9800 WLC上でのGUI用RADIUS & TACACS+の & CLI認証の設定

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>読み取り専用ユーザの制限</u>
<u>WLC用のRADIUS認証の設定</u>
RADIUS用のISEの設定
<u>TACACS+ WLCの設定</u>
<u>TACACS+ ISEの設定</u>
トラブルシュート
<u>WLC CLIを介したWLC GUIまたはCLI RADIUS/TACACS+アクセスのトラブルシューティング</u>
<u>ISE GUIを介したWLC GUIまたはCLITACACS+アクセスのトラブルシューティング</u>

はじめに

このドキュメントでは、RADIUSまたはTACACS+外部認証用にCatalyst 9800を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Catalyst Wireless 9800設定モデル
- AAA、RADIUS、およびTACACS+の概念

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• C9800-CL v17.9.2

• ISE 3.2.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

ユーザがWLCのCLIまたはGUIにアクセスしようとすると、ユーザ名とパスワードの入力を求めら れます。デフォルトでは、これらのクレデンシャルは、デバイス自体に存在するユーザのローカ ルデータベースと比較されます。または、入力クレデンシャルをリモートAAAサーバと比較する ようにWLCに指示することもできます。WLCは、RADIUSまたはTACACS+を使用してサーバと 通信できます。

設定

この例では、AAAサーバ(ISE)上の2種類のユーザ、それぞれadminuserとhelpdeskuserが設定されます。これら のユーザは、それぞれのadmin-groupとhelpdesk-groupのグループに属しています。 admin-groupの一部であるユーザadminuserには、 WLCへのフルアクセス権が付与される必要があります。一方、helpdeskuserはhelpdesk-groupの一部で、WLCに対するモニタ権限の みを付与します。したがって、設定にアクセスすることはできません。

この記事では、最初にRADIUS認証用にWLCとISEを設定し、後でTACACS+用に同じ設定を行います。

読み取り専用ユーザの制限

TACACS+またはRADIUSを9800 WebUI認証に使用する場合、次の制限があります。

• 特権レベル0のユーザが存在するが、GUIにアクセスできない

特権レベル1~14のユーザは、Monitorタブのみを表示できます(これは、ローカルで認証された読み取り専用ユーザの特権レベルに相当します)

特権レベル15のユーザはフルアクセスが可能

特権レベル15を持ち、特定のコマンドのみを許可するコマンドセットを持つユーザはサポートされません。ユーザは、引 き続きWebUIを使用して設定変更を実行できます

WLC用のRADIUS認証の設定

ステップ1:RADIUSサーバを宣言します。

<u>GUIから:</u>

まず、WLC上にISE RADIUSサーバを作成します。 これを行うには、https://<WLC-IP>/webui/#/aaaでアクセス可能なGUI WLCペー ジのタブServers/Groups > RADIUS > Serversを使用するか、Configuration > Security > AAA(WLC)に移動します(下図参照)。

Q. Search Menu Items	Configuration * > Security * > AAA
Dashboard Image: Configuration	AAA Wizard Servers / Groups AAA Method List AAA Advanced + Add × Delete
Administration →	RADIUS Servers Server Groups
C Licensing	TACACS+ Name Y Address Y Auth Port Y Acct Port Y
X Troubleshooting	LDAP ISE-lab 10.48.39.134 1812 1813
	For Radius Fallback to work, please make sure the Dead Criteria and Dead Time configuration exists on the device
Walk Me Through >	

WLCにRADIUSサーバを追加するには、図の赤いフレームで囲まれたAddボタンをクリックします。これにより、スクリーンショ ットに示されたポップアップウィンドウが開きます。

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 🔻)	
Real Configuration	PAC Key	0	CoA Server Key (i)]	
O Administration	Кеу Туре	Clear Text 🔻	Confirm CoA Server Key]	
C Licensing	Key* (i)		Automate Tester	0		т
X Troubleshooting	Confirm Key*					
	Auth Port	1812				
	Acct Port	1813				
Walk Me Through >	Server Timeout (seconds)	1-1000				
	Retry Count	0-100				
	Cancel				🖂 Annhute Device	
					Apply to Device	

このポップアップウィンドウでは、次の項目を指定する必要があります。

- サーバ名(ISEシステム名と一致する必要はありません)
- ・ サーバIPアドレス
- WLCとRADIUSサーバ間の共有秘密

認証やアカウンティングに使用されるポートなど、その他のパラメータも設定できますが、これらは必須ではなく、このドキュメ ントではデフォルトのままになっています。

CLIから:

<#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

ステップ2:RADIUSサーバをサーバグループにマッピングします。

<u>GUIから:</u>

認証に使用できる複数のRADIUSサーバがある場合は、すべてのサーバを同じサーバグループにマッピングすることを推奨します 。WLCは、サーバグループ内のサーバ間で異なる認証のロードバランシングを行います。RADIUSサーバグループは、図に示すよ うに、ステップ1で説明したものと同じGUIページのServers/Groups > RADIUS > Server Groupsタブで設定します。

Q Search Menu Items	Configuration * > Security	y~ > AAA			
🚃 Dashboard	+ AAA Wizard				
Monitoring >	Servers / Groups AAA	Method List AAA Advanced			
Configuration >	RADIUS				
O Administration	TACACS+	Server Groups			
C Licensing	1010	Name	Y Server 1	Server 2	Server 3
X Troubleshooting	LUAP	RADIUS-Group	ISE-lab	N/A	N/A 1 - 1 of 1 items
Walk Me Through >					

サーバの作成では、次に示すAddボタン(前の図でフレーム化されています)をクリックすると、ポップアップウィンドウが表示 されます。

٩	Search Menu Items	Config	uration * > Security * > AAA Create AAA Radius Server	Group		
		+ 4	Name*	RADIUS-Group		
C		Serve	Group Type	RADIUS		
Z,		->	MAC-Delimiter	none v		
Ś		> R4	MAC-Filtering	none 🗸		
C		TA	C Dead-Time (mins)	5		Server 3
×		LD	Load Balance	DISABLED		No items to display
8.6			Source Interface VLAN ID			
			Available Servers	Assigned Servers		
				ISE-lab in (in () (() (() (() (() (
			Cancel	[Apply to Device	

ポップアップでグループに名前を付け、目的のサーバを「割り当てられたサーバ」リストに移動します。

<u>CLIから:</u>

<#root>

-

WLC-9800(config)# aaa group server radius

RADIUS-Group

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

<u>ISE-lab</u>

ステップ3:RADIUSサーバグループをポイントするAAA認証ログインメソッドを作成します。

<u>GUIから:</u>

_

引き続きGUIページからhttps://<WLC-IP>/webui/#/aaa、AAA Method List > Authenticationタブに移動し、次の図に示すように認証方 式を作成します。

Q	Search Menu Items		Configuration * > Se	ecurity *	>	AAA													
	Dashboard		+ AAA Wizard Servers / Groups	AAA Me	etho	od List AA/	۹ Ac	dvanced											
3 3	Configuration	> >	Authentication		+	- Add		ete											
Q	Administration	>	Accounting			Name	Ŧ	Туре	Ŧ	Group Type	٣	Group1	Ŧ	Group2	Ŧ	Group3	Ŧ	Group4	Ŧ
C	Licensing				0	default		login		local		N/A		N/A		N/A		N/A	
×	Troubleshooting				0	radius-authe- method		login		local		RADIUS-Group		N/A		N/A		N/A	
					H	≤ 1 ≥	(H)	10 🔻										1 - 2 of 2	items
	Walk Me Through >																		

通常どおり、Addボタンを使用して認証方式を作成すると、次の図に示すような設定ポップアップウィンドウが表示されます。

Q Search Menu Items		Configuration * > Security * > AAA					
Dashboard		+ AAA Wizard Quick Setup: AAA Authenti	cation				
Monitoring	>	Method List Name*	radius-authe-m	ethod			
	>	Type*	login	• i			
	>	Group Type	local	•			
C Licensing		Available Server Groups		Assigned Server Groups		N/A	N/A
X Troubleshooting	l	radius Idap tacacs+	< > <	RADIUS-Group	× × V		
		Cancel			Apply to Device		

このポップアップウィンドウで、メソッドの名前を指定します。Type as log inを選択し、前の手順で作成したグループサーバを Assigned Server Groupsのリストに追加します。Group Typeフィールドについては、いくつかの設定が可能です。

- グループタイプとしてローカルを選択した場合、WLCは最初にユーザクレデンシャルがローカルに存在するかどうか をチェックし、次にサーバグループにフォールバックします。
- グループとしてGroup Typeを選択し、Fall back to localオプションをチェックしない場合、WLCではサーバグループに 対してユーザクレデンシャルがチェックされるだけです。
- グループとしてGroup Typeを選択し、Fallback to localオプションをチェックすると、WLCはサーバグループに対してユ ーザクレデンシャルをチェックし、サーバが応答しない場合にだけローカルデータベースに照会します。サーバがrejectを 送信すると、ローカルデータベースに存在できるユーザであっても、そのユーザは認証されます。

CLIから:

ユーザクレデンシャルが最初にローカルで見つからない場合にのみ、サーバグループでユーザクレデンシャルをチェックするには 、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

local group

RADIUS-Group

ユーザクレデンシャルをサーバグループでのみチェックする場合は、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

ユーザクレデンシャルをサーバグループでチェックし、この最後のエントリがローカルエントリで応答しない場合は、次のコマン ドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

local

この設定例では、ローカルでのみ作成されるユーザとISEサーバでのみ作成されるユーザが存在するため、最初のオプションを使用します。

ステップ4:RADIUSサーバグループをポイントするAAA認可EXEC方式を作成します。

<u>GUIから:</u>

アクセス権を付与するには、ユーザも承認されている必要があります。引き続きGUI Page Configuration > Security > AAAから、 AAA Method List > Authorizationタブに移動し、次の図に示すように認可方式を作成します。

Q. Search Menu Items	Configuration * > Security	• > A	AA												
🚃 Dashboard	+ AAA Wizard														
Monitoring >	Servers / Groups	Method	List AAA	A Adv	vanced										
Configuration	Authentication	+ /	Add × (te										
(○) Administration →	Authorization	N	ame 1	T	Туре	T	Group Type 🛛 🝸	Group1	Ŧ	Group2	Ŧ	Group3	r	Group4	Ŧ
C Licensing	Accounting	O de	efault	e	exec		local	N/A		N/A		N/A	r	N/A	
\$ <i>1</i> .		O m	idius-autho- iethod	e	exec		local	RADIUS-Group		N/A		N/A	1	N/A	
X Troubleshooting		14	< 1 ×	ы. ¹¹	10 🗸									1 - 2 of 2 item	ns
Walk Me Through 5															



Addボタンを使用して新しい認証方式を追加すると、図に示すような認証方式設定のポップアップが表示されます。

Q. Search Menu Items	Configuration * > Security * > AAA				
Dashboard	+ AAA Minord Quick Setup: AAA Authori	zation	×		
Monitoring →	Server Method List Name*	radius-autho-method			
Configuration	Aut Type*	exec 🔻			
O Administration	Aut Group Type	local 🔹		▼ Group3	Group4
C Licensing	Acc Authenticated			N/A	N/A
Troubleshooting	Available Server Groups radius Idap tacacs+	Assigned Server Groups > RADIUS-Group	× × ×		
Walk Me Through >	Cancel		Apply to Device		

この設定ポップアップで、許可方式の名前を指定し、タイプとしてexecを選択し、ステップ3で認証方式に使用したものと同じグ ループタイプの順序を使用します。

<u>CLIから:</u>

認証方式では、最初に認可が割り当てられ、ユーザがローカルエントリと照合され、次にサーバグループのエントリと照合されま す。

<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

local group

RADIUS-Group

ステップ5:HTTP設定およびTelnet/SSHに使用するVTY回線にメソッドを割り当てます。

<u>GUIから:</u>

作成された認証および許可方式は、HTTPまたはTelnet/SSHユーザ接続に使用できます。これは、次の図に示すように、AAA Advanced > AAA Interfaceタブから、まだhttps://<WLC-IP>/webui/#/aaaでアクセス可能なGUI WLCページから設定できます。

Q Search Menu Items	Configuration * > Secu	irity -> AAA			
🚃 Dashboard	+ AAA Wizard	A Method List	unned 1		
	> Servers / Groups A	AA Method List	vanced		
	Global Config				巴 Apply
O Administration	RADIUS Fallback		Authentication	Authorization	Accounting
C Licensing	Attribute List Name	Console	None 🔻 💈	None 🔻 💈	None 🔻 💈
	Device Authentication	VTY	radius-authe-method 🗸 💈	radius-autho-method 🗸 💈	None 🔻 💈
S Troubleshouting	AP Policy	HTTP	radius-authe-method 🗸	radius-autho-method 🗸 💈	None 👻 💈
	Password Policy				
Walk Me Through >	AAA Interface				
		_			

GUI認証用CLI:

<#root>

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

radius-authe-method

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

radius-autho-method

Telnet/SSH認証用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

HTTP設定を変更した場合は、HTTPおよびHTTPSサービスを再起動するのが最善の方法です。これは、次のコマンドを使用して実 行できます。

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

RADIUS用のISEの設定

ステップ1:WLCをRADIUS用のネットワークデバイスとして設定します。

<u>GUIから:</u>

前のセクションで使用したWLCをISEのRADIUSのネットワークデバイスとして宣言するには、次の図に示すように、 Administration > Network Ressources > Network Devicesに移動し、Network devicesタブを開きます。

■ Cisco ISE		Administration · N	letwork Resource	S	A Evaluation	Mode 82 Days Q ⑦ 등로 🕸
Network Devices Net	work Device Groups	Network Device Profile	es External RAD	IUS Servers RADIUS	Server Sequences	More ~
Network Devices	Network	Devices				
Device Security Settings						Selected 0 Total 1 🦪 🗔
	C Edit + Add	📋 Duplicate 🕁 Imp	oort 🏦 Export 🗸	👌 Generate PAC 🏾 🏮 Del	ete 🗸	\sim IIA
	Name	∧ IP/Mask	Profile Name	Location	Туре	Description
	WLC-980	10.48.39.133/32	🗯 Cisco (All Locations	All Device Types	

ネットワークデバイスを追加するには、[追加]ボタンを使用して、新しいネットワークデバイス設定フォームを開きます。

		Administration · Netw	ork Resources	🛕 Evalua	ation Mode 82 Days Q	0	50	٩
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 List	> New Network Device						
	Name	WLC-9800						
	Description							
	IP Addres	s ∨ ^{* IP :} 10.48.39.13	13 [/] 32 🖗					
	Device Profile	📸 Cisco	~ ()					
	Model Name		~					
	Software Versio	n	~					
	Network Device	Group						
	Location	All Locations	✓ Set To Defa	ault				
	IPSEC	Is IPSEC Device	✓ Set To Defa	ault				
	Device Type	All Device Types	Set To Defa	ault				
	Z V RADI	US Authentication Setting	S					
	RADIUS	UDP Settings						
	Protocol	RADIUS						
	Shared S	ecret	Show					
	Use S	econd Shared Secret 🕠 Second Shared Secret		Show				
	CoA Port	1700	Set To De	fault				
	RADIUS	DTLS Settings 🕕						
	DTLS	Required (i)						
	Shared S	ecret radius/dtls	©					

新しいウィンドウで、ネットワークデバイスの名前を入力し、そのIPアドレスを追加します。RADIUS Authentication Settingsを選 択し、WLCで使用されているものと同じRADIUS共有秘密を設定します。

ステップ2:特権を返す許可結果を作成します。

<u>GUIから:</u>

管理者のアクセス権を持つには、adminuserに特権レベル15が必要です。これにより、execプロンプトシェルにアクセスできます。 一方、helpdeskuserはexecプロンプトのシェルアクセスを必要としないため、15より低い特権レベルで割り当てることができます 。適切な特権レベルをユーザに割り当てるには、認可プロファイルを使用できます。これらは、次の図に示すタブのISE GUI Page Policy > Policy Elements > Resultsで設定Authorization > Authorization Profilesできます。

≡ Cisco ISE			Policy	Policy Elements	🔺 Evaluati	on Mode 82 Days Q ⑦ 등의 🐡
Dictionaries Con	nditions	Results				
Authentication Authorization Authorization Profiles Downloadable ACLs	>	Star For Policy	Adard Authori	Zation Profiles > System > Backup & Restore > Policy Exp	oort Page	Selected 0 Total 11 😅 🧔
Profiling	>		Name	Profile	∧ Description	
Posture	>		9800-admin-priv	🗰 Cisco 🕧		
Client Provisioning	>		9800-helpdesk-priv	🗰 Cisco 👔		
			Block_Wireless_Access	🗰 Cisco 🕦	Default profile used to	block wireless devices. Ensure ti
			Cisco_IP_Phones	🗯 Cisco 🕧	Default profile used fo	r Cisco Phones.
			Cisco_Temporal_Onboard	🚓 Cisco 👔	Onboard the device w	ith Cisco temporal agent
			Cisco_WebAuth	🗰 Cisco 🕕	Default Profile used to	redirect users to the CWA portal
			NSP_Onboard	🗰 Cisco 🕕	Onboard the device w	ith Native Supplicant Provisioning
			Non_Cisco_IP_Phones	🗰 Cisco 🕦	Default Profile used fo	r Non Cisco Phones.
			UDN	🗰 Cisco 🕕	Default profile used fo	r UDN.
			DenyAccess		Default Profile with ac	cess type as Access-Reject
		-				

新しい認可プロファイルを設定するには、新しい認可プロファイル設定フォームを開くAddボタンを使用します。adminuserに割り 当てられるプロファイルを設定するには、このフォームが特に次のように表示される必要があります。

=	Cieco	ISE
_	CISCU	1 JL

Policy · Policy Elements

Dictionaries Conditions	Results
Authentication >	Authorization Profiles > New Authorization Profile
Authorization \sim	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
	 Common Tasks Advanced Attributes Settings ii Cisco:cisco-av-pair v shell:priv-lvi=15 v = + Attributes Details Access Type = ACCESS_ACCEPT cisco-av-pair = shell:priv-Hr=15
	Submit Cancel

この設定では、関連付けられているすべてのユーザに特権レベル15が付与されます。すでに説明したように、これは次の手順で 作成されるadminuserの正常な動作です。ただし、helpdeskuserにはより低い特権レベルが必要なので、2番目のポリシー要素を作成 する必要があります。

helpdeskuserのポリシー要素は、文字列をshell:priv-lvl=Xに変更し、Xを目的の権限レベルに置き換える必shell:priv-lvl=15 要がある 点を除き、上で作成したようなものです。この例では、1 が使用されます。

ステップ3: ISEでユーザグループを作成します。

GUIで次の手順を実行します。

ISEユーザグループは、画面キャプチャに示されているAdministration > Identity Management > Groups GUI PageのタブUser Identity Groupsから作成されます。

≡ Cisco ISE	Administration · Identity Manag	gement	Levaluation Mode 82 Days Q	0 5	9
Identities Groups External Identity Source	es Identity Source Sequences	Settings			
Identity Groups User SQ < 12	Identity Groups		Selected 0 Total	10 📿 All ~	@ 7
	A helpdesk-group	This is the group containing all users with rea	ad-only privileges.		
	😤 admin-group	This is the group containing all users with adr	ministrator privileges.		
	Monthead and the second	Default OWN_ACCOUNTS (default) User Grou	qu		
	A GuestType_Weekly (default)	Identity group mirroring the guest type			
	Number 2 SocialLogin (default)	Identity group mirroring the guest type			
	Number 2018 Strategy (default)	Identity group mirroring the guest type			
	Main GuestType_Contractor (default)	Identity group mirroring the guest type			
	SROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Gr	roup		
	A Employee	Default Employee User Group			
	聲 ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group	2		

新しいユーザを作成するには、Addボタンを使用して、次に示すように新しいユーザIDグループ設定フォームを開きます。

≡ Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 82 Days Q 🕜 🕞 🏟
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings	
Identities Groups External Iden Identity Groups S □ Endpoint Identity Groups S □ User Identity Groups	ntity Sources Identity Source Sequences Settings User Identity Groups > New User Identity Group Identity Group * Name admin-group Description This is the group containing all users with administrator privileges. Submit	Cancel

作成するグループの名前を入力します。admin-groupとhelpdesk-groupの2つのユーザグループを作成します。

ステップ4:ISEでユーザを作成します。

<u>GUI で次の手順を実行します。</u>

ISEユーザは、画面キャプチャに示されているAdministration > Identity Management > Identities GUI PageのタブUsersから作成されます。

■ Cisco ISE		Administration · Identity Man	agement		A Evaluation Mode 8	12 Days Q () ,a	٩
Identities Groups	External Identity Sources	Identity Source Sequences	Settings					
Users Latest Manual Network Scan Res	Network A	Access Users						
	🖉 Edit 🕂 Add	🛞 Change Status 🗸 🕁 Import	1 Export 🗸 🔋 Delete	✓ Duplicate		Selected 0 Total	2 💭 All 🗸	© 7
	Status	Username \land Description	First Name Last Name	Email Address	Jser Identity Groups	Admin		
	🗌 🛛 🖉 Enabled	d 👤 adminuser			admin-group			
	🗌 🗧 Enabled	d 👤 helpdeskus		1	helpdesk-group			

新しいユーザを作成するには、[追加]ボタンを使用して、次に示すように新しいネットワークアクセスユーザ設定フォームを開き ます。

≡ Cisco ISE	Administration · Identity Management	🛕 Evaluation Mode 82 Days 📿 💮 声로 🕸
Identities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users List > New Network Access User	
	✓ Network Access User	
	* Username adminuser	
	Status Enabled ~	
	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 (i)
	Enable Password	Generate Password ()
	> User Information	
	> Account Options	
	> Account Disable Policy	
	✓ User Groups	
	🗄 _admin-group 🗸 💿 🕇	

ユーザのクレデンシャル(ユーザ名とパスワード)を入力します。これは、WLCでの認証に使用されます。また、ユーザのステ ータスがEnabledであることも確認します。最後に、手順4.で作成した関連グループにユーザを追加し、フォームの最後にUser Groupsドロップダウンメニューを表示します。

上記で説明した2人のユーザ、adminuserとhelpdeskuserを作成します。

ステップ5:ユーザを認証します。

<u>GUIから:</u>

このシナリオでは、すでに事前設定されているISEのデフォルトのポリシーセットの認証ポリシーにより、デフォルトのネットワ ークアクセスが許可されます。このポリシーセットは、次の図に示すように、ISE GUIページのPolicy > Policy Setsから確認できま す。したがって、これを変更する必要はありません。

≡ Cisco	ISE		Policy · Policy Sets		A Evaluation Mode 82 Days Q	0 ,9 ¢
Policy Sets	→ Default			Reset	Reset Policyset Hitcounts	Save
Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Se	quence Hits
Q Sear	ch					
0	Default	Default policy set			Default Network Access	⊠ ∽+ o
\vee Authentic	ation Policy (3)					
🕂 Stat	us Rule Name	Conditions		Use	н	lits Actions
Q Sea	ırch					
			MAB	Internal	Endpoints 🛛 🗸 🗸	
e	MAB	OR	OR		ns	• {Ç}
		Wind	002.1V	All_User	_ID_Stores 🛛 🗸 🗸	
٩	Dot1X	OR Wirele	OR Image: Wired_802.1X Image: Wireless_802.1X		ns	• දිරූදි
				All_User	ID_Stores	
٢	Default			> Optic	ns	• ক্ট্ৰ

手順6:ユーザを許可します。

<u>GUIから:</u>

ログイン試行が認証ポリシーを通過した後、認証ポリシーを承認する必要があり、ISEは以前に作成した認証プロファイル(permit accept、および特権レベル)を返す必要があります。

この例では、ログイン試行がデバイスのIPアドレス(WLCのIPアドレス)に基づいてフィルタリングされ、ユーザが属するグルー プに基づいて、付与される特権レベルが区別されます。この例では、各グループに1人のユーザしか含まれていないため、ユーザ 名に基づいてユーザをフィルタリングするという方法も有効です。

cy Sets-	→ Default				Reset Policyset H	Hitcounts
Status	Policy Set Name	Descripti	ion Conditions		Allowed Protocol	s / Server Sequence
Q Searc	ch					
٢	Default	Default	policy set		Default Network A	Access $\boxtimes \lor +$
uthentica	ation Policy (3)					
uthorizat	ion Policy - Local Exception	IS				
uthorizat	ion Policy - Global Exceptio	ns (2)				
				Results		
Stat	us Rule Name	Cond	litions	Profiles	Security Groups	Hits Acti
• Stat	us Rule Name	Cond	litions	Profiles	Security Groups	Hits Acti
	rch	Cond	Ititions Network Access-Device IP Address EQUALS 10.48.39.133	Profiles	Security Groups	Hits Acti
	rch 9800 Helpdesk Users	AND	Ititions Ititions Retwork Access-Device IP Address EQUALS 10.48.39.133 Retwork Access-Device IP EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	Profiles 9800-helpdesk-priv × × +	Security Groups	Hits Acti
Q Sea	verse	AND	Ititions Ititions Retwork Access-Device IP Address EQUALS 10.48.39.133 Request State EQUALS User Identity Groups:helpdesk-group Retwork Access-Device IP Address EQUALS 10.48.39.133	Profiles 9800-helpdesk-priv × · · ·	Select from list	Hits Acti

この手順が完了すると、adminuser およびhelpdeskユーザ用に設定されたクレデンシャルを使用して、GUIまたはTelnet/SSH経由でWLCで認証できます。

Reset

TACACS+ WLCの設定

ステップ1: TACACS+サーバを宣言します。

<u>GUIから:</u>

まず、WLC上にTACACS+サーバISEを作成します。 これは、Servers/Groups > TACACS+ > Serversでアクセス可能なGUIのWLCペ ージのタブからhttps://<WLC-IP>/webui/#/aaa、またはこの図に示すようにConfiguration > Security > AAAに移動して実行できます。

Cisco Cataly	/st 9800-CL Wireless Controlle	Welcome <i>admin</i>		iearch APs and Clients Q	2 🕩
Q. Search Menu Items Image: Dashboard Image: Only on the second	Configuration * > Security * > AAA + AAA Wizard Servers / Groups AAA Method Lis + Add × Delete RADIUS Servers	st AAA Advanced			
C Licensing	LDAP	Name ISE-lab	Server Address 10.48.39.134	Y Port Y 49 1 - 1 of 1 items	r
Walk Me Through >					

WLC上にTACACSサーバを追加するには、上の図の赤いフレームで囲まれたAddボタンをクリックします。図に示すポップアップ ウィンドウが開きます。

¢	Cisc	co Catal	vst 9800-CL	Wireless Controller					
	CISCO 17.9.2		,	W	/elcome admin st login 12/07/2022 14:14:33	🗣 🗛 🗎 🌣	🧐 🕜 🎜 🛛 Sear	rch APs and Clients Q	Feedback 🖉
٩	Search Menu Items		Configuration *	> Security -> AAA					
			+ AAA Wizard	Create AAA Tacacs Se	rver				
		>	Servers / Grou	Name*	ISE-lab				
2J		>	+ Add	Server Address*	10.48.39.134				
ŝ		>	RADIUS	Кеу Туре	Clear Text 🗸				
C			TACACS+	Key*				▼ Port	T
×			LDAP	Confirm Key*					No items to display
				Port	49				
				Server Timeout (seconds)	1-1000				
				Cancel			Apply to Device		

ポップアップウィンドウが開いたら、サーバ名(ISEシステム名と一致している必要はありません)、IPアドレス、共有キー、使 用しているポート、タイムアウトを入力します。

このポップアップウィンドウでは、次の項目を指定する必要があります。

٠

サーバ名(ISEシステム名と一致する必要はありません)

- ・ サーバIPアドレス
- WLCとTACACS+サーバ間の共有秘密

認証やアカウンティングに使用されるポートなど、その他のパラメータを設定できますが、これらは必須ではなく、このドキュメ ントではデフォルトのままにしておきます。

CLIから:

<#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

ステップ2: TACACS+サーバをサーバグループにマッピングします。

<u>GUIから:</u>

認証に使用できるTACACS+サーバが複数ある場合は、すべてのサーバを同じサーバグループにマッピングすることを推奨します。次に、WLCは、サーバグループ内のサーバ間で異なる認証のロードバランシングを行います。TACACS+サーバグループは、図に示されているステップ1で説明したGUIページと同じGUIページのServers/Groups > TACACS > Server Groupsタブで設定します。

Cisco Cisco Catalyst 9800-CL W	ireless Controller	Welcome admin Last login 12/07/2022 14:14:43	* * 4	B \$ (602	Search APs and Clients	Q	Feedback 2 ³⁴	•
Q. Search Menu Items Configuration * > Dashboard + AAA Wizard Monitoring Servers / Groups Configuration + Add Administration RADIUS	Security -> AAA AAA Method List > Delete Servers	AAA Advanced							
Licensing LDAP Troubleshooting		Name TACACS-Group 1 P P 10 V	Y Server 1 ISE-lab		Server 3	2	Server 3 N/A	1 - 1 of 1 items	
Walk Me Through >									

サーバの作成では、イメージに示されている前のイメージのフレームで囲まれたAddボタンをクリックすると、ポップアップウィンドウが表示されます。

F	ahaha	Cisco	Cata	vst 9800-CL Wireless Controller			
	CISCO	17.9.2		,	Welcome admin Last login 12/07/2022 14:14:43	B & @ 0 C	arch APs and Clients Q
٩	Search Menu I	tems		Configuration • > Security • > AAA			
				+ AAA Wizard			
3			>	Server Create AAA Tacacs Serve	er Group		×
Z,			>	Name*	TACACS-Group		
ঠ্য			>	RAI Group Type	TACACS	_	
C				TAC Available Servers	Assigned Servers		Server 3
×					<		No items to display
					«	Ľ	
(Cancel		Apply to De	evice

ポップアップでグループに名前を付け、目的のサーバをAssigned Serversリストに移動します。

CLIから:

<#root>

WLC-9800(config)#aaa group server tacacs+

TACACS-Group

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

ISE-lab

ステップ3: TACACS+サーバグループをポイントするAAA認証ログインメソッドを作成します。

GUIから:

引き続きGUIページからhttps://<WLC-IP>/webui/#/aaa、AAA Method List > Authenticationタブに移動し、図に示すように認証方式を 作成します。



通常どおり、Addボタンを使用して認証方式を作成すると、次の図に示すような設定ポップアップウィンドウが表示されます。

¢	alialia cisco	Cisco	Catal	yst 9800)-CL Wireless Controller											
		17.9.4				Welcome admin	n 🔗 🕈		a 🌣	1 10			d Clients Q		Feedback	* 🗭
٩	, Search Menu I	tems		Configur	ration • > Security • > AAA											
				+ A4	Quick Setup: AAA Authent	ication						×				
C			>	Server	Method List Name*	tacacs-authe-r	method									
			>	Aut	Type*	login	• (i)									
			>	Aut	Group Type Available Server Groups	local	Assigned Se	rver Groups	-				Group3	Ŧ	Groun4	Ţ
C					radius Idap	Þ	TACACS-Group			~			N/A		N/A	
×					tacacs+ RADIUS-Group	<				^ ~			N/A		N/A	
						«				Ľ					1 - 2 01 2 10	
					Cancel						Apply to [Device				

このポップアップウィンドウで、メソッドの名前を入力し、loginとしてTypeを選択し、前の手順で作成したグループサーバを Assigned Server Groupsリストに追加します。Group Typeフィールドについては、いくつかの設定が可能です。

• グループタイプとしてローカルを選択した場合、WLCは最初にユーザクレデンシャルがローカルに存在するかどうか をチェックし、次にサーバグループにフォールバックします。

• グループとしてGroup Typeを選択し、Fall back to localオプションをチェックしない場合、WLCではサーバグループに 対してユーザクレデンシャルがチェックされるだけです。

 グループとしてGroup Typeを選択し、Fallback to localオプションをチェックすると、WLCはサーバグループに対してユ ーザクレデンシャルをチェックし、サーバが応答しない場合にだけローカルデータベースに照会します。サーバがrejectを 送信すると、ローカルデータベースに存在できるユーザであっても、そのユーザは認証されます。

CLIから:

ユーザクレデンシャルが最初にローカルで見つからない場合にのみ、サーバグループでユーザクレデンシャルをチェックするには 、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

local group

TACACS-Group

ユーザクレデンシャルをサーバグループでのみチェックする場合は、次のコマンドを使用します。

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

ユーザクレデンシャルをサーバグループでチェックし、この最後のエントリがローカルエントリで応答しない場合は、次のコマン ドを使用します。 <#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

local

この設定例では、ローカルでのみ作成されるユーザとISEサーバでのみ作成されるユーザが存在するため、最初のオプションを使用します。

ステップ4:TACACS+サーバグループをポイントするAAA認可EXEC方式を作成します。

<u>GUIから:</u>

また、アクセス権を付与するには、ユーザが承認されている必要があります。 引き続きGUIページからConfiguration > Security > AAAを使用してAAA Method List > Authorizationタブに移動し、図に示すように認可方式を作成します。

CISCO Cisco Ca	atalyst 9800-CL Wireless C	ontroller	Welcome Last login 12/07/	admin 12022 14:14:43	ñ	A 7	B	* 3 0	ŝ	Search APs an	d Clier	nts Q	E Feedback	к ^я . (•)
Q Search Menu Items	Configuration - > Security	> AAA												
Dashboard	Servers / Groups AAA N	lethod List	AAA /	Advanced										
Configuration	> Authentication	+ Add	- X De	elete										
Administration	Authorization Accounting	Name		Туре	Ŧ	Group Type	Ŧ	Group1	Ŧ	Group2	T G	àroup3 Y	Group4	Ŧ
C Licensing		radius metho	autho-	exec		local		RADIUS-Group		N/A	N	1/A	N/A	
		metho	d 1 F F	exec		local		TACACS-Group	0	N/A	N	1/A	N/A 1 - 3 of 3 its	ems
Walk Me Through >														

Cisco Catalyst 9800-CL Wireless Controller **(** 🖌 🍖 🛕 🖺 🌣 👰 🕢 🎜 Search APs and Clients 🔍 🛛 🗷 Feedback 🦨 🗭 Welcome admin Configuration - > Security - > AAA Method List Name* tacacs-autho-method exec • (i) Type* local • (i) Group Type Authenticated Group3 Group4 T Available Server Groups Assigned Server Groups N/A N/A TACACS-Group radius N/A N/A > **^** Idap tacacs+ RADIUS-Group < ^ ~ > ¥ « Cancel

Addボタンを使用して新しい認証方式を追加すると、図に示すような認証方式設定のポップアップが表示されます。

この設定ポップアップで、認証方式の名前を指定し、execとしてTypeを選択し、前のステップで認証方式に使用したものと同じ Group Typeの順序を使用します。

CLIから:

<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

local group

TACACS-Group

ステップ5:HTTP設定およびTelnet/SSHに使用するVTY回線にメソッドを割り当てます。

<u>GUIから:</u>

作成された認証および許可方式は、HTTPおよび/またはTelnet/SSHユーザ接続に使用できます。これは、図に示すように、AAA Advanced > AAA Interfaceタブから、まだhttps://<WLC-IP>/webui/#/aaaでアクセス可能なGUI WLCページから設定できます。

Cisco Cataly	yst 9800-CL Wireless Controller	Welcome admin Last login 12/07/2022 14:14:43	A 7 A	B 🗘 🕅	Search APs	and Clients Q	Feedback 🖌
Q. Search Menu Items Image: Dashboard Image: Optimized Control of the second	Configuration • > Security • > AAA • AAA Wizard Servers / Groups AAA Method List	AAA Advanced					
Configuration > Image:	Global Config RADIUS Fallback Attribute List Name Console Device Authentication VTY AP Policy HTTP		Authentication None acacs-authe-method acacs-authe-method	• 2 5• 2	Authorization None Categories Categories None Categories Categorie	Accou	Apply inting
Walk Me Through 2	Password Policy AAA Interface						

CLIから:

GUI認証の場合:

<#root>

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

tacacs-authe-method

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

Telnet/SSH認証の場合

<#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

HTTP設定を変更した場合は、HTTPおよびHTTPSサービスを再起動するのが最善の方法です。これは、次のコマンドを使用して実 行できます。

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の設定 ステップ1:WLCをTACACS+のネットワークデバイスとして設定します。

<u>GUIから:</u>

前のセクションで使用したWLCをISEのRADIUSのネットワークデバイスとして宣言するには、次の図に示すように Administration > Network Resources > Network Devicesに移動し、Network devicesタブを開きます。



この例では、RADIUS認証用にWLCがすでに追加されています(「<u>RADIUS ISEの設定</u>」セクションのステップ1を参照)。したがって、TACACS認証を設定するために設定を変更するだけで済みます。この操作は、ネットワークデバイスリストでWLCを選択してEditボタンをクリックすることで実行できます。これにより、次の図に示すネットワークデバイス設定フォームが開きます。

≡ Cisco ISE	Administration · Network Resources	🛕 Evaluation Mode 82 Days Q 🕜 🕫 🕸
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers	s RADIUS Server Sequences More \vee
Network Devices	General Settings	
Default Device	Enable KeyWrap 🕦	
Device Security Settings	Key Encryption Key Shi	ow
	Message Authenticator Code Key	ow
	Key Input Format ● ASCII ◯ HEXADECIMAL	
	✓ TACACS Authentication Settings	
	Shared Secret Show	
	Enable Single Connect Mode	
	 Legacy Cisco Device 	
	O TACACS Draft Compliance Single Connect Support	
	SNMP Settings	
	□ ∨ Advanced TrustSec Settings	
	 TACACS Draft Compliance Single Connect Support SNMP Settings Advanced TrustSec Settings 	

新しいウィンドウが開いたら、TACACS Authentication Settingsセクションまでスクロールダウンして、これらの設定を有効にし、 <u>TACACS+ WLCの設定</u>セクションのステップ1で入力した共有秘密を追加します。

ステップ2:ノードのデバイス管理機能を有効にします。



注:ISEをTACACS+サーバとして使用するには、デバイス管理ライセンスパッケージと、BaseまたはMobilityライセンスのいずれかが必要です。

<u>GUIから:</u>

デバイス管理ライセンスをインストールしたら、ISEをTACACS+サーバとして使用できるようにするために、ノードのデバイス管 理機能を有効にする必要があります。そのためには、使用するISE導入ノードの設定を編集します。このノードはAdministrator > Deploymentの下にあり、名前をクリックするか、Editボタンを使用して編集します。

■ Cisco ISE	Administration · System)ays Q 🕜 न्व 🕸
Deployment Licensing Certi	ficates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Settings
Deployment < 🕲 🗇 > 🕸 Deployment > PAN Failover	Deployment Nodes Edit e Register	ncted 0 Total 1 💭 🍪 All ∨ 🏹 Node Status

ノード設定ウィンドウが開いたら、次の図に示すように、Policy Serviceセクションの下にあるEnable Device Admin Serviceオプショ ンにチェックマークを付けます。

≡ Cisco ISE	Administration · System	🛕 Evaluation Mode 82 Days Q 🕜 🔎
Deployment Licensing Certifi	ates Logging Maintenance Upgrade Health Checks	Backup & Restore Admin Access Settings
Deployment Image: Second system Image: Second system Image: Second system Image: Second system	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)	
	Role STANDALONE Administration Monitoring Role PRIMARY Other Monitoring Node	~
	 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 Passive Identity Service () 	~ 0
	> pxtirid (j)	Reset Save

ステップ3:特権を返すためのTACACSプロファイルの作成。

<u>GUIから:</u>

管理者のアクセス権を持つには、adminuserに特権レベル15が必要です。これにより、execプロンプトシェルにアクセスできます。 一方、helpdeskuserはexecプロンプトのシェルアクセスを必要としないため、15より低い特権レベルで割り当てることができます 。適切な特権レベルをユーザに割り当てるには、認可プロファイルを使用できます。これらは、次の図に示すように、ISE GUIペ ージWork Centers > Device Administration > Policy ElementsのタブResults > TACACS Profilesで設定できます。

≡ Cisco ISE			Work Centers · D	Device A	dministration		🛕 Evaluation Mode 82 Days 📿 ⊘ 🕞 🕸
Overview Identities	User I	dentity Groups	Ext Id Sources	Netwo	ork Resources	Policy Elements	Device Admin Policy Sets More \vee
Conditions Library Conditions Smart Conditions	~ 1	FACACS F	Profiles			Rows/Pag	e <u>6</u> → < < <u>1</u> / 1 > > <u>Go</u> 6 Total Rows
Network Conditions	> 6	Add Duplicat	te Trash 🗸 Edit				Filter 🗸 🕲
Results	~	Name		Туре	Description		
Allowed Protocols TACACS Command Sets		Default Shell Pro	ofile	Shell	Default Shell Profile		
TACACS Profiles		Deny All Shell Pr	rofile	Shell	Deny All Shell Profil	e	
		IOS Admin		Shell	Assigned to each us	ser in the group admin-grou	up
		IOS Helpdesk		Shell	Assigned to each us	ser in the group helpdesk-g	roup
		WLC ALL		WLC	WLC ALL		
		WLC MONITOR		WLC	WLC MONITOR		

新しいTACACSプロファイルを設定するには、Addボタンを使用して、図に示すような新しいプロファイル設定フォームを開きま す。adminuserに割り当てられるプロファイル(つまり、シェル権限レベル15)を設定するには、このフォームが特に次のように表示 される必要があります。

■ Cisco ISE		Work Centers ·	Device Administration		🛕 Evaluation Mode	82 Days Q	0	9
Overview Identities	User Identity Gr	oups Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More \vee		
onditions	> TACACS Profile TACACS P	s > IOS Admin rofile						
etwork Conditions	> Nama		-					
esults	V IOS Admin							
Allowed Protocols								
TACACS Profiles	Description Assigned to admin-grou	each user in the group p]					
	Task Attribut	e View Raw View	<u></u>					
	Common 1	asks						
	Common Tas	k Type Shell 🗸 🗸						
		Default Privilege	15	✓ (Select 0 t)	o 15)			
		Maximum Privilege	15	✓ (Select 0 t)	o 15)			
		Access Control List		~				
		Auto Command		~				
		No Escape		✓ (Select true)	le or false)			
		Timeout		V Minutes (0	-9999)			
		Idle Time		V Minutes (0	-9999)			
	Custom At	tributes						
	Add Track	Edit					~	
	Add Trash	C EUR					¢.	
	_ Туре	Name	Value					
	No data found.							

helpdeskプロファイルに対して操作を繰り返します。最後に、デフォルト権限と最大権限はどちらも1に設定されます。

ステップ4: ISEでユーザグループを作成します。

これは、このドキュメントの「<u>RADIUS ISEの設定</u>」セクションのステップ3で示したものと同じです。

ステップ5: ISEでユーザを作成します。

これは、このドキュメントの「<u>RADIUS ISEの設定</u>」セクションのステップ4で示したものと同じです。

手順6:デバイス管理ポリシーセットを作成します。

<u>GUIから:</u>

RADIUSアクセスに関しては、ユーザが作成された後も、適切なアクセス権を付与するために認証ポリシーと認可ポリシーを ISEで定義する必要があります。TACACS認証は、次に示すようにWork Centers > Device Administration > Device Admin Policy Sets GUI Pageから設定できる、終端に対するデバイス管理ポリシーセットを使用します。

≡ Cisco ISE	Work Centers · Device Administration	🛕 Evaluation Mode 82 Days Q 🕜 🕫 🤤
Overview Identities User Identity Groups	Ext Id Sources Network Resources Polic	y Elements Device Admin Policy Sets More ~
Policy Sets		Reset Policyset Hitcounts Save
(+) Status Policy Set Name Description	on Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
WLC TACACS Authentication	P Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin $ \lor \lor + 0$
Oefault Tacacs Def	ault policy set	Default Device Admin
		Reset Save

デバイス管理ポリシーセットを作成するには、上の図の赤い枠で囲まれた追加ボタンを使用します。これにより、ポリシーセット リストに項目が追加されます。新しく作成したセットの名前、適用する必要がある条件、およびAllowed Protocols/Server Sequence(ここではDefault Device Adminで十分)を入力します。ポリシーセットの追加を完了するには、Saveボタンを使用します。 また、右側の矢印を使用して、図に示すように設定ページにアクセスします。

	5C		Work Centers · Dev	vice Administration			A Contraction in	ode 82 Days	QC	0-0
erview l	dentities User Identi	ty Groups	Ext Id Sources	Network Resources	Policy Element	ts Device	Admin Policy Set	s More	~	
olicy Sets→	WLC TACACS Auther	ntication				Reset	Reset Policys	set Hitcounts		Save
Status P	Policy Set Name	Description	Condition	IS			Allowed Proto	ocols / Server	Seque	nce Hits
Q Search										
0	WLC TACACS Authentication		R Ne	etwork Access-Device IP Add	ress EQUALS 10.48.	39.133	Default Devi	ce Admin	⊗ ∖	<u> </u>
 Authentication 	on Policy (1)									
🕂 Status	Rule Name	Condition	s			Use			Hits	Actions
Q Search	h									
				+						
						AII_U	ser_ID_Stores	∞ ∨		
٢	Default					> Ob	otions		0	ŝ
Authorization	Default n Policy - Local Exceptions					> Ot	otions		0	ŝ
 Authorization Authorization 	Default n Policy - Local Exceptions n Policy - Global Exceptions					> Or	otions		0	ŝ
Authorization Authorization Authorization Authorization	Default n Policy - Local Exceptions n Policy - Global Exceptions n Policy (3)					> Op	tions		0	ŝ
Authorization Authorization Authorization Authorization	Default n Policy - Local Exceptions n Policy - Global Exceptions n Policy (3)	,		Results		> Ot	tions		0	\$\$
Authorization Authorization Authorization Authorization Status	Default n Policy - Local Exceptions n Policy - Global Exceptions n Policy (3)	Condition	s	Results Command Se	ts	> Or Shell P	rofiles		O	¢> Actions
Authorization Authorization Authorization Authorization (Status Q Search	Default n Policy - Local Exceptions n Policy - Global Exceptions n Policy (3) Rule Name	Condition	s	Results Command Se	ts	> Op Shell P	rofiles		0 Hits	۵۵۲ Actions
Authorization Authorization Authorization Authorization Status Q Search	Default Defaul	Condition	s nalUser-IdentityGroup EQUAI	LS User AllowAllCom	rts mands ×	> Op Shell P	rofiles	∞ ~+	0 Hits	ش Actions
 Authorization Authorization Authorization Status Q Search Q Search Q Search 	Default Defaul	Condition	s nalUser-IdentityGroup EQUAL ity Groups:helpdesk-group nalUser-IdentityGroup EQUAL ity Groups:admin-group	LS User AllowAllCom	nts mands × mands ×	> Op Shell P > + IOS F > + IOS A	rofiles telpdesk kdmin	<u>∞</u> ~+ ∞ ~+	0 Hits 0	۵ Actions ۵ ۵ ۵ ۵ ۵ ۵ ۵ ۵ ۵ ۵ ۵ ۵ ۵

Reset Save

この例の特定のポリシーセット「WLC TACACS Authentication」では、例のC9800 WLCのIPアドレスと同じIPアドレスを持つ要求 をフィルタリングします。

認証ポリシーとして、ユーザのニーズを満たすため、デフォルトルールが残されています。次の2つの認可ルールが設定されてい ます。

最初のトリガーは、ユーザが定義されたグループadmin-groupに属している場合にトリガーされます。すべてのコマンドを(デフォルトPermit_allルールを使用して)許可し、特権15を(定義されたIOS_Admin TACACSプロファイルを使用して)割り当てます。

• 2番目のトリガーは、ユーザが定義されたグループhelpdesk-groupに属している場合にトリガーされます。 すべてのコ マンドを(デフォルトPermit_all ルールを介して)許可し、特権1を(定義されたIOS_Helpdesk TACACSプロファイルを介して)割り当てます。 この手順が完了すると、adminuserおよびhelpdeskユーザ用に設定されたクレデンシャルを使用して、GUI経由またはTelnet/SSHを 通じてWLCで認証できます。

トラブルシュート

RADIUSサーバでservice-type RADIUSアトリビュートの送信が想定されている場合は、WLCで次のコマンドを追加できます (WLCのIPアドレスを使用)。

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

WLC CLIを介したWLC GUIまたはCLI RADIUS/TACACS+アクセスのトラブルシューティング

WLCのGUIまたはCLIへのTACACS+アクセスをトラブルシューティングするには、terminal monitor 1に加えてdebug tacacsコマンド を発行し、ログインの試行時のライブ出力を確認します。

たとえば、ログインに成功した後にadminuserユーザからログアウトすると、この出力が生成されます。

<#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 これらのログから、TACACS+サーバが正しい特権(AV priv-lvl=15)を返していることがわかります。

RADIUS認証を実行すると、RADIUSトラフィックに関する同様のデバッグ出力が表示されます。

debug aaa authenticationコマンドおよびdebug aaa authorizationコマンドは、代わりに、ユーザがログインしようとするときにWLCが 選択する方式リストを表示します。

ISE GUIを介したWLC GUIまたはCLI TACACS+アクセスのトラブルシューティング

ページOperations > TACACS > Live Logsから、過去24時間までにTACACS+で行われたすべてのユーザ認証を表示できます。 TACACS+認可または認証の詳細を展開するには、このイベントに関連するDetailsボタンを使用します。

E Cisco ISE			Ope	rations · TACACS		A Evaluation Mode 82 Da	ys Q @ 55) ()
ve Logs								
ට් 🗘 Export To 🗸					Refresh Never	Show V Latest 20 records	Vithin Last 3 hours	~ @
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	N
×		~	Identity	~~	Authentication Policy	Authorization Policy	lse Node	N
Dec 08, 2022 06:51:46.1	2	à	helpdeskuser	Authorization		WLC TACACS Authentication >	ise	w
Dec 08, 2022 06:51:46.0		à	helpdeskuser	Authentication	WLC TACACS Authentication >		ise	w
Dec 08, 2022 06:38:38.2	2	à	adminuser	Authorization		WLC TACACS Authentication >	ise	w
Dec 08, 2022 06:38:38.1		à	adminuser	Authentication	WLC TACACS Authentication >		ise	w
Dec 08, 2022 06:34:54.0	~	à	adminuser	Authorization		WLC TACACS Authentication >	ise	w
Dec 08, 2022 06:34:53.9		ò	adminuser	Authentication	WLC TACACS Authentication >		ise	w
ast Updated: Thu Dec 08 202	22 12:57:09	GMT+0100 (C	entral European	Standard Time)			Records Sho	wn: 6

展開すると、helpdeskuserの認証の試行が成功した場合は次のようになります。

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
Network Device Groups Device Type	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types
Network Device Groups Device Type Location	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types Location#All Locations
Network Device Groups Device Type Location Device Port	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types 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

この出力から、認証ポリシーWLC TACACS Authentication > Defaultを使用してユーザhelpdeskuserがネットワークデバイスWLC-9800に対して正常に認証されたことがわかります。さらに、許可プロファイルIOS Helpdeskがこのユーザに割り当てられ、特権レ ベル1が付与されています。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。