配置9800 WLC大厅大使,使用RADIUS和 TACACS+身份验证

目录

<u>简介</u> <u>先决条件</u> 要求 使用的组件 背景信息 配置 网络图 验证RADIUS 配置ISE - RADIUS 验证TACACS+ 在WLC上配置TACACS+ 配置ISE - TACACS+ 验证 故障排除 验证RADIUS 验证TACACS+

简介

本文档介绍如何使用身份服务引擎(ISE)为Lobby Ambassador用户配置Catalyst 9800无线LAN控制器的RADIUS和TACACS+外部身份验证。

先决条件

要求

Cisco 建议您了解以下主题:

- Catalyst无线9800配置型号
- AAA、RADIUS和TACACS+概念

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Catalyst 9800无线控制器系列(Catalyst 9800-CL)
- Cisco IOS®-XE Gibrator 16.12.1s
- ISE 2.3.0

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始(默认

)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

大厅大使用户由网络管理员创建。Lobby Ambassador用户能够创建访客用户的用户名、密码、说 明和生命期。它还能删除访客用户。访客用户可通过GUI或CLI创建。

配置

网络图



在本例中,配置了Lobby Advasisors "lobby"和"lobbyTac"。大厅大使"大厅"应根据RADIUS服务器进 行身份验证,大厅大使"lobbyTac"应根据TACACS+进行身份验证。

首先为RADIUS Lobby Ambassador配置,最后为TACACS+ Lobby Ambassador配置。RADIUS和 TACACS+ ISE配置也是共享的。

验证RADIUS

在无线局域网控制器(WLC)上配置RADIUS。

步骤1.声明RADIUS服务器。在WLC上创建ISE RADIUS服务器。

GUI:

0

导航至Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add,如图所示

Q Search Menu Items	Configuration * > Sec	curity * > AAA						
🚃 Dashboard	+ AAA Wizard							
Monitoring	Servers / Groups	AAA Method List	AAA Advanced					
Configuration	> + Add × Dele							
() Administration	RADIUS		0					
💥 Troubleshooting	TACACS+	Servers Server	Groups					
	LDAD	Name	 Address 	~	Auth Port	~	Acct Port	~
	LDAP	RadiusLobby	192.168.166.8		1812		1813	
			10 🔻 items per page				1 -	1 of 1 items

当配置窗口打开时,必需的配置参数是RADIUS服务器名称(它不必与ISE/AAA系统名称匹配)、 RADIUS服务器IP地址和共享密钥。任何其他参数都可保留默认值或根据需要进行配置。

CLI :

Tim-eWLC1(config)#radius server RadiusLobby
Tim-eWLC1(config-radius-server)#address ipv4 192.168.166.8 auth-port 1812 acct-port 1813
Tim-eWLC1(config-radius-server)#key 0 Cisco1234
Tim-eWLC1(config)#end

步骤2.将RADIUS服务器添加到服务器组。定义服务器组并添加已配置的RADIUS服务器。这是用于 对Lobby Ambassador用户进行身份验证的RADIUS服务器。如果WLC中配置了多个RADIUS服务器 ,可用于身份验证,建议将所有Radius服务器添加到同一服务器组。如果执行此操作,则允许 WLC在服务器组中的RADIUS服务器之间平衡身份验证。

GUI:

导航至Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add,如图所示。

Q Search Menu Items	Configuration * > Secu	rity* > AAA			
🔜 Dashboard	+ AAA Wizard				
Monitoring >	Servers / Groups	AAA Method List AA	A Advanced		
🔾 Configuration 🛛 🔸	+ Add × Delet				
() Administration ›	RADIUS				
💥 Troubleshooting	TACACS+	Servers Server G	iroups		
	LDAD	Name	 Server 1 	Server 2	Server 3
	LUAF	GroupRadLobby	RadiusLobby	N/A	N/A
			10 🔻 items per page		1 - 1 of 1 items

当配置窗口打开以为组指定名称时,将已配置的RADIUS服务器从可用服务器列表移到已分配服务 器列表。

CLI :

Tim-eWLC1(config)#aaa group server radius GroupRadLobby Tim-eWLC1(config-sg-radius)#server name RadiusLobby Tim-eWLC1(config-sg-radius)#end

步骤3.创建身份验证方法列表。身份验证方法列表定义您查找的身份验证类型,并将其附加到您定 义的服务器组。您将知道身份验证是在WLC本地完成还是在RADIUS服务器外部完成。

GUI:

导航至Configuration > Security > AAA > AAA Method List > Authentication > + Add,如图所示。



当配置窗口打开时,提供名称,选择类型选项作为"登录",并**分配**之前创建的服务器组。

组类型为本地。

GUI:

如果选择Group Type(组类型)为"local",WLC将首先检查用户是否存在于本地数据库中,然后仅 在本地数据库中找不到Lobby Ambassador用户时才回退到服务器组。

CLI :

Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod local group GroupRadLobby Tim-eWLC1(config)#end

注意:请注意Bug <u>CSCvs87163</u> 当您首先使用本地时。此问题在17.3中修复。

组类型为组。

GUI:

如果选择Group Type(组类型)为"group",且未选中回退到本地选项,则WLC将仅根据服务器组 检查用户,不会签入其本地数据库。

CLI :

Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby Tim-eWLC1(config)#end

Group Type as a group和Fallback to local选项已选中。

GUI:

如果选择Group Type(组类型)作为"group",并且选中了回退到本地选项,则WLC将根据服务器 组检查用户,并仅在RADIUS服务器在响应中超时时查询本地数据库。如果服务器响应,WLC将不 触发本地身份验证。

CLI :

步骤4.创建授权方法列表。授权方法列表定义大厅大使需要的授权类型,在本例中为"exec"。 它还 将连接到定义的同一服务器组。它还允许选择身份验证是在WLC上本地完成还是在RADIUS服务器 外部完成。

GUI:

导航至Configuration > Security > AAA > AAA Method List > Authorization > + Add,如图所示。

Q Search Menu Items	Configuration * > Secu	rity * > AAA						
📻 Dashboard	+ AAA Wizard							
Monitoring >	Servers / Groups	AAA Method List	AAA Advan	ced				
🔾 Configuration 🔹 🔸	Authentication							
() Administration	Authorization	+ Add \times D						
💥 Troubleshooting	Accounting	Name 🖂	Туре 🗠	Group 🛛 🗹	Group1 ×	Group2 V	Group3 ×	Group4 ×
		AuthozLobby	exec	local	GroupRadLob	N/A	N/A	N/A

当配置窗口打开以提供名称时,选择类型选项为"exec"并分配之前创建的服务器组。

请注意,组类型的应用方式与"身份验证方法列表"部分中的说明相同。

CLI :

组类型为本地。

Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod local group GroupRadLobby Tim-eWLC1(config)#end

组类型为组。

Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby Tim-eWLC1(config)#end

Group Type as group和回退到本地选项已选中。

Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby local Tim-eWLC1(config)#end

步骤5.分配方法。配置方法后,必须将其分配给选项以登录WLC,以创建访客用户,如线路 VTY(SSH/Telnet)或HTTP(GUI)。

这些步骤无法从GUI完成,因此需要从CLI完成。

HTTP/GUI身份验证:

Tim-eWLC1(config)#ip http authentication aaa login-authentication AuthenLobbyMethod Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozLobbyMethod Tim-eWLC1(config)#end 对HTTP配置执行更改时,最好重新启动HTTP和HTTPS服务: Tim-eWLC1(config)#no ip http server Tim-eWLC1(config)#no ip http secure-server Tim-eWLC1(config)#ip http server Tim-eWLC1(config)#ip http secure-server Tim-eWLC1(config)#end line.ut/

line vty.

Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AuthenLobbyMethod
Tim-eWLC1(config-line)#authorization exec AuthozLobbyMethod
Tim-eWLC1(config-line)#end

步骤6.此步骤仅在17.5.1或17.3.3之前的软件版本中是必需的,在CSCvu29748的这些版本之后则不 <u>是必需的</u>已实施。定义远程用户。在ISE上为Lobby Ambassador创建的用户名必须定义为WLC上 的远程用户名。如果WLC中未定义远程用户名,则身份验证将正确进行,但是,将授予用户对 WLC的完全访问权限,而不是仅授予对Lobby Ambassador权限的访问权限。此配置只能通过CLI完 成。

CLI :

Tim-eWLC1(config)#aaa remote username lobby

配置ISE - RADIUS

步骤1.将WLC添加到ISE。导航至**管理>网络资源>网络设备>添加**。WLC需要添加到ISE。将WLC添加到ISE时,启用RADIUS身份验证设置并配置所需的参数,如图所示。

dentity Services Engine	Home Context	Visibility > Ope	erations Policy	✓Administration	Work Centers			
System Identity Management	▼Network Resources	Device Portal M	lanagement pxGrid	Services Feed Service	e Fhreat Centric NA	٨C		
Network Devices Network Device	Groups Network Devi	ice Profiles Extern	nal RADIUS Servers	RADIUS Server Sequence	es NAC Managers	External MDM	Location Services	
	•							
Network Devices	Network Devic	es						
Default Device	A	Bartin B						
Device Security Settings	/ Edit Add	Lo Duplicate	Import P Export V	Generate PAC XI	elete 🔻			Show
	Name	 IP/Mask 	Profile Name	Locatio	1	Type		Description
	Tim-eWLC1	192.168.166.7.	👬 Cisco 🕀	All Loca	tions	All Device Typ	pes	9800

当配置窗口打开时,提供名称IP ADD,启用RADIUS身份验证设置,在Protocol Radius下输入所需的共享密钥。

步骤2.在ISE上创建Lobby Ambassador用户。导航至管理>身份管理>身份>用户>添加。

向ISE添加分配给创建访客用户的Lobby Ambassador的用户名和密码。这是管理员将分配给大厅大使的用户名。

dentity Services Engine	Home Conte	xt Visibility	► Policy	ation Vork Centers						
System Identity Management	Network Resources	Device Portal Manageme	nt pxGrid Services F	eed Service						
✓Identities Groups External Ident	tity Sources Identity	Source Sequences	gs							
Users	Network Acces	ss Users								
Latest Manual Network Scan Results	🥖 Edit 🛛 🕂 Add	🔀 Change Status 👻 🅵 Im	port 🔹 Export 🗸 🗙 Dele	te 👻 📭 Duplicate						
	Status	Name	Description	First Name Last Name						
	🗌 🗹 Enabled	👤 lobby								

当配置窗口打开时,请为Lobby Ambassador用户提供名称和密码。另外,确保状态已启用。

步骤3.创建结果授权配置文件。导航至**策略>Policy元素>结果>授权>授权配置文件>添加**。创建结果 授权配置文件,以便返回WLC和Access-Accept,并使用所需属性,如图所示。

dentity Services Engine Hon	ne Context Visibility Operations	Policy Administration Work Centers
Policy Sets Profiling Posture Client F	Provisioning Policy Elements	
Dictionaries Conditions Results		
0		
▶ Authentication	Standard Authorization Profiles	- Reduce & Redden - Refer Fund Rese
- Authorization	For Policy Export go to Administration > System	> backup & Restore > Policy Export Page
Authorization Profiles	🖊 Edit 🕂 Add 🕞 Duplicate 🗙 Delete	
Downloadable ACLs	Name Name	Profile
Downloadable AGES	9800RadiusLobby	diste Cisco 🕀

确保配置文件配置为发送接入(如图所示)。

dualus Identit	ty Services Er	ngine	Home	► Cor	ntext Visibility	• (Operations	✓ Policy		
Policy Sets	Profiling Po	osture C	lient Provisi	ioning	▼Policy Ele	ments				
Dictionaries	Conditions		ts							
		G								
Authenticati	▶ Authentication			Authorization Profile						
✓ Authorizatio	on		Auche	, include	* Name	9800Ra	adiusLobby			
Authorizatio	n Profiles			_	Description					
Downloadal	ble ACLs			* /	ccess Type	ACCESS	S_ACCEPT	*		

您需要在Advanced Attributes Settings下手动添加属性。要将用户定义为Lobby Ambassador,并提 供权限,以便允许Lobby Ambassador进行所需的更改,需要这些属性。

Advanced Attributes Settings





步骤4.创建策略以处理身份验证。导航至**策略>策略集>添加**。配置策略的条件取决于管理员的决定 。此处使用网络访问用户名条件和默认网络访问协议。

必须确保在授权策略下选择在结果授权下配置的配置文件,这样您就可以将所需的属性返回到 WLC,如图所示。

cisco	Identity Se	rvices Engine	Home	Context Visibility	Operations	olicy Administration	Work Centers			
Policy	Sets Pro	ofiling Posture	Client Provisio	oning + Policy Elem	ents					
Polic	y Sets									
+	Status	Policy Set Nan	ne	Description	Cond	litions		Allo	wed Protocols / Serve	er Sequence
Searc	:h									
	Ø	9800LobbyRadiu	S		1	Network Access UserNar	ne EQUALS lobby	De	fault Network Access	× • +

当配置窗口打开时,配置授权策略。身份验证策略可保留为默认值。

Policy	Sets →	9800LobbyRadius					Reset
	Status	Policy Set Name	Description	Conditions		Allowed Protocols / S	erver Sequence
Search							
	0	9800LobbyRadius		Network Access-UserName EQUALS lobby		Default Network Acces	s x * +
> Auth	entication	n Policy (1)					
> Auth	orization	Policy - Local Exceptions					
> Auth	orization	Policy - Global Exceptions					
✓ Auth	orization	Policy (2)					
					Results		
	Status	Rule Name	Conditions		Profiles	Security Groups	Hits
Search	h						
	Ø	9800LobbyAutho	Network Access-UserNan	THE EQUALS HODBY	× 9800RadiusLobby	+ Select from list	+ 0

验证TACACS+

在WLC上配置TACACS+

步骤1.声明TACACS+服务器。在WLC中创建ISE TACACS服务器。

GUI:

导航至Configuration > Security > AAA > Servers/Groups > TACACS+ > Servers > + Add,如图所示。

Q Search Menu Items	Configuration * > Security	AAA <			
📻 Dashboard	+ AAA Wizard				
Monitoring >	Servers / Groups AA	AA Method List AAA Advanced			
Configuration 5	+ Add × Delete				
() Administration	RADIUS				
💥 Troubleshooting	TACACS+	Server Groups			
	1040	Name ~	Server Address ~	Port	~
	LDAP	TACACSLobby	192.168.166.8	49	
		≪ <1 >> > 10 → items	per page		1 - 1 of 1 items

当配置窗口打开时,必需的配置参数是TACACS+服务器名称(它不必与ISE/AAA系统名称匹配)、 TACACS服务器IP地址和共享密钥。任何其他参数都可保留默认值或根据需要进行配置。

CLI :

Tim-eWLC1(config)#tacacs server TACACSLobby Tim-eWLC1(config-server-tacacs)#address ipv4 192.168.166.8 Tim-eWLC1(config-server-tacacs)#key 0 Cisco123 Tim-eWLC1(config-server-tacacs)#end 步骤2.将TACACS+服务器添加到服务器组。定义服务器组并添加所配置的所需TACACS+服务器。 这将是用于身份验证的TACACS+服务器。

GUI:

导航至Configuration > Security > AAA > Servers / Groups > TACACS > Server Groups > + Add,如图所示。

Q Search Menu Items	Configuration * > Sec	curity * > AAA			
📻 Dashboard	+ AAA Wizard				
Monitoring	> Servers / Groups	AAA Method List A	AAA Advanced		
🔾 Configuration	> + Add × Dele				
() Administration	> RADIUS				
💥 Troubleshooting	TACACS+	Servers Server	Groups		
	LDAD	Name	Y Server 1	Server 2	Server 3
	LDAP	GroupTacLobby	TACACSLobby	N/A	N/A
			10 🔻 items per page		1 - 1 of 1 items

当配置窗口打开时,为组指定名称,并将所需的TACACS+服务器从Available Servers列表移动到 Assigned Servers列表。

CLI :

Tim-eWLC1(config)#aaa group server tacacs+ GroupTacLobby Tim-eWLC1(config-sg-tacacs+)#server name TACACSLobby

Tim-eWLC1(config-sg-tacacs+)#end

步骤3.创建身份验证方法列表。身份验证方法列表定义所需的身份验证类型,并将其附加到已配置的服务器组。它还允许选择身份验证是在WLC上本地完成还是在TACACS+服务器外部完成。

GUI:

导航至Configuration > Security > AAA > AAA Method List > Authentication > + Add,如图所示。

Q Search Menu Items		Configuration * > Se	curity	• > AAA									
📻 Dashboard		+ AAA Wizard											
Monitoring		Servers / Groups	AA	A Method List	AAA Advance	ed							
🔾 Configuration	>	Authentication	_	_									
() Administration	>	Authorization	L	+ Add × De									
X Troubleshooting		Accounting		Name 🗸	Туре 🗸	Group ~ Type	Group1 ~	Group2	~	Group3	~	Group4	~
			0	AutheTacMeth	login	local	GroupTacLobby	N/A		N/A		N/A	

当配置窗口打开时,提供名称,选择类型选项作为"登录",并**分配**之前创建的服务器组。

组类型为本地。

GUI:

如果选择Group Type作为"local",WLC将首先检查本地数据库中是否存在该用户,然后仅在本地数 据库中找不到Lobby Ambassador用户时才回退到服务器组。

注意:请注意此漏<u>洞CSCvs87163</u>在17.3中修复。

Tim-eWLC1(config)#aaa authentication login AutheTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end

组类型为组。

GUI:

如果选择组类型作为组,并且未选中回退到本地选项,WLC将仅根据服务器组检查用户,不会签入 其本地数据库。

CLI :

Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby Tim-eWLC1(config)#end

Group Type as group和回退到本地选项已选中。

GUI:

如果选择Group Type(组类型)为"group",并且选中Fallback to local(回退到本地)选项,则 WLC将根据服务器组检查用户,并仅在TACACS服务器在响应中超时时查询本地数据库。如果服务 器发送拒绝,则即使用户在本地数据库上存在,也不会对其进行身份验证。

CLI :

Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local Tim-eWLC1(config)#end

步骤4.创建授权方法列表。

授权方法列表将定义大厅大使需要的授权类型,在本例中,该授权类型将执行。它还连接到所配置 的同一服务器组。还可以选择身份验证是在WLC上本地完成还是在TACACS+服务器外部完成。

GUI:

导航至Configuration > Security > AAA > AAA Method List > Authorization > + Add,如图所示。

Q Search Menu Items		Configuration * > Se	curity	• > AA	A												
📻 Dashboard		+ AAA Wizard															
	>	Servers / Groups	AA	A Metho	d List	AAA	A Advanc	ed									
	>	Authentication															
() Administration	>	Authorization		+ Add													
💥 Troubleshooting		Accounting															
				Name	~	Туре	\sim	Group Type	×.	Group1	G	aroup2	\sim	Group3	\sim	Group4	\sim
			0	AuthozTa	acMe	exec		local		GroupTacLob	. N	I/A		N/A		N/A	
			ŀ	∈ ⊲ 1	►	▶ (10 🔻	tems per page	9							1 - 1 of 1 iten	ns

当配置窗口打开时,提供名称,选择type选项作为exec并分配之前创建的服务器组。

请注意,组类型的应用方式与"身份验证方法列表"部分中的解释方式相同。

CLI :

组类型为本地。

Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end

组类型为组。

Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby Tim-eWLC1(config)#end

Group Type as group和Fallback to local选项已选中。

Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby local Tim-eWLC1(config)#end

步骤5.分配方法。配置方法后,必须将其分配给选项,才能登录WLC以创建访客用户,如线路 VTY或HTTP(GUI)。 这些步骤无法从GUI完成,因此需要从CLI完成。

HTTP/GUI身份验证:

Tim-eWLC1(config)#ip http authentication aaa login-authentication AutheTacMethod Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozTacMethod Tim-eWLC1(config)#end

更改HTTP配置时,最好重新启动HTTP和HTTPS服务:

Tim-eWLCl(config)#no ip http server Tim-eWLCl(config)#no ip http secure-server Tim-eWLCl(config)#ip http server Tim-eWLCl(config)#ip http secure-server Tim-eWLCl(config)#end line vty:

Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AutheTacMethod
Tim-eWLC1(config-line)#authorization exec AuthozTacMethod
Tim-eWLC1(config-line)#end

步骤6.定义远程用户。在ISE上为Lobby Ambassador创建的用户名必须定义为WLC上的远程用户名 。如果WLC中未定义远程用户名,则身份验证将正确进行,但是,将授予用户对WLC的完全访问权 限,而不是仅授予对Lobby Ambassador权限的访问权限。此配置只能通过CLI完成。

CLI:

Tim-eWLC1(config)#aaa remote username lobbyTac

配置ISE - TACACS+

步骤1.启用Device Admin。导航至**管理>系统>部署**。在继续之前,选择**Enable Device Admin** Service 并确保ISE已启用,如图所示。

-ilial cisco	dentity Services I	Engine I	Home	Context Visibility	 Operations 	▶ Policy ▼A	Administration	Work Centers
•	System Identity Ma	nagement 🕨	Network Re	sources	Portal Managemen	t pxGrid Service	es 🔸 Feed Serv	ice Fhreat Centric NAC
De	ployment Licensing	 Certificates 	Loggi	ng Maintenance	Upgrade 🕨 B	ackup & Restore	Admin Access	 Settings
	Deployment			Deployment Node	s List > timise23			
	(- • E •		÷.	Edit Node				
	Deployment			General Settings	Profiling Cont	figuration		
	🔆 PAN Failover							
				Hostname	tim	ise23		
				FQDN IR Address	tim 19/	115e23.clsco.com		
				Node Type	Ide	ntity Services En	gine (ISE)	
							•	
					_			
				Role STANDA		ake Primary		
				Administ	ration			
				🗹 👻 Monitorin	g			
				Role	2	PRIMARY	-	
					-			
				Oth	er Monitoring Node	5		
				Policy Se	rvice			
				V V E	nable Session Se	rvices ①		
					Include Node	in Node Group N	ione	* (7)
				✓ E	nable Profiling Se	rvice (j)		
				E E	nable Threat Cent	ric NAC Service @		
				□) E	able SXP Servic	e 🕡		
				V E	Enable Device Adm	in Service (j)		

步骤2.将WLC添加到ISE。导航至**管理>网络资源>网络设备>添加**。WLC需要添加到ISE。将WLC添加到ISE时,启用TACACS+身份验证设置并配置所需的参数,如图所示。

dentity Services Engine	Home Context Visibility		Administration Vork Centers		
System Identity Management	Network Resources Device	e Portal Management pxGrid Servic	es	AC	
▼Network Devices Network Device	Groups Network Device Profiles	External RADIUS Servers RADI	US Server Sequences NAC Managers	External MDM Location Services	
(•				
Network Devices	Network Devices				
Default Device					
Device Security Settings	/ Edit - Add Dupli	ate 👔 Import 😨 Export 👻 🔘	Senerate PAC X Delete V		Show
	Name 🔺 IP/M	ask Profile Name	Location	Туре	Description
	Tim-eWLC1 192.	68.166.7 🗰 Cisco 🕀	All Locations	All Device Types	9800

当配置窗口打开以提供名称IP ADD时,启用TACACS+ Authentication Settings,并输入所需的共享密钥。

步骤3.在ISE上创建Lobby Ambassador用户。导航至**管理>身份管理>身份>用户>添加**。添加到 ISE,分配给将创建访客用户的Lobby Ambassador的用户名和密码。这是管理员分配给大厅大使的 用户名,如图所示。

dentity Services Engine	Home	y ▶ Operations	Policy Administration	Work Centers
► System Identity Management	Network Resources De	vice Portal Management	pxGrid Services Feed	Service
✓Identities Groups External Identity	y Sources Identity Source S	equences • Settings		
0				
Users	Network Access Users	5		
Latest Manual Network Scan Results				
	/ Edit 🕂 Add 🔢 Cha	inge Status 👻 🔀 Import	Export - XDelete -	Duplicate
	Status 👻 Name		Description	First Name Last Name
	🗌 🔽 Enabled 🙎 lobb	/Tac		

当配置窗口打开时,请为Lobby Ambassador用户提供名称和密码。另外,确保状态已启用。

步骤4.创建结果TACACS+配置文件。导航到工**作中心(Work Centers)>设备管理(Device** Administration)>策略元素(Policy Elements)>结果(Results)> TACACS配置文件(TACACS Profiles),如图所示。使用此配置文件,将所需属性返回到WLC,以便将用户置为接待大使。

dentity Services Engine	Home Context Vis	ibility	▶ Policy ▶ Admin	nistration Vork Centers
Network Access Guest Access	TrustSec BYOD	Profiler Posture	Device Administration	n PassiveID
Overview Identities User Ident	ity Groups Ext Id Source	Network Resources	▼Policy Elements	Device Admin Policy Sets
G				
▶ Conditions	TACACS Profile	S		
Network Conditions	0 Selected			
✓ Results	${\cal C}$ Refresh $ig+$	Add Duplicate	Trash 🔻 🕜 Edit	
Allowed Protocols	Name		Туре D	escription
TACACS Command Sets	Default Shell	Profile	Shell D	efault Shell Profile
TACACS Profiles	Deny All She	Il Profile	Shell D	eny All Shell Profile
	WLC ALL		WLC V	/LC ALL
	WLC MONIT	OR	WLC W	LC MONITOR

当配置窗口打开时,为配置文件提供名称,并将默认特权15和自定义属性配置为Type Mandatory,名称配置为user-type,值lobb-admin。此外,如图**所示,将"**常见任务类型"选为"壳"。

	Task Attribute View	Raw View						
Comme	Common Tasks							
Commor	n Task Type Shell	•						
	 Default Privilege 	15	0	(Select 0 to 15)				
	Maximum Privileg	e	0	(Select 0 to 15)				
	Access Control Li	st	0]				
	Auto Command		0]				
	No Escape		0	(Select true or false)				
	Timeout		0	Minutes (0-9999)				
	Idle Time		0	Minutes (0-9999)				
Custon	n Attributes							
1 Selecte	ed							
🕈 Ad	d 💼 Trash▼ 🕑 E	dit						
e	Туре	Name	Value					
	MANDATORY	user-type	lobby-admin					

步骤5.创建策略集。导航至**工作中心(Work Centers)>设备管理(Device Administration)>设备管理策 略集(Device Admin Policy Sets),如**图所示。配置策略的条件取决于管理员的决定。对于本文档 ,使用网络访问用户名条件和默认设备管理协议。必须确保在授权策略下选择在结果授权下配置的 配置文件,这样您才能将所需属性返回到WLC。

altaba cisco	Identity Ser	vices Engine	Home)	Context Visibilit	y	▶ Polic	y ▶ Adminis	stration	▼ Work Centers			Q	0	• •
► Ne	twork Access	Guest Access	 TrustSec 	BYOD F	Profiler Posture	- Device	Administration	 Pass 	ivelD					
► Ov	verview • Id	entities User Ident	tity Groups	Ext Id Sources	Network Resource	s Pol	icy Elements	Device Ad	Imin Policy Sets	Reports Settings				
Polic	cy Sets											F	Reset	Save
+	Status	Policy Set Name		Description		Conditio	ons			Allowed Protocols	/ Server Sequence	Hits	Actions	View
Sea	rch													
	Ø	9800TacacsLobby				1	Network Access- EQUALS lobby	•UserNam Tac	e	Default Device Adm	in × v 🕇	0	¢	>

当配置窗口打开时,配置授权策略。如图所示,身份验证策略可保留为默认状态。

Policy Sets → 9800TacacsLobby

Reset Save

	Status Policy Set Name Description Conditions						er Sequence	e Hits
Search								
	0	9800TacacsLobby		Network Access UserName EQUALS lobbyTac		Default Device Admin	x • +	0
> Auth	enticatio	n Policy (1)						
> Auth	orization	Policy - Local Exceptions						
> Auth	orization	Policy - Global Exceptions						
∀ Auth	orization	Policy (2)						
					Results			
•	Status	Rule Name	Conditions		Command Sets	Shell Profiles	Hits	Actions
Searc	h							
	Ø	9800TacacsAuth	Network Access-UserNar	me EQUALS lobbyTac	Select from list	9800TacacsLobby × -	• •	٥

验证

使用本部分可确认配置能否正常运行。

```
show run aaa
show run | sec remote
show run | sec http
show aaa method-lists authentication
show aaa method-lists authorization
show aaa servers
show tacacs
```

这是Lobby Ambassador GUI在成功身份验证后的外观。

Q Search Menu Items	+ Add × Delete			
	User Name	 Description 	 Created By 	Υ.
	H 4 0 ► H 10 ¥ items p	er page		No items to display

故障排除

本部分提供的信息可用于对配置进行故障排除。

验证RADIUS

对于RADIUS身份验证,可以使用以下调试:

Tim-eWLC1#debug aaa authentication Tim-eWLC1#debug aaa authorization Tim-eWLC1#debug aaa attr Tim-eWLC1#terminal monitor 确保从调试中选择了正确的方法列表。此外.ISE服务器会返回具有正

```
确保从调试中选择了正确的方法列表。此外,ISE服务器会返回具有正确用户名、用户类型和权限
的所需属性。
```

7FBA5500C870 0 00000081 username(450) 5 lobby Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(0000000): add attr: sublist(0x7FBA5500C860) index(1): 7FBA5500C8B0 0 00000001 user-type(1187) 4 lobby-admin Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(2): 7FBA5500C8F0 0 00000001 priv-lvl(335) 4 15(F) Feb 5 02:35:27.683: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host

192.168.166.104 by user 'lobby' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'

确保使用正确的用户名和ISE IP ADD处理身份验证。此外,应看到状态"PASS"。在同一调试中,在 身份验证阶段之后,将显示授权过程。在此授权中,阶段确保正确的用户名与正确的ISE IP ADD一 起使用。从此阶段,您应该能够看到在ISE上配置的属性,这些属性将WLC指定为具有权限的Lobby

验证TACACS+

对于TACACS+身份验证,可以使用此调试:

Feb 5 02:06:48.245: TPLUS: Using server 192.168.166.8

Feb 5 02:06:48.267: TPLUS: Using server 192.168.166.8

Feb 5 02:06:48.279: TPLUS: Processed AV user-type=lobby-admin

Feb 5 02:06:48.279: TPLUS: received authorization response for 0: PASS

Feb 5 02:06:48.279: TPLUS: Processed AV priv-lvl=15

要禁用调试,可以使用以下命令:

Tim-eWLC1#undebug all

Tim-eWLC1#terminal monitor

Tim-eWLC1#debug tacacs

Ambassador用户。

身份验证阶段示例:

授权阶段示例:

Feb 5 02:06:48.245: TPLUS: Queuing AAA Authentication request 0 for processing Feb 5 02:06:48.245: TPLUS: Authentication start packet created for O(lobbyTac)

Feb 5 02:06:48.250: TPLUS: Received authen response status GET_PASSWORD (8) Feb 5 02:06:48.266: TPLUS(0000000)/0/7FB7819E2100: Processing the reply packet

Feb 5 02:06:48.267: TPLUS: Queuing AAA Authorization request 0 for processing Feb 5 02:06:48.267: TPLUS: Authorization request created for O(lobbyTac)

Feb 5 02:06:48.279: TPLUS(0000000)/0/7FB7819E2100: Processing the reply packet

前面提到的RADIUS和TACACS+的调试示例包含成功登录的关键步骤。调试更详细,输出也更大。

Feb 5 02:06:48.266: TPLUS: Received authen response status PASS (2)