# 为安全防火墙机箱管理器(FCM)配置ISE RADIUS身份验证

# 目录

# 简介

本文档介绍如何为带有ISE的Secure Firewall Chasis Manager配置RADIUS授权/身份验证访问的过程。

# 先决条件

#### 要求

思科建议了解以下主题:

- 安全防火墙机箱管理器(FCM)
- 思科身份服务引擎(ISE)
- RADIUS 身份验证

使用的组件

- 思科Firepower 4110安全设备FXOS v2.12
- 思科身份服务引擎(ISE) v3.2补丁4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采 用原始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 配置

#### 配置

#### 安全防火墙机箱管理器

步骤1:登录到Firepower机箱管理器GUI。 第二步:导航到平台设置

verview Interfaces	s Logical Dev	vices Security Engi	ne Platform	Settings				Sys	tem Tools Help adn
FPR4K-1-029A78 Model: Cisco Fi	B 172.16.	0.130 Security Appliance	Version:	2.12(0.8) Op	erational State: O	perable	Chassi	s Uptime 00:0	6:02:19 <b>じ</b> の①
Network Module 1       ONSOLE MGMT       USB       Power 1 - Running       Power 2 - Removed									
FAULTS 3(3) ⊗ CRITICAL	<b>0(0)</b>	INTERFACES 3 ODWN	5 🕜 UP	INSTANCES O O DOWN	1 (*) UP	LICENSE Smart Agent UNREGISTERED	INVENTORY 1(1) Security Engine	<b>6(6)</b> ☆ Fans	1(2) ⇒ Power Supplies
Select All Faults Cancel	Selected Faults A	cknowledge						•	
Severity	Description				Cause	Occurrence	1	lime	Acknowledged
CRITICAL	FPGA version lo	ower than 2.00 is detected	. A critical upgrad	e from the firmwar	fpga-upgrade-requ	ired 1	2022-02-20	DT22:32:45.641	no
	Network Modul	le 3 removed when in onli	ne state. It is recor	nmended to set m	module-suprise-rem	noval 1	2022-11-0	7T09:03:02.022	no
Successful Login in last 24 hr	rs - <u>View Details</u>   Th	u Feb 01 2024 at 17:00:55 f	rom - 172.16.0.35						،،ا،، cise

第三步:从左侧菜单中单击over AAA。 选择Radius并Add一个新的RADIUS提供程序。

Overview Interfaces Logic	cal 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					Add
Access List				l	
MAC Pool	Hostname	Order	Service	Auth Port	
Resource Profiles					
Network Control Policy					
Chassis URL					
	Save Cancel				
8 Successful Login in last 24 hrs - View I	Details   Thu Feb 01 2024 at 17:00:55 from	- 172.16.0.35			ri ri ri cisco

第四步:使用Radius提供程序的请求信息填写提示菜单。Click OK.

Overview Interfaces Logi	cal Devices Security Engin	e Platform Settings			System Tools Help	admin
NTP SSH SNMP HTTPS AAA	LDAP RADIUS TACAC	S Add RADIUS Provider		(7) X		
Sysiog DNS FIPS and Common Criteria Access List MAC Pool Resource Profiles Network Control Policy Chassis URL	RADIUS Providers Hostname	Hostname/FQDN/IP Address:* Order:* Key: Confirm Key: Authorization Port:* Timeout:* Retries:*	172.16.0.12 lowest-available ••••••• 1812 5 1	Set: No	Auth Port	Add
8 Successful Login in last 24 hrs - <u>View I</u>	Save Cancel	rom - 172.16 0.35	ОК	Cancel		altatu cisco

#### 第五步:导航到系统>用户管理

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

第六步:点击Settings选项卡,将下拉菜单中的Default Authentication设置为Radius,然后向下滚动 并保存配置。

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



## 身份服务引擎

步骤1:添加新的网络设备。

导航到位于左上角≡汉堡图标> Administration > Network Resources > Network Devices > +Add。



第二步:填写有关新网络设备信息的请求参数。

2.1选中RADIUS复选框

2.2配置与FCM Radius配置相同的共享密钥。

2.1向下滚动并点击Submit。

🔳 Cisco ISE		Administration	- Network Resources	🛦 Evaluation Moder 18 Days 🔍 🛞 🕼 🗇
Network Devices	Network Device Groups Network Device Profiles Exte	ernal RADIUS Servers RADIUS Server Sequences	NAC Managers External MDM pxGrid Direct Connectors	Location Services
Network Devices Default Device Device Security Settings	Network Devices List > New Network Device Network Devices			
	Name FPR-4110 Description			
	1 PAdress	<sup>1</sup> <u>32</u> O		
	Device Profile Cisco	<u> </u>		
	Model Name FPR-4110	~		
	Software Version 2.12	~		
	Location All Locations	😒 Set To Default		
	IPSEC Is IPSEC Device	✓ Set To Default		
	Device Type All Device Types	Set To Default		
	RADIUS Authentication Settings			
	RADIUS UDP Settings			
	Protocol RADIUS	Electric Control of Co		
	Use Second Shared Secret ()	000/00		
	Second Shared Secret	Show		

#### 第三步:验证新设备是否显示在Network Devices下。

≡ Cisco ISE	Administration - Network 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	// Edit 🕂 Add 📋 Duplicate 🕁 Import む Export 🗸 🔒 Generate PAC 🌘 Delete 🗸		Selected 0 Total 1 🔗 🚳
	□ Name ∧ IP/Mask Profile Name Location Type	Description	
	FPR-4110 172.16.0 at Cisco 🕤 All Locations All Device Types		

第四步: 创建所需的用户身份组。导航到位于左上角≡汉堡图标> Administration > Identity Management > Groups > User Identity Groups > + Add

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 ⊘ 🕫 🗇
Identities Groups External Ide	intity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 18 O	_	Selected O Total 9 😥 🗔
> 🗁 Endpoint Identity Groups	Z Edit + Add     O Delete      ✓	All $\checkmark$ $\nabla$
> 🗅 User Identity Groups	Name   Description	
	KALL_ACCOUNTS (default)     Default ALL_ACCOUNTS (default) User Group	
	Default Employee User Group	
	GROUP_ACCOUNTS (default)     Default GROUP_ACCOUNTS (default) User Group	
	□ ≹ GuestType_Contractor (default) Identity group mirroring the guest type	
	□ ≹ GuestType_Daily (default) Identity group mirroring the guest type	
	☐ Ž GuestType_SocialLogin (default) Identity group mirroring the guest type	
	C & GuestType_Weekly (default) Identity group mirroring the guest type	
	ACCOUNTS (default)     Default OWN_ACCOUNTS (default) User Group	

### 第五步:为管理员用户身份组设置名称,然后点击提交以保存配置。

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💿 👼 🚭
Identities Groups External Id	entity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups > New User Identity Group Identity Groups * Name FPR-4110-Admin User Group for Administrator. Description	Cancel

## 5.1对只读用户重复相同的过程。

≡ Cisco ISE			Administration - Identity M	Management		A Evaluation Mode 18 Days	2 0	Ø 6	
Identities Group	s External Iden	tity Sources	Identity Source Sequences Settings						
Identity Groups	Identity Groups	User Identity Gro Identity Gro * Name Description	ps > New User Identity Group IP FPR-4110-ReadOnly User Group for Read Only Users:		Submit	Cancel			

第六步:验证新的用户组显示在User Identity Groups下。

E Cisco ISE	Administration · Identity Manage	ment 🛕 Evaluation Mode 18 Days Q 💿 🖉
Identities Groups External Ide	tity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 12 Ø		Selected 0 Total 11 😢 🍥
> 🛅 Endpoint Identity Groups	🖉 Edit 🕂 Add 🔋 Delete 🗸 🕁 Import 🖒 Export 🗸	$\nabla$ $\sim$ IA
> 🛅 User Identity Groups	Name	
	ALL_ACCOUNTS (default)     Default ALL_ACCOUNTS (default)	) User Group
	Default Employee User Group	
	KFR-4110-Admin     User Group for Administrator.	
	KPR-4110-ReadOnly     User Group for Read Only Users.	
	GROUP_ACCOUNTS (default)     Default GROUP_ACCOUNTS (default)	ault) User Group
	GuestType_Contractor (default)     Identity group mirroring the guest	t type
	☐ ≹ GuestType_Daily (default) Identity group mirroring the gues	t type
	GuestType_SocialLogin (default)     Identity group mirroring the gues	t type
	GuestType_Weekly (default)     Identity group mirroring the guest	t type
	ACCOUNTS (default)     Default OWN_ACCOUNTS (default)	It) User Group
	Radius	

步骤 7. 创建本地用户并将其添加到其往来行组。 导航到汉堡图标≡ > Administration > Identity Management > Identities > + Add。

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q 🛛 🖓
Identities Groups Ex	ternal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected 0 Total 0 💋 🚳
	🖉 Edit 🕂 Add 🛞 Change Status 🗸 🕁 Import 🛆 Export 🗸 🚯 Delete 🗸 🌔 Duplicate	$\sim$ V
	Status Username  Description First Name Last Name Email Address User Identity Groups Admin	
	No data avallable	

7.1添加具有管理员权限的用户。设置名称和口令,并将其分配给FPR-4110-Admin,然后向下滚动 并单击Submit以保存更改。

≡ Cisc	o ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q 💿 🕼 💿
Identities	Groups	External Identity Sources Identity Source Sequences Settings		
Users Latert Manual Ne	twork Scan Res	V Network Access User Userame Usename Cico_admin Status Cicout Name Alas Cimat V Passwords		
		Passed Difference With Equitation © Passed Biology Passed Biology Passed Biology		
		* Logio Passerot	Generate Password         O           Generate Password         O	
		User Information     Account Options     Account Disable Policy		
		∨ User Groups E FPR-4110-Admin v ⊙		

7.2添加具有只读权限的用户。设置名称和口令,并将其分配给FPR-4110-ReadOnly,然后向下滚 动并单击Submit以保存更改。

E Cisco ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q. 💿 🕼 🚭
Identities Groups Ex	ternal identity Sources Identity Source Sequences Settings		
User Loter Manuel Noteon Scon Res	✓ Network Access User     * Usersano     * Usersano     Santa     Santa     Could Name Allas     Could     Cou		
	Passavord Type: Veternel Univer v Passavord Lifetime: O With Equation 0: Passavord anii reapire n 66 days O Never Expires 0:		
	Password Re-Enter Password * Login Password Chable Password	Generate Password     O       Generate Password     O	
	User Information     Account Options     Account Disable Policy		
	✓ User Groups E FPR-4110-ReadONy		

7.3验证用户是否处于网络访问用户下。

😑 Cisco ISE	Ad	Iministration - Identity Management	🛦 Evaluation Mode 18 Days Q 💿 🕼	0
Identities Groups Exte	nal Identity Sources Identity Source Sequences Settings			
Users Latest Manual Network Scan Res	Network Access Users			
			Selected 0 Total 2 👩 🧔	
	$ / \ {\rm Ent} \ \ + \ {\rm Add} \ \ \otimes \ {\rm Change Status} \ \lor \ \ \oplus \ {\rm Import} \ \ \oplus \ {\rm Export} \ \lor \ \ \otimes \ {\rm Change Status} \ \lor \ \ \oplus \ {\rm Import} \ \ \oplus \ {\rm Import} \ \ \odot \ \ \oplus \ {\rm Import} \ \ \odot \ \ \oplus \ {\rm Import} \ \ \odot \ \ \oplus \ \ \ \ \oplus \ \ \ \ \oplus \$		$M \sim - \nabla$	
	Status Username 🔿 Description First Name Last Name Email Ad	Idress User Identity Groups Admin		
	BEnabled 1 cisco_admin	FPR-4110-Admin		
	Enabled 1 cisco_readonly	FPR-4110-ReadOnly		

第8步:创建管理员用户的授权配置文件。

FXOS机箱包括以下用户角色:

- Administrator —对整个系统的完全读写访问权限。默认情况下,为默认管理员帐户分配此角 色,且无法更改。
- 只读-对系统配置的只读访问权限,没有修改系统状态的权限。
- 操作-对NTP配置、智能许可的Smart Call Home配置和系统日志(包括系统日志服务器和故障)的读写访问权限。对系统的其余部分具有读取访问权限。
- AAA -对用户、角色和AAA配置的读写访问。对系统其余部分的读取权限

每个角色的属性:

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

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

cisco-av-pair=shell : roles="read-only"



注意:此文档仅定义管理员和只读属性。

导航到汉堡图标≡>策略>Policy元素>结果>授权>授权配置文件> +Add。

定义授权配置文件的名称,将访问类型保留为ACCESS\_ACCEPT,然后在Advanced Attributes Settings下添加cisco-av-pair=shell:roles="admin",然后点击Submit。

= Cisco ISE	Policy - Policy Elements	Evaluation Mode 17 Date	1ª Q	0 53	0
Dictionaries Conditions	Results				
Authentication >	Authorization Profile > FPR-4110-Admins Authorization Profile				
Authorization Profiles	* Name EOP410Admise				
Downloadable ACLs	Description				
Profiling >	* Access Type ACCESS ACCEPT V				
Client Provisioning >	Network Device Profile  Constraints Constr				
	Passive Identity Tracking				
	ACL IPv6 (Fitter-ID)				
	✓ Advanced Attributes Settings       E <u>Giscoccisco-av-pair</u> <ul> <li>★</li> <li>sheltroles**admin*</li> <li>✓</li> <li>★</li> </ul>				
	✓ Attributes Details Access type = ACCESS_ACCEPT dice-br-par = bhdtrides="admet"				
		Submit		Cancel	

## 8.1 重复上述步骤为只读用户创建授权配置文件。这次使用值read-only Administrator创建 RADIUS类。

= Cisco ISE	Policy - Policy Elements	Evaluation Mode 18 Days	Q ()	50	٥
Dictionaries Conditions	Results				
Authentication >	Authorization Profile > New Authorization Profile Authorization Profile				
Authorization Profiles Downloadable ACLs	* Name FPR-4110-ReadOnly Description				
Profiling >	* Access Type ACCESS_ACCEPT ~				
Client Provisioning	Network Device Profile Cisco V®				
	Track Movement C Agenticss Posture C Passive Identity Tracking C				

ACL IPv6 (Filter-ID)		
✓ Advanced Attributes Settings		
Cisco:cisco-av-pair     v     ahelt:roles*'read-only*     v     +		
✓ Attributes Details Access type = ACCESS_ACCEP1 docs-av-pair = 3-ddLordes_*read-only*		
	Submit	Cancel

第9步:创建与FMC IP地址匹配的策略集。这是为了防止其他设备向用户授予访问权限。

导航到左上角的≡ > Policy > Policy Sets > Add图标符号。

≡ Cisco ISE	Policy - Policy Sets	🛕 Evaluation Mode 17 Days Q 🕥 🕫 🔯
Policy Sets		Reset Reset Policyset Hitcounts Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
	+	
Oefault Default policy set		Default Network Access 🥜 + 58 🔅 🕻
		Reset Save

#### 9.1新行位于策略集的顶部。单击Add 图标以配置新条件。

🕒 Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search				
٥	New Policy Set 1		+	Select from list 🥒 + 🚳 🕨
٥	Default	Default policy set		Default Network Access 🥒 + 58 🔅 🗲

9.2为RADIUS NAS-IP-Addressattribute添加与FCM IP地址匹配的顶部条件,然后点击使用。

Library							
Search by Name							
● <u>1</u> ⊙ <u>3</u> <u>5</u> <del>3</del> <del>4</del> <u>9</u> <u>4</u> <u>9</u> <u>4</u> 0 <u>5</u> <del>9</del>	£ 🕈						
:: 📑 5G							
E Gatalyst_Switch_Local_Web_Authentication							
🗄 📄 Radius							
: Switch_Local_Web_Authentication							
E Switch_Web_Authentication							
:: B Wired_802.1X							
E Wired_MAB							
E Wireless_802.1X							
E Wireless_Access							
E Wireless_MAB							
# B WLC_Web_Authentication							

Editor

0

V Attri	Calant at	tribute for conditio					
la pol			100 B B C	1 (	9 E 🕈	Wrong value	View
is not	Di	ictionary	Attribute	ID	Info		
	A	I Dictionaries 🗸	Attribute	ID			>
	Mic	crosoft	MS-User-IPv4-Address	61	0		>
	Ne	twork Access	ISE Host Name		0		
	• Ra	dius	DNS-Server-IPv6-Address	169	0		
	• Ra	dius	Framed-IP-Address	8	0		Save
	• Ra	dius	Framed-IPv6-Address	168	0		
	Ra	dius	NAS-IP-Address	4	0		
	Q Ra	dius	Stateful-IPv6-Address-Pool	172	0		



## 9.3完成后单击Save。

≡ Cisco IS	SE	Policy - Policy Sets			A Evaluation Mode	17 Days	Q (0)	58 ¢
Policy Sets				Reset	Reset Policyset	Hitcount	•	Save
🕣 Status	Policy Set Name	Description	Conditions	Allowed Protocol:	s / Server Sequenc	e Hits	Actions	View
Q Search						_		
٥	New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0.130	Default Network	Access 🕲 🗸 -		ø	>
۰	Default	Default policy set		Default Network /	iccess 🥒 -	58	٨	>
							_	
						Reset		Save



提示:在本练习中,我们允许使用默认网络访问协议列表。您可以创建一个新列表并根据 需要缩小其范围。

步骤 10 通过点击行尾部的>图标来查看新的策略集。

Policy Sets		Reset Reset Policyset Hitcounts Save
Status Policy Set Name Descrip	tion Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q. Search		
New Policy Set 1	Radius-NAS-IP-Address EQUALS 172.16.0.130	Default Network Access 💿 🗸 + 🚳 🗲

10.1展开Authorization Policy菜单并单击(+)添加新条件。

$\sim I$	uthorizatio	on Policy (1)						
					Results			
0	Status	s Rule Name	Conditions		Profiles	Security Groups	Hitr	s Actions
	Q Searc	ch						
	٥	Authorization Rule 1		+	Select from list	+ Select from list	0 +	ŵ

10.2设置条件以匹配DictionaryIdentity组与AttributeName Equals User Identity Groups: FPR-4110-Admins(在步骤7中创建的组名)并单击Use。

isco la	Conditions Studio			hallan	Dollars Cate						A 2-1-1-17-1	0	×
50	Library	Editor											
atu S	Search by Name	-	Identity	iroup Na	me								2
		) .	Equals	Sele	ct attribute for condition				×				
on	E 56 O		Set to 'is	•	Distingues		0 1	0 t 7	]		Duplicate	Save	
	E Catalyst_Switch_Local_Web_Authentication				All Dictionaries V	Attribute	ID	ento					
	E Compliance_Unknown_Devices			-	CWA.	CWA_ExternalGroups Description		0					
	E Compliant_Devices			٠	IdentityGroup	Name		0					
5	E EAP-MSCHAPV2			-	InternalUser PassiveID	IdentityGroup PassiveID_Groups		0					
	II DEAP-TLS O				administrator	ExternalGroups		0					
	II 📴 MAC_in_SAN 📀												
	: Network_Access_Authentication_Passed												
	E Non_Cisco_Profiled_Phones												
	E Non_Compliant_Devices												
	Redus												
										Close		Use	

brary	E	ditor		
Search by Name			IdentityGroup Name	
• • • • • • • • • • •	) <b>1 0</b> E 🕈		Equals User Identity Groups: FPR-4110- +	
i 🖪 50		•	Autimi V	
BYOD_is_Registered			Set to 'is not'	Save
Catalyst_Switch_Local_Web_Authentication			NEW AND OR	
Compliance_Unknown_Devices				
Compliant_Devices				
EAP-MSCHAPv2				
EAP-TLS				
Cuest_Flow				
MAC_in_SAN				
Network_Access_Authentication_Passed				
Non_Cisco_Profiled_Phones				
Non_Compliant_Devices				
🗄 Radius				

#### 第10.3步验证在授权策略中配置的新条件,然后在配置文件下添加用户配置文件。

∨ Au	<ul> <li>Authorization Policy (1)</li> </ul>											
					Results							
۲	Status	Rule Name	Conditions		Profiles		Security Groups		Hits	Actions		
Q Search												
	۰	Authorization Rule 1	A IdentityGroup Name EQUALS User Identity Groups/FR-4110-Admin	E	FPR-4110-Admins ×	~+	Select from list	~+		٨		
	۰	Default			DenyAccess	1+	Select from list	2 +	0	\$		

t Save

步骤 11对只读用户重复步骤9中的相同过程,然后点击保存。

#### 验证

- 1. 尝试使用新的Radius凭证登录FCM GUI
- 2. 导航至>工序> Radius >实时日志≡的汉堡图标。
- 3. 显示的信息显示用户是否成功登录。

=	≡ Cisco ISE							Operations - RADIUS								A Evaluation Mode 17 Days Q (2) 58 (2)						
Liv	e Logs	Live Sessions																				
	Misco	nfigured Supplicants 🕕				Misconfigured	Network Devices 🕕				RADIUS Drop	• 0			c	lient Stopped Resp	onding 🕕				Repeat Co	unter 🕕
		0					0				1					0					C	)
	ø	🖆 Reset Repeat Counts 🚽	🖞 Export To 🗸														Ne	esh ver	Latest 20	records 🗸	Within Last 3 hou Filter 🗸	e
		Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address		Network De	Device Port	Identity Group	Posture .	Server	Mdm Ser	IMEISV		Usecasi
	$\times$				×.	identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	~ 1	Network Devic	Device Port	Identity Group	Posture St	a Server	Mdm Serve	IMEISV		Usecase
		Feb 03, 2024 01:51:51.0 Feb 03, 2024 01:50:48.9	•	0		cisco_readonly cisco_admin			New Polic	New Polic	FPR-4110		1	FPR-4110		User Identity Group		marpatiniSE marpatiniSE				

4. 从安全防火墙机箱CLI验证已记录的用户角色。

FPR4K-1-029A78B# scope se security service-profile server FPR4K-1-029A78B# scope security FPR4K-1-029A78B /security # show remote-user detail Remote User cisco\_admin: Description: User Roles: Name: admin Name: read-only FPR4K-1-029A78B /security #

故障排除

1. 在ISE GUI上,导航至汉堡图标=> Operations > Radius > Live logs。

1.1验证日志会话请求是否到达ISE节点。 1.2对于失败状态,请查看会话详细信息。

≡ Cisco ISE	0	perations - RADIUS	🛓 Evaluation Mo	de 18 Days Q 🔘 🕫 🖨
Live Logs Live Sessions				
Misconfigured Supplicants 🕕	Misconfigured Network Devices 📀	RADIUS Drops 📀	Client Stopped Responding 🕠	Repeat Counter 🕕
0	1	1	0	3
ල් 🕁 Reset Repeat Counts රෝ Export To 🗸			Never V Latest 20 re	cords v Hours v Filter v 0
Time Status	Details Repea Identity Endpoint ID	Endpoint Authenti Authoriz Authoriz IP A	Address Network De Device Port Identity Group Post	ure Server Mdm Ser
×	V Identity Endpoint ID	Endpoint Pr Authenticat Authorizatic Authorizatic IP A	Iddress 🗸 Network Device Device Port Identity Group Postu	re Sta Server Mdm Sen
Feb 02, 2024 07:32:18.8 O	cisco_admin	Default >> Default	FPR-4110 User Identity Group:	marpatin/SE
Feb 02, 2024 07:23:20.1	G cisco_readonly	Default >> Default >> PermitAcc	FPR-4110 User Identity Groups	marpatinISE
Feb 02, 2024 07:15:32.2	G cisco_admin	Default >> Default >> PermitAcc	FPR-4110 User Identity Groups	marpatinISE

2. 对于未显示在RADIUS实时日志中的请求,请查看UDP请求是否通过数据包捕获到达ISE节点。

导航到>操作>故障排除>诊断工具> TCP转储≡的汉堡图标。添加新的捕获并将文件下载到本地计算 机,以查看UDP数据包是否到达ISE节点。

2.1请填写所需信息,向下滚动并单击Save。

E Cisco ISE	Operations - Troubleshoot	🛦 Evaluation Mode 17 Days Q. 🔘 🕼 🔘
Diagnostic Tools Downlos	ad Logs Debug Wizard	
General Tools V RADIUS Authentication TroubL	TCP Surp > New	
Execute Network Device Com Evaluate Configuration Validat Posture Troubleshooting	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.  Host Name*	
Agentiess Posture Troublesho EndPoint Debug TCP Dump	margatist5E V	
Session Trace Tests	Notock <sup>1</sup> Notock <sup>2</sup> (Up, Running) $\smile$	
TrustSec Tools	Pater ip host 172.16.0.130 E.g: (p host 10.77.122.123 and not 10.177.122.119	

2.2选择并启动捕获。



2.3当ISE捕获运行时,尝试记录到安全防火墙机箱

2.4停止ISE中的TCP转储并将文件下载到本地计算机。

2.5查看流量输出。

预期输出:

数据包编号1。从安全防火墙通过端口1812 (RADIUS)向ISE服务器发出的请求数据包No2。ISE服务器回复接受初始请求。



#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。