print Serv				
CISCO	Buntur + Beguntu + Configure + Condon + Belip +					
AAA	Export Task List					
Change Password	Please cut and paste the appropriate protocol data below into the ourtom/vendor-specific attribute field in your AAA server.					
Local Password Policy	TALACS+ Custom Attributes RADIUS Custom Attributes					
AAA Node	roldowisot					
Users	haibertAckSa Servers Windeser-WCS-task2eftAckSa Servers haibertAckSa Servers WindeserVCS-task2eftAckSa Servers					
Groups	Neiden-Logong Windess WCS Red-Art-Logong RedSin-Logong Windess WCS Red-Art-Logong					
Active Sessions	Tasist-Scheduled Tasis and Data Collection Wireless-WCS tasist=Scheduled Tasis and Data Collection TasisT=Oser Indexences WCS tasisT=Oser Indexences					
TREACS+	Past = 1 years before task = 2 years = 1 task = 1 tas					
RADIUS	Nakisi - vive Aleris will Siente Nordese will Siente Nakisi - vive Aleris Nordese will Siente Nakisi - Contgore Contg Groups Nordese will Siente Nakisi - Contgore Aleris - Norde Nordese will Siente Nakisi - Contgore Aleris - Norde Nordese will Siente Nakisi - Contgore Aleris - Norde Nordese will Siente Nakisi - Contgore Contg Groups Nordese will Siente Nakisi - Contgore Aleris - Norde Nordese will Siente Nakisi - Contgore Contg Groups Nordese will Siente Nakisi - Contgore Contg Groups Nordese will Siente Nakisi - Contgore Contg Groups Nordese will Siente Nakisi - Contgore Contgore Contgore Nordese will Siente Nakisi - Contgore Contgore Contgore Nordese will Siente Nak					

- 3. 選擇以前建立的使用者/組並轉到TACACS+設定。
- 4. 在ACS GUI中,選中與之前建立的Wireless-WCS服務對應的覈取方塊。
- 5. 在ACS GUI中, 選中Custom attributes框。
- 6. 在自定義屬性下面的文本框中,輸入從WCS複製的此角色和任務資訊。例如,輸入超級使用 者允許的任務清單。

CISCO SYSTEMS	Group Setup
	Jump To TACACS+
User Setup	L Custom attributes
Group Setup	
Components	
Configuration	Wireless-WCS HTTP
System Configuration	Custom attributes
Configuration	task0=Users and Groups
Administration Control	task1=Audit Trails task2=TACACS+ Servers
Databases	
Posture Validation	
Network Access Profiles	Cisco IOS/PIX 6.x RADIUS Attributes ?
Reports and Activity	[009\001] cisco-av-pair
Documentation	

7. 然後,在ACS中使用新建立的使用者名稱/密碼登入WCS。



<u>從WLC為role1=ALL調試</u>

(Cisco Controller) >debug aaa tacacs enable

(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22

Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
從WLC調試多個角色

(Cisco Controller) >debug aaa tacacs enable

Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2 session_id=b561ad88 length=16 encrypted=0 Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88 length=6 encrypted=0 Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0 Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN] Wed Feb 28 17:59:34 2007: arg[1] = [16] [role2=CONTROLLER] Wed Feb 28 17:59:34 2007: arg[2] = [14] [role3=SECURITY] Wed Feb 28 17:59:34 2007: arg[3] = [14] [role4=COMMANDS] Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150 從WLC調試授權失敗

(Cisco Controller) >debug aaa tacacs enable

```
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007: User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

相關資訊

- 適用於Web驗證的Cisco無線LAN控制器(WLC)和Cisco ACS 5.x(TACACS+)組態範例
- <u>設定TACACS+</u>
- 如何在ACS 5.1中為管理員和非管理員使用者配置TACACS身份驗證和授權
- TACACS+ 和 RADIUS 比較
- 技術支援與文件 Cisco Systems