Cisco统一无线网络TACACS+配置

目录

简介 先决条件 要求 使用的组件 规则 控制器中的 TACACS+ 实施 身份验证 授权 记账 WLC 中的 TACACS+ 配置 添加 TACACS+ 身份认证服务器 添加 TACACS+ 授权服务器 添加 TACACS+ 记帐服务器 配置身份认证顺序 验证配置 配置 Cisco Secure ACS 服务器 网络配置 接口配置 用户/组设置 Cisco Secure ACS 中的记帐记录 WCS 中的 TACACS+ 配置 使用虚拟域的 WCS 配置 Cisco Secure ACS 以使用 WCS 网络配置 接口配置 用户/组设置 调试 从 WLC 进行的 role1=ALL 调试 从 WLC 进行的多个角色调试 从 WLC 进行的身份认证失败调试 相关信息

<u>简介</u>

本文档为 Cisco 统一无线网络提供 Cisco 无线 LAN 控制器 (WLC) 和 Cisco 无线控制系统 (WCS) 中的终端访问控制器访问控制系统 + (TACACS+) 的配置示例。本文档还提供一些基本的故障排除 技巧。 TACACS+ 是客户端/服务器协议,为尝试获得对路由器或网络接入服务器的管理访问权限的用户提供集中式的安全保障。TACACS+ 提供以下 AAA 服务:

- 对尝试登录到网络设备的用户进行身份认证
- 对确定用户应具有的访问级别进行授权
- 对记录用户进行的所有更改进行记帐

有关 AAA 服务和 TACACS+ 功能的详细信息,请参阅<u>配置 TACACS+。</u>

有关 TACACS+ 和 RADIUS 之间的比较,请参阅<u>比较 TACACS+ 和 RADIUS。</u>

<u>先决条件</u>

<u>要求</u>

Cisco 建议您了解以下主题:

- •关于如何为基本操作配置 WLC 和轻量接入点 (LAP) 的知识
- •轻量级接入点协议(LWAPP)和无线安全方法知识
- RADIUS 和 TACACS+ 的基本知识
- Cisco ACS 配置的基本知识

<u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- Cisco Secure ACS for Windows 版本 4.0
- •运行版本4.1.171.0的思科无线局域网控制器。软件版本4.1.171.0或更高版本支持WLC上的 TACACS+功能。
- 运行版本4.1.83.0的思科无线控制系统。WCS上的TACACS+功能在软件版本4.1.83.0或更高版 本上受支持。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

<u>规则</u>

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

控制器中的 TACACS+ 实施

<u>身份验证</u>

身份认证可以采用使用用户名和口令的本地数据库、RADIUS 或 TACACS+ 服务器进行。实施不是 完全模块化。身份认证和授权服务互相关联。例如,如果使用 RADIUS/本地数据库进行身份认证 ,授权则不会使用 TACACS+ 进行。将会使用与本地数据库或 RADIUS 数据库中的用户相关的权限 ,例如只读或只写。但是,当使用 TACACS+ 进行身份认证时,授权则与 TACACS+ 关联。

在配置多个数据库的情况下,提供 CLI 以规定应引用后端数据库的顺序。

<u>授权</u>

授权是基于任务的,而非基于实际的每个命令。任务映射到对应当前位于 Web GUI 上的七个菜单 栏项的各种选项卡上。以下是菜单栏项:

- •监控 (MONITOR)
- WLANS
- 控制器
- 无线
- 安全
- 管理
- 命令

此映射的原因基于这一事实,即大多数客户使用 Web 接口配置控制器而不是 CLI。

接待管理员管理 (LOBBY) 的附加角色适用于仅需要具有接待管理员特权的用户。

对用户授权的任务是使用自定义属性值 (AV) 对在 TACACS+ (ACS) 服务器中配置的。可以对用户 授权一个或多个任务。最低授权仅为 MONITOR,最高授权为 ALL(授权执行全部七个选项卡)。 如果未对用户授权特定的任务,该用户仍能以只读模式访问该任务。如果启用了身份认证,并且认 证服务器变得不可达或不能授权,用户则无法登录到控制器。

注意:为了通过TACACS+成功进行基本管理身份验证,必须在WLC上配置身份验证和授权服务器 。记帐配置为可选项。

<u>记账</u>

每当特定用户启动的操作成功执行时,都将进行记帐。更改的属性和以下内容一起记录在 TACACS+ 记帐服务器中:

- •进行更改的个人的用户 ID
- 用户登录使用的远程主机
- •执行命令的日期和时间
- 用户的授权级别
- •提供关于所执行操作和所提供值的信息的字符串

如果记帐服务器变得不可达,用户仍可以继续会话。

注意:在软件版本4.1或更低版本中,不会从WCS生成记帐记录。

<u>WLC 中的 TACACS+ 配置</u>

WLC 软件版本 4.1.171.0 和更高版本引入了新的 CLI 和 Web GUI 更改,以在 WLC 上启用 TACACS+ 功能。本部分列出了引入的 CLI 以供参考。在 Security 选项卡下,添加了对 Web GUI 做出的相应更改。

本文档假设 WLC 的基本配置已完成。

为了在 WLC 控制器中配置 TACACS+, 您需要完成以下步骤:

1. <u>添加 TACACS+ 身份认证服务器</u>

- 2. <u>添加 TACACS+ 授权服务器</u>
- 3. <u>添加 TACACS+ 记帐服务器</u>
- 4. 配置身份认证顺序

添加 TACACS+ 身份认证服务器

请完成以下步骤,以添加 TACACS+ 身份认证服务器:

1. 使用 GUI, 然后转到 Security > TACACS+ > Authentication。

alialia cisco	MONITOR MLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	ΨU	Sage Configuration	Eing Logout Befresh
Security	TACACS+ Authentic	cation Servers						New
AAA General FADJUS Authentication Accounting TACACS+ Authentication Accounting Authentication	Server Index	Server Address	Pert	Admin Sta	us.			

2. 添加 TACACS+ 服务器的 IP 地址,然后输入共享密钥。如果需要,请更改 TCP/49 的默认端口。

ululu cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY M	WAGEMENT COMMANDS	Sage Configuration Bing Logout, Befresh HELP
Security	TACACS+ Authentication	Servers > New		< Back Apply
AAA General Authentication Accounting TACACS+	Server Index (Priority) Server IPAddress Shared Secret Format	1 2		
Authentication Accounting Authorization LDAP Local Net Users MAC Filtering	Shared Secret Confirm Shared Secret			
Disabled Clients User Login Policies AP Policies	Port Number	49		
Local EAP Priority Order Access Control Lists	Server Status Retransmit Timeout	Enabled v 2 seconds		

3. 单击 Apply。您可以使用 config tacacs auth add *<Server Index> <IP addr> <port> [ascii/hex] <secret> 命令从 CLI 完成此操作:*

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

添加 TACACS+ 授权服务器

请完成以下步骤,以添加 TACACS+ 授权服务器:

- 1. 从 GUI 中,转到 Security > TACACS+ > Authorization。
- 2. 添加 TACACS+ 服务器的 IP 地址,然后输入共享密钥。如果需要,请更改 TCP/49 的默认端口。

սիսիս cisco	MONITOR WLANS CONTR	OLLER WIPELESS	SECURITY	MANAGEMENT	COMMANDS	Hero.	Sage Configuration	5m	Logovt Befresh
Security	TACACS+ Authorization	Servers > New					< 84	ck 🗌	Apply
- AAA General	Server Index (Priority)	3 ¥							
 RAD3US Authentication 	Server IPAddress	10.1.1.12]					
Accounting TACACS + Authentication	Shared Secret Format	45011 💌							
Accounting Authorization	Shared Secret	*****]			
LDAP Local Net Users MAC Filtering	Confirm Shared Secret	*****]			
User Login Policies AP Policies	Port Number	49							
+ Local EAP	Server Status	Enabled 💌							
Priority Order Access Control Lists	Retransmit Timeout	2 seconds							

3. 单击 Apply。您可以使用 config tacacs athr add *<Server Index> <IP addr> <port> [ascii/hex] <secret> 命令从 CLI 完成此操作:*

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

添加 TACACS+ 记帐服务器

请完成以下步骤,以添加 TACACS+ 记帐服务器:

- 1. 使用 GUI, 然后转到 Security > TACACS+ > Accounting。
- 2. 添加服务器的 IP 地址, 然后输入共享密钥。如果需要, 请更改 TCP/49 的默认端口。

cisco	MONITOR MUNIS CO	WTROLLER WIRELESS	SECURITY MOUNT	емент соминос	RUP	Sage Configuration Bing	Logaut Befresh
Security	TACACS+ Accountin	g 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 Cleents	Confirm Shared Secret	****					
User Login Policies AP Policies	Port Number	49					
+ Local EAP	Server Status	Enabled 💌					
+ Priority Order		-					
Access Control Lists	Retransmit Timeout	seconds					

3. 单击 Apply。您可以使用 config tacacs acct add *<Server Index> <IP addr> <port> [ascii/hex] <secret> 命令从 CLI 完成此操作:*

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

配置身份认证顺序

此步骤说明在配置了多个数据库时如何配置身份认证的 AAA 顺序。身份认证的顺序可能是 local and RADIUS 或 local and TACACS。身份认证顺序的默认控制器配置是 *local and RADIUS*。

请完成以下步骤,以配置身份认证的顺序:

- 1. 从 GUI 中,转到 Security > Priority Order > Management User。
- 2. 选择身份认证的优先级。在本示例中,选择了 TACACS+。
- 3. 单击 Apply 以应用选择。

ululu cisco	MONITOR MLANS	CONTROLLER	WPELESS	SECURITY	MOVAGEMENT	COMMANDS	Rena	Sage Configuration Brig Logaut Befresh
Security	Priority Order > M	anagement U	ser					Apoly
ALA General RADOUS Authentication Accounting TACACS+ Authentication Accounting Authentication Authentication Local Net Users MAC Filtering Disabled Cleants User Loop Policies AP Policies Priority Order	Authentication Priori	ts 16 the first server i	O Redux @	TACACS+				

您可以使用config aaa auth mgmt <server1> **<server2>命令从CLI完成此**操作:

(Cisco Controller) >config aaa auth mgmt tacacs local

<u>验证配置</u>

本部分描述用于验证 WLC 上的 TACACS+ 配置的命令。以下是一些有用的 show 命令,帮助您确 认配置是否正确:

```
• show aaa auth — 提供关于身份认证顺序的信息。
 (Cisco Controller) >show aaa auth
Management authentication server order:
   1.....local
   2..... Tacacs
• show tacacs summary — 显示 TACACS+ 服务和统计信息的汇总。
 (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 — 显示 TACACS+ 身份认证服务器的统计信息。
 (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	3
Reject Responses	0
Error Responses	0
Restart Responses	0
Follow Responses	0
GetData Responses	0
Encrypt no secret Responses	0
Challenge Responses	0
Malformed Msgs	0
Bad Authenticator Msgs	0
Timeout Requests	12
Unknowntype Msgs	0
Other Drops	0
。show tacacs athr stats — 显示 TACACS+ 授权 暇	冬哭的统计信息。
(CISCO Controller) >snow tacaes athr statistics	
Authorization Servers.	
Correct Index	1
Server Midex	10 1 1 10
Mag Bound Trip Time	0 (1/100 gogord)
First Dequests	2
Pilst Requests	3
Reciy Requests	3
Authorization Success	3
Authorization Failure	0
Challenge Regnonges	0
Malformed Mags	0
Rad Athrenticator Msgs	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0
obow toopoo cost state 目示 TACACC+ 记帐呢	。 冬哭的体计后自
	方面的纵川后态。
(Cisco Controller) >show tacacs acct statistics	
Accounting Servers.	
Sorver Index	1
Server Address	⊥ 10 1 1 12
Mag Pound Trip Time	0 (1/100 second)
First Dequests	122
Petry Pequests	0
Accounting Response	0
Accounting Response	0
Accounting Request Success	0
Malformed Maga	0
Rad Authenticator Maga	0
Timeout Requests	399
Unknowntype Msgs	0
Other Drops	0
	-

配置 Cisco Secure ACS 服务器

本部分提供 TACACS+ ACS 服务器中包含的步骤,用于创建服务和自定义属性以及将角色分配到用 户和组。

本部分未说明用户和组的创建。假设根据需要创建了用户和组。有关如何创建用户和用户组的信息 ,请参阅 <u>Cisco Secure ACS for Windows Server 4.0 用户指南。</u> 完成以下步骤:

添加控制器管理 IP 地址作为 AAA 客户端,身份认证机制作为 TACACS+ (Cisco IOS)。



接口配置

请完成以下步骤:

- 1. 在 Interface Configuration 菜单中,选择 TACACS+ (Cisco IOS) 链接。
- 2. 启用 New Services。
- 3. 选中 User 和 Group check 框。
- 4. 针对服务输入 ciscowlc, 针对协议输入 common。
- 5. 启用 Advanced TACACS+ Features。

User Group PPP IP PPP IP PPP IP PPP IPX PPP IP PPP IPX PPP Multilink PPP Multilink PPP Apple Talk PPP VPDN PPP VPDN PPP LCP ARAP Shell (exec) PIX Shell (pixshell) SLIP New Services Service Protocol Image: Service Protocol			TACACS+ Serv	lices	2
Image: PPP IP Image: PPP IPX Image: PPP IPX Image: PPP Multilink Image: PPP Apple Talk Image: PPP VPDN Image: PP VPDN	User	Group			
□ PPP IPX □ PPP Multilink □ PPP Apple Talk □ PPP VPDN □ PPP LCP □ ARAP □ PIX Shell (exec) □ PIX Shell (pixshell) □ SLIP		V	PPP IP		
PPP Multilink PPP Apple Talk PPP VPDN PPP LCP ARAP Shell (exec) PIX Shell (pixshell) SLIP			PPP IPX		
PPP Apple Talk PPP VPDN PPP LCP ARAP Shell (exec) PIX Shell (pixshell) SLIP			PPP Multilink		
□ PPP VPDN □ PPP LCP □ ARAP □ ARAP □ PIX Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Protocol ✓ ✓ ✓ Ciscowlc □ □ □ □			PPP Apple Talk		
□ PPP LCP □ ARAP □ Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Service Service Protocol ✓ Ciscowlc □ □			PPP VPDN		
□ ARAP □ Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Service Service Protocol ✓ ✓ <t< td=""><td></td><td></td><td>PPP LCP</td><td></td><td></td></t<>			PPP LCP		
□ ✓ Shell (exec) □ PIX Shell (pixshell) □ SLIP New Services Protocol ✓ ✓ ○ ciscowlc □ □ □ □			ARAP		
□ PIX Shell (pixshell) □ SLIP New Services Protocol ☑ Ciscowlc common □ □ □ □ □ □		V	Shell (exec)		
SLIP New Services Service Protocol Image: Common Image: Common			PIX Shell (pixshell)		
New Services Service Protocol Common Common			SLIP		
Service Protocol Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service Image: Service <td>New S</td> <td>ervices</td> <td></td> <td></td> <td></td>	New S	ervices			
Image: Construction Image: Construction <td></td> <td></td> <td>Service</td> <td>Protocol</td> <td></td>			Service	Protocol	
		V	ciscowlc	common	
				· · · · · · · · · · · · · · · · · · ·	
			Advanced Configurat	ion Options	

6. 单击 Submit 以应用更改。

用户/组设置

请完成以下步骤:

- 1. 选择一个先前创建的用户/组。
- 2. 转到 TACACS+ Settings。
- 3. 选中与接口配置部分中创建的 ciscowlc 服务对应的复选框。
- 4. 选中 Custom attributes 复选框。

Cisco Systems	Group Setup
	Jemp To Access Restrictions
User Setup	Shell Command Authorization Set
A Group	C None
Setup	Assign a Shell Command Authorization Set for any network device
Shared Profile Components	
Network	Unmatched Cisco IOS commands
Contrigue action	O Permit
Configuration	C Deny
Configuration	Command:
a Administration	
Control	Arguments:
Databases	×
www.Posture Validation	
Network Access	Unlisted annuments
Profiles	C Permit
Activity	@ Deny
Documentation	
	E ciscowic common
	Custom attributes
	role1=ALL
	-
	·
	Wireless-WCS HTTP
	Custom attributes
	×
	IETF RADIUS Attributes
	C [006] Service-Type
	Caliback NAS Dromot
	Submit Submit + Restart Cancer

- 5. 如果创建的用户仅需要访问 WLAN、SECURITY 和 CONTROLLER 的权限,则在 Custom attributes 下的文本框中输入此文本: role1=WLAN role2=SECURITY role3=CONTROLLER。 如果用户仅需要访问 SECURITY 选项卡的权限,则输入此文本: role1=SECURITY。角色对 应控制器 Web GUI 中的七个菜单栏项。菜单栏项分别为 MONITOR、WLAN、 CONTROLLER、WIRELESS、SECURITY、MANAGEMENT 和 COMMAND。
- 6. 在 role1、role2 等角色中输入用户需要的角色。如果用户需要所有角色,则应使用关键字 ALL。对于接待管理员角色,应使用关键字 LOBBY。

<u>Cisco Secure ACS 中的记帐记录</u>

WLC 的 TACACS+ 记帐记录适用于报告和活动的 TACACS+ 管理中的 Cisco Secure ACS。

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										
Seller.		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	10.10.80.3	
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 never a an	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	nid 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	10.10.80.3	- 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	10.10.80.3	
		02/22/2007 16:26:52	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 of the	Averal	(C) CS Lip	-Parend.	 Clinic 	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

WCS 中的 TACACS+ 配置

请完成以下步骤:

- 1. 从 GUI 中,使用根帐户登录到 WCS。
- 2. 添加 TACACS+ 服务器。转到 Administration > AAA > TACACS+ > Add TACACS+ Server。

ababa	Wireless Control System	Username: root Logout Refresh Print View 20
cisco	Bonitor • Beports • Configure • Location • Administration • Belo •	
AAA	TACACS+	Select a command 💌 60
Change Password	No TACACS+ Servers found in the system	
AAA Node		
Users		
Groups		
Active Sessions		
TACACS+		
RADIUS		

3. 添加 TACACS+ 服务器的详细信息,例如 IP 地址、端口号(默认为 49)和共享密钥。

ahaha	Wireless Control S	ystem	Username: root Logout 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	
	Shared Secret		
Groups	Confirm Shared Secret		
Active Sessions	Retransmit Timeout	5 seconds	
TACACS+	Retries	1	
	Authentication Type	PAP 💌	
RADIUS	Submit Cancel		

4. 针对 WCS 中的管理启用 TACACS+ 身份认证。转到 Administration > AAA > AAA Mode > Select TACACS+。

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

使用虚拟域的 WCS

虚拟域是WCS 5.1版中引入的一项新功能。WCS虚拟域由一组设备和映射组成,并将用户的视图限 制为与这些设备和映射相关的信息。通过虚拟域,管理员可以确保用户只查看该用户负责的设备和 映射。另外,借助虚拟域的过滤器,用户可以配置、查看警报并且仅生成其分配的网络部分的报告 。管理员为每个用户指定一组许可虚拟域。用户登录时,这些域中仅有一个域为活动状态。用户可 以通过从屏幕顶部的 Virtual Domain 下拉菜单中选择不同的许可虚拟域更改当前的虚拟域。所有报 告、警报和其他功能现在都由该虚拟域过滤。

如果系统中仅定义了一个虚拟域(根),并且用户的 TACACS+/RADIUS 服务器的自定义属性字段 中没有任何虚拟域,则在默认情况下,该用户会被分配到根虚拟域。

如果有多个虚拟域,并且用户没有任何指定的属性,则该用户在登录时会受到阻止。为了允许用户 登录,必须将虚拟域自定义属性导出到 Radius/TACACS+ 服务器。

Virtual Domain Custom Attributes 窗口使您可以为每个虚拟域指示适当的特定于协议的数据。 Virtual Domain Hierarchy 侧边栏上的 Export 按钮预先格式化虚拟域的 RADIUS 和 TACACS+ 属性 。您可以复制这些属性并将其粘贴到 ACS 服务器中。此操作使您可以仅将适用的虚拟域复制到 ACS 服务器屏幕上,并确保用户仅具有访问这些虚拟域的权限。

为了将预先格式化的 RADIUS 和 TACACS+ 属性应用于 ACS 服务器,请完成<u>虚拟域 RADIUS 和</u> TACACS+ 属性部分中的所述步骤。

配置 Cisco Secure ACS 以使用 WCS

本部分提供 TACACS+ ACS 服务器中包含的步骤,用于创建服务和自定义属性以及将角色分配到用 户和组。

本部分未说明用户和组的创建。假设根据需要创建了用户和组。

网络配置

完成以下步骤:

添加 WCS IP 地址作为 AAA 客户端,身份认证机制作为 TACACS+ (Cisco IOS)。

CISCO SYSTEMS	Network Configuration		
tilltutilltu	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>接口配置</u>

请完成以下步骤:

- 1. 在 Interface Configuration 菜单中,选择 TACACS+ (Cisco IOS) 链接。
- 2. 启用 New Services。
- 3. 选中 User 和 Group check 框。
- 4. 针对服务输入 Wireless-WCS, 针对协议输入 HTTP。注意: HTTP必须在CAPS中。
- 5. 启用 Advanced TACACS+ Features。

CISCO SYSTEMS	Inte	rface	Configuration	
		•	PPP IP	
User			PPP IPX	
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 Control	New	Servio	es	
- L External liser			Service	Protocol
Databases		\checkmark	ciscowlc	common
Posture Validation		•	Wireless-WCS	НТТР
Network Access				
Reports and Activity		Ac	lvanced Configuratio	on Options 🧖
Online Documentation	V A	dvance	ed TACACS+ Features	

6. 单击 Submit 以应用更改。

<u>用户/组设置</u>

请完成以下步骤:

 在 WCS GUI 中,导航到 Administration > AAA > Groups 以选择预先配置的任何用户组,例 如 WCS 中的超级用户。

ababa	Wireless Control System			Username: root Legout Refresh Print View
CISCO	Honitor * Beports * Configure * Location * Administration * Help *			
AAA	All Groups			
Change Password	Farmer Name	Nembers	Audit Tout	Frend
Local Password Policy	Admin	-	2	Two List
AAA Node	Confictionecers	-	28	Tauk List
Users	Sautern Mentaring		2	Task List
Groups	Users Assistant		20	Task List
Active Services	Lobbs Ambassadur	bilder	20	Tank List
	ManiferLife	-	2	Task List
TALACS+	North Bound AFI		20	Tank Lint
RADOUS	SuperStats		22	Task List
	fast	and	22	Task List
	User Defined 1		20	Task List
	User.Defined.2	-	2	Task List
	User.Defined.3		20	Task List
	User Defined 4		20	Tank List

2. 为预先配置的用户组选择任务列表,然后复制并粘贴到 ACS。

ababa	Wireless Control System	Username: root Legout	Refresh	Print View		
CISCO	Bunkus + Bepunts + Configure + Location + Belainstration + Belain					
AAA	Export Task List					
Change Password	Please cut and paste the appropriate protocol data below into the custom/rendor-specific attribute field in your AAA server.					
Local Password Policy	TACACS+ Custom Attributes RADIUS Custom Attributes					
AAA Node	roled-shot winings-wC3.ruled-shot winings-wC3.ruled-shot winings-wC3.ruled-shot winings-wC3.ruled-shot winings-wC3.ruled-shot winings-wC3.ruled-shot					
Users	Nask2wTACACC4 Servers Windows WCS-task2wTACACC4 Servers Nak2wRACt05 Servers Windows WCS-task2wTACACC4 Servers					
Groups	Nasilini-Logang Wardense W.C.S. Nasilini-Logang Nasilini-Logang Wardense W.C.S. Nasilini-Logang					
Active Sessions	Raske-Scheduled Tasks and Data Collection Wiveless-WCS tasks=Scheduled Tasks and Data Collection RaskT=User Invelorences WCS tasks=Scheduled Tasks and Data Collection					
TACACS+	Last - System Settingen Last - Settingen der Bestern der B Bestern der Bestern der Bester					
RADIUS	Nation Service Marchaeve					

- 3. 选择先前创建的用户/组,然后转到 TACACS+ Settings。
- 4. 在 ACS GUI 中,选择对应早些时候创建的 Wireless-WCS 服务的复选框。
- 5. 在 ACS GUI 中,选中 Custom attributes 框。
- 6. 在 Custom attributes 下的文本框中,输入此角色和从 WCS 复制的任务信息。例如,输入超级用户许可的任务列表。

CISCO SYSTEMS	Group Setup
	Jump To TACACS+
User Setup	L Custom attributes
Group Setup	
Shared Profile Components	
Network Configuration	✓ Wireless-WCS HTTP
System Configuration	Custom attributes
Configuration	roleO=SuperUsers
Administration Control	task1=Audit Trails task2=TACACS+ Servers task3=RADIUS Servers
External User Databases	
Posture Validation	
Network Access Profiles	Cisco IOS/PIX 6.x RADIUS Attributes ?
Reports and Activity	[009\001] cisco-av-pair
Online Documentation	

7. 然后,使用 ACS 中新创建的用户名/口令登录到 WCS。



<u>从 WLC 进行的 role1=ALL 调试</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: user has the following mgmtRole fffffff8
M WLC 进行的多个角色调试

(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 从 WLC 进行的身份认证失败调试

(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
```

相关信息

- <u>用于 Web 身份验证的 Cisco 无线 LAN 控制器 (WLC) 和 Cisco ACS 5.x (TACACS+) 配置示例</u>
- 配置 TACACS+
- 如何在 ACS 5.1 中配置 TACACS 身份认证以及管理员与非管理员的身份认证
- TACACS+ 和 RADIUS 的比较
- 技术支持和文档 Cisco Systems