Firepower可扩展操作系统(FXO) 2.2 : 远程管理 的机箱认证/授权与ISE使用RADIUS

目录

<u>简介</u>

本文描述如何通过身份服务引擎(ISE)配置RADIUS验证和授权Firepower可扩展操作系统的(FXO)机 箱的。

FXO机箱包括以下用户角色:

- •管理员-对整个系统的完整读写访问。默认管理帐户分配此角色默认情况下,并且不可能更改。
- •只读-对系统配置的只读访问没有权限修改系统状态。
- •操作-对NTP配置、聪明的Call Home配置聪明许可授权的和系统日志的读写访问,包括系统日志服务器和故障。对系统的其余的读访问。

• AAA -对用户、角色和AAA配置的读写访问。对系统的其余的读访问。 通过CLI这能被看到如下:

fpr4120-TAC-A /security * #请显示角色

角色:

角色命名Priv

----- ---

aaa aaa

admin admin

操作操作

只读只读

贡献用托尼雷米雷斯,何塞索托, Cisco TAC工程师。

<u>先决条件</u>

<u>要求</u>

Cisco 建议您了解以下主题:

- •知识Firepower可扩展操作系统(FXO)
- ISE配置知识

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Cisco Firepower 4120安全工具版本2.2
- 虚拟思科身份服务引擎2.2.0.470

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。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

配置

配置的目标对:

- 验证登录FXOS的基于Web的GUI和SSH的用户通过ISE
- •认证登录FXOS的基于Web的GUI和SSH的用户根据他们的各自用户角色通过ISE。
- 通过ISE验证认证和授权正常操作在FXO的

网络图



配置

配置FXO机箱

创建使用机箱管理器的RADIUS供应商

步骤1.导航对平台设置>AAA。

步骤2.点击RADIUS选项。

Add 🔇

第三步:每个RADIUS供应商您想要添加(16个供应商)。

- 3.1. 在RADIUS供应商地区中,请单击**添加。**
- 3.2. 一旦添加RADIUS供应商对话框打开,请输入需要的值。
- 3.3. 点击OK键关闭添加RADIUS供应商对话框。

Í	Edit 10.88.244.50		?×
	Hostname/FQDN(or IP Address):*	10.88.244.50	
1	Order:*	1	
	Key:	•••••	Set:Yes
1	Confirm Key:	•••••	
	Authorization Port:*	1812	
	Timeout:*	5 Secs	
	Retries:*	1	
		ОК	ancel

步骤4.点击**"Save"**。

Overview Interfaces Logic	al Devices Security Engine	Platform Settings			
NTP	LDAP RADIUS TACACS				
SSH SNMP	Properties				
HTTPS	Timeout:* 5 Secs				
Syslog	Retries:* 1				
DNS ETPS and Common Criteria	RADIUS Providers				
Access List					Add
	Hostname	Order	Service	Auth Port	
	10.88.244.50	1	authorization	1812	a 6
	Save Cancel				

步骤5.导航对**系统>用户管理>设置**。

第六步:在默认验证下请选择**RADIUS**。

Overview Interfaces Logic	cal Devices Security Engine Platform Settings		() ()	System Too	ols Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	RADIUS v "Local is failback authentication method				
Console Authentication	Local 💌				
Remote User Settings					
Remote User Role Policy	SAssign Default Role 🗌 No-Login				

创建使用CLI的RADIUS供应商

步骤1.为了启用RADIUS验证,请运行以下命令。

fpr4120-TAC-A#范围安全

fpr4120-TAC-A /security #范围默认验证

fpr4120-TAC-A /security/default-auth #集领域radius

第二步:请使用detail命令的显示显示结果。

fpr4120-TAC-A /security/default-auth #显示详细信息

默认验证:

Admin领域:Radius

可操作的领域:Radius

Web会话刷新期限(以秒):600

会话超时(以秒) Web的, SSH,远程登录会话:600

绝对会话超时(以秒) Web的, SSH,远程登录会话: 3600

串行控制台会话超时(以秒):600

串行控制台绝对会话超时(以秒):3600

Admin认证服务器组:

可操作的认证服务器组:

使用第2个要素:无

步骤3.为了配置RADIUS服务器参数请运行以下命令。

fpr4120-TAC-A#**范围安全**

fpr4120-TAC-A /security #范围radius

fpr4120-TAC-A /security/radius #回车服务器10.88.244.50

fpr4120-TAC-A /security/radius/server #集descr "ISE服务器"

fpr4120-TAC-A /security/radius/server * #集密钥

输入密钥:******

确认密钥:******

第四步:请使用detail命令的显示显示结果。

fpr4120-TAC-A /security/radius/server * #请显示详细信息

RADIUS服务器:

主机名、FQDN或者IP地址:10.88.244.50

Descr :

命令:1

验证波尔特:1812

密钥:****

超时:5

配置ISE服务器

添加FXO作为网络资源

步骤1.导航到Administration >网络资源>网络设备。

步骤2.单击**添加**

dentity Services Engine	Home Context	Visibility • Operations	► Policy - Ad	ministration V	ork Centers					
System Identity Management	✓ Network Resources	Device Portal Managem	ent pxGrid Services	Feed Service	Threat Centric NAC					
Network Devices Network Device G	roups Network Devic	ce Profiles External RADI	US Servers RADIUS	S Server Sequences	NAC Managers Ex	ternal MDM	Location Services			
G	0									
Network devices	Network Device	es								
Default Device										
Device Security Settings	/ Edit 🕂 Add 🛙	Duplicate	Export O Generati	e PAC X Delete						
	Name	IP/Mask Prof	le Name	Location		Туре		Description		
							No data a	available		

步骤3.输入需要的值(名称、IP地址、设备类型和Enable (event) RADIUS和添加KEY),单击提交。

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
(
Network devices	Network Devices	
Default Device	I Name EVOC	
Device Security Settings		
	Description	
	* IP Address: 10.83.180.6 / 32	
	* Device Profile dete Cisco 👻 🕀	
	Model Name	
	Software Version	
	Network Device Group	
	Device Type FXOS Set To Default	
	IPSEC To TOPEC Device	
	All Locations 💟 Set To Default	
	✓ RADIUS Authentication Settings	
	KADIUS UDP Settings	
	Protocol RADIUS	
	- Shared Secret Show	
	CoA Port 1700 Set To Default	
	RADIUS DTLS Settings (j)	
	DTLS Required 🔲 👔	
	Shared Secret radius/dtls (j)	
	CoA Port 2083 Set To Default	
	Issuer CA of ISE Certificates for CoA Select if required (optional)	

创建标识组和用户

步骤1.导航给Administration >身份管理> Groups >用户标识组。

步骤2.单击**添加。**

dent	tity Services	s Engine	Home	Context Visibility	▸ Operations	▶ Policy	- Administration	
System	✓ Identity N	lanagement	Network	Resources Devic	e Portal Managemer	it pxGrid S	Services Feed Se	rvice
Identities	Groups	External Ider	ntity Sources	Identity Source Sec	uences F Setting	IS		

Identity Groups	User Identity Groups							
🤄 🕇 🗄 👻 🙀	/ Edit 🕂 Add 🗙 Delete 👻 🛃 Import 😭 Export 👻							
Endpoint Identity Groups	Name							
User Identity Groups	ALL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group							
	Default Employee User Group							
	GROUP_ACCOUNTS (default) Default GROUP_ACCOUNTS (default) User Group	i i						
	GuestType_Contractor (default) Identity group mirroring the guest type							
	GuestType_Daily (default) Identity group mirroring the guest type							
	GuestType_Weekly (default) Identity group mirroring the guest type							
	OWN_ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group							

步骤3.输入名称的值并且单击**提交。**

dentity Services Engine	Home	Operations Policy		
System Identity Management	Network Resources Dev	ice Portal Management pxGrid	Services + Feed Service + Threat C	antric NAC
Identities Groups External Ident	tity Sources Identity Source So	equences > Settings		
Identity Groups	User Identity G Identity G · Name Description Submit	Groups > New User Identity Grou POUP FXOS ADMIN Cancel	P	

步骤4.重复所有所需的用户角色的步骤3。

dent	ity Service	s Engine	Home	Context Visibility	 Operations 	▶ Policy	- Administration	Work Centers
System	- Identity N	lanagement	Network F	Resources Device	Portal Management	t pxGrid S	Services + Feed Se	ervice
Identities	Groups	External Ider	tity Sources	Identity Source Sequ	uences	6		

Identity Groups	P	User Identity Groups					
↓ E •	<u>نې</u>		. •				
Endpoint Identity Groups		Name	Description				
User Identity Groups		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group				
		Employee	Default Employee User Group				
		🗌 🖉 FXOS AAA					
		E A FXOS ADMIN					
		E PROS OPER					
		FXOS Read Only					
			DEFUE ODOLD ACCOUNTS (J.C. III) USE OFFIC				

步骤5.导航对Administration >身份管理>标识> Users。

步骤6.单击**添加。**

Context Visibility Op	erations Policy	- Administration	Work Centers						
Resources	Management pxGrid S	ervices + Feed Se	rvice						
Identities Groups External Identity Sources Identity Source Sequences ▶ Settings									
0									
Users Network Access Users									
Add 📴 Change Status	Export	X Delete	uplicate						
tus Name	 Description 	n Fin	st Name Last Name	Email Address	User Identity Groups	Admin			
				1	No data available				
	Context Visibility Op Resources Device Portal I Identity Source Sequences rk Access Users Change Status tus Name	Context Visibility Operations Policy Resources Device Portal Management pxGrid S Identity Source Sequences Settings rk Access Users Change Status Change Status Name Description	Context Visibility Operations Policy Administration Resources Device Portal Management pxGrid Services Feed Se Identity Source Sequences Settings rk Access Users Change Status Primort Primo	• Context Visibility • Operations • Policy • Administration • Work Centers • More Centers • Device Portal Management pxGrid Services • Feed Service • Threat Centric NAC Identity Source Sequences • Settings • Kaccess Users • Change Status • Perform • Description • Perform • Perform	• Context Visibility • Operations • Policy • Administration • Work Centers • Mork Centers • More • Mork •	 Context Viability Operations Pelicy Administration Work Centers Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC Identity Source Sequences Settings Add Grange Status Perport Export Delete Delete Puplicate tus Name Description First Name Last Name Email Address User Identity Groups No data available	Context Visibility Operations > Policy ~ Administration > Work Centers Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC Identity Source Sequences > Settings		

步骤7.输入需要的值(名称、用户组,密码)。

cisco le	dentity Service	s Engine	Home	 Context Visi 	ibility 🕨	Operations	Policy	▼ Adm	ninistration	Work Ce	nters
 Systematic 	em 🔽 Identity M	Management	Network	Resources +	Device Port	tal Managemen	t pxGrid	Services	Feed Ser	rvice + Th	reat Centric NAC
✓Identi	ties Groups	External Identit	y Sources	Identity Source	ce Sequenci	es	s				
		0	Notwork	Access Linem							
Users				thurst Accord		Network Acces	suser				
Latest Ma	anual Network So	an Results	* ne	LWORK ACCess	suser						
			• Na	me fxosadmin	n						
			Sta	tus 🔽 Enab	oled 👻						
			En	nail							
			▼ P	asswords							
			Pa	ssword Type:	Internal Us	sers					
					Password			Re-Enter	Password		
			· .	ogin Password	•••••			•••••			Generate Password (i)
			En	able Password							Generate Paceword
				abie r assirera							
			▼ U	ser Informati	ion						
			Fin	st Name							
			La	st Name							
			▼ A	ccount Option	ns						
					Description	n					
			Ch	ange password	on next logir	n 🗆					
			- A	ccount Disab	le Policy						
				count bisab	roncy						
				Disable accou	unt if date ex	ceeds 2018-	03-01		()))))	y-mm-dd)	
			₹ U	ser Groups							
			E	XOS ADMIN		<u> </u>					
			Subr	nit Cancel)						
					,						

步骤8.重复全部必需用户的步骤6。

dentity Services Engine	Home	bility	Policy Administra	tion Work Centers			
System Identity Management	Network Resources	Device Portal Management	pxGrid Services + Fe	ed Service + Threat C	entric NAC		
◄ Identities Groups External Identit	ty Sources Identity Source	ce Sequences + Settings					
0							
Users	Network Access Us	ers					
Latest Manual Network Scan Results	/ Edit 🕂 Add 🐻 Cl	hange Status 👻 🎲 Import	🕞 Export 👻 🗙 Delete 👻	Duplicate			
	Status Nam	ne 🔺	Description	First Name Las	t Name Email Address	User Identity Groups	Admin
	🗌 🛃 Enabled 🛛 👤 fi	xosaaa				FXOS AAA	
	🗌 🔽 Enabled 🙎 fi	xosadmin				FXOS ADMIN	
	🗌 🛃 Enabled 🛛 👤 fi	xosoper				FXOS OPER	
	🗌 🛃 Enabled 🛛 👤 f	xosro				FXOS Read Only	

创建每个用户角色的授权配置文件

步骤1.导航对**策略>Policy元素>结果>授权>授权配置文件。**

dentity Services Engine	Home	▸ Operations ▼Policy	Administration Work Centers	
Authentication Authorization Profili	ng Posture Client Provisioning			
Dictionaries + Conditions - Results	s			
0				
Authentication	Standard Authorization	n Profiles		
Authorization	For Policy Export go to Admin	istration > System > Backup &	& Restore > Policy Export Page	
Philliphiadon	/ Edit + Add Duplicat	e XDelete		
Authorization Profiles	Name		Profile	Description
Downloadable ACLs	Blackhole Wireless An	9966	dth Ciero El	Default profile used to blacklist wireless devices. Ensu
▶ Profiling			the Cost of Co	Default profile used for Olean Dhannes
	Cisco_IP_Phones		and UISCO (D)	Derault profile used for Cisco Phones.
▶ Posture	Cisco_WebAuth		🚓 Cisco 🕀	Default Profile used to redirect users to the CWA port
	NSP_Onboard		📸 Cisco 🕀	Onboard the device with Native Supplicant Provisionin
Client Provisioning	Non_Cisco_IP_Phones		🗰 Cisco 🕀	Default Profile used for Non Cisco Phones.
	DenyAccess			Default Profile with access type as Access-Reject
	PermitAccess			Default Profile with access type as Access-Accept

步骤2.填装授权配置文件的所有属性。

2.1. 配置配置文件名称。

Authentication Authorization Profilin	g Posture Client Provisioning Policy Elements	
Dictionaries Conditions Results		
0		
Authentication	Authorization Profiles > FXOS-ADMIN-PROFILE Authorization Profile	
- Authorization	Name FXOS-ADMIN-PROFILE	
Authorization Profiles	Description	
Downloadable ACLs	Access Type ACCESS_ACCEPT T	
▶ Profiling	Network Device Profile 🛛 🗮 Cisco 👻 🕀	

2.2. 在先进的属性设置请配置以下CISCO-AV-PAIR

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

 Advanced Attributes Settings 		
Cisco:cisco-av-pair	= shell:roles="admin"	⊘ = +

2.3. Click Save.

Save	Reset	

步骤3.使用以下Cisco AV对,重复剩余的用户角色的步骤2

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

cisco-av-pair=shell : roles= "操作"

cisco-av-pair=shell : "只读"的roles=





 Advanced Attributes Settings 		
Cisco:cisco-av-pair	= shell:roles="read-only"	⊘ — ∔

dentity Services Engine Ho	ne Context Visibility Operations Policy Ad	Iministration				
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements					
Dictionaries + Conditions - Results						
0						
Authentication	Standard Authorization Profiles					
Authorization	For Policy Export go to Administration > System > Backup & Restore	e > Policy Export Page				
Addionzation	/ Edit - Add Dyplicate					
Authorization Profiles		Drafila				
Downloadable ACLs		Profile				
Des fille a	Blackhole_Wireless_Access	disto Cisco 🕀				
► Profiling	Cisco_IP_Phones	disto Cisco 🕀				
▶ Posture	Cisco_WebAuth	diste Cisco ⊕				
	FXOS-AAA-PROFILE	📸 Cisco 🕀				
Client Provisioning	FXOS-ADMIN-PROFILE	dete Cisco ⊕				
	FXOS-OPER-PROFILE	👑 Cisco 🕀				
	FXOS-ReadOnly-PROFILE	🚓 Cisco 🕀				

步骤1.导航对策略>验证>并且单击箭头在旁边编辑您要创建规则的地方。



第二步:设置简单;它可以是执行的更加粒状,但是对于此示例我们将使用设备类型:

名称:FXO验证规则

IF挑选新团体/值:设备:设备类型等于所有设备类型#FXOS

允许协议:默认网络网络访问

使用:内部用户

 FXOS AUTHENTICATION RULE : If DEVICE:Device Type EQUALS All Device Types#FXOSAllow Protocols : Default Network Access and

 Default
 :use Internal Users

创建授权策略

步骤1.导航对策略>授权>并且点击箭头网编辑您要创建规则的地方。

cisce identity	Services Engin	Home + Context Visibility + Operations	nten	🕕 Q 🕛 O O					
Authentication	Authorization	Profiling Posture Client Provisioning + Policy Elements		Click here to do wireless setup and visibility setup Do not show this again. X					
Authorizatio Define the Author For Policy Export	Authorization Policy University Seeup and Vesseling Seeup and Vess								
Exception	s (0)								
Standard									
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions						
	Default	If no matches, then DenyAccess		Insert New Rule Above					

步骤2.输入授权规则的值与要求的参数。

2.1. 规则名称: Fxos <USER ROLE>规则。



2.2. 如果:用户标识Groups>挑选<USER ROLE>。

Conditions (identity groups and other con	nditions) Permissions
FX and Condition(s)) 🛟 then AuthZ Pr
ma	
FXOS ADMIN	
	User Identity Groups
	⟨= • = •
	FXOS AAA
	GuestType_Weekly (default)
	OWN_ACCOUNTS (default)
	GROUP_ACCOUNTS (default)
	EXOS ADMIN
	FXOS OPER
	Employee
	GuestType_Daily (default)
	GuestType_Contractor (default)
	ALL_ACCOUNTS (default)

2.3. 并且:创建新的情况>设备:设备类型等于**所有设备类型#FXOS**。

Conditions (identity groups	s and other conditions) Permissions	
if FX 🛟 and	DEVICE:Device Type EQUALS All 🗢 then Select an item 💠	
if no matches, then DenyA	Ad All Conditions Below to Library	
	Condition Name Description ↓ DEVICE:Device Ty ♥ Equals ▼ All Device Types# ♥	
	All Device Types	
	All Device Types#FXOS	
	Alcatel-Lucent >	
	🗕 Aruba 🛛 🛸	
	Brocade >>	
	CERTIFICATE >	
	Cisco >	
	Cisco-BBSM >	
	Cisco-VPN3000 >	
	🚞 CWA 🔹 🔪	

2.4. 权限:英文虎报>选择**用户角色配置文件**

Permissions		
then FXOS-A		
FXOS-ADMIN-PROFILE	⊘ +-	
	Standard	
	Blackhole_Wireless_Access	
	Cisco_IP_Phones	
	😪 Cisco_WebAuth	
	C DenyAccess	
	S FXOS-AAA-PROFILE	
	C FXOS-ADMIN-PROFILE	
	S FXOS-OPER-PROFILE	
	G FXOS-ReadOnly-PROFILE	
	😪 NSP_Onboard	
	😪 Non_Cisco_IP_Phones	
	RermitAccess	
Status Rule Name	Conditions (identity groups and other conditions)	Permissions

1	Fxos Admin Rule	If FXOS ADMIN AND DEVICE:Device Type EQUALS All Device	FXOS-ADMIN-PROFILE
		Types#FXOS	

步骤3.重复所有用户角色的步骤2。

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Fxos Admin Rule	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device types#FXOS	hen FXOS-ADMIN-PROFILE
~	Fxos AAA Rule	FXOS AAA AND DEVICE:Device Type EQUALS All Device types#FXOS	hen FXOS-AAA-PROFILE
	Fxos Oper Rule	FXOS OPER AND DEVICE:Device Type EQUALS All Device types#FXOS	hen FXOS-OPER-PROFILE
	Fxos Read only Rule	FXOS Read Only AND DEVICE:Device Type EQUALS All Device types#FXOS	hen FXOS-ReadOnly-PROFILE
	Default	no matches, then DenyAccess	

步骤4.单击**"Save"**在页底端。





<u>验证</u>

您可以当前测试每个用户和验证已分配用户角色。

FXO机箱验证

1. Telnet或SSH对FXO机箱和登录使用任何已创建用户ISE的。 用户名:fxosadmin

密码:

fpr4120-TAC-A#范围安全

fpr4120-TAC-A /security #显示远程用户详细信息

远程用户**fxosaaa** :

说明:

用户角色:

名称:**aaa**

名称:**只读**

远程用户**fxosadmin** :

说明:

用户角色:

名称:admin

名称:**只读**

远程用户**fxosoper**:

说明:

用户角色:

名称 : **操作**

名称:**只读**

远程用户fxosro :

说明:

用户角色:

名称:**只读**

根据输入FXO机箱cli的用户名只将显示为用户角色授权的命令分配。

管理员用户角色。

fpr4120-TAC-A /security # ?

确认确认

结算用户塞申斯Clear user塞申斯

创建创建托管对象

删除删除托管对象

禁用功能失效服务

enable (event) 启用服务

回车输入托管对象

范围更改电流模式

设置集合属性值

显示Show system information

终止激活cimc会话

fpr4120-TAC-A#连接fxos

fpr4120-TAC-A (fxos) # debug aaa AAA请求

fpr4120-TAC-A (fxos) #

只读用户角色。

fpr4120-TAC-A /security # ?

范围更改电流模式

设置集合属性值

显示Show system information

fpr4120-TAC-A#连接fxos

fpr4120-TAC-A (fxos) # debug aaa AAA请求

%为角色拒绝的权限

2. 使用任何ISE的,已创建用户浏览对FXO机箱IP地址和登录。 管理员用户角色。

Overview Interfaces Logica	Devices Security Engine Platform	Settings						System	Tools Help	fxosadmin
NTP SSH SNMP HTTPS	LDAP RADIUS TACACS Properties				_			 		
AAA Syslog DNS IIIS and Common Criteria	Retries:* 1 RADIUS Providers		Add RADIUS Provider							
Access List	Hostname	Order	Order:* Key:	lowest-available	Set:No	O Add				
	10.88.244.16	1	Confirm Key: Authorization Port:" Timeout:" Retries:"	1812 5 Secs 1 OK Cent	:el	/ 5				

只读用户角色。

erview	Interfaces	Logical	Devices	ecurity Engine	Platform Settings			
NTP			LDAP R	DEUS TACACS				
SSH			Properties					
HTTPS			Timeout:*	5 Secs				
Syslog			Retries:*					
DNS FIPS and	Common Criteria	.	RADOUS Pro	oen.				0
Access Li	st		Hostname		Order	Service	Auth Port	0
			10.88.244	16	1	authorization	1812	9.8

Note:注意Add按钮变灰。

ISE 2.0验证

1. 导航对操作> RADIUS> Live 日志。您应该能发现成功和失败的尝试。

altalta cisco	Identity Services Engl	ne Home	Context V	Isibility • Opera	ations P	blicy	Administration	Work Centers				(0 0 0	4
▼RA	DIUS Threat-Centric N	AC Live Logs 🔶	TACACS +	Troubleshoot + A	daptive Netwo	rk Cont	trol Reports				Click here to do wirele	ess setup and visibility	setup Do not show this agai	n.
Live L	.ogs Live Sessions													
		Misconfigured S	upplicants O	Misco	Misconfigured Network Devices O			RADIUS Drops 🙂	Client Stopped Responding O		Repeat Counter 🥹			
	0			0			0	0			0			
									Refresh	Never	• Show La	atest 20 records	Within Last 3 hours	•
C R	efresh O Reset Repe	at Counts 💆 E	Export To 🕶										¥ Fiter -	۰ م
	Time	Status	Details	Repeat C	Identity		Authentication Pol	licy	Authorization Policy	Aut	thorization Profiles	Network Dev	Identity Group	
×					Identity		Authentication Polic	У	Authorization Policy	Au	thorization Profiles	Network Device	Identity Group	
	Jan 20, 2018 10:14:09		0		fxosadmin		Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Admin Rule	FX	OS-ADMIN-PROFILE	FXOS	User Identity Groups:FXC	s
	Jan 20, 2018 10:13:59	. 💿	0		fxosadmin		Default >> FXOS AU	THENTICATION RULE >> Default				FXOS	User Identity Groups:FXC	s
	Jan 20, 2018 10:09:01		0		fxosro		Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Read only R	ule FX	OS-ReadOnly-PROFILE	FXOS	User Identity Groups:FXC	s
	Jan 20, 2018 10:08:50	. 0	0		fxosro		Default >> FXOS AU	THENTIGATION RULE >> Default				FXOS	User Identity Groups:FXC	s
	Jan 20, 2018 10:06:17	. 😐	0		fxosro		Default >> FXOS AU	THENTIGATION RULE >> Default				FXOS	User Identity Groups:FXC	s
	Jan 20, 2018 10:05:15	. 😐	0		fxosro		Default >> FXOS AU	THENTIGATION RULE >> Default				FXOS	User Identity Groups:FXC	s
	Jan 20, 2018 10:04:23	. 🖉	0		fxosadmin		Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Admin Rule	FX	OS-ADMIN-PROFILE	FXOS	User Identity Groups:FXC	s
	Jan 20, 2018 10:02:59	. 🛛 🗹	à +		fxosadmin	÷	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Admin Rule	FX	OS-ADMIN-PROFILE	FXOS	User Identity Groups:FXC	s

<u>故障排除</u>

为了debug aaa authentication和授权运行以下in命令FXO cli。

fpr4120-TAC-A (fxos) # debug aaa AAA请求 fpr4120-TAC-A (fxos) # debug aaa事件 fpr4120-TAC-A (fxos) # debug aaa错误 fpr4120-TAC-A (fxos) # term mon 在成功认证尝试,您将看到以下输出后。 2018简20 17:18:02.410275 aaa : 验证的aaa_req_process。会话没有0 2018简20 17:18:02.410297 aaa : aaa reg process : 常规从appIn的AAA请求: 登录 appln_subtype : 默认 2018简20 17:18:02.410310 aaa : try next aaa method 2018简20 17:18:02.410330 aaa :配置的总方法是1,将尝试的当前索引是0 2018简20 17:18:02.410344 aaa : handle reg using method 2018简20 17:18:02.410356 aaa : AAA_METHOD_SERVER_GROUP 2018简20 17:18:02.410367 aaa : aaa_sg_method_handler group= radius 2018简20 17:18:02.410379 aaa : 使用通过对此功能的sg protocol 2018简20 17:18:02.410393 aaa : 发送请求对RADIUS服务 2018简20 17:18:02.412944 aaa : mts_send_msg_to_prot_daemon : 有效载荷长度= 374 2018简20 17:18:02.412973 aaa : 会话: 0x8dfd68c被添加到会话表1 2018简20 17:18:02.412987 aaa : 已配置的方法组继之后 2018简20 17:18:02.656425 aaa : aaa_process_fd_set 2018简20 17:18:02.656447 aaa : aaa_process_fd_set : 在aaa_q的mtscallback 2018简20 17:18:02.656470 aaa : mts_message_response_handler : mts答复 2018简20 17:18:02.656483 aaa : prot_daemon_reponse_handler 2018简20 17:18:02.656497 aaa : 会话: 从会话表删除的0x8dfd68c 0 2018简20 17:18:02.656512 aaa :is_aaa_resp_status_success状态= 1 2018简20 17:18:02.656525 aaa : is aaa resp status success真 2018简20 17:18:02.656538 aaa : 验证的aaa_send_client_response。session->flags=21.aaa_resp->flags=0.

fpr4120-TAC-A#连接fxos

2018简20 17:18:02.656550 aaa : AAA_REQ_FLAG_NORMAL

2018简20 17:18:02.656577 aaa : 成功的mts_send_response

2018简20 17:18:02.700520 aaa : aaa_process_fd_set : 在aaa_accounting_q的mtscallback

2018简20 17:18:02.700688 aaa : 旧有操作码: accounting_interim_update

2018简20 17:18:02.700702 aaa :aaa_create_local_acct_req :user= , session_id= , log=added用户fxosro

2018简20 17:18:02.700725 aaa :核算的aaa_req_process。会话没有0

2018简20 17:18:02.700738 aaa : MTS请求参考是NULL。本地请求

2018简20 17:18:02.700749 aaa : 设置AAA_REQ_RESPONSE_NOT_NEEDED

2018简20 17:18:02.700762 aaa :aaa_req_process :常规从appIn的AAA请求:默认 appIn_subtype :默认

2018简20 17:18:02.700774 aaa : try_next_aaa_method

2018简20 17:18:02.700798 aaa : 为默认默认配置的没有方法

2018简20 17:18:02.700810 aaa : 此请求的没有配置联机

2018简20 17:18:02.700997 aaa : 核算的aaa_send_client_response。session->flags=254.aaa_resp->flags=0.

2018简20 17:18:02.701010 aaa : 旧有库认为的请求的答复将被发送作为成功

2018简20 17:18:02.701021 aaa : 为此请求没需要的答复

2018简20 17:18:02.701033 aaa : AAA_REQ_FLAG_LOCAL_RESP

2018简20 17:18:02.701044 aaa : aaa_cleanup_session

2018简20 17:18:02.701055 aaa : 应该释放aaa_req。

2018简20 17:18:02.701067 aaa : 后退成功的方法本地

2018简20 17:18:02.706922 aaa : aaa_process_fd_set

2018简20 17:18:02.706937 aaa : aaa_process_fd_set : 在aaa_accounting_q的mtscallback

2018简20 17:18:02.706959 aaa : 旧有操作码: accounting_interim_update

2018简20 17:18:02.706972 aaa :aaa_create_local_acct_req :user=, session_id=, log=added用户:对角色的fxosro :只读

在失败的认证尝试,您将看到以下输出后。

2018简20 17:15:18.102130 aaa : aaa_process_fd_set

2018简20 17:15:18.102149 aaa : aaa_process_fd_set : 在aaa_q的mtscallback 2018简20 17:15:18.102267 aaa : aaa process fd set 2018简20 17:15:18.102281 aaa : aaa process fd set : 在aaa g的mtscallback 2018简20 17:15:18.102363 aaa : aaa_process_fd_set 2018简20 17:15:18.102377 aaa : aaa process fd set : 在aaa g的mtscallback 2018简20 17:15:18.102456 aaa : aaa process fd set 2018简20 17:15:18.102468 aaa : aaa_process_fd_set : 在aaa_q的mtscallback 2018简20 17:15:18.102489 aaa : mts aaa reg process 2018简20 17:15:18.102503 aaa : 验证的aaa reg process。会话没有0 2018简20 17:15:18.102526 aaa :aaa_req_process :常规从appIn的AAA请求:登录 appln_subtype : 默认 2018简20 17:15:18.102540 aaa : try next aaa method 2018简20 17:15:18.102562 aaa : 配置的总方法是1,将尝试的当前索引是0 2018简20 17:15:18.102575 aaa : handle_req_using_method 2018简20 17:15:18.102586 aaa : AAA METHOD SERVER GROUP 2018简20 17:15:18.102598 aaa : aaa sg method handler group= radius 2018简20 17:15:18.102610 aaa : 使用通过对此功能的sg_protocol 2018简20 17:15:18.102625 aaa : 发送请求对RADIUS服务 2018简20 17:15:18.102658 aaa : mts send msg to prot daemon : 有效载荷长度= 371 2018简20 17:15:18.102684 aaa :会话:0x8dfd68c被添加到会话表1 2018简20 17:15:18.102698 aaa : 已配置的方法组继之后 2018简20 17:15:18.273682 aaa : aaa process fd set 2018简20 17:15:18.273724 aaa : aaa_process_fd_set : 在aaa_q的mtscallback 2018简20 17:15:18.273753 aaa : mts message response handler : mts答复 2018简20 17:15:18.273768 aaa : prot_daemon_reponse_handler 2018简20 17:15:18.273783 aaa : 会话: 从会话表删除的0x8dfd68c 0 2018简20 17:15:18.273801 aaa : is_aaa_resp_status_success状态= 2

2018简20 17:15:18.273815 aaa : is_aaa_resp_status_success真 2018简20 17:15:18.273829 aaa : 验证的aaa_send_client_response。session->flags=21.aaa_resp->flags=0. 2018简20 17:15:18.273843 aaa : AAA_REQ_FLAG_NORMAL 2018简20 17:15:18.273877 aaa : 成功的mts_send_response 2018简20 17:15:18.273902 aaa : aaa_cleanup_session 2018简20 17:15:18.273916 aaa : 请求数据mts_drop 2018简20 17:15:18.273935 aaa : 应该释放aaa_req。 2018简20 17:15:18.280416 aaa : aaa_process_fd_set 2018简20 17:15:18.280443 aaa : aaa_process_fd_set : 在aaa_q的mtscallback 2018简20 17:15:18.280454 aaa : aaa_enable_info_config : aaa登录错误消息的GET_REQ 2018简20 17:15:18.280460 aaa : 获得的上一步回归值配置运行 : 未知安全项目

相关信息

当TACACS/RADIUS验证启用, Ethanalyzer on命令FX-OS cli将提示输入密码的密码。此行为是由 bug引起的。

Bug ID : CSCvg87518