為9800 WLC上的GUI &; CLI Auth配置RADIUS &; TACACS+

目錄
· · · · · · · · · · · · · · · · · · ·
<u>必要條件</u>
採用元件
<u>背景資訊</u>
<u>唯讀使用者限制</u>
為WLC配置RADIUS身份驗證
為RADIUS配置ISE
配置TACACS+ WLC
TACACS+ ISE配置
<u>疑難排解</u>
排除WLC GUI或透過WLC CLI訪問CLI RADIUS/TACACS+的故障
透過ISE GUI排除WLC GUI或CLITACACS+訪問故障

簡介

本文說明如何配置Catalyst 9800進行RADIUS或TACACS+外部身份驗證。

必要條件

需求

思科建議您瞭解以下主題:

- Catalyst無線9800組態型號
- AAA、RADIUS和TACACS+概念

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- C9800-CL v17.9.2
- ISE 3.2.0

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。

背景資訊

當使用者嘗試存取WLC的CLI或GUI時,系統會提示使用者輸入使用者名稱和密碼。預設情況下,這 些憑證會與本地使用者資料庫(裝置本身就有)進行比較。或者,可以指示WLC將輸入憑據與遠端 AAA伺服器進行比較:WLC可以使用RADIUS或TACACS+與伺服器通訊。

設定

在本示例中,在AAA伺服器(ISE)上配置了兩種型別的使用者,分別為adminuser和helpdeskuser。這些使用者分別是admin-group和helpdesk-group組的一部分。使用者adminuser是admin-group的一部分,應該被授予對WLC的完全訪問許可權。另一方面,helpdeskuser是helpdesk-group的一部分,用於僅向WLC授予監控許可權。因此,沒有配置訪問許可權。

本文首先配置WLC和ISE進行RADIUS身份驗證,然後對TACACS+執行相同操作。

唯讀使用者限制

使用TACACS+或RADIUS進行9800 WebUI驗證時,存在以下限制:

• 許可權級別為0的使用者存在,但無權訪問GUI

•

許可權級別為1-14的使用者只能檢視Monitor頁籤(這相當於本地身份驗證的只讀使用者的許可權級別)

許可權級別為15的使用者具有完全訪問許可權

不支援許可權等級為15的使用者,以及僅允許特定命令的命令集。使用者仍可透過WebUI執行組態變更

這些考量無法變更或修改。

為WLC配置RADIUS身份驗證

步驟 1.宣告RADIUS伺服器。

<u>在 GUI 上:</u>

首先,在WLC上建立ISE RADIUS伺服器。這可以在https://<WLC-IP>/webui/#/aaa中訪問的GUI WLC頁面的Servers/Groups > RADIUS > Servers頁籤中完成,或者導航到Configuration > Security > AAA(Webex,或Webex)進行(如圖所示)。

Q Search Menu Items	Configuration • > Secu	urity * > AAA				
Dashboard Configuration	+ AAA Wizard Servers / Groups A + Add × Det	AA Method List AAA Advance	d			
O Administration	> RADIUS	Servers Server Groups				
C Licensing	TACACS+	Name	▼ Address	T Auth Port	Y Acct Port	Ŧ
X Troubleshooting	LDAP	ISE-lab	10.48.39.134	1812	1813	
Walk Me Through >		For Radius Fallback to work, ple	ase make sure the Dead Criteria and	Dead Time configuration exists or	the device	

要在WLC上增加RADIUS伺服器,請按一下映像中以紅色框住的「增加」按鈕。這會開啟熒幕擷取畫面中描繪的躍現式視窗。

Q. Search Menu Items	Configuration * >	Security* > AAA			
	Create AAA Radius Server				×
Dashboard	Name*	ISE-lab	Support for CoA (i)	ENABLED	
Monitoring	Server Address*	10.48.39.134	CoA Server Key Type	Clear Text 🗸	
	PAC Key	0	CoA Server Key (i)		
	Кеу Туре	Clear Text 👻	Confirm CoA Server Key		
C Licensing	Key* (i)		Automate Tester	0	T
X Troubleshooting	Confirm Key*				items to display
	Auth Port	1812			
	Acct Port	1813			
Walk Me Through >	Server Timeout (seconds)	1-1000			
	Retry Count	0-100			
					_
	"D Cancel			📓 Apply to [Device

在此彈出窗口中,必須提供:

- 伺服器名稱(請注意,它不必與ISE系統名稱匹配)
- 伺服器IP地址
- WLC和RADIUS伺服器之間的共用金鑰

在 CLI 上:

<#root>

WLC-9800(config)#radius server

ISE-lab

WLC-9800(config-radius-server)#address ipv4

10.48.39.134

auth-port 1812 acct-port 1813
WLC-9800(config-radius-server)#key

Ciscol23

步驟 2.將RADIUS伺服器對映到伺服器組。

<u>在 GUI 上:</u>

如果有多個可用於身份驗證的RADIUS伺服器,建議將所有這些伺服器對映到同一個伺服器組。WLC負責對伺服器組中伺服器之間的 不同身份驗證進行負載均衡。RADIUS伺服器組在與步驟1.中所提到的GUI頁面的Servers/Groups > RADIUS > Server Groups頁籤上配 置,如圖所示。



至於伺服器的建立,當您按一下「新增」(Add)按鈕時,會出現一個躍現式視窗(上一個影像中的架構),如下圖所示。

Q Search Menu Items	Configuration - > Security - > AAA Create AAA Radius Server	Group ×	
Dashboard	Name*	RADIUS-Group	
Monitoring >	Group Type	RADIUS	
	MAC-Delimiter	none 🗸	
	RAI MAC-Filtering	none	
C Licensing	TAC Dead-Time (mins)	5	Server 3
Y Troubleshooting	LD/ Load Balance	DISABLED	No items to display
676 	Source Interface VLAN ID	1 2	
	Available Servers	Assigned Servers ISE-lab	
	Cancel	Apply to Device	

在彈出窗口中,為組提供一個名稱,並將所需的伺服器移到Assigned Servers清單中。

<u>在 CLI 上:</u>

<#root>

WLC-9800(config)# aaa group server radius

.

RADIUS-Group

.

WLC-9800(config-sg-radius)# server name

<u>ISE-lab</u>

-

步驟 3.建立指向RADIUS伺服器組的AAA身份驗證登入方法。

<u>在 GUI 上:</u>

仍在GUI頁面https://<WLC-IP>/webui/#/aaa中,導覽至AAA Method List > Authentication索引標籤,然後建立驗證方法,如下圖所示。

Q Search Menu Items	Configuration * > Security	• >	AAA													
📻 Dashboard	+ AAA Wizard Servers / Groups AAA	Metho	od List AAA	A	dvanced											
Monitoring Monitoring	Authentication															
() Administration	Authorization		Name	T	Type	-	Group	Ŧ	Group1	•	Group2	T	Group3	•	Group4	-
C Licensing	, locol ang	ο	default	,	login	,	local		N/A	1	N/A	,	N/A	,	N/A	
X Troubleshooting		0	radius-authe- method		login		local		RADIUS-Group		N/A		N/A		N/A	
		н	< 1 ≥	H	10 🔻										1 - 2 of 2	items
Walk Mc Through >																

通常,當您使用「增加」按鈕建立身份驗證方法時,會出現配置彈出窗口,類似於本圖中所示的窗口。

Q Search Menu Items	Configuration * > Security * > AAA			
Dashboard	+ AAA Wizard Quick Setup: AAA Authentication			
Monitoring >	Method List Name* radius-authe-metho	зd		
Configuration >	Type* login	• 0		
O Administration	Group Type	• 0		Count -
C Licensing	Available Server Groups	Assigned Server Groups	N/A	N/A
X Troubleshooting	radius Idap tacacs+ C *	ADIUS-Group		
Walk Me Through >	Cancel	Apply to Device		

在此彈出窗口中,提供方法的名稱。選擇Type作為登入,並且將在上一步中建立的組伺服器增加到Assigned Server Groups清單中。對於Group Type欄位,可以進行若干配置。

• 如果您選擇「群組型別」作為「本機」,WLC會先檢查使用者身份證明是否在本機存在,然後回到伺服器群組。

• 如果您選擇「群組型別」作為群組且未核取「轉至本機」選項,WLC只會檢查伺服器群組的使用者認證。

• 如果選擇組型別作為組並選中回退到本地選項,則WLC將根據伺服器組檢查使用者憑據,並且僅當伺服器未響應時才查 詢本地資料庫。如果伺服器傳送拒絕訊息,則使用者必須經過驗證,即使該使用者可以存在於本機資料庫上。

在 CLI 上:

如果您希望只有在本機找不到使用者身份證明時,才使用伺服器群組來檢查使用者身份證明,請使用:

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

local group

RADIUS-Group

如果您希望僅對伺服器群組檢查使用者身份證明,請使用:

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

如果您想要使用伺服器群組檢查使用者身份證明,而且如果最後未使用本機專案回應,請使用:

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

local

在此示例設定中,有些使用者僅在本機建立,而有些使用者僅在ISE伺服器上,因此,使用第一個選項。

步驟 4.建立指向RADIUS伺服器組的AAA授權exec方法。

<u>在 GUI 上:</u>

使用者還必須獲得授權才能獲得訪問許可權。仍在GUI Page Configuration > Security > AAA頁籤中,導航到AAA Method List > Authorization頁籤,然後建立授權方法(如圖所示)。

Q Search Menu Items	Configuration • > Securit + AAA Wizard	ty* > AAA											
Monitoring	> Servers / Groups	Method List	AAA Ad	dvanced									
	Authorization	+ Add	× Dela	ete			-		_		_		_
	Accounting	Name	Ť	Туре	Group Type	Group1	T	Group2	T	Group3	T	Group4	Υ.
C Licensing		C radius-autho- method		exec	local	RADIUS-Group		N/A		N/A		N/A	
Troubleshooting		8 8 1	F H	10 👻								1 - 2 of 2 ite	ems
Walk Me Through 3													

授權方法建立

當您使用Add按鈕增加新授權方法時,會出現與所描述配置類似的授權方法配置彈出窗口。

Q Search Menu Items	Configuration * > Security * > AAA		
Dashboard	Quick Setup: AAA Authorization *		
Monitoring >	Server Method List Name* radius-autho-method		
Configuration	Aut Type*		
(⑦ Administration >	Group Type	▼ Group3 ▼	Group4
© Licensing	Acc Authenticated Available Server Groups Assigned Server Groups	N/A	N/A
X Troubleshooting	radius idap idap tacacs+ @		
Walk Me Through >	Cancel		

在此配置彈出窗口中,為授權方法提供一個名稱,選擇Type作為exec,並使用Group Type與步驟3中用於身份驗證方法的順序相同的 順序。

<u>在 CLI 上:</u>

對於身份驗證方法,首先分配授權以根據本地條目檢查使用者,然後根據伺服器組中的條目檢查使用者。

WLC-9800(config)#aaa authorization exec

radius-autho-method

local group

RADIUS-Group

步驟 5.將方法分配給HTTP配置和用於Telnet/SSH的VTY線路。

<u>在 GUI 上:</u>

建立的身份驗證和授權方法可用於HTTP和/或Telnet/SSH使用者連線,您可以從AAA Advanced > AAA Interface頁籤上的GUI WLC頁 進行配置(可透過https://<WLC-IP>/webui/#/aaa訪問),如下圖所示:

Q Search Menu Items		Configuration * > Secur	ity > AAA							
🚃 Dashboard		+ AAA Wizard	A Mathed List	AA Advaced	1					
Monitoring	>	Servers / Groups AA	A Method List	AA Advanced						
	>	Global Config							🖹 Ag	pply
O Administration	>	RADIUS Fallback			Authentication	Authorization		Accountin	g	
C Licensing		Attribute List Name	Console		None 👻	None	• 2	None	•	8
		Device Authentication	VTY		radius-authe-method v	radius-autho-method	•	None	•	8
Sol in the second sec		AP Policy	HTTP		radius-authe-method v	radius-autho-method	•	None	¥	
		Password Policy								
Walk Me Through >		AAA Interface	1							
			-							

用於GUI身份驗證的CLI:

WLC-9800(config)#ip http authentication aaa login-authentication

radius-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-autho-method

用於Telnet/SSH身份驗證的CLI:

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-autho-method

請注意,當對HTTP配置執行更改時,最好重新啟動HTTP和HTTPS服務。這可以透過以下命令來實現:

WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server WLC-9800(config)#ip http s

為RADIUS配置ISE

步驟 1.將WLC配置為RADIUS的網路裝置。

<u>在 GUI 上:</u>

要將上一部分中使用的WLC宣告為ISE中RADIUS的網路裝置,請導航到Administration > Network Ressources > Network Devices並打開 Network devices頁籤,如下圖所示。



要增加網路裝置,請使用Add按鈕,該按鈕將打開新的網路裝置配置表單。

		Administration · Netw	vork Resources	🛕 Evalu	ation Mode 82 Days	Q ()	50	¢
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More \vee			
Network Devices Default Device Device Security Settings	Network Devices Li Network Devi	st > New Network Device						
	Name	WLC-9800						
	Description							
	IP Addre	ss 🗸 * IP : 10.48.39.13	33 / 32 🔯					
	Device Profile	atta Cisco	× (j)					
	Model Name		~					
	Software Version	on	~					
	Network Device	e Group						
	Location	All Locations	✓ Set To Def.	ault				
	IPSEC	Is IPSEC Device	✓ Set To Def	ault				
	Device Type	All Device Types	✓ Set To Def	ault				
	🗹 🗸 RAD	IUS Authentication Setting	js					
	RADIUS	UDP Settings						
	Protocol	RADIUS						
	Shared S	Secret	Show					
	Uses	Second Shared Secret () Second Shared Secret		Show				
	CoA Por	t 1700	Set To De	fault				
	RADIUS	DTLS Settings 🕕						
		Required (i)						
	Shared S	Secret radius/dtls						

在新窗口中,為網路裝置提供一個名稱,並增加其IP地址。選擇RADIUS身份驗證設定並配置與WLC上使用的RADIUS共用金鑰相同的RADIUS共用金鑰。

步驟 2.建立授權結果以返回許可權。

<u>在 GUI 上:</u>

要具有管理員訪問許可權,adminuser需要具有15級的特權,它允許訪問exec提示符shell。另一方面,helpdeskuser不需要exec提示外殼 訪問,因此可以為它分配低於15的特權級別。為了將適當的許可權級別分配給使用者,可以使用授權配置檔案。這些可以從ISE GUI Page Policy > Policy Elements > Results頁籤下配置,下圖顯示了Authorization > Authorization Profiles。

≡ Cisco ISE			Policy	Policy Elements	A Evaluation Mode 82 Day	\$ D D 21
Dictionaries Co	onditions	Results				
Authentication Authorization Authorization Profiles Downloadable ACLs	>	Star For Policy	Adard Authori	Zation Profiles - System > Backup & Restore > Policy Export F Ocidente	Page Selected	0 Total 11 <i>글 ۞</i> All ~ ▽
Profiling	>		Name	Profile	∧ Description	
Posture	>		9800-admin-priv	🗰 Cisco 👔		
Client Provisioning	>		9800-helpdesk-priv	🚓 Cisco 🕧		
			Block_Wireless_Access	ដ Cisco 🕕	Default profile used to block wireles	s devices. Ensure ti
			Cisco_IP_Phones	🗰 Cisco 🕧	Default profile used for Cisco Phone	IS.
			Cisco_Temporal_Onboard	🗰 Cisco 🕕	Onboard the device with Cisco temp	ooral agent
			Cisco_WebAuth	ដ Cisco 🕕	Default Profile used to redirect user	s to the CWA portal
			NSP_Onboard	ដ Cisco 🕕	Onboard the device with Native Sup	plicant Provisioning
			Non_Cisco_IP_Phones	ដ Cisco 🕕	Default Profile used for Non Cisco P	hones.
			UDN	ដ Cisco 🕕	Default profile used for UDN.	
			DenyAccess		Default Profile with access type as A	Access-Reject
		-				

要配置新的授權配置檔案,請使用Add按鈕,打開新的授權配置檔案配置表。要配置分配給adminuser的配置檔案,此表單尤其必須如 下所示。

=	Cieco	ISE
_	CISCU	1 JL

Policy · Policy Elements

Dictionaries Conditions	Results
Authentication >	Authorization Profiles > New Authorization Profile
Authorization \vee	Authorization Profile
Authorization Profiles	* Name 9800-admin-priv
Downloadable ACLs	Description
Profiling >	
Posture >	* Access Type ACCESS_ACCEPT ~
Client Provisioning	Network Device Profile 🗰 Cisco 🗸 🕀
	Service Template
	Track Movement
	Agentless Posture
	Passive Identity Tracking 🗌 🕕
	Common Tasks Advanced Attributes Settings
	· Advanced Attributes Settings
	Image: Cisco:cisco-av-pair Image: shell:priv-lvl=15 Image: mage: shell:priv-lvl=15
	Attributes Details Access Type = ACCESS_ACCEPT
	cisco-av-pair = shell:priv-lvi=15
	Submit Cancel

配置顯示將許可權級別15授予與其關聯的任何使用者。如前所述,這是下一步建立的adminuser的預期行為。但是,helpdeskuser必須 具有較低的許可權級別,因此必須建立第二個策略元素。

helpdeskuser的策略元素類似於上面建立的策略元素,不同之處在於字串必shell:priv-lvl=15 須更改為shell:priv-lvl=X,然後將X替換為 所需的許可權級別。在本例中,使用1。

步驟 3.在ISE上建立使用者組。

<u>在 GUI 上:</u>

Administration > Identity Management > Groups GUI Page ISE使用者組是從的使用者身份組頁籤(如螢幕截圖所示)中建立的。

	Administration · Identity Mana	gement	A Evaluation Mode 82 Days Q	0	P	٩
ity Sources	Identity Source Sequences	Settings				
User	Identity Groups	▲ Export ∨ Description	Selected 0 Tota	I 10 🔮	3 4	\$ \$
	😤 helpdesk-group	This is the group containing all users with re	ad-only privileges.			
	😤 admin-group	This is the group containing all users with ad	dministrator privileges.			
	VWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Gro	up			
	A GuestType_Weekly (default)	Identity group mirroring the guest type				
	Number 2 Social Login (default)	Identity group mirroring the guest type				
	Note: The Content of the State	Identity group mirroring the guest type				
	Number 2018 Sector (default)	Identity group mirroring the guest type				
	SROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User G	ŝroup			
	😤 Employee	Default Employee User Group				
	ALL_ACCOUNTS (defauit)	Default ALL_ACCOUNTS (default) User Grou	p			
	ty Sources	Administration - Identity Mana ty Sources Identity Source Sequences User Identity Groups	Administration - Identity Management ty Sources Identity Source Sequences Settings User Identity Groups	Administration · Identity Management Evaluation Mode 82 Days Q ty Sources Identity Source Sequences Settings Selected 0 User Identity Groups Selected 0 V Edit + Ada Delete import Export Name Oescription Mamin-group This is the group containing all users with read-only privileges. if admin-group This is the group containing all users with administrator privileges. if admin-group This is the group containing all users with administrator privileges. if GuestType_Weekly (default) Identity group mirroring the guest type if GuestType_Daily (default) Identity group mirroring the guest type if GuestType_Daily (default) Identity group mirroring the guest type if GuestType_Contractor (default) Identity group mirroring the guest type if GuestType_Contractor (default) Identity group mirroring the guest type if GuestType_Contractor (default) Identity group mirroring the guest type if GuestType_Daily (defau	Administration - Identity Management Evaluation Mode 82 Days Q ty Sources Identity Source Sequences Settings User Identity Groups Selected 0 Total 10 C C Edit Add Mame Description Add C Addmin-group This is the group containing all users with read-only privileges. Addmin-group This is the group containing all users with administrator privileges. Identity group mirroring the guest type Addit-SecouNTS (default) Identity group mirroring the guest type Identity group mirroring the guest type Addition_group_Daily (default) Identity group mirroring the guest type Identity group mirroring the guest type Addition_group_Contractor (default) Identity group mirroring the guest type Identity group mirroring the guest type Addition_group_Contractor (default) Identity group mirroring the guest type <t< th=""><th>Administration - Identity Management Image: Column 1 Image: Column 2 Image: Col</th></t<>	Administration - Identity Management Image: Column 1 Image: Column 2 Image: Col

要建立新使用者,請使用「增加」按鈕,該按鈕將打開新的使用者身份組配置表單,如下所示。

≡ 0	Cisco	ISE		,	Administration · Identity N		A Evaluation Mode 82 Days	Q	0	P	٥		
Identiti	ies	Groups	External Ide	ntity Sources	Identity Source Sequenc	es Settings							
Iden EQ >>	tity Gron	ups dpoint Ident wer Identity C	tity Groups	User Identity Grou Identity Grou * Name Description	ups > New User Identity Group UP admin-group This is the group containing all users with	th administrator privileges.	Submit	Cancel					

提供所建立群組的名稱。建立上面討論的兩個使用者組,即admin-group 和helpdesk-group。

步驟 4.在ISE上建立使用者。

<u>在 GUI 上:</u>

ISE使用者透過Administration > Identity Management > Identities GUI Page的使用者頁籤建立,如螢幕截圖所示。

	≡ Cisc	o ISE		[Administration · Identity Mar	nagement			A Evaluation Mode	82 Days	9) ,9	٥
le	dentities	Groups	External Identi	ty Sources	Identity Source Sequences	Settings							
Use	rs est Manual Ne	etwork Scan Res	Netv	vork A	ccess Users								
			🖉 Edit	+ Add	🛞 Change Status 🗸 🛃 Import	① Export ∨	Delete	C Duplicate	liser Identity Groups	Selected	0 Total :	≥ Ç All ∨	© 7
				Enabled	2 adminuser	rii st Maine	Last Name	Linail Address	admin-group	Admin			
				Enabled	2 helpdeskus				helpdesk-group				

要建立新使用者,請使用Add按鈕打開新的網路訪問使用者配置表單,如下所示。

≡	Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 82 Days 📿 ⊘ д 🏟
Ide	ntities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest	Manual Network Scan I	Network Access Users List > New Network Access User	
		✓ Network Access User	_
		* Username adminuser	
		Status Zabled V	
		Account Name Alias	
		Email	
		✓ Passwords	
		Password Type: Internal Users ~	
		Password Lifetime: With Expiration Password will expire in 60 days Never Expires	
		Password Re-Enter Password	
		* Login Password ····· ···	Generate Password (j
		Enable Password	Generate Password ()
		> User Information	
		> Account Options	
		> Account Disable Policy	
		✓ User Groups	
		ii _admin-group 🗸 🕕 🕂	

向使用者提供憑證,即使用者名稱和密碼,用於在WLC上進行驗證。並且,確保使用者的狀態為Enabled。最後,將使用者增加到其 相關組(已在步驟4.中建立),表單末尾的User Groups下拉選單。

建立上面討論的兩個使用者,即adminuser和helpdeskuser。

步驟 5.驗證使用者。

<u>在 GUI 上:</u>

在此場景中,已預配置的ISE預設策略集的身份驗證策略允許預設網路訪問。此策略集可從ISE GUI頁面的Policy > Policy Sets檢視 ,如下圖所示。因此,沒有必要對其進行更改。

≡	Cisco IS	E			Policy · Policy Sets]		A Evaluation Mode 82 Days) ,a ¢
Polic	y Sets→	Default				Re	set	Reset Policyset Hitcounts		Save
	Status Po	licy Set Name	Descripti	ion	Conditions			Allowed Protocols / Server	Seque	ence Hits
	2 Search									
	0	Default	Default	policy set				Default Network Access		<u>~</u> + o
\sim A	uthentication	n Policy (3)								
0	Status	Rule Name	Cond	litions		U	se		Hits	Actions
	Q Search									
				E Wired	_MAB	_	Internal E	indpoints 🛛 🗸 🗸		~
	•	MAB	OR	E Wirele	ss_MAB	>	Option	าร	0	< <u>5</u> 5
				E Wired	802.1X	_	All_User	ID_Stores 🛛 🗸 🗸		
	0	Dot1X	OR	E Wirele	ss_802.1X	>	Option	าร	0	ţĝ
Г			-				All_User_	ID_Stores 🛛 🗸 🗸		
	0	Default				>	Option	าร	0	<u>{</u> \$}

步驟 6.授權使用者。

<u>在 GUI 上:</u>

登入嘗試透過身份驗證策略後,需要授權該策略,並且ISE需要返回之前建立的授權配置檔案(允許接受,以及許可權級別)。

在本示例中,登入嘗試是根據裝置IP地址(即WLC IP地址)過濾的,並根據使用者所屬的組區分要授予的許可權級別。另一個有效的方法是根據使用者的使用者名稱過濾使用者,因為在本示例中,每個組只包含一個使用者。

	ico IS	E			Policy · Policy S	Sets		A Evaluation M	lode 82 Days (20	P
icy Se	ets→ I	Default					Rese	t Reset Policy	set Hitcounts		Save
State	us Po	licy Set Name	Descript	ion	Conditions			Allowed Prote	ocols / Server	Sequer	nce
Q s	Search										
	0	Default	Default	policy	set			Default Netwo	ork Access <	× ×	- 1
Auther	nticatior	Policy (3)									
Author	rization	Policy - Local Exception	ıs								
Author	rization	Policy - Global Exception	ons (2)								
						Results					
÷ \$	Status	Rule Name	Cond	litions		Profiles	Sec	urity Groups		Hits	Actio
Q	Search										
		9800 Helpdack Licare	AND	₽	Network Access-Device IP Address EQUALS 10.48.39.133	9800-belodesk-priv ×		alact from list	~ +	,	£
	× .	JUOU HEIDUUSK USEIS		0	InternalUser-IdentityGroup	Sood Helbreak bills Y				÷.	202
				~	Groups:helpdesk-group						
		0000 Admin Linear	AND	₽	Reducts User relative Groups:helpdesk-group Network Access-Device IP Address EQUALS 10.48.39.133	0000 admin.priu v		alaat from list			5

完成此步驟後,為adminuser 和helpdesk使用者配置的憑據可用於透過GUI或Telnet/SSH在WLC中進行身份驗證。

配置TACACS+WLC 步驟 1.宣告TACACS+伺服器。 <u>在 GUI 上:</u> 首先,在WLC上建立Tacacs+伺服器ISE。可以在https://<WLC-IP>/webui/#/aaa中的GUI WLC頁面上的頁籤Servers/Groups > TACACS+ > Servers中執行此操作,或者在導航到Configuration > Security > AAA時執行此操作,如下圖所示。

Reset

Cisco Cata	alyst 9800-CL Wireless Controller	Welcome admin & 🕷 🔹 🛕	💾 🌣 🖄 🛛 🎜 Search /	VPs and Clients Q
Q. Search Menu Items Dashboard Image: Configuration Configuration Administration	Configuration * > Security * > AAA + AAA Wizard Servers / Groups AAA Method List + Add × Delete RADIUS Servers	t AAA Advanced Server Groups		
 Licensing Troubleshooting 	LDAP	Name	Server Address 10.48.39.134	Y Port Y 49 1 - 1 of 1 items
Walk Me Through 3				

要在WLC上增加TACACS伺服器,請按一下上圖中以紅色框住的「增加」按鈕。這樣會開啟描繪的躍現式視窗。

Cisco	Cata	lyst 9800-CL	Wireless Controlle	er		
CISCO 17.9.2		,		Welcome admin	🔺 🖺 🌣 🖄 🛛 🎗 Sear	ch APs and Clients Q
Q Search Menu Items		Configuration	Security -> AA	A		
Dashboard		+ AAA Wizard	Create AAA Tacac	s Server	×	
Monitoring	>	Servers / Grou	Name*	ISE-lab		
	>	+ Add	Server Address*	10.48.39.134		
O Administration	>	RADIUS	Кеу Туре	Clear Text 🔹		
C Licensing		TACACS+	Key*			T Port
Troubleshooting		LDAP	Confirm Key*			No items to display
•••			Port	49		
Walk Me Through >			Server Timeout (seconds)	1-1000		
			Cancel		Apply to Device	

當彈出窗口打開時,提供伺服器名稱(它不必與ISE系統名稱匹配)、其IP地址、共用金鑰、使用的埠和超時。 在此彈出窗口中,必須提供:

• 伺服器名稱(請注意,它不必與ISE系統名稱匹配)

伺服器IP地址

• WLC和TACACS+伺服器之間的共用金鑰

可以配置其他引數,例如用於身份驗證和記賬的埠,但這些不是必需的,保留為本文檔的預設設定。

在 CLI 上:

<#root>

WLC-9800(config)#tacacs server

ISE-lab

WLC-9800(config-server-tacacs)#address ipv4

10.48.39.134

WLC-9800(config-server-tacacs)#key

Cisco123

步驟 2.將TACACS+伺服器對映到伺服器組。

<u>在GUI上:</u>

如果您有多個可用於驗證的TACACS+伺服器,建議將這些伺服器對應到同一個伺服器群組。然後,WLC會處理伺服器群組中伺服器 之間不同驗證作業的負載平衡。TACACS+伺服器組是在第1步中提及的相同GUI頁面的Servers/Groups > TACACS > Server Groups頁籤 上配置的,如下圖所示。

Cisco Cataly	st 9800-CL Wireless Controlle	Welcome admin Last login 12/07/2022 14:14:43	• • A B • • •	Search APs and Client	s Q
Q. Search Menu Items Image: Dashboard Image: Omega Image: Omega	Configuration • > Security • > AAu + AAA Wizard Servers / Groups AAA Method Li + Add × Delete RADIUS Servers	st AAA Advanced			
C Licensing Troubleshooting	LDAP	Name TACACS-Group	Server 1 ISE-lab	Server 2 N/A	Server 3 N/A 1 - 1 of 1 items
Walk Me Through >					

至於伺服器的建立,當您按一下先前影像(如該影像所示)中的「新增」按鈕架構時,會出現一個躍現式視窗。

Cisco Cata	lyst 9800-CL Wireless Controller	Welcome admin 🛛 希 😵 🛕 🖺	🔉 🗘 🛛 🎜 Search APs ar	nd Clients Q
Q. Search Menu Items Image: Dashboard Image: Optimized Control Image: Monitoring	Configuration • > Security • > AAA + AAA Wizard Server Create AAA Tacacs Server	r Group	×	
Configuration Administration Configuration	RAI Group Type Available Servers	TACACS-Group TACACS Assigned Servers ISE-lab C B C C D D C C D C C D C C C C C C C C	× × ×	Server 3 No items to display
Walk Me Through 1	Cancel		Apply to Device	

在彈出窗口中,為組指定名稱,並將所需伺服器移至Assigned Servers清單。

在 CLI 上:

<#root>

TACACS-Group

WLC-9800(config-sg-tacacs+)#server name

ISE-lab

步驟 3.建立指向TACACS+伺服器組的AAA身份驗證登入方法。

<u>在 GUI 上:</u>

仍在GUI頁面https://<WLC-IP>/webui/#/aaa中,導航到AAA Method List > Authentication頁籤,然後建立身份驗證方法(如圖所示)。



通常,當您使用「增加」按鈕建立身份驗證方法時,會出現配置彈出窗口,類似於本圖中所示的窗口。

¢	alialia cisco	Cisco	Catal	yst 9800)-CL Wireless Controller										
		17.9.2				Welcome admin	n 🔗	A	8	0 0	C Sea	rch APs and Clients	Q	Feedback	** 🗭
٩	Search Menu It	tems		Configur	ration • > Security • > AAA	ication						×			
	Dashboard Monitoring		>	Server	Method List Name*	tacacs-authe-	method								
			>	Aut Aut	Type* Group Type	login	• (i) • (i)								
©			Í	Acc	Available Server Groups radius Idap	Þ	Assigned TACACS-Grou	l Server Group up	ps	Ā		Group3	т	Group4	T
×					tacacs+ RADIUS-Group	<				< > ¥		N/A		N/A 1 - 2 of 2 ite	
					Cancel						Apply to De	vice			

在此彈出窗口中,提供方法的名稱,選擇login型別,並將上一步中建立的組伺服器增加到Assigned Server Groups清單中。對於Group Type欄位,可以進行若干配置。

- 如果您選擇「群組型別」作為「本機」,WLC會先檢查使用者身份證明是否在本機存在,然後回到伺服器群組。
- 如果您選擇「群組型別」作為群組且未核取「轉至本機」選項,WLC只會檢查伺服器群組的使用者認證。
- 如果選擇組型別作為組並選中回退到本地選項,則WLC將根據伺服器組檢查使用者憑據,並且僅當伺服器未響應時才查 詢本地資料庫。如果伺服器傳送拒絕訊息,則使用者必須經過驗證,即使該使用者可以存在於本機資料庫上。

在 CLI 上:

如果您希望只有在本機找不到使用者身份證明時,才使用伺服器群組來檢查使用者身份證明,請使用:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

local group

TACACS-Group

如果您希望僅對伺服器群組檢查使用者身份證明,請使用:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

如果您想要使用伺服器群組檢查使用者身份證明,而且如果最後未使用本機專案回應,請使用:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

local

在此示例設定中,有些使用者僅在本機建立,而有些使用者僅在ISE伺服器上,因此使用第一個選項。

步驟 4.建立指向TACACS+伺服器組的AAA授權exec方法。

<u>在GUI上:</u>

使用者還必須獲得授權才能獲得訪問許可權。 Configuration > Security > AAA 仍在GUI頁面中, 導航到AAA Method List > Authorization頁籤, 然後建立授權方法(如圖所示)。



當您使用Add按鈕增加新授權方法時,會出現與所描述配置類似的授權方法配置彈出窗口。

Configuration * > Security * > AAA Dashboard Image: Configuration Image: Configuration </th <th>Cisco Cata</th> <th>ilyst 9800-CL Wireless Controller</th> <th>Welcome admin</th> <th>🗘 🔯 😧 🎜 Search APs and</th> <th>Clients Q</th> <th>E Feedback 🦨 🕞</th>	Cisco Cata	ilyst 9800-CL Wireless Controller	Welcome admin	🗘 🔯 😧 🎜 Search APs and	Clients Q	E Feedback 🦨 🕞
Dashboard Image: Configuration	Q Search Menu Items	Configuration · > Security · > AAA + AA Quick Setup: AAA Authori	zation			
Administration Admin	Dashboard Monitoring	Server Method List Name*	tacacs-autho-method			
Addressing Acc Available Server Groups Assigned Server Groups N/A N/A Image: Comparison of the server Groups Troubleshooting Image: Comparison of the server Groups Image: Comparison of the server Groups Image: Comparison of the server Groups N/A N/A Image: Comparison of the server Groups Image: Comparison of	Configuration	Aut Group Type				
Walk Me Through > Image in the provide state in the provide sta	© Licensing	Acc Acc Available Server Groups	Assigned Server Groups TACACS-Group	Ā	Group3 ▼ N/A N/A	N/A
Walk Me Through >	X Troubleshooting	tacacs+ RADIUS-Group				1 - 2 of 2 items
Cancel	Walk Me Through >	Cancel		Apply to Device		

在此配置彈出窗口中,為授權方法提供一個名稱,選擇Type作為exec,並使用Group Type的順序與上一步中用於身份驗證方法的順序 相同。

在 CLI 上:

<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

local group

TACACS-Group

步驟 5.將方法分配給HTTP配置和用於Telnet/SSH的VTY線路。

<u>在 GUI 上:</u>

建立的身份驗證和授權方法可用於HTTP和/或Telnet/SSH使用者連線,您可以從AAA Advanced > AAA Interface頁籤上的GUI WLC頁 進行配置(可透過https://<WLC-IP>/webui/#/aaa訪問),如圖所示。

Cisco Catal	yst 9800-CL Wireless Contro	Welcome admin Last login 12/07/2022 14:14:43	* * A B	* @ 0 2	Search APs and Clients	Q Eeedback	
Q. Search Menu Items Dashboard Monitoring	Configuration * > Security * > A + AAA Wizard Servers / Groups AAA Method	List AAA Advanced					
Configuration	Global Config RADIUS Fallback		Authentication	Auth	orization	Accounting	Apply
C Licensing Troubleshooting	Authoritication VTY Authentication VTY AP Policy HTT	sole P	None v tacacs-authe-methodv tacacs-authe-methodv	None Image: Constraint of the second seco	v 2 ho-methodv 2 ho-methodv 2	None v None v None v) ©) ©) ©
Walk Me Through >	Password Policy AAA Interface						



對於GUI身份驗證:

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

tacacs-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

tacacs-autho-method

對於Telnet/SSH身份驗證:

<#root>

WLC-9800(config)#line vty 0 15
WLC-9800(config-line)#login authentication

tacacs-authe-method

WLC-9800(config-line)#authorization exec

tacacs-autho-method

請注意,當對HTTP配置執行更改時,最好重新啟動HTTP和HTTPS服務。這可以透過這些命令來實現。

WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server

TACACS+ ISE配置 步驟 1.將WLC配置為TACACS+的網路裝置。

<u>在 GUI 上:</u>

要將上一部分中使用的WLC宣告為ISE中RADIUS的網路裝置,請導航到Administration > Network Resources > Network Devices並打開 「網路裝置」頁籤,如此圖中所示。

≡ Cisco ISE		Administration · Ne	twork Resources	A Evalu	uation Mode 82 Days Q 🕜 🥫 🕸
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More \sim
Network Devices	Networ	rk Devices			
Device Security Settings					Selected 1 Total 1 🦪 🗔
	2 Edit +	Add 🌔 Duplicate 🕁 Impor	t 🏦 Export 🗸 👌 Generate PAG	Delete 🗸	All \vee ∇
	🗌 Nar	me 🗠 IP/Mask Profile	Name Location	Туре	Description
	wL	C-9800 10.48.39 🗰 Cis	co (i) All Locations	All Device Types	

在本示例中,已為RADIUS身份驗證增加了WLC(請參閱<mark>配置RADIUS ISE</mark>部分的步驟1。)因此,只需修改其配置即可配置TACACS身 份驗證,只需在網路裝置清單中選擇WLC並按一下Edit按鈕即可。這將打開網路裝置配置表,如下圖所示。

■ Cisco ISE	Administration · Network Resources		🔺 Evalua	ation Mode 82 Days Q	05	0 \$
Network Devices	Network Device Groups Network Device Profiles Exter	nal RADIUS Servers	RADIUS Server Sequences	More \sim		
Network Devices	General Settings					
Default Device	Enable KeyWrap 🕕					
Device Security Settings	Key Encryption Key Message Authenticator Code Key	Show				
	Key Input Format ASCII O HEXADECIMAL					
	Shared Secret	Show				
	Enable Single Connect Mode Egacy Cisco Device TACACS Draft Compliance Single Connect	: Support				
	 SNMP Settings Advanced TrustSec Settings 					

打開新窗口後,向下滾動到「TACACS Authentication Settings」部分,啟用這些設定,並增加在<u>Configure TACACS+ WLC</u>部分的步驟 1中輸入的共用金鑰。

步驟 2.啟用節點的裝置管理功能。



注意:要將ISE用作TACACS+伺服器,您必須擁有裝置管理許可證軟體套件和基礎許可證或移動許可證。

<u>在 GUI 上:</u>

安裝裝置管理許可證後,必須啟用節點的裝置管理功能,才能將ISE用作TACACS+伺服器。為此,請編輯所用ISE部署節點的配置(可 以在Administrator > Deployment下找到),然後按一下其名稱或藉助Edit按鈕執行此操作。

	E Cisco ISE		Administration · System	4	, Evaluation Mode 82 Days 🔍 💮 💭 🏟
	Deployment Licensing	Certificates Logging	Maintenance Upgrade	Health Checks Backup & Restore	Admin Access Settings
L	Deployment < 열 > 꽃 Deployment 꽃 PAN Failover	Deployme Correction Co	ent Nodes ter Syncup Deregister e A Personas Administration, Monitor	Role(s) Services	Selected 0 Total 1 2 3 All V V Node Status

打開節點配置窗口後,請選中Policy Service部分下的Enable Device Admin Service選項,如下圖所示。

≡ Cisco ISE	Administration · System	🛕 Evaluation Mode 82 Days Q 🕜 🔎
Deployment Licensing Certifi	ates Logging Maintenance Upgrade Health Checks	Backup & Restore Admin Access Settings
Deployment C The Composition of	Deployment Nodes List > ise Edit Node General Settings Profiling Configuration Hostname ise FQDN ise.cisco.com IP Address 10.48.39.134 Node Type Identity Services Engine (ISE)	
	Administration Administration Role PRIMARY Other Monitoring Node	<u>~</u>
	 Dedicated MnT () Policy Service Enable Session Services () Include Node in Node Group None Enable Profiling Service () Enable Threat Centric NAC Service () > Enable SXP Service () Enable Device Admin Service () Enable Device Identity Service () 	 ✓ ①
	> pxGrid ()	Reset

步驟 3.建立TACACS設定檔,以傳回許可權。

<u>在 GUI 上:</u>

要具有管理員訪問許可權,adminuser需要具有15級的特權,它允許訪問exec提示符shell。另一方面,helpdeskuser不需要exec提示外殼 訪問,因此可以為它分配低於15的特權級別。為了將適當的許可權級別分配給使用者,可以使用授權配置檔案。這些可以從ISE GUI頁面Work Centers > Device Administration > Policy Elements的Results > TACACS Profiles頁籤下配置,如下圖所示。

≡ Cisco ISE		Work Centers - D	evice A	dministration		🛕 Evaluation Mode 82 Days 📿 ⊘ 🕫
Overview Identities	User Identity	y Groups Ext Id Sources	Netwo	ork Resources	Policy Elements	Device Admin Policy Sets More $ \smallsetminus $
Conditions Library Conditions Smart Conditions	~ TAC	ACS Profiles			Rows/Page	e 6 🗸 < < 1 / 1 > > Go 6 Total Rows
Network Conditions	> 2 4	dd Duplicate Trash ∽ Edit				Filter 🗸 🔘
Results	~ D N	lame	Туре	Description		
Allowed Protocols TACACS Command Sets		Pefault Shell Profile	Shell	Default Shell Profile		
TACACS Profiles		eny All Shell Profile	Shell	Deny All Shell Profile	e	
		OS Admin	Shell	Assigned to each us	ser in the group admin-grou	up
		DS Helpdesk	Shell	Assigned to each us	ser in the group helpdesk-g	group
	_ w	VLC ALL	WLC	WLC ALL		
	_ w	VLC MONITOR	WLC	WLC MONITOR		

要配置新的TACACS配置檔案,請使用Add按鈕,打開與圖中所示類似的新配置檔案配置表。此表單在配置分配給adminuser(即,具 有shell許可權級別15)的配置檔案時,必須特別像這樣。

≡ Cisco ISE 🛕 Evaluation Mode 82 Days Q 🕜 🔎 🕸 Work Centers · Device Administration Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets More \vee TACACS Profiles > IOS Admin Conditions TACACS Profile Network Conditions IOS Admin Results Allowed Protocols TACACS Command Sets Description TACACS Profiles Assigned to each user in the group admin-group Task Attribute View Raw View Common Tasks Common Task Type Shell ~ (Select 0 to 15) 15 Default Privilege Maximum Privilege 15 (Select 0 to 15) V Access Control List \sim Auto Command (Select true or false) No Escape Minutes (0-9999) Timeout Minutes (0-9999) Idle Time Custom Attributes Add Trash 🗸 🛛 Edit 103 🗌 Туре Name Value No data found. Cancel

對輪廓重複操作helpdesk。對於最後一個, Default Privilege和Maximum Privilege均設定為1。

步驟 4.在ISE上建立使用者組。

這與本文檔<u>配置RADIUS ISE</u>部分的步驟3中的說明相同。

步驟 5.在ISE上建立使用者。

這與本文檔<u>配置RADIUS ISE</u>部分的步驟4中的說明相同。

步驟 6.建立裝置管理策略集。

<u>在 GUI 上:</u>

對於RADIUS訪問,使用者建立後,仍需要在ISE上定義其身份驗證和授權策略以授予其正確的訪問許可權。TACACS身份驗證為此 ,使用裝置管理策略集,可從Work Centers > Device Administration > Device Admin Policy Sets GUI Page進行配置,如下所示。

≡ Cisco	SE	Work Cent	ters •	Device Administration				A Evaluation Mode 8	2 Days	Q (2)	\$ D
Overview	Identities User Identit	ty Groups Ext Id Sou	rces	Network Resources	Policy Elemen	its	Device Ad	min Policy Sets	More	~	
Policy Sets						1	Reset	Reset Policyset H	itcounts		Save
(+) Status	Policy Set Name	Description	Con	nditions		Allowe	d Protocols	/ Server Sequence	Hits	Actions	View
Q Search											
۲	WLC TACACS Authentication		₽	Network Access-Device IP Add EQUALS 10.48.39.133	ress	Defau	It Device A	dmin \times \vee +	0	\$ \$ }	>
ø	Default	Tacacs Default policy set				Defau	It Device A	dmin $\propto \sim +$	0	ŝ	>
									Reset		Save

若要建立裝置管理原則集,請使用上一個影像中以紅色框住的「新增」按鈕,這樣會將專案新增至原則集清單。為新建立的組提供一個名稱、必須應用該組的條件以及允許的協定/伺服器序列(此處,Default Device Admin為足夠)。使用Save按鈕完成增加策略集,並使用其右邊的箭頭來訪問其配置頁(如圖中所示)。

=	Cisco IS	SE		Work Centers · D	Device Administration		🛕 Evalu	ation Mode 82 Days	Q (
verv	iew lo	dentities User Identi	ty Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Poli	cy Sets More	~	
olic	y Sets→	WLC TACACS Authen	tication				Reset	Policyset Hitcounts		Save
:	Status P	Policy Set Name	Description	Conditi	ions		Allowe	d Protocols / Serve	r Seque	nce Hits
(λ Search									
	0	WLC TACACS Authentication			Network Access-Device IP Ad	dress EQUALS 10.48.39.1	33 Defau	It Device Admin		<u>_</u> + •
∨ Ai	uthenticatio	on Policy (1)								
Œ	Status	Rule Name	Condition	s			Use		Hits	Actions
	Q Search	h								
					+					
							All_User_ID_Stor	es 🙁 🗸		
	0	Default					> Options		0	礅
> Ai	uthorizatior	n Policy - Local Exceptions								
> Ai	uthorizatior	n Policy - Global Exceptions								
∨ Ai	uthorization	n Policy (3)								
					Results					
e	Status	Rule Name	Condition	S	Command S	Sets	Shell Profiles		Hits	Actions
	Q Search	h								
	۲	Helpdesk users authorization	n A Inter Ident	nalUser-IdentityGroup EQ tity Groups:helpdesk-grou	UALS User AllowAllCom	mmands \times \sim -	IOS Helpdesk	<u>∞</u> +	0	ŝ
	٢	Admin users authorization	A Inter	nalUser-IdentityGroup EQ tity Groups:admin-group	UALS User AllowAllCon	mmands \times \checkmark -	IOS Admin	∞ ~+	0	ţŷş

Reset Save

此示例中的特定策略集「WLC TACACS Authentication」過濾IP地址等於示例C9800 WLC IP地址的請求。

作為身份驗證策略,預設規則已保留,因為它滿足使用需要。已設定兩個授權規則:

• 當使用者屬於定義的群組admin-group時,會觸發第一個動作。它允許所有命令(透過預設Permit_all規則)並分配許可權 15(透過定義的IOS_Admin TACACS配置檔案)。

• 當使用者屬於定義的組helpdesk-group時,將觸發第二個。它允許所有命令(透過預設Permit_all 規則)並分配許可權1(透過 定義的IOS_HelpdeskTACACS配置檔案)。

疑難排解

如果您的RADIUS伺服器預期會傳送服務型別RADIUS屬性,您可以新增WLC:

radius-server attribute 6 on-for-login-auth

透過WLC CLI排除WLC GUI或CLI RADIUS/TACACS+訪問故障

要排除TACACS+對WLC GUI或CLI的訪問故障,請發出debug tacacs命令以及terminal monitor one,並在嘗試登入時檢視即時輸出。 例如,成功登入後註銷adminuser使用者,即可生成以下輸出。

<#root>

WLC-9800#

terminal monitor

WLC-9800#

debug tacacs

TACACS access control debugging is on WLC-9800# Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro

從這些記錄中可以看到,TACACS+伺服器傳回正確的許可權(即AV priv-lvl=15)。

執行RADIUS驗證時,會顯示類似的偵錯輸出,其中涉及RADIUS流量。

而命令debug aaa authentication和debug aaa authorization會顯示WLC在使用者嘗試登入時選擇的方法清單。

透過ISE GUI排除WLC GUI或CLI TACACS+訪問故障

在第Operations > TACACS > Live Logs頁中,可以檢視過去24小時內透過TACACS+進行的每個使用者身份驗證。要展開TACACS+授 權或身份驗證的詳細資訊,請使用與此事件相關的「詳細資訊」按鈕。

Cisco ISE			Ope	rations · TACACS		A Evaluation Mode 82 Day	/s Q @ 53	0
ve Logs								
ට් 🖞 Export To 🗸					Refresh Never	Show Latest 20 records	✓ Within Last 3 hours Filter ✓	0
Logged Time	Statue	Dataile	Identity	Tumo	A she she she she belles	Authorization Ballou		
Logged Time	Status	Details	identity	rype	Authentication Policy	Authorization Policy	Ise Node	
×	Status	×	Identity		Authentication Policy	Authorization Policy	Ise Node	
>> Dec 08, 2022 06:51:	46.1	~	Identity	Authorization	Authentication Policy	Authorization Policy Authorization Policy WLC TACACS Authentication >	Ise Node	
Cogged Time X Dec 08, 2022 06:51: Dec 08, 2022 06:51:	46.1 V		Identity Identity helpdeskuser	Authorization Authentication	Authentication Policy Authentication Policy WLC TACACS Authentication >	Authorization Policy Authorization Policy WLC TACACS Authentication >	Ise Node Ise Node ise	
Dec 08, 2022 06:51: Dec 08, 2022 06:51: Dec 08, 2022 06:51:	46.1 🗹		Identity Identity helpdeskuser helpdeskuser adminuser	Authorization Authorization Authorization	Authentication Policy Authentication Policy WLC TACACS Authentication >	Authorization Policy Authorization Policy WLC TACACS Authentication > WLC TACACS Authentication >	Ise Node Ise Node ise ise	
Dec 08, 2022 06:51: Dec 08, 2022 06:51: Dec 08, 2022 06:38: Dec 08, 2022 06:38:	46.1 2 46.0 2 38.2 2 38.1 2		Identity Identity helpdeskuser adminuser adminuser	Authorization Authorization Authorization Authorization	Authentication Policy Authentication Policy WLC TACACS Authentication > WLC TACACS Authentication >	Authorization Policy Authorization Policy WLC TACACS Authentication > WLC TACACS Authentication >	Ise Node Ise Node ise ise ise	
Logged Time Dec 08, 2022 06:51: Dec 08, 2022 06:51: Dec 08, 2022 06:38: Dec 08, 2022 06:38: Dec 08, 2022 06:38: Dec 08, 2022 06:38:	46.1 2 46.0 2 38.2 2 38.1 2 54.0 2		Identity Identity helpdeskuser adminuser adminuser adminuser	Authorization Authorization Authorization Authorization Authorization Authorization	Authentication Policy Authentication Policy WLC TACACS Authentication > WLC TACACS Authentication >	Authorization Policy Authorization Policy WLC TACACS Authentication > WLC TACACS Authentication > WLC TACACS Authentication >	Ise Node Ise Node ise ise ise ise ise	

展開時,helpdeskuser的身份驗證成功嘗試如下所示:

Cisco ISE

Overview	
Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Location Device Port	Location#All Locations tty5

Steps

13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Network Access.Device IP Address
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
13045	TACACS+ will use the password prompt from global TACACS+ configuration
13015	Returned TACACS+ Authentication Reply
13014	Received TACACS+ Authentication CONTINUE Request (
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - InternalUser.IdentityGroup
13015	Returned TACACS+ Authentication Reply

從這裡可以看出,使用者helpdeskuser已經在驗證原則WLC TACACS Authentication > Default的幫助下成功地透過驗證到網路裝置 WLC-9800。此外,授權配置檔案IOS Helpdesk已分配給此使用者,並授予許可權級別1。

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)。