# Configuration de l'authentification ISE Radius pour Secure Firewall Chassis Manager (FCM)

# Table des matières

# Introduction

Ce document décrit le processus de configuration de l'accès d'autorisation/authentification Radius pour Secure Firewall Chassis Manager avec ISE.

# Conditions préalables

## Exigences

Cisco recommande de connaître les sujets suivants :

- Gestionnaire de châssis de pare-feu sécurisé (FCM)
- Cisco Identity Services Engine (ISE)
- Authentification RADIUS

## Composants utilisés

- Appareil de sécurité Cisco Firepower 4110 FXOS v2.12
- Correctif 4 de Cisco Identity Services Engine (ISE) v3.2

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.

## Configurer

## Configurations

## Gestionnaire de châssis de pare-feu sécurisé

Étape 1. Connectez-vous à l'interface utilisateur graphique du Firepower Chassis Manager. Étape 2. Accéder aux paramètres de la plate-forme

verview Interfaces	s Logical Dev	vices Security Engine Platform	Settings				System	Tools Help adn
FPR4K-1-029A78 Model: Cisco Fi	B 172.16.	0.130 9 Security Appliance Version:	2.12(0.8) Of	perational State: <b>O</b> J	perable	Chassis Upt	time 00:06:02	:19 <b>心</b> の①
ONSOLE MGMT USB	-	Power 2 - Removed	Network Module 1	Retwork M	dodule 2 : Empty	Network	: Module 3 : Emp	ty
FAULTS 3(3) © CRITICAL	<b>0(0)</b>	INTERFACES 3 5 OOWN (1) UP	INSTANCES O O DOWN	1 10 UP	LICENSE Smart Agent UNREGISTERED	INVENTORY 1(1) Security Engine	<b>6(6)</b> ☆ Fans a	1(2) Power Supplies
Select All Faults Cancel	Selected Faults A	cknowledge				k		
Severity	Description			Cause	Occurrence	Time		Acknowledged
CRITICAL	FPGA version I	ower than 2.00 is detected. A critical upgrad	le from the firmwar	fpga-upgrade-requi	ired 1	2022-02-20T22	:32:45.641	no 👔
	Network Modu	le 3 removed when in online state. It is reco	mmended to set m	module-suprise-rem	oval 1	2022-11-07T09	:03:02.022	no
uccessful Login in last 24 hr	rs - <u>View Details</u>   Th	u Feb 01 2024 at 17:00:55 from - 172.16.0.35						ر، ۱۱، از

Étape 3. Dans le menu de gauche, cliquez sur AAA. Sélectionnez Radius et ajoutez un nouveau fournisseur RADIUS.

Overview Interfaces Logica	I Devices Security Engine	Platform Settings			System	Tools Help	admin
NTP	LDAP RADIUS TACACS						
SSH							
SNMP	Properties						
HTTPS	Timeout:* 5 Secs						
► AAA							
Syslog	Retries:* 1						
DNS	RADIUS Providers						
FIPS and Common Criteria						0	Add
Access List	Hestname	Order	Sar	nulsa	Auth Dort		
MAC Pool	nostname	Order	Ser	rvice	Auth Port		
Resource Profiles							
Network Control Policy							
Chassis URL							
	Save Cancel						
	Carre Conver						
8 Successful Login in last 24 hrs - View De	tails   Thu Feb 01 2024 at 17:00:55 fro	n - 172.16.0.35					

Étape 4. Remplissez le menu d'invite avec les informations demandées du fournisseur Radius. Click OK.

Overview Interfaces Logic	al Devices Security Engir	e Platform Settings			System Tools Help admin
NTP SSH SNMP HTTPS AAA Syslog DNS FIPS and Common Criteria Access List MAC Pool	LDAP RADIUS TACAO Properties Timeout:* 5 Sec Retries:* 1 RADIUS Providers Hostname	s Add RADIUS Provider Hostname/FQDN/IP Address:* Order:* Kee	172.16.0.12 lowest-available	Image: Set Market Auth P	Add
Resource Profiles Network Control Policy Chassis URL		Key: Confirm Key: Authorization Port:* Timeout:* Retries:*	інні і 1812 5 1 ОК	Set: No	
8 Successful Login in last 24 hrs - <u>View I</u>	Save Cancel	from - 172.16.0.35			ոլիսիս ciśco

Étape 5. Accédez à Système > Gestion des utilisateurs

Overview Interfaces Logi	cal Devices Security Engine	Platform Settings			System <sup>1</sup> Tools	Help admin
			Configuratio	n Licensing	Updates User	Management
SSH SNMP HTTPS AAA	Properties Timeout:* 5 Secs					1
Syslog DNS FIPS and Common Criteria	Retries:* 1 RADIUS Providers					Add
Access List	Hostname	Order	Service	Auth Port		
Resource Profiles Network Control Policy Chassis URL	172.16.0.12	1	authorization	1812		
	Save					
wascript:void(0) last 24 hrs - View	Details   Thu Feb 01 2024 at 17:00:55 fro	m - 172.16.0.35				cisco

Étape 6. Cliquez sur l'onglet Paramètres et définissez l'authentification par défaut dans le menu déroulant sur Radius, puis faites défiler vers le bas et enregistrez la configuration.

Overview Interfaces Logica	al Device	es Security Engine Platform Settings			System	Tools Help admin
			Configuration	Licensing	Updates	User Management
Local Users Settings						
Default Authentication	Local Local	*Local is fallback authentication method				
Console Authentication	RADIUS LDAP	• -				
Remote User Settings	TACACS	;				
Remote User Role Policy	None	No-Login				
Local User Settings						
Password Strength Check	Enab	le				
History Count	5	(0-disabled,1-15)				
Change Interval	48	🕑 (1-730 hours)				
Change Count	2	(1-10)				
No Change Interval		(1-730 hours)				
Days until Password Expiration	0	(0-never,1-9999 days)				
Password Expiration Warning Period	0	(0-9999 days)				
Expiration Grace Period	0	(0-9999 days)				
Password Reuse Interval	0	(0-disabled,1-365 days)				
Session Timeout(web UI,ssh,telnet)	600	(0-never.3600 seconds)				
8 Successful Login in last 24 hrs - View De	<u>etails</u>   Thu	Feb 01 2024 at 17:00:55 from - 172.16.0.35				cisco



Remarque : la configuration de FCM est terminée à ce stade.

## **Identity Service Engine**

Étape 1. Ajoutez un nouveau périphérique réseau.

Accédez à l'icône Burger ≡ située dans l'angle supérieur gauche > Administration > Network Resources > Network Devices > +Add.

≡ Cisco ISE			Administration · Netv	work Resources			🔺 Evaluation Mode 18 Days Q 🕜 🕫 🚳
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors More $\vee$
Network Devices							
Default Device	Network	< Devices					
Device Security Settings							Selected 0 Total 0 🧭 🚳
	2 Edit + Ad	td 🚺 Duplicate 🕁 Import	🗄 Export 🗸 🛛 👌 Generate P/	AC 🔋 Delete 🗸			$\sim$ $\gamma$
	Name	e 🔿 IP/Mask	Profile Name	Location Type		Description	
				No data available			

Étape 2. Renseignez les paramètres demandés sur les informations relatives aux nouveaux périphériques réseau.

- 2.1 Cochez la case RADIUS
- 2.2 Configurez la même clé secrète partagée que dans la configuration FCM Radius.
- 2.1 Faites défiler la page vers le bas et cliquez sur Submit.

E Cisco ISE	Administration - Network Resources	A Evaluation Mode 18 Days	2 © 5	2 O	
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Servers Sequences NAC Managers External MDM pxGrid Direct Connectors Location Services				
Network Devices Default Device Device Security Settings	Network Devices Network Devices Name FPR-4110				
	Description				
	Device Profile         III. Caco         V           Model Name         \$PR-4110         V				
	Software Version 2.12 V Network Device Group				
	Location All Locations V Set To Default UPSEC Is PSEC Device V Set To Default Device Type All Device Types V Set To Default				
	RADIUS Authentication Settings				
	RADIUS LDP Settings Protocol RADIUS Shared Secret Bhow				
	Use Second Shared Secret     Secret     Secret				

Étape 3. Vérifiez que le nouveau périphérique figure sous Network Devices (Périphériques réseau).

≡ Cisco ISE		Administration - Netv	work Resources			🔺 Evaluation Mode 18 Days Q 💿 😡	٥
Network Devices	Network Device Groups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors More $\vee$	
Network Devices	Notwork Dovices						
Default Device	Network Devices						
Device Security Settings						Selected 0 Total 1 🤗 🚳	
	🖉 Edit 🕂 Add 🚺 Duplicate 🕁 Import	📩 Export \vee 🛛 👌 Generate PA	C 🔋 Delete 🗸			$_{AB} \sim - \nabla$	
	Name ^ IP/Mask Profile	Name Location	Туре	Description			
	FPR-4110 172.16.0 # Cisc	All Locations	All Device Types				

Étape 4. Créez les groupes d'identités utilisateur requis. Accédez à l'icône Burger ≡ située dans l'angle supérieur gauche > Administration > Identity Management > Groups > User Identity Groups > + Add

■ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💮 🕫 🗇
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 8 0	_	Selected 0 Total 9 🧭 🔞
> 🛅 Endpoint Identity Groups	Edit + Add     Delete      Gui import     Gui Export     Continue     Conti	AI 🗸 🗸
> 🛅 User Identity Groups	Name   Description	
	ALL_ACCOUNTS (default)     Default ALL_ACCOUNTS (default) User Group	
	Default Employee User Group	
	GROUP_ACCOUNTS (default)     Default GROUP_ACCOUNTS (default) User Group	
	Carter and the set of	
	CouestType_Daily (default) Identity group mirroring the guest type	
	☐ ∯ GuestType_SocialLogin (default) Identity group mirroring the guest type	
	□ ≹ GuestType_Weekly (default) Identity group mirroring the guest type	
	ACCOUNTS (default)     Default OWN_ACCOUNTS (default) User Group	

Étape 5. Définissez un nom pour le groupe d'identités d'utilisateur Admin et cliquez sur Submit afin d'enregistrer la configuration.

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💿 👼 🚭
Identities Groups External Id	entity Sources Identity Source Sequences Settings	
Identity Groups	User identify Groups > New User identify Group Identity Group * Name PPR-4110-Admin User Group for Administrato: Description	ancel

5.1 Répétez la même procédure pour les utilisateurs ReadOnly.

E Cisco ISE	Administration - Identity Management	🛦 Evaluation Mode 18 Days Q 🕥 🗔 🗇
Identities Groups External Iden	tity Sources Identity Source Sequences Settings	
Edentity Groups SQ < 188 ♥ > Endpoint Identity Groups > User Identity Groups	User Identity Groups > New User Identity Group  * Name  FPR-4110-ReadOnly User Group for Read Only Users. Description	Submit

Étape 6. Vérifiez que les nouveaux groupes d'utilisateurs s'affichent sous Groupes d'identités d'utilisateurs.

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q 💮 🖉
dentities Groups External Ide	ntity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
C B O	🖉 Elitt 🕂 Add 🕘 Delate 🗸 🕁 Import 🖒 Export 🗸	Selected 0 Total 11 🧷 🔕
> 🗅 User Identity Groups	Name	
	ALL_ACCOUNTS (default)     Default ALL_ACCOUNTS (default) User Group	
	Default Employee User Group	
	User Group for Administrator.	
	User Group for Read Only Users.	
	GROUP_ACCOUNTS (default)     Default GROUP_ACCOUNTS (default) User Group	
	KoustType_Contractor (default)     Identity group mirroring the guest type	
	GuestType_Daily (default)     Identity group mirroring the guest type	
	KoustType_SocialLogin (default)     Identity group mirroring the guest type	
	KoustType_Weekly (default)     Identity group mirroring the guest type	
	KOWN_ACCOUNTS (default)     Default OWN_ACCOUNTS (default) User Group	
	C Mittation	

Étape 7. Créez les utilisateurs locaux et ajoutez-les à leur groupe correspondant. Accédez à l'icône burger ≡ > Administration > Identity Management > Identities > + Add.



7.1 Ajout de l'utilisateur avec des droits d'administrateur Définissez un nom, un mot de passe et attribuez-le à FPR-4110-Admin, faites défiler vers le bas et cliquez sur Submit pour enregistrer les modifications.

≡ Cisc	o ISE				Administration - Identity Management	A Evaluation Mode 18 Days	209	8 Ø
Identities	Groups	External Identity Sources	Identity Source Sequences	Settings				
Users Latest Manual Ne	hvort Scan Res.	V Network Access Usename Status Account Name Atlas Emai V Passwords Password Type: Im Password Type:	User cisco, semin Consist ~ emarticiaes. ~					
		Password will expi Never Expires () * Login Password Enable Password	e in 60 days assword	Re-Enter Password	Generate Password     ()       Generate Password     ()			
		User Informatio     Account Option     Account Disable	n is e Policy					
		✓ User Groups	min 🗸 🖲 🌒					

7.2 Ajouter l'utilisateur avec des droits ReadOnly. Définissez un nom, un mot de passe et attribuez-le à FPR-4110-ReadOnly, faites défiler vers le bas et cliquez sur Submit pour enregistrer les modifications.

E Cisco ISE		Administration - Identity Management	Liveluation Mode 18 Days Q. () (28 ()
Identities Groups Ex	ternal Identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	Network Access User     Useramia cisce,readouty Status:     Control Name Alias     Email		
	✓ Passwords Password Type: Internet Users.      ✓ Password Lifetime:     With Equiption ①     Password all exprise 16 days     Never Explores ①		
	Password Re-Enter Password * Login Password Enable Password	Generate Password     O       Generate Password     O	
	User Information     Account Options     Account Disable Policy		
	✓ User Groups E FPR-4110-ReadOnly  ③ ●		

7.3 Vérifier que les utilisateurs se trouvent sous Network Access Users.



Étape 8. Créez le profil d'autorisation pour l'utilisateur Admin.

Le châssis FXOS comprend les rôles d'utilisateur suivants :

- Administrateur Accès complet en lecture et en écriture à l'ensemble du système. Ce rôle est attribué par défaut au compte d'administrateur par défaut et ne peut pas être modifié.
- Lecture seule : accès en lecture seule à la configuration du système sans privilèges permettant de modifier l'état du système.
- Opérations : accès en lecture et écriture à la configuration NTP, à la configuration Smart Call Home pour Smart Licensing et aux journaux système, y compris les serveurs et les pannes syslog. Accès en lecture au reste du système.
- AAA : accès en lecture-écriture aux utilisateurs, aux rôles et à la configuration AAA. Accès en lecture au reste du système

Attributs pour chaque rôle :

cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operations"

cisco-av-pair=shell : roles="lecture seule"



Remarque : cette documentation définit uniquement les attributs admin et lecture seule.

Accédez à l'icône Burger ≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

Définissez un nom pour le profil d'autorisation, laissez le type d'accès comme ACCESS\_ACCEPT et sous Advanced Attributes Settings ajoutez cisco-av-pair=shell : roles="admin" avec et cliquez sur Submit.

≡ Cisco I	SE	Policy - Policy Elements	A Evaluation Mode 17 Days	Q	0 57	0
Dictionaries	Conditions	Results				
Authentication	>	Authorization Profile Authorization Profile				
Authorization Profil	les	* Name EPR-4110-Admiss				
Downloadable ACL	La	Description				
Profiling	>	* Access Type ACCESS_ACCEPT V				
Client Provisioning	>	Network Device Profile  Case  Case				
		ACL IPv6 (Fitter-ID)				
		Advanced Attributes Settings <sup>III</sup> Cisco:cisco-av-pair v * shelt:roles=*admin* v = +				
		Attributes Details Access type = ACCESS_ACCET dice-ar-pair = dheltrobes="admini"				
			Submit		Cancel	

8.1 Répétez l'étape précédente pour créer le profil d'autorisation pour l'utilisateur ReadOnly. Cette fois, créez la classe Radius avec la valeur read-only Administrator.

= Cisco ISE	Policy - Policy Elements	Evaluation Mode 18 Days	Q (2)	59	٥
Dictionaries Conditions	Results				
Authentication >	Authorization Profiles > New Authorization Profile Authorization Profile				
Authorization Profiles Downloadable ACLs	* Name FPR+4110-ReadOnly				
	Description				
Profiling					
Posture	ACCESS_ACCEPT V				
Client Provisioning	Network Device Profile 🗰 Cisco 🗸 🕀				
	Service Template  Track Movement  O Apentless Posture  O Passive Identity Tracking  O O				

C ACL IPv6 (Filter-ID)	
Advanced Attributes Settings	
Attributes Details     Access Type = ACCES, ACCEPT	
dice-ar-pair = shelt-tride="read-only"	

Étape 9.Créez un ensemble de stratégies correspondant à l'adresse IP FMC. Cela permet d'empêcher d'autres périphériques d'accorder l'accès aux utilisateurs.

Accédez à  $\equiv$  > Policy > Policy Sets > Add icon sign dans l'angle supérieur gauche.

≡ Cisco IS	SE			Policy · Policy Sets				A Evaluation Mode	17 Days	Q (1)	6 B
Policy Sets							Reset	Reset Policyset	Hitcounts		Save
Status	Policy Set Name	Description	Conditions			A	llowed Protocol	/ Server Sequenc	e Hits	Actions	View
Q Search											
				+							
۰	Default	Default policy set					Default Network /	ccess / -	58		>
									Reset		Save

9.1 Une nouvelle ligne est placée en haut de vos ensembles de stratégies. Cliquez sur l'icône Ajouter pour configurer une nouvelle condition.

🕘 Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequ	ence H	Hits Acti	ns View
Q Searc								
٥	New Policy Set 1			+	Select from list	+	0	>
٥	Default	Default policy set			Default Network Access	+ •	sa -{ĝ;	>

9.2 Ajoutez une condition supérieure pour l'attribut RADIUS NAS-IP-Address correspondant à l'adresse IP FCM, puis cliquez sur Use.

Library	Library											
Search by Name												
	F 🕹											
:: 🖻 sG												
E Catalyst_Switch_Local_Web_Authentication												
🗄 📄 Radius												
: Switch_Local_Web_Authentication												
B Switch_Web_Authentication												
:: B Wired_802.1X												
E Wired_MAB												
E Wireless_802.1X												
E Wireless_Access												
H Wireless_MAB												
# B WLC_Web_Authentication												

Editor

Ŷ

Radius-NAS-IP-Address Equals v Attri	Selec	t attribute for conditio	n 2 8 8 0	1	<b>)</b> t 🕈	X Wrong value	©
Set to 'is not'		Dictionary	Attribute	ID	Info	Duplicate	
		All Dictionaries	Attribute	ID			>
	۰	Microsoft	MS-User-IPv4-Address	61	0		
	۰	Network Access	ISE Host Name		0		
	•	Radius	DNS-Server-IPv6-Address	169	0		
	•	Radius	Framed-IP-Address	8	0		Save
	•	Radius	Framed-IPv&-Address	168	0	1	
	•	Radius	NAS-IP-Address	4	0		
	۰	Radius	Stateful+IPv6+Address+Pool	172	0		



## 9.3 Une fois terminé, cliquez sur Enregistrer.

≡ 0	Cisco IS	SE		Policy - Policy Sets		A Evaluation Mode	17 Days	Q (0)	6 R
Policy	Sets				Reset	Reset Policyset	Hitcounts		Save
۲	Status	Policy Set Name	Description	Cenditions	Allowed Protocol	s / Server Sequenc	e Hits	Actions	View
Q	Search								
	۰	New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0.130	Default Network	Access 🛛 🗸 🕂		(2)	>
	۰	Default	Default policy set		Default Network	Access 🥒 🕂	58		>
								_	
							Reset		Save



Conseil : pour cet exercice, nous avons autorisé la liste des protocoles d'accès réseau par défaut. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

Étape 10. Affichez le nouvel ensemble de règles en cliquant sur l'icône > située à la fin de la ligne.

Policy Sets			Reset	Reset Policyset Hitco	unts	Save
Status Policy Set Name	Description	Conditions	Allowed Protocol	s / Server Sequence H	its Actions	s View
Q Search						
New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0.130	Default Network	Access 🛛 🗸 +	¢	>

10.1 Développez le menu Stratégie d'autorisation et cliquez sur (+) pour ajouter une nouvelle condition.

$\lor$ A	Authorization Policy (1)									
				Results						
6	Status Rule Name	Conditions		Profiles	Security Groups	Hits	Actions			
	Q Search									
	Authorization Rule 1		+	Select from list	Select from list	+	\$			

10.2 Définissez les conditions pour faire correspondre le groupe DictionaryIdentity avecAttributeName Equals User Identity Groups : FPR-4110-Admins(le nom de groupe créé à l'étape7) et cliquez sur Use.

Library		Editor									
Search by Name			Identity0	iroup-Na	me						
	9 1 0 t 7		Equals	Sele	ct attribute for conditio	n			×		
ii 📴 sa			Set to 'Is	•	11 O 🔹 🔍 🖵	¥ 8 ∞ 2 ≞	01	0 E 🕈		Duplicate	Save
🗄 📑 BYOD_is_Registered					Dictionary	Attribute	ID	Info			
: Catalyst_Switch_Local_Web_Authentication					All Dictionaries	Attribute	ID				
E Compliance_Unknown_Devices				-	IdentityGroup	Description					
E Compliant_Devices					IdentityGroup	Name		0			
EAP-MSCHAPv2					InternalUser	IdentityGroup		0			
🗄 🃒 EAP-TLS					PassiveID	PassiveID_Groups		0			
🗄 📵 Guest_Flow				-	administrator	ExternalGroups		0			
E MAC_in_SAN											
E Network_Access_Authentication_Passed											
: Non_Gisco_Profiled_Phones											
E Non_Compliant_Devices											
🗄 📴 Radius											
1 🗇 Raitch Local Web Authentication											

Conditions Studio					0 ×	
Library		Editor				
Search by Name			IdentityGroup Name		۲	
Q         Q         B	10 t 🕈		Equals Vier Identity Groups:FPR-4110-			
1 1 50			Aumin		4	
E BYOD_is_Registered			Set to 'ts not'	Duplicate Sa		
E Catalyst_Switch_Local_Web_Authentication			NEW AND OR			
E Compliance_Unknown_Devices						
E Compliant_Devices						
EAP-MSCHAPv2						
🗄 🔝 EAP-TLS						
: [] Guest_Flow						
🗄 📳 MAC_In_SAN						
E Network_Access_Authentication_Passed						
: [] Non_Cisco_Profiled_Phones						
I INon_Compliant_Devices						
🗄 💽 Radius						
B Switch_Local_Web_Authentication	0					.
			Close	Use		

Étape 10.3 Validez la nouvelle condition configurée dans la stratégie d'autorisation, puis ajoutez un profil utilisateur sous Profils.

~ Authorization	Policy (1)								
<ul> <li>Status</li> </ul>	Rule Name	Conditions	Ri	esults		Security Groups		Hits	Actions
Q Search						_			
۰	Authorization Rule 1	R IdentityGroup Name EQUALS User Identity Groups FPR-4110-Admin	F	PR-4110-Admins ×	<u>~</u> +	Select from list	$\sim$ +		٢
۰	Default		D	lenyAccess	/+	Select from list	/+	0	٨

Étape 11. Répétez le même processus à l'étape 9 pour les utilisateurs en lecture seule et cliquez sur Enregistrer.

Vérifier

1. Essayez de vous connecter à l'interface utilisateur graphique de FCM à l'aide des nouvelles informations d'identification Radius

- 2. Accédez à l'icône Burger = > Operations > Radius > Live logs.
- 3. Les informations affichées indiquent si un utilisateur s'est connecté avec succès.

■ Cisco ISE		Operations - RADIUS	4	Evaluation Mode 17 Days Q 🕥 58 🕼
Live Logs Live Sessions				
Misconfigured Supplicants 🕥	Misconfigured Network Devices 🔘	RADIUS Drops 🕓	Client Stopped Responding 🕠	Repeat Counter 💿
0	0	1	0	0
🖉 Schwart Report Counts 🖒 Datert To 🗸			Befrydt Hever	Show Latest 20 records         Within Last 3 hours         v           Filter         V         0
Time Status Details Reg	pea Identity Endpoint ID Endpoint	Authenti Authoriz IP Address Netw	twork De Device Port Identity Group Posture Server	Mdm Ser IMEISV Usecasi
×	identity Endpoint ID Endpoint Pr	Authenticat Authorizatic IP Address	twork Device PortIdentity GroupPosture StaServer	Mdm Serve INEISV Usecase
Feb 03, 2024 01:51:51.0	cisco_readonly	New Polic New Polic FPR+4110 FPR+	4110 User Identity Group: marpatini5E	
Feb 03, 2024 01:50:48.9 🖬 👸	cisco_admin	New Polic New Polic FPR-4110 FPR-	1-4110 User Identity Group: marpatinISE	

4. Validez le rôle d'utilisateur connecté à partir de l'interface de ligne de commande Secure Firewall Chassis.

	FPR4K-1-029A78B#	scope se		
	security	server	service-pr	ofile
	FPR4K-1-029A78B#	scope security		
	FPR4K-1-029A78B /	/security # show	remote-user	detail
	Remote User cisco	o_admin:		
	Description:			
	User Roles:			
	Name: adm	m1n		
	Name: rea	ad-only		
	FPR4K-1-029A78B	/security #		
I		,		

# Dépannage

1. Sur l'interface utilisateur graphique d'ISE , accédez à l'icône burger ≡ > Operations > Radius > Live logs.

- 1.1 Vérifier si la demande de session de journalisation atteint le noeud ISE.
- 1.2 Pour connaître l'état d'échec, consultez les détails de la session.

=	Cis	co ISE					0	perations • R	ADIUS							🛦 Evalu	ation Mode 18 Day	• Q (	2	•
Liv	e Logs	Live Sessions																		
	Misco	nfigured Supplicants 🕕			Mis	configured Network	Devices 🕕		RA	DIUS Drops 🤇			c	lient Stoppe	d Responding 🤇			Repea	t Coun	ter 🕕
		0				1				1					0				3	
	ø	🕤 Reset Repeat Counts 🔹	🖞 Expert To 🗸												Refresh Never	↓ Show Late:	it 20 records 🔨	Within Last 3	hours	•
		Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address	Net	twork De	Device Port	Identity Group	Posture	Server	Md	lm Sei
	$\times$				~	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	√ Ne	twork Device	Device Port	Identity Group	Posture Sta	Server	Md	im Sen
		Feb 02, 2024 07:32:18.8	۰	ò		cisco_admin			Default >>	Default			FPR	-4110		User Identity Group		marpatinISI		
		Feb 02, 2024 07:23:20.1		0		cisco_readonly			Default >>	Default >>	PermitAcc		FPR	-4110		User Identity Group	. 1	marpatin/SI		
		Feb 02, 2024 07:15:32.2		à		cisco_admin			Default >>	Default >>	PermitAcc		FPR	-4110		User Identity Group	e 1	marpatin/SI		

2. Pour les demandes qui n'apparaissent pas dans les journaux Radius Live , vérifiez si la demande UDP atteint le noeud ISE par le biais d'une capture de paquets.

Accédez à l'icône Burger ≡ > Operations > Troubleshoot > Diagnostic Tools > TCP dump. Ajoutez une nouvelle capture et téléchargez le fichier sur votre machine locale afin de vérifier si les paquets UDP arrivent sur le noeud ISE.

2.1 Remplissez les informations demandées, faites défiler la page vers le bas et cliquez sur Save.



#### 2.2 Sélection et démarrage de la capture

E Cisco ISE	Cisco ISE Operations - Troubleshoot												
Diagnostic Tools Download	Diagnostic Tools Download Logs Debug Wizard												
General Tools	The	TCP Dump utility page is to m	nonitor the contents of pack	ets on a network interface an	d troubleshoot problems on	the network as	they appe	ar					
RADIUS Authentication Troubl												Rows/Page 1 →  < < 1 / 1 > >  Go 1 Total Rows	
Execute Network Device Com Evaluate Configuration Validat	ø	Add 2 Edt () Train 1	Start O Stop	Download								rae 😪 🛛 🕀	
Posture Troubleshooting		Host Name	Network Interface	Filter	File Name	Reposito	File S	Number of	Time Limit	Promiscuous M	Status		
Agentiess Posture Troublesho EndPoint Debug	8	marpatin/SE.marpatin.com	GigabitEthemet 0 [Up, Run	ip host 172.16.0.130	marpatinISE_GigabitEthernet		10	1	5	false	RUNNING		
TCP Dump													
Session Trace Tests													
TrustSec Tools													

2.3 Tentative de connexion au châssis du pare-feu sécurisé pendant l'exécution de la capture ISE

2.4 Arrêtez le vidage TCP dans ISE et téléchargez le fichier sur un ordinateur local.

2.5 Analyse du trafic généré.

Résultat attendu :

Paquet n° 1. Requête du pare-feu sécurisé au serveur ISE via le port 1812 (RADIUS) Paquet n° 2. Réponse du serveur ISE acceptant la requête initiale.



#### 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.