Configuration de RADIUS & TACACS+ pour l'authentification CLI de & GUI sur les WLC 9800

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Restrictions utilisateur en lecture seule
Configurer l'authentification RADIUS pour le WLC
Configurer ISE pour RADIUS
Configuration du WLC TACACS+
Configuration de TACACS+ ISE
<u>Dépannage</u>
Dépannage de l'interface graphique WLC ou de l'accès CLI RADIUS/TACACS+ via l'interface CLI WLC
Dépannage de l'interface graphique WLC ou de l'accès CLITACACS+ via l'interface ISE

Introduction

Ce document décrit comment configurer un Catalyst 9800 pour l'authentification externe RADIUS ou TACACS+.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- Concepts AAA, RADIUS et TACACS+

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• C980-CL v17.9.2

• ISE 3.2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lorsqu'un utilisateur tente d'accéder à l'interface de ligne de commande ou à l'interface graphique du WLC, il est invité à entrer un nom d'utilisateur et un mot de passe. Par défaut, ces informations d'identification sont comparées à la base de données locale des utilisateurs, qui est présente sur le périphérique lui-même. Alternativement, le WLC peut être instruit afin de comparer les informations d'identification d'entrée avec un serveur AAA distant : le WLC peut soit parler au serveur avec l'utilisation de RADIUS ou TACACS+.

Configurer

Dans cet exemple, deux types d'utilisateurs sur le serveur AAA (ISE), respectivement le adminuser, et le helpdeskuser sont configurés. Ces utilisateurs font respectivement partie des admin-group et deshelpdesk-group groupes. L'utilisateur adminuser, qui fait partie de la admin-group, doit se voir accorder un accès complet au WLC. D'un autre côté, le helpdeskuser, qui fait partie de la helpdesk-group, est destiné à n'être accordé que des privilèges de surveillance au WLC. Il n'y a donc pas d'accès à la configuration.

Cet article commence par configurer le WLC et ISE pour l'authentification RADIUS, puis il effectue la même opération pour TACACS+.

Restrictions utilisateur en lecture seule

Lorsque TACACS+ ou RADIUS est utilisé pour l'authentification WebUI 9800, les restrictions suivantes existent :

- Les utilisateurs disposant du niveau de privilège 0 existent mais n'ont pas accès à l'interface utilisateur graphique
- •

Les utilisateurs ayant des niveaux de privilège de 1 à 14 peuvent uniquement afficher l'onglet Monitor (équivalent au niveau de privilège d'un utilisateur authentifié localement en lecture seule)

Les utilisateurs disposant du niveau de privilège 15 ont un accès complet

.

Les utilisateurs disposant de privilèges de niveau 15 et d'un jeu de commandes autorisant uniquement des commandes spécifiques ne sont pas pris en charge. L'utilisateur peut toujours exécuter des modifications de configuration via l'interface utilisateur Web

Ces considérations ne peuvent pas être modifiées.

Configurer l'authentification RADIUS pour le WLC

Étape 1. Déclarez le serveur RADIUS.

À partir de la GUI :

Tout d'abord, créez le serveur RADIUS ISE sur le WLC. Cela peut être fait à partir de l'onglet Servers/Groups > RADIUS > Servers de la page GUI WLC accessible dans <u>https://<WLC-IP>/webui/#/aaa.</u> ou si vous naviguez vers Configuration > Security > AAA, comme le montre cette image.

Q Search Menu Items	Configuration * > Security * > A4	A			
Dashboard Monitoring Configuration	+ AAA Wizard Servers / Groups AAA Method I + Add × Delete	List AAA Advanced			
Administration	RADIUS	s Server Groups			
© Licensing	TACACS+	Name T	Address T	Auth Port	Acct Port
💥 Troubleshooting	LDAP	ISE-lab	10.48.39.134	1812	1813 1 - 1 of 1 items
	For Ra	idius Fallback to work, please make su	re the Dead Criteria and Dead Time	configuration exists on the device	
Walk Me Through >					

Pour ajouter un serveur RADIUS sur le WLC, cliquez sur le bouton Ajouter encadré en rouge dans l'image. La fenêtre contextuelle illustrée dans la capture d'écran s'ouvre.

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 💌	
Nonfiguration	PAC Key	0	CoA Server Key (i)		_
O Administration	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			
	Cancel			Apply to Device	

Dans cette fenêtre contextuelle, vous devez fournir :

- Le nom du serveur (notez qu'il ne doit pas nécessairement correspondre au nom du système ISE)
- Adresse IP du serveur
- Le secret partagé entre le WLC et le serveur RADIUS

D'autres paramètres peuvent être configurés, tels que les ports utilisés pour l'authentification et la gestion des comptes, mais ils ne sont pas obligatoires et sont conservés par défaut pour cette documentation.

À partir de CLI :

<#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

À partir de la GUI :

Si vous disposez de plusieurs serveurs RADIUS pouvant être utilisés pour l'authentification, il est recommandé de mapper tous ces serveurs au même groupe de serveurs. Le WLC s'occupe de l'équilibrage de charge des différentes authentifications parmi les serveurs dans le groupe de serveurs. Les groupes de serveurs RADIUS sont configurés à partir de l'ongletServers/Groups > RADIUS > Server Groups de la même page GUI que celle mentionnée à l'étape 1., comme illustré dans l'image.

Q Search Menu Items	Configuration * > Security	- > AAA			
Dashboard	+ AAA Wizard Servers / Groups AAA I + Add × Delete	Method List AAA Advanced			
Configuration >	RADIUS TACACS+	Servers Server Groups	▼ Server 1	Server 2	Server 3
Troubleshooting	LDAP	RADIUS-Group	ISE-lab	N/A	N/A 1 - 1 of 1 items
Walk Me Through >					

En ce qui concerne la création du serveur, une fenêtre contextuelle apparaît lorsque vous cliquez sur le bouton Ajouter (encadré dans l'image précédente), qui est représenté ici.

Q Search Menu Items	Configu	uration * > Security * > AAA Create AAA Radius Server (Group	×	
Dashboard	+ A4 Server	Name*	RADIUS-Group		
Monitoring	> Genter	Group Type	RADIUS		
	·	MAC-Delimiter	none 🔻		
O Administration	RAI	MAC-Filtering	none		
C Licensing	TAC	Dead-Time (mins)	5		Server 3
	LD/	Load Balance	DISABLED		No items to display
M Houbleshooting		Source Interface VLAN ID	1 🔹		
		Available Servers	Assigned Servers		
			ISE-lab	Ā	
Walk Me Through >			< »	▲▲	
			«	Ξ	
		Cancel		Apply to Device	

Dans la fenêtre contextuelle, attribuez un nom au groupe et déplacez les serveurs souhaités vers la liste Serveurs affectés.

À partir de CLI :

.

<#root>

WLC-9800(config)# aaa group server radius

.

RADIUS-Group

.

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

.

<u>ISE-lab</u>

.

. _

Étape 3. Créez une méthode de connexion d'authentification AAA qui pointe vers le groupe de serveurs RADIUS.

À partir de la GUI :

Toujours à partir de la page GUIhttps://<WLC-IP>/webui/#/aaa, accédez à l'ongletAAA Method List > Authentication et créez une méthode d'authentification comme illustré dans cette image.



Comme d'habitude, lorsque vous utilisez le bouton Ajouter pour créer une méthode d'authentification, une fenêtre contextuelle de configuration s'affiche, semblable à celle illustrée dans cette image.

Q Search Menu Items	Configuration *	> Security * > AAA					
🚃 Dashboard	+ AAA Wizard	Setup: AAA Authentic	cation		×	l	
Monitoring	Aut	d List Name*	radius-authe-m	nethod			
Configuration	Type*		login	• i			
(O) Administration	Group	Туре	local	•		Group3	Group4
C Licensing	Availab	le Server Groups		Assigned Server Groups		N/A	N/A
X Troubleshooting	radius Idap tacac:	5+	> <	RADIUS-Group	× × ×		
Walk Me Through >	ා Car	ncel			Apply to Device		

Dans cette fenêtre contextuelle, attribuez un nom à la méthode. Choisissez Type comme connexion et ajoutez le serveur de groupe créé à l'étape précédente à la Assigned Server Groups liste. En ce qui concerne le champ Type de groupe, plusieurs configurations sont possibles.

• Si vous choisissez Group Type comme local, le WLC vérifie d'abord si les informations d'identification de l'utilisateur existent localement, puis revient au groupe de serveurs.

• Si vous choisissez Group Type comme groupe et ne cochez pas l'option Fall back to local, le WLC vérifie simplement les informations d'identification de l'utilisateur par rapport au groupe de serveurs.

• Si vous choisissez Group Type comme groupe et cochez l'option Fallback to local, le WLC vérifie les informations d'identification de l'utilisateur par rapport au groupe de serveurs et interroge la base de données locale uniquement si le serveur ne répond pas. Si le serveur envoie un refus, l'utilisateur doit être authentifié, même s'il peut exister dans la base de données locale.

À partir de CLI :

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs uniquement si elles ne sont pas trouvées localement en premier, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

local group

RADIUS-Group

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées uniquement avec un groupe de serveurs, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

RADIUS-Group

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs et si ce dernier ne répond pas par une entrée locale, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

local

Dans cet exemple de configuration, certains utilisateurs sont uniquement créés localement et d'autres uniquement sur le serveur ISE. Par conséquent, utilisez la première option.

Étape 4. Créez une méthode d'exécution d'autorisation AAA qui pointe vers le groupe de serveurs RADIUS.

À partir de la GUI :

L'utilisateur doit également être autorisé pour se voir accorder l'accès. Toujours à partir de la GUI Page Configuration > Security > AAA, accédez à l'onglet, AAA Method List > Authorization et créez une méthode d'autorisation comme illustré dans cette image.

Q Search Menu Items	Configuration * > Security *	> AAA									
Dashboard	+ AAA Wizard Servers / Groups AAA M	ethod List AAA	Advanced								
Monitoring Monitoring Configuration	Authentication		alata								
(O) Administration	Authorization	Name T	Туре	Y Group Type	▼ Group1	▼ Group	o2 T	Group3	Ŧ	Group4	Ŧ
C Licensing		 default radius-autho- method 	exec	local	N/A RADIUS-Grou	p N/A		N/A N/A		N/A N/A	
<i>6</i> 76		H H I > >	10 🔻							1 - 2 of 2 it	ems
Walk Me Through 3											

Création de méthode d'autorisation

Une fenêtre contextuelle de configuration de méthode d'autorisation similaire à celle illustrée s'affiche lorsque vous en ajoutez une nouvelle à l'aide du bouton Ajouter.

Q. Search Menu Items	Configuration * > Security * > AAA	
Dashboard	Quick Setup: AAA Authorization	×
Monitoring >	Server Method List Name* radius-autho-method	
	Aut Type*	
(Ô) Administration →	Aut Group Type	Y Group3 Y Group4 Y
C Licensing	Act Authenticated	N/A N/A
Y Troubleshooting	Available Server Groups Assigned Server Groups	1 - 1 of 1 items
Walk Me Through >		pply to Device

Dans cette fenêtre contextuelle de configuration, attribuez un nom à la méthode d'autorisation, sélectionnez le type exec, puis utilisez le même ordre de type de groupe que celui utilisé pour la méthode d'authentification à l'étape 3.

À partir de CLI :

En ce qui concerne la méthode d'authentification, l'autorisation est d'abord attribuée pour vérifier les utilisateurs par rapport aux entrées locales, puis par rapport aux entrées d'un groupe de serveurs.

WLC-9800(config)#aaa authorization exec

radius-autho-method

local group

RADIUS-Group

Étape 5. Attribuez les méthodes aux configurations HTTP et aux lignes VTY utilisées pour Telnet/SSH.

À partir de la GUI :

Les méthodes d'authentification et d'autorisation créées peuvent être utilisées pour la connexion utilisateur HTTP et/ou Telnet/SSH, qui est configurable à partir de l'onglet AAA Advanced > AAA Interface, toujours à partir de la page WLC de l'interface utilisateur graphique accessible dans https://<WLC-IP>/webui/#/aaa, comme illustré dans cette image :

Q Search Menu Items		Configuration * > Secu	irity * > AAA						
Dashboard		+ AAA Wizard Servers / Groups A	AA Method List	AAA Advanced					
	>								
Configuration	>	Global Config							Apply
O Administration	>	RADIUS Fallback			Authentication		Authorization	Accounting	
C Licensing		Attribute List Name	Console		None 🔻		None 🔻	None] 🛛
Ye Troubleshooting		Device Authentication	VTY		radius-authe-method v] 🗖	radius-autho-method 🗸	None] 🛛
Sale increases and a second se		AP Policy	HTTP		radius-authe-method v		radius-autho-method v	None] 🛛
		Password Policy							
Walk Me Through >		AAA Interface							
			-						

CLI pour l'authentification GUI :

<#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

CLI pour l'authentification Telnet/SSH :

<#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

Notez que lorsque des modifications sont apportées aux configurations HTTP, il est préférable de redémarrer les services HTTP et HTTPS. Pour ce faire, utilisez les commandes suivantes :

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

Configurer ISE pour RADIUS

Étape 1. Configurez le WLC comme périphérique réseau pour RADIUS.

À partir de la GUI :

Afin de déclarer le WLC utilisé dans la section précédente comme périphérique réseau pour RADIUS dans ISE, naviguez jusqu'à Administration > Network Ressources > Network Devices et ouvrez l'onglet Périphériques réseau, comme illustré dans l'image suivante.



Pour ajouter un périphérique réseau, utilisez le bouton Ajouter, qui ouvre le nouvel écran de configuration du périphérique réseau.

Cisco ISE		Administration · Netw	ork Resources	🔺 Evalu	ation Mode 82 Days	Q (0)	6	٢
Network Devices N	etwork Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More \vee			
Network Devices Default Device Device Security Settings	Network Devices Li	st > New Network Device						
	Name	WLC-9800						
	Description							
	IP Addre	ss 🗸 * IP : 10.48.39.13	33 / 32 🚳					
	Device Profile	da Cisco	<u> </u>					
	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					
	Use	Second Shared Secret 🕠 Second Shared Secret		Show				
	CoA Por	t 1700	Set To De	əfault				
	RADIUS	DTLS Settings 🕕						
		Required (i)						
	Shared	Secret radius/dtls						

Dans la nouvelle fenêtre, indiquez le nom du périphérique réseau et ajoutez son adresse IP. Choisissez les paramètres d'authentification RADIUS et configurez le même secret partagé RADIUS que celui utilisé sur le WLC.

Étape 2. Créez un résultat d'autorisation pour renvoyer le privilège.

À partir de la GUI :

Pour avoir des droits d'accès d'administrateur, le adminuser doit avoir un niveau de privilège de 15, ce qui permet d'accéder à l'interpréteur de commandes d'invite d'exécution. D'autre part, le helpdeskuser n'a pas besoin d'un accès rapide à l'interpréteur de commandes exec et peut donc être attribué avec un niveau de privilège inférieur à 15. Afin d'attribuer le niveau de privilège approprié aux utilisateurs, des profils d'autorisation peuvent être utilisés. Vous pouvez les configurer à partir de l'ISE GUI Page Policy > Policy Elements > Results, sous l'onglet Authorization > Authorization Profiles présenté dans l'image suivante.

≡ Cisco ISE			Policy	Policy Elements		A Evaluation Mode 82 Days	Q Ø	,9 ¢
Dictionaries Cond	ditions	Results						
Authentication Authorization Authorization Profiles Downloadable ACLs	>	Star For Policy	Hand Authoriz	Zation Profiles • System > Backup & Restore > Policy E	xport Page	Selected 0 1	fotal 11	© 7
Profiling	>		Name	Profile	∧ Descriptio	in		
Posture	>		9800-admin-priv	🗰 Cisco 🕧				
Client Provisioning	>		9800-helpdesk-priv	🗯 Cisco 👔				
			Block_Wireless_Access	🗰 Cisco 🕧	Default pro	ofile used to block wireless de	evices. Ens	ure ti
			Cisco_IP_Phones	🗰 Cisco 🕕	Default pro	ofile used for Cisco Phones.		
			Cisco_Temporal_Onboard	🚓 Cisco 🕧	Onboard t	he device with Cisco tempora	l agent	
			Cisco_WebAuth	🗰 Cisco 🕧	Default Pr	ofile used to redirect users to	the CWA p	ortal
			NSP_Onboard	att Cisco 🕕	Onboard t	he device with Native Supplic	ant Provisio	ning
			Non_Cisco_IP_Phones	🗰 Cisco 🕧	Default Pr	ofile used for Non Cisco Phon	ies.	
			UDN	🗰 Cisco 👔	Default pr	ofile used for UDN.		
			DenyAccess		Default Pr	ofile with access type as Acce	ess-Reject	
		-				an an a		

Pour configurer un nouveau profil d'autorisation, utilisez le bouton Ajouter, qui ouvre le formulaire de configuration du nouveau profil d'autorisation. Ce formulaire doit notamment ressembler à ceci pour configurer le profil qui est attribué à l'adminuser.

	_		
_	\sim		ICE
		ISCO.	
	U	300	

Policy · Policy Elements

Dictionaries Conditions	Results
Authentication >	Authorization Profiles > New Authorization Profile
Authorization \vee	Authorization Profile
Authorization Profiles	* Name 9800-admin-priv
Downloadable ACLs	
Profiling >	Description
Posture >	* Access Type ACCESS_ACCEPT ~
Client Provisioning	Network Device Profile Cisco V
	Service Template
	Track Movement
	Agentless Posture
	Passive Identity Tracking U ()
	> Common Tasks
	Advanced Attributes Settings
	iii Cisco:cisco-av-pair ~ * shell:priv-lvl=15 ~ +
	✓ Attributes Details
	Access Type = ACCESS_ACCEPT
	\u2\u2\u2\u2\u2\u2\u2\u2\u2\u2\u2\u2\u2\
	Submit Cancel

La configuration affichée accorde le niveau de privilège 15 à tout utilisateur auquel elle est associée. Comme indiqué précédemment, il s'agit du comportement attendu pour le adminuser qui est créé lors de l'étape suivante. Cependant, le helpdeskuser doit avoir un niveau de privilège inférieur, et par conséquent un deuxième élément de politique doit être créé.

L'élément de stratégie pour le helpdeskuser est similaire à celui créé ci-dessus, à ceci près que la chaîne shell:priv-lvl=15 doit être remplacée par shell:priv-lvl=X, et remplacer X par le niveau de privilège souhaité. Dans cet exemple, l'adresse 1 est utilisée.

Étape 3. Créez des groupes d'utilisateurs sur ISE.

À partir de la GUI :

Les groupes d'utilisateurs ISE sont créés à partir de l'onglet User Identity Groups du Administration > Identity Management > Groups GUI Page, qui est affiché dans la capture d'écran.

E Cisco ISE		Administration - Identity Manag	gement A Evaluation Mode 82 Days Q	0	9	٩
dentities Groups External Ide	ntity Sour	ces Identity Source Sequences	Settings			
Identity Groups	Use	r Identity Groups	Selected 0 Tot	al 10 All	Q ~	\$ 7
> 🗅 User Identity Groups		Name ~	Description			
		A helpdesk-group	This is the group containing all users with read-only privileges.			
		🕂 admin-group	This is the group containing all users with administrator privileges.			
		NUN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group			
		SuestType_Weekly (default)	Identity group mirroring the guest type			
		Number 2 SocialLogin (default)	Identity group mirroring the guest type			
		Note: The term of term	Identity group mirroring the guest type			
		Magazin GuestType_Contractor (default)	Identity group mirroring the guest type			
		SROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group			
		A Employee	Default Employee User Group			
		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group			

Pour créer un nouvel utilisateur, utilisez le bouton Ajouter, qui ouvre le formulaire de configuration du nouveau groupe d'identités d'utilisateur comme illustré.

≡	Cisco	ISE	SE Administration - Identity Management Strougs External Identity Sources Identity Groups Submit Cancel								
Ide	ntities	Groups	External Ide	ntity Sources	Identity Source Sequences	Settings					
	adentity Gro	indpoint Identi Jser Identity G	ty Groups	User Identity Grou Identity Grou * Name Description	ups > New User Identity Group UP admin-group This is the group containing all users with a	administrator privileges.	Submit	Cancel			

Fournissez le nom du groupe qui est créé. Créez les deux groupes d'utilisateurs décrits ci-dessus, à savoir le admin-group et le helpdesk-group.

Étape 4. Créez des utilisateurs sur ISE.

À partir de la GUI :

Les utilisateurs ISE sont créés à partir de l'onglet Utilisateurs du Administration > Identity Management > Identities GUI Page, qui est affiché dans la capture d'écran.

≡ Cisco ISE	Administration · Identity Management	A Evaluation Mode 82 Days Q	\$ 54 \$
Identities Groups External Ident	tity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res Net	work Access Users		
🖉 Edit	+ Add 🛞 Change Status 🗸 🕁 Import 🕆 Export 🗸 🏮 Delete 🗸 🚺 Duplica	Selected 0 To	otal 2 📿 🚱 All 🗸 🏹
	Status Username \wedge Description First Name Last Name Email Address	User Identity Groups Admin	
	Enabled <u>1</u> adminuser	admin-group	
	Enabled <u>1</u> helpdeskus	helpdesk-group	

Pour créer un nouvel utilisateur, utilisez le bouton Ajouter pour ouvrir le formulaire de configuration du nouvel utilisateur d'accès au réseau, comme illustré.

≡	Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 82 Days 📿 🔗 👼
lder	ntities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest	Manual Network Scan Res	Network Access Users List > New Network Access User	
		Vetwork Access User Vsername adminuser	
		Status Status	
		Account Name Alias	
		Email	
		\vee Passwords	
		Password Type: Internal Users ~	
		Password Lifetime: With Expiration Password will expire in 60 days Never Expires Password Lifetime:	
		Password Re-Enter Password	
		* Login Password ····· ···	Generate Password (i)
		Enable Password	Generate Password
		> User Information	
		> Account Options	
		> Account Disable Policy	
		✓ User Groups	
		🗄 admin-group 🗸 📵 🕒	

Fournissez les identifiants aux utilisateurs, à savoir son nom d'utilisateur et son mot de passe, qui sont ceux qui sont utilisés pour s'authentifier sur le WLC. Vérifiez également que l'état de l'utilisateur est Enabled. Enfin, ajoutez l'utilisateur à son groupe associé, créé à l'étape 4., avec le menu déroulant Groupes d'utilisateurs à la fin du formulaire.

Créez les deux utilisateurs mentionnés ci-dessus, à savoir le adminuser et le helpdeskuser.

Étape 5. Authentifiez les utilisateurs.

À partir de la GUI :

Dans ce scénario, la stratégie d'authentification des ensembles de stratégies par défaut d'ISE, qui est déjà préconfigurée, autorise l'accès réseau par défaut. Cet ensemble de stratégies est visible à partir Policy > Policy Sets de la page de l'interface utilisateur graphique ISE, comme illustré dans cette image. Il n'est donc pas nécessaire de la modifier.

≡	Cisco IS	E	[Policy · Policy Sets		A Evaluation Mode 82 Days	2 0	90 ¢
Poli	cy Sets→	Default			Reset	Reset Policyset Hitcounts		Save
	Status Po	blicy Set Name De	escription	Conditions		Allowed Protocols / Server S	Sequenc	e Hits
	Q Search							
	٢	Default	Default policy set			Default Network Access	∞ ~	+ o
\sim	Authentication	n Policy (3)						
	+ Status	Rule Name	Conditions		Use		Hits	Actions
	Q Search							
			. Wired_	мав	Internal	Endpoints 🛛 🗸		-^
		MAB	OR 📃 Wireles	s_MAB	> Opti	ons	0	ζ <u>Ο</u> Σ
			E Wired	802.1X	All_Use	r_ID_Stores 🛛 🗸 🗸		
	0	Dot1X	OR 📃 Wireles	\$_802.1X	> Opti	ons	0	ŝ
Г	_				All_Use	r_ID_Stores 🛛 🛛 🗸	-	
	0	Default			> Opti	ons	0	ŝ

Étape 6. Autorisez les utilisateurs.

À partir de la GUI :

Une fois que la tentative de connexion a réussi la stratégie d'authentification, elle doit être autorisée et ISE doit renvoyer le profil d'autorisation créé précédemment (permit accept, ainsi que le niveau de privilège).

Dans cet exemple, les tentatives de connexion sont filtrées en fonction de l'adresse IP du périphérique (qui est l'adresse IP du WLC) et distinguent le niveau de privilège à accorder en fonction du groupe auquel un utilisateur appartient. Une autre approche valide consiste à filtrer les utilisateurs en fonction de leurs noms d'utilisateur, car chaque groupe ne contient qu'un seul utilisateur dans cet exemple.

-			Policy · Policy S	Sets		🛕 Eva	aluation Mode 82 Days	Q (?) ,9	
Default						Reset Rese	et Policyset Hitcounts		Save	
licy Set Name	Descript	ion	Conditions			Allow	ed Protocols / Server	Seque	nce H	
Default	Default	policy set				Defau	It Network Access	× -	+ 152	
Policy (3)										
Policy - Local Exception	s									
Policy - Global Exceptio	ns (2)									
				Results						
Rule Name	Cond	litions		Profiles		Security Groups		Hits	Action	
	_									
		Retwork Ad ↓ Address EQUALS 1	cess Device IP 0.48.39.133			0.1			~	
9800 Helpdesk Users	AND	R EQUALS U Groups:hel	r-IdentityGroup ser Identity pdesk-group	9800-helpdesk-priv ×	~ +	Select from list	~+	1	{Q}	
		Network Address EQUALS 1	cess Device IP	0000 odzia privo		Soloot from list			2	
9800 Admin Users	AND	InternalUse R EQUALS U	r-IdentityGroup ser Identity	9800-admin-priv ×	~ +	Select from list	~ +	2	£Ç3	
	efault cy Set Name Pefault Policy (3) olicy - Local Exception olicy - Global Exception Rule Name 9800 Helpdesk Users	efault icy Set Name Descript iefault Default Default Default Policy (3) iolicy - Local Exceptions (2) Rule Name Set Obal Exceptions (2) 9800 Helpdesk Users AND	efault cy Set Name Description lefault pelault pelault policy (3) olicy - Local Exceptions olicy - Global Exceptions solicy - Global E	Icy Set Name Description Conditions befault Default policy set Image: Conditions Policy (3) Image: Conditions Image: Conditions rolicy - Local Exceptions Image: Conditions Image: Conditions rolicy - Global Exceptions (2) Image: Conditions Image: Conditions g800 Helpdesk Users Image: Conditions Image: Conditions 9800 Helpdesk Users Image: Conditions Image: Conditions	efault cy Set Name Description Conditions Default policy set Default Default policy set Policy (3) Policy - Local Exceptions Volicy - Local Exceptions Volicy - Global Exceptions Poloe Rule Name Conditions Profiles Results Results Results Profiles Profiles Profiles Profiles Profiles Profi	efault cy Set Name Description Conditions efault Default policy set Policy (3) Policy (3) Policy - Local Exceptions Policy - Local Exceptions Policy - Global Exceptions (2) Rule Name Policy - Global Exceptions (2) Policy - Global Exceptions Policy - Global Exception Policy - Global	Result Result Result InternalUser-IdentityGroup Select from list 9800 Helpdesk Users Allow	Rest Rest Policyset Hitcourts International Conditions Conditions Allowed Protocols / Server International Conditions Conditions Allowed Protocols / Server Description Default Network Access Or Policy 3) International Conditions Results Results Results Results Results Security Groups Select from list + Select from list + Results Select from list + Select from list + Select from list + Results International Colspan="4">Select from list + Select from list <th c<="" td=""><td>Rest Rest <threst< th=""> Rest Res</threst<></td></th>	<td>Rest Rest <threst< th=""> Rest Res</threst<></td>	Rest Rest <threst< th=""> Rest Res</threst<>

Une fois cette étape terminée, les informations d'identification configurées pour adminuser et helpdesk l'utilisateur peuvent être utilisées pour s'authentifier dans le WLC via l'interface graphique utilisateur ou via Telnet/SSH.

Reset

Configuration du WLC TACACS+

Étape 1. Déclarez le serveur TACACS+.

À partir de la GUI :

Tout d'abord, créez le serveur ISE Tacacs+ sur le WLC. Cela peut être fait à partir de l'onglet Servers/Groups > TACACS+ > Servers de la page GUI WLC accessible dans le <u>https://<WLC-IP>/webui/#/aaa</u>, ou si vous naviguez vers Configuration > Security > AAA, comme le montre cette image.

Cisco Catalyst	t 9800-CL Wireless Controller	Welcome admin & 🕷 🔹 🛕	🖺 🏟 🖗 📿 Search APs	and Clients Q
Q. Search Menu Items Image: Configuration items Image: Configuration items Image: Configuration items Image: Configuration items Image: Configuration items	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				

Pour ajouter un serveur TACACS sur le WLC, cliquez sur le bouton Add encadré en rouge dans l'image ci-dessus. La fenêtre contextuelle illustrée s'ouvre.

F	Cise	co Cata	lyst 9800-CL	Wireless Controller					
	17.9.2			1 L	Welcome admin All All All All All All All All All Al	🗣 🗛 🛱 🌣	🔯 🛛 🎜 🛛 Sear	ch APs and Clients Q	Feedback
٩	Search Menu Items		Configuration •	> Security * > AAA					
			+ AAA Wizard	Create AAA Tacacs S	erver		×		
\bigcirc		>	Servers / Gron	Name*	ISE-lab				
Z,		>	+ Add	Server Address*	10.48.39.134				
කු		>	RADIUS	Кеу Туре	Clear Text 🗸				
C			TACACS+	Key*				▼ Port	Ť
×			LDAP	Confirm Key*					No items to display
670				Port	49				
				Server Timeout (seconds)	1-1000				
(Canaal					
				5 Cancer			Apply to Device		

Lorsque la fenêtre contextuelle s'ouvre, indiquez le nom du serveur (il ne doit pas nécessairement correspondre au nom du système ISE), son adresse IP, la clé partagée, le port utilisé et le délai d'attente.

Dans cette fenêtre contextuelle, vous devez fournir :

• Le nom du serveur (notez qu'il ne doit pas nécessairement correspondre au nom du système ISE)

- Adresse IP du serveur
- Le secret partagé entre le WLC et le serveur TACACS+

D'autres paramètres peuvent être configurés, tels que les ports utilisés pour l'authentification et la comptabilité, mais ils ne sont pas obligatoires et restent par défaut pour cette documentation.

À partir de CLI :

<#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

Ciscol23

Étape 2. Mappez le serveur TACACS+ à un groupe de serveurs. À partir de la GUI :

Si vous disposez de plusieurs serveurs TACACS+ pouvant être utilisés pour l'authentification, il est recommandé de mapper tous ces serveurs au même groupe de serveurs. Le WLC s'occupe ensuite de l'équilibrage de charge des différentes authentifications parmi les serveurs dans le groupe de serveurs. Les groupes de serveurs TACACS+ sont configurés à partir de l'ongletServers/Groups > TACACS > Server Groups de la même page GUI que celle mentionnée à l'étape 1, qui est illustrée dans l'image.

Cisco Catalyst 9800-CL Wirele	Welcome admin Last login 12/07/2022 14:14:43	* * 4 8 * 0	Search APs and Client	s Q
Q. Search Menu Items Configuration * > Sec Dashboard + AAA Wizard Monitoring Servers / Groups Configuration + Add Configuration RADIUS	curity - > AAA AAA Method List AAA Advanced elete Servers Server Groups			
C Licensing LDAP C Troubleshooting	Name TACACS-Group	Y Server 1 ISE-lab	Server 2 N/A	Server 3 N/A 1 - 1 of 1 items
Walk Me Through 3				

En ce qui concerne la création du serveur, une fenêtre contextuelle apparaît lorsque vous cliquez sur le bouton Ajouter encadré dans l'image précédente, qui est représentée dans l'image.

Cisco Cata	ilyst 9800-CL Wireless Controller		🌣 🗿 😧 Search APs an	d Clients Q
Q. Search Manu Items Image: Dashboard Image: Monitoring	Configuration * > Security * > AAA + AAA Wizard Server Create AAA Tacacs Server	r Group	×	
Configuration > Administration > Licensing Troubleshooting	Name* RAI Group Type TAL Available Servers	TACACS-Group TACACS Assigned Servers ISE-lab C Assigned Levers		Server 3 No items to display
Walk Me Through >	Cancel		Apply to Device	

Dans la fenêtre contextuelle, attribuez un nom au groupe et déplacez les serveurs souhaités vers la liste Serveurs affectés.

À partir de CLI :

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

TACACS-Group

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

ISE-lab

Étape 3. Créez une méthode de connexion d'authentification AAA qui pointe vers le groupe de serveurs TACACS+.

À partir de la GUI :

Toujours à partir de la page GUIhttps://<WLC-IP>/webui/#/aaa, accédez à l'AAA Method List > Authentication onglet et créez une méthode d'authentification comme illustré dans l'image.

C search Menu terms Image: Dashboard		sco Catal	yst 9800-CL Wire	eless Cont	Welcome Last login 12/07	admin 1/2022 14:14:43	*	▲ 🎝	B	¢ @ 0	-	Search AP	's and	Clients Q	(Feedback	~
Authentication Authentication Authorization Configuration Configuration <t< td=""><td>Q Search Menu Items</td><td></td><td>Configuration • > 3 + AAA Wizard Servers / Groups</td><td>Security - ></td><td>AAA od List AAA</td><td>Advanced</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Q Search Menu Items		Configuration • > 3 + AAA Wizard Servers / Groups	Security - >	AAA od List AAA	Advanced											
Accounting Accou		>	Authentication Authorization		+ Add × D	elete											
Consisting Incubleshooting Incube	Of Administration	· · ·	Accounting		Name	Туре	Ŧ	Group Type	۲	Group1	Ŧ	Group2	Ŧ	Group3	Ŧ	Group4	Ŧ
Troubleshooting radius-authe- login local RADIUS-Group N/A N/A N/A <td>C) Licensing</td> <td></td> <td></td> <td>0</td> <td>default</td> <td>login</td> <td></td> <td>local</td> <td></td> <td>N/A</td> <td></td> <td>N/A</td> <td></td> <td>N/A</td> <td></td> <td>N/A</td> <td></td>	C) Licensing			0	default	login		local		N/A		N/A		N/A		N/A	
Walk Me Through 3	Troubleshooting			0	radius-authe- method	login		local		RADIUS-Group		N/A		N/A		N/A	
Walk Me Through >				O H	tacacs-authe- method	login		local		TACACS-Group		N/A		N/A		N/A 1 - 3 of 3 i	tems
	Walk Me Through >																

Comme d'habitude, lorsque vous utilisez le bouton Ajouter pour créer une méthode d'authentification, une fenêtre contextuelle de configuration s'affiche, semblable à celle illustrée dans cette image.

÷		Cisco (Catal	lyst 9800	0-CL Wireless Controller											
		7.9.2				Welcome admir	n 🛛 🖌 🖌	A	8	1 1 1	ວ ສ [and Clients Q		Feedback	ы ^ж (Ф
٩	Search Menu Items	8	ו	Configu	ration • > Security • > AAA											
				1	Quick Setup: AAA Authent	ication						×				
3			>	Server	Method List Name*	tacacs-authe-r	method									
			>	Aut	Туре*	login	• i									
ঠ্য			>	Aut	Group Type	local	• i	enver Groups								
C				Acc	radius		TACACS-Group		·	(=)			Group3	Ţ	Group4	T
×					Idap tacacs+ RADIUS-Group	<				<u>^</u>			N/A		N/A	
						>				× ¥					1 - 2 of 2 it	
					L	1										
					Cancel						Apply to	Device				

Dans cette fenêtre contextuelle, attribuez un nom à la méthode, choisissez Type comme login, puis ajoutez le serveur de groupe créé à l'étape précédente à la liste Groupes de serveurs affectés. En ce qui concerne le champ Type de groupe, plusieurs configurations sont possibles.

• Si vous choisissez Group Type comme local, le WLC vérifie d'abord si les informations d'identification de l'utilisateur existent localement, puis revient au groupe de serveurs.

- Si vous choisissez Group Type comme groupe et ne cochez pas l'option Fall back to local, le WLC vérifie simplement les informations d'identification de l'utilisateur par rapport au groupe de serveurs.
- Si vous choisissez Group Type comme groupe et cochez l'option Fallback to local, le WLC vérifie les informations d'identification de l'utilisateur par rapport au groupe de serveurs et interroge la base de données locale uniquement si le serveur ne répond pas. Si le serveur envoie un refus, l'utilisateur doit être authentifié, même s'il peut exister dans la base de données locale.

À partir de CLI :

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs uniquement si elles ne sont pas trouvées localement en premier, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

local group

TACACS-Group

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées uniquement avec un groupe de serveurs, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs et si ce dernier ne répond pas avec une entrée locale, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

local

Dans cet exemple de configuration, certains utilisateurs sont uniquement créés localement, et d'autres uniquement sur le serveur ISE. Par conséquent, utilisez la première option.

Étape 4. Créez une méthode d'exécution d'autorisation AAA qui pointe vers le groupe de serveurs TACACS+. À partir de la GUI :

L'utilisateur doit également être autorisé pour se voir accorder l'accès. Toujours à partir de la page GUI, Configuration > Security > AAAaccédez à l'AAA Method List > Authorization onglet et créez une méthode d'autorisation comme illustré dans l'image.

Cisco	Cisco Catal	lyst 9800–CL Wi	reless Cont	roller Welcom Last login 12	ne <i>admin</i> 2/07/2022 14:14:43	*	•	ħ	• 19	0 2	Search APs and	Clients Q	Feedback	₆ × ⊕
Q. Search Menu I Dashboard Omitoring Configuration	lems > >	Configuration • > • AAA Wizard Servers / Groups Authentication	Security ->	AAA od List AA	A Advanced									
 Administrati Licensing Troubleshood 	on >	Authorization		Name default radius-autho- method tacacs-autho- method d	▼ Type exec exec exec ⊨ 10 ▼	T	Group Type local local	T	Group1 N/A RADIUS-C	▼ Group	Group2 T N/A N/A N/A	Group3 T N/A N/A N/A	Group4 N/A N/A N/A 1 - 3 of 3 it	T
Walk Me Throu														

Une fenêtre contextuelle de configuration de méthode d'autorisation similaire à celle illustrée s'affiche lorsque vous en ajoutez une nouvelle à l'aide du bouton Ajouter.

F	alialia	Cisco	Cata	lvst 9800	0-CL Wireless Controller												
	cisco	17.9.2				Welcome au Last login 12/07/20	dmin 022 14:14:43	* 	A 🖪	• 19	0 0			lients Q		E Feedback	** (*
٩	Search Menu I	tems		Configu	ration * > Security * > AAA	ation a											
				+ 🗚	Quick Setup: AAA Authoriz	tation	tho-method	1				×	1				
Ċ			>	Server	Type*	exec	•	(i)									
Ľ			>	Aut	Group Type	local	٠	(1)									
Ś			>		Authenticated					_			т	Group3	Ŧ	Group4	Ŧ
C				ACC	Available Server Groups		Assigned Ser	ver Groups		7				N/A		N/A	
2.00					radius Idap		TACAC	S-Group		Ā]			N/A		N/A	
26					tacacs+ RADIUS-Group	<]					1 - 2 of 2	
						*				Ľ]						
										_							
					່ ວ Cancel						🗎 Арр	ly to Device					

Dans cette fenêtre contextuelle de configuration, attribuez un nom à la méthode d'autorisation, choisissez Type as exec et utilisez le même ordre de type de groupe que celui utilisé pour la méthode d'authentification à l'étape précédente.

À partir de CLI :

<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

local group

TACACS-Group

Étape 5. Attribuez les méthodes aux configurations HTTP et aux lignes VTY utilisées pour Telnet/SSH.

À partir de la GUI :

Les méthodes d'authentification et d'autorisation créées peuvent être utilisées pour la connexion utilisateur HTTP et/ou Telnet/SSH, qui est configurable à partir de l'onglet AAA Advanced > AAA Interface, toujours à partir de la page GUI WLC accessible dans https://<WLC-IP>/webui/#/aaa, comme illustré dans l'image.

¢	cisco	Cisco 17.9.2	Cataly	yst 9800-CL Wirele	ss Controller	Welcome <i>admin</i> Last login 12/07/2022 14:14:43	*	1	A 🖪	¢	1		Search APs	and Clients	Q	Feedback	₂ × ⊕
Q Se	arch Menu It	lems		Configuration • > Sec	urity • > AAA												
👼 Da	ashboard onitoring		>	+ AAA Wizard Servers / Groups	AAA Method List	AAA Advanced											
2 c			>	Global Config													pply
ې ۸ (ئ	dministratio	on	>	RADIUS Fallback			Au	thentica	tion			Auth	orization			Accounting	
© Lie	censing			Attribute List Name	Console		None		•	8		None	•] 🖬	None	٠	
X Tr	oubleshoo	ting		Device Authentication	VTY		tacacs-	authe-m	iethod y	2		acacs-au	ho-method y		None	٠	8
				AP Policy	HTTP		tacacs-	authe-m	iethod y		Ľ	acacs-au	ho-method y	•	None	•	
	alk Me Throus	th 2		Password Policy	_												
				AAA Interface													

À partir de CLI :

Pour l'authentification GUI :

<#root>

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

tacacs-authe-method

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

Pour l'authentification Telnet/SSH :

<#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

Notez que lorsque des modifications sont apportées aux configurations HTTP, il est préférable de redémarrer les services HTTP et HTTPS. Ces commandes permettent d'y parvenir.

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

Configuration de TACACS+ ISE Étape 1. Configurez le WLC en tant que périphérique réseau pour TACACS+.

À partir de la GUI :

Afin de déclarer le WLC utilisé dans la section précédente comme périphérique réseau pour RADIUS dans ISE, naviguez jusqu'à Administration > Network Resources > Network Devices et ouvrez l'onglet Périphériques réseau, comme illustré dans cette image.



Dans cet exemple, le WLC a déjà été ajouté pour l'authentification RADIUS (référez-vous à l'étape 1. de la section <u>Configurer RADIUS ISE</u>). Par conséquent, sa configuration doit simplement être modifiée pour configurer l'authentification TACACS, ce qui peut être fait lorsque vous choisissez le WLC dans la liste des périphériques réseau et cliquez sur le bouton Edit. L'écran de configuration du périphérique réseau s'ouvre, comme illustré dans cette image.

≡ Cisco ISE		Administration · Netv	🛕 Evalu	ation Mode 82 Days Q	05	9 🔅	
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More $ \smallsetminus $		
Network Devices	Genera	al Settings					
Default Device	Ena	ble KeyWrap 🥡					
Device Security Settings	Кеу	Encryption Key	Show				
	Me: Aut Key	ssage henticator Code	Show				
	Key	Input Format					
	0	ASCII O HEXADECIMAL					
		CACS Authentication Settin	ıgs				
	Shared	Secret ·····	Show				
	Ena	ble Single Connect Mode					
	0	Legacy Cisco Device					
	0	TACACS Draft Compliance Single	e Connect Support				
	🗆 ~ SN	MP Settings					
	🗌 🗸 Adv	vanced TrustSec Settings					

Une fois la nouvelle fenêtre ouverte, faites défiler jusqu'à la section TACACS Authentication Settings, activez ces paramètres et ajoutez le secret partagé entré au cours de l'étape 1. de la section <u>Configure TACACS+WLC</u>.

Étape 2. Activez la fonctionnalité Device Admin pour le noeud.



Remarque : pour utiliser ISE comme serveur TACACS+, vous devez disposer d'un package de licence Device Administration et d'une licence Base ou Mobility.

À partir de la GUI :

Une fois les licences Device Administration installées, vous devez activer la fonctionnalité Device Admin pour le noeud afin de pouvoir utiliser ISE comme serveur TACACS+. Pour ce faire, modifiez la configuration du noeud de déploiement ISE utilisé, qui se trouve sous Administrator > Deployment, et cliquez sur son nom ou effectuez-le à l'aide du Edit bouton.

≡	Cisco ISE		Administration · System	4	Evaluation Mode 82 Days Q 🕜 🗔 🕸
Depl	oyment Licensing	Certificates Logging	Maintenance Upgrade	Health Checks Backup & Restore	Admin Access Settings
De	> S Deployment	Deploym	ent Nodes		Selected 0 Total 1 🔗 🗔 All ~ 🏹
		Hostna	me ^ Personas	Role(s) Services	Node Status
		ise	Administration, Monito	pring, Policy Service STANDALO SESSION,	PROFILER

Une fois la fenêtre de configuration du noeud ouverte, vérifiez l'option Enable Device Admin Service sous la section Policy Service, comme illustré dans cette image.

≡ Cisco ISE	Administration · System	🛕 Evaluation Mode 82 Days Q 🕜 🔎
Deployment Licensing Certific	ates Logging Maintenance Upgrade Health Checks	Backup & Restore Admin Access Settings
Deployment C C C C C C C C C C C C C C C C C C C	Deployment Nodes List > ise Edit Node Profiling Configuration Mestname ise FQDN ise.cisco.com IP Address 10.48.39.134 Node Type Identity Services Engine (ISE)	
	Role STANDALONE Make Primary Administration Monitoring Role PRIMARY Other Monitoring Node	~
	 Dedicated MnT () Policy Service C Enable Session Services () Include Node in Node Group None Enable Profiling Service () Enable Threat Centric NAC Service () Enable Device Admin Service () Enable Device Admin Service () 	~ •
	> pxGrid ()	Reset Save

Étape 3. Créez des profils TACACS pour renvoyer le privilège.

À partir de la GUI :

Pour avoir des droits d'accès d'administrateur, le adminuser doit avoir un niveau de privilège de 15, ce qui permet d'accéder à l'interpréteur de commandes d'invite d'exécution. D'autre part, le helpdeskuser n'a pas besoin d'un accès rapide à l'interpréteur de commandes exec et peut donc être attribué avec un niveau de privilège inférieur à 15. Afin d'attribuer le niveau de privilège approprié aux utilisateurs, des profils d'autorisation peuvent être utilisés. Vous pouvez les configurer à partir de la page de l'interface utilisateur graphique ISEWork Centers > Device Administration > Policy Elements, sous l'onglet Results > TACACS Profiles, comme illustré dans l'image suivante.

≡ Cisco ISE		Work Centers · Device	Administration	🛕 Evaluation Mode 82 Days Q ⑦ 등로 🕸
Overview Identities	User Identity Groups	Ext Id Sources Netv	ork Resources	Policy Elements Device Admin Policy Sets More ~
Conditions Library Conditions Smart Conditions	✓ TACACS I	Profiles		Rows/Page 6 → I< < 1 / 1 > >I Go 6 Total Rows
Network Conditions	> 2 Add Duplice	ite Trash 🗸 Edit		Filter 🗸 🐵
Results	✓ □ Name	Туре	Description	
Allowed Protocols TACACS Command Sets	Default Shell Pr	ofile Shell	Default Shell Profile	file
TACACS Profiles	Deny All Shell F	Profile Shell	Deny All Shell Profi	ofile
	IOS Admin	Shell	Assigned to each u	h user in the group admin-group
	IOS Helpdesk	Shell	Assigned to each u	n user in the group helpdesk-group
	U WLC ALL	WLC	WLC ALL	
	WLC MONITOR	WLC	WLC MONITOR	

Afin de configurer un nouveau profil TACACS, utilisez le bouton Ajouter, qui ouvre le nouveau formulaire de configuration de profil similaire à celui illustré dans l'image. Ce formulaire doit notamment ressembler à ceci pour configurer le profil qui est assigné à la adminuser (c'est-à-dire, avec des privilèges d'interpréteur de commandes de niveau 15).

		work Centers -	Device Administration		A Evaluation mode	oz bays Q (-97 <u>-</u> 0
Overview Identities	User Identity Group	os Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More \vee	
nditions	> TACACS Profiles > TACACS Profiles >	IOS Admin					
twork Conditions	>		_				
sults Allowed Protocols	V IOS Admin						
FACACS Command Sets	Description						
IACACS Profiles	Assigned to ea admin-group	ach user in the group					
	Task Attribute V	iew Raw View	6				
	Common Tas	sks					
	Common Task T	ype Shell 🗸					
		Default Privilege	15	 ✓ (Select 0 to 	o 15)		
		Maximum Privilege	15	✓ (Select 0 to	5 15)		
		Access Control List		~			
		Auto Command		~			
		No Escape		✓ (Select tru	e or false)		
		Timeout		✓ Minutes (0-	9999)		
		Idle Time		✓ Minutes (0-	9999)		
	Custom Attri	butes					
	Add 🛛 Trash 🗠	Edit					٥
	🗆 Туре	Name	Value				
	No data found.						
	the second fulling.						

Répétez l'opération pour le profilhelpdesk. Pour ce dernier, le privilège par défaut, ainsi que le privilège maximal, sont tous deux définis sur 1.

Étape 4. Créez des groupes d'utilisateurs sur ISE.

Il s'agit du même que celui présenté à l'étape 3. de la section Configurer RADIUS ISE de ce document.

Étape 5. Créez les utilisateurs sur ISE.

Il s'agit du même que celui présenté à l'étape 4. de la section Configurer RADIUS ISE de ce document.

Étape 6. Créez un ensemble de stratégies d'administration de périphériques.

À partir de la GUI :

~ .

En ce qui concerne l'accès RADIUS, une fois les utilisateurs créés, leurs stratégies d'authentification et d'autorisation doivent encore être définies sur ISE afin de leur accorder les droits d'accès appropriés. L'authentification TACACS utilise des ensembles de stratégies d'administration de périphériques à cette fin, qui peuvent être configurés à partir de la Work Centers > Device Administration > Device Admin Policy Sets GUI Page comme illustré.

Work Centers · Device Administration	🔺 Evaluation Mode 82 Days 🔍 🧑 👼
ps Ext Id Sources Network Resources Polic	cy Elements Device Admin Policy Sets More ~
	Reset Policyset Hitcounts Save
ription Conditions	Allowed Protocols / Server Sequence Hits Actions View
P Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin $ \simeq \checkmark + $ 0 $ $
s Default policy set	Default Device Admin $ \checkmark + 0$
	Reset
	Work Centers · Device Administration ups Ext Id Sources Network Resources Poli eription Conditions Image: Retwork Access-Device IP Address EQUALS 10.48.39.133

Pour créer un ensemble de stratégies d'administration de périphériques, utilisez le bouton Ajouter encadré en rouge dans l'image précédente, afin d'ajouter un élément à la liste des ensembles de stratégies. Donnez un nom au jeu nouvellement créé, une condition dans laquelle il doit être appliqué et les protocoles autorisés/la séquence de serveur (ici, les Default Device Admin suffisent). Save Utilisez le bouton pour finaliser l'ajout de l'ensemble de stratégies et utilisez la flèche située sur son droit pour accéder à sa page de configuration, telle qu'elle apparaît sur la page représentée.

E Ci	sco IS	E		Work Centers · [Device Administrati	🛕 Evaluation Mode 82 Days Q 🕜 📈					
verviev	v Id	entities User Identit	y Groups	Ext Id Sources	Network Resource	es Policy Ele	ments	Device Admin Policy Set	s More	/	
olicy S	Sets→	WLC TACACS Authent	tication					Reset Policys	set Hitcounts		Save
Sta	atus Po	olicy Set Name D	escription	Condit	ions			Allowed Proto	cols / Server S	Sequence	e Hit
Q	Search										
	0	WLC TACACS Authentication			Network Access-Device	P Address EQUALS	0.48.39.133	Default Devi	ce Admin	<u>∞</u> ~+	- 0
 Auth 	enticatio	n Policy (1)									
۲	Status	Rule Name	Condition	15				Use		Hits A	ctions
Q	Search										
					+						
								All_User_ID_Stores	∞ ~		
	0	Default						> Options		0	\$ \$ }
> Auth	orization	Policy - Local Exceptions									
Auth	orization	Policy - Global Exceptions									
Auth	orization	Policy (3)									
					Results						
•	Status	Rule Name	Condition	15	Comma	nd Sets		Shell Profiles		Hits A	ctions
Q	Search										
	0	Helpdesk users authorization	유 Inter Iden	nalUser-IdentityGroup EQ tity Groups:helpdesk-grou	UALS User AllowAl	ICommands \times	~+	IOS Helpdesk	∞ ~+	0	ŝ
	0	Admin users authorization	R Inter Iden	nalUser-IdentityGroup EQ tity Groups:admin-group	UALS User AllowAl	ICommands \times	~+	IOS Admin	∞ ~+	0	ŝ
	0	Default			DenyAl	Commands $ imes$	~+	Deny All Shell Profile	∞ ~+	0	<i>t</i> ĝ}

L'ensemble de stratégies spécifique 'Authentification TACACS WLC' dans cet exemple filtre les requêtes avec l'adresse IP égale à l'exemple d'adresse IP WLC C9800.

Reset

En tant que stratégie d'authentification, la règle par défaut a été conservée car elle répond au besoin de la casse d'utilisation. Deux règles d'autorisation ont été définies :

• La première est déclenchée lorsque l'utilisateur appartient au groupe défini admin-group. Elle autorise toutes les commandes (via la règle par défautPermit_all) et attribue le privilège 15 (via le profil TACACS définiIOS_Admin).

• Le second est déclenché lorsque l'utilisateur appartient au groupe défini helpdesk-group. Elle autorise toutes les commandes (via la Permit_all règle par défaut) et attribue le privilège 1 (via le profil TACACS définiIOS_Helpdesk).

s'authentifier dans le WLC via l'interface graphique utilisateur ou avec Telnet/SSH.

Dépannage

Si votre serveur RADIUS attend l'envoi de l'attribut RADIUS de type de service, vous pouvez ajouter sur le WLC :

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

Dépannage de l'interface graphique WLC ou de l'accès CLI RADIUS/TACACS+ via l'interface CLI WLC

Afin de dépanner l'accès TACACS+ à l'interface graphique WLC ou CLI, émettez la commande, debug tacacs avec terminal monitor one et voyez le résultat en direct quand une tentative de connexion est faite.

Par exemple, une connexion réussie suivie d'une déconnexion de l'adminuser utilisateur génère cette sortie.

<#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
```

Ces journaux indiquent que le serveur TACACS+ renvoie le privilège correct (qui est AV priv-lvl=15).

Lorsque vous effectuez l'authentification RADIUS, une sortie de débogage similaire s'affiche, qui concerne le trafic RADIUS.

Les commandes debug aaa authentication et debug aaa authorization, à la place, montrent quelle liste de méthodes est choisie par le WLC quand

l'utilisateur essaie de se connecter.

Dépannage de l'interface graphique WLC ou de l'accès CLI TACACS+ via l'interface graphique ISE

Depuis cette pageOperations > TACACS > Live Logs, chaque authentification utilisateur effectuée avec TACACS+ jusqu'aux dernières 24 heures peut être visualisée. Pour développer les détails d'une autorisation ou d'une authentification TACACS+, utilisez le bouton Détails associé à cet événement.

≡	Cisco ISE			Oper	ations · TACACS]	A Evaluation Mode 82	Jays Q 🕜 💆) 🗇
Live	Logs								
g						Refres Neve	h Show r ~ Latest 20 records	i → Within Last 3 hours Filter →	~
	Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	N
×			~	Identity	~	Authentication Policy	Authorization Policy	Ise Node	N
	Dec 08, 2022 06:51:46.1		à	helpdeskuser	Authorization		WLC TACACS Authentication >	ise	w
	Dec 08, 2022 06:51:46.0		ò	helpdeskuser	Authentication	WLC TACACS Authentication	>	ise	w
	Dec 08, 2022 06:38:38.2		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
Last	Updated: Thu Dec 08 202	2 12:57:09	GMT+0100 (C	entral European S	itandard Time)			Records Show	wn: 6

Une fois développée, une tentative d'authentification réussie pour le helpdeskuser ressemble à ceci :

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 IP	10.48.39.133 IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Network Device IP Network Device Groups Device Type	10.48.39.133 IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types
Network Device IP Network Device Groups Device Type Location	10.48.39.133 IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types Location#All Locations
Network Device IP Network Device Groups Device Type Location Device Port	10.48.39.133 IPSEC#IS IPSEC Device#No,Location#All Locations,Device Type#All Device Types Device Type#All Device Types Location#All Locations tty5

Steps

Received TACACS+ Authentication START Request
Evaluating Policy Group
Evaluating Service Selection Policy
Queried PIP - Network Access.Device IP Address
Evaluating Identity Policy
Selected identity source sequence - All_User_ID_Stores
Selected Identity Source - Internal Users
Looking up User in Internal Users IDStore
Found User in Internal Users IDStore
TACACS+ will use the password prompt from global TACACS+ configuration
Returned TACACS+ Authentication Reply
Received TACACS+ Authentication CONTINUE Request (
Evaluating Identity Policy
Selected identity source sequence - All_User_ID_Stores
Selected Identity Source - Internal Users
Looking up User in Internal Users IDStore
Found User in Internal Users IDStore
Authentication Passed
Evaluating Authorization Policy
Queried PIP - Network Access.UserName
Queried PIP - InternalUser.IdentityGroup
Returned TACACS+ Authentication Reply

De là, vous pouvez voir que l'utilisateur helpdeskuser a été authentifié avec succès sur le périphérique réseau WLC-9800 à l'aide de la stratégie d'authentification WLC TACACS Authentication > Default. En outre, le profil d'autorisation IOS Helpdesk a été attribué à cet utilisateur et a obtenu le niveau de privilège 1.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.