Firepower可扩展操作系统(FXOS)2.2:使用 TACACS+的ISE进行远程管理的机箱身份验证/授 权

目录

简介

本文档介绍如何通过身份服务引擎(ISE)为Firepower可扩展操作系统(FXOS)机箱配置TACACS+身份验证和授权。

FXOS机箱包括以下用户角色:

- 管理员 完成对整个系统的读写访问。默认管理员帐户默认分配此角色,且无法更改。
- 只读 对系统配置的只读访问,无权修改系统状态。
- 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。读取系统其余部分的访问权限。

• AAA — 对用户、角色和AAA配置的读写访问。读取系统其余部分的访问权限。

通过CLI,可以看到如下内容:

fpr4120-TAC-A /security* # show role

角色:

角色名称优先级

aaa

管理员

运营

只读只读只读

作者:Tony Remirez、Jose Soto, Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题:

- Firepower可扩展操作系统(FXOS)知识
- ISE配置知识
- ISE中需要TACACS+设备管理许可证

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科Firepower 4120安全设备版本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

配置的目标是:

- 通过ISE对登录FXOS基于Web的GUI和SSH的用户进行身份验证
- •通过ISE根据用户角色授权用户登录FXOS基于Web的GUI和SSH。
- 通过ISE验证FXOS上身份验证和授权的正确操作

网络图



配置

配置FXOS机箱

创建TACACS+提供程序

步骤1.导航至Platform Settings > AAA。

步骤2.单击TACACS选项卡。

Overview Interfaces Logic	al Devices Security Engine	Platform Settings		
NTP	LDAP RADIUS TACACS			
SSH				
SNMP	Properties			
HTTPS	Timeout:* 5 Secs			
AAA				
Syslog	TACACS Providers			
DNS				O Add
FIPS and Common Criteria	Hostname	Order	Port	
Access List	Hostining	01001	Port	

步骤3.对于要添加的每个TACACS+提供程序(最多16个提供程序)。

3.1.在TACACS提供程序区域中,单击**添加。**

3.2.打开"添加TACACS提供程序"对话框后,输入所需的值。

3.3.单击"确定"关闭"添加TACACS提供程序"对话框。

Í	Add TACACS Provider		?×	
	Hostname/FQDN(or IP Address):*	10.88.244.50]	
l	Order:*	lowest-available]	
I	Key:	•••••	Set:No	
l	Confirm Key:	•••••]	
l	Port:*	49		
l	Timeout:*	5 Secs		
l		OK Car	ncel	

步骤4.单击"保**存"**。

Overview Interfaces Logic	al Devices Security Engine Platform Setting	gs		
NTP	LDAP RADIUS TACACS			
SNMP	Properties			
HTTPS	Timeout:* 5 Secs			
Syslog	TACACS Providers			
DNS				Add
FIPS and Common Criteria	Hostname	Order	Port	
Access List	10.88.244.50	1	49	28
	Save Cancel			

步骤5.导航至System > User Management > Settings。

步骤6.在Default Authentication下,选择**TACACS**。

Overview Inte	erfaces Logical Dev	ces Security Engine	Platform Settings							System Too	ls Help fx	kosadmin
								Configuration	Licensing	Updates	User Mana	agement
Local Users Set	ttings											
Default Authentic	TACA	s v *Local	is fallback authentication method									
Console Authenti	ication Local	٣										
Remote User Se	ettings											
Remote User Rol	le Policy OASS	pn Default Role 🔿 No-Logi										

使用CLI创建TACACS+提供程序

步骤1.要启用TACACS身份验证,请运行以下命令。

fpr4120-TAC-A#范围**安全**

fpr4120-TAC-A /security # scope default-auth

fpr4120-TAC-A /security/default-auth # set realm tacacs

步骤2.使用show detail命令验证配置。

fpr4120-TAC-A /security/default-auth # show detail

默认身份验证:

管理领域:**塔卡奇**

运营领域:**塔卡奇**

Web会话刷新期(秒):600

Web、ssh、telnet会话的会话超时(秒):600

Web、ssh、telnet会话的绝对会话超时(秒):3600

串行控制台会话超时(秒):600

串行控制台绝对会话超时(秒):3600

管理员身份验证服务器组:

操作身份验证服务器组:

第2因素的使用:无

步骤3.要配置TACACS服务器参数,请运行以下命令。

fpr4120-TAC-A#范围安全

fpr4120-TAC-A /security # scope tacacs

fpr4120-TAC-A /security/tacacs # 输入server 10.88.244.50

fpr4120-TAC-A /security/tacacs/server # set descr "ACS Server"

fpr4120-TAC-A /security/tacacs/server* # set key

输入密钥:******

确认密钥:******

步骤4.使用show detail命令检验配置。

fpr4120-TAC-A /security/tacacs/server* # show detail

TACACS+ 服务器:

主机名、FQDN或IP地址:10.88.244.50

描述:

订单:1

端口:49

密钥:****

超时:5

配置ISE服务器

将FXOS添加为网络资源

步骤1.导航至Administration > Network Resources > Network Devices。

步骤2.单击ADD。



步骤3.输入所需的值(Name、IP Address、Device Type和Enable TACACS+并添加KEY),单击 Submit。

dentity Services Engine	Home ► C	ontext Visibility	 Operations 	Policy	Administration	Work Centers		
System Identity Management	- Network Resou	urces Device P	ortal Management	pxGrid Servi	ces Feed Servic	Threat Centric N	NAC	
Network Devices Network Device C	Groups Networ	rk Device Profiles	External RADIUS	Servers RAE	OUS Server Sequence	es NAC Managers	External MDM	Location Services
0								
Network devices	Network Dev	ices List > FXOS						
Default Device	HELWOIK	Vevices	* Name EVO	c	_			
Device Security Settings			Description	5				
	* IP A	ddress: 10.83.180	0.6 /	32				
		• De	vice Profile	Cisco 👻 🕀				
		M	odel Name					
		Softwa	are Version					
	* Netwo	ork Device Group						
	Device	Type FXOS	<u>ଁ</u>	et To Default				
	IP	SEC No	Si Si	et To Default				
	Loca	ation All Locations	<u>ତ</u> ୍ର	et To Default				
	RA	DIUS Authentication	Settings					
	🗹 🔻 TA(CACS Authentication	n Settings					
			Sha	ared Secret .	•••••	Show		
			Enable Single Cor	nnect Mode				
				•	Legacy Cisco Device TACACS Draft Com	e bliance Single Connect	Support	
	□ ► SN	MP Settings						
	Adv	vanced TrustSec Se	ttings					
	Save	leset						

创建身份组和用户

步骤1.导航至Administration > Identity Management > Groups > User Identity Groups。

步骤2.单击ADD。

Indentity Services Engine Home	Context Visibility Operations Policy Adn	inistration Work Centers
► System Identity Management Network	Resources	Feed Service Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups ✓ Edit ♣Add ★Delete ▼ ♣Import ♣ Export	*
Endpoint Identity Groups	Name	Description
User Identity Groups	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Employee	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
	GuestType_Weekly (default)	Identity group mirroring the guest type
	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

步骤3.输入名称值,然后单击"提**交"。**

dentity Services Engine Ho	me	
System Identity Management Net	twork Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Identities Groups External Identity Se	ources Identity Source Sequences	
Identity Groups	User Identity Groups > New User Identity Group Identity Group Name FXOS ADMIN Description Submit Cance	

步骤4.对所有所需的用户角色重复步骤3。

dent	ity Service:	s Engine	Home	Context Visibility	 Operations 	▶ Policy	 Administration 	Work Centers	
System	- Identity N	lanagement	Network F	Resources Device	e Portal Manageme	nt pxGrid S	Services + Feed Se	rvice	
Identities	Groups	External Ider	tity Sources	Identity Source Seq	uences Settin	gs			

Identity Groups	P	User Identity Groups	
↓ E •	<u>نې</u>	✓ Edit ♣Add XDelete ▼ ♣Import ♣ Export	•
Endpoint Identity Groups		Name	Description
User Identity Groups		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
		Ame: Currently Sorted	Default Employee User Group
		🗌 💐 FXOS AAA	
		E A FXOS ADMIN	
		E PROS OPER	
		FXOS Read Only	
			Default cholin Accolings (default) lies come

步骤5.导航至Administration > Identity Management > Identity > Users。

步骤6.单击ADD。

-thata Identity Services Engine	Home	Operations Policy Administration	n					
System Identity Management	Network Resources	tal Management pxGrid Services + Fee	Service					
Identities Groups External Identity Sources Identity Source Sequences ▶ Settings								
G								
Users	Network Access Users							
Latest Manual Network Scan Results	/ Edit Add RChange Status	Import Export X Delete	Duplicate					
	Status Name	 Description 	First Name Last Name Email Address	User Identity Groups Admin				
				No data available				

步骤7.输入所需的值(Name、User Group、Password)。

dentity Serv	vices Engine Home	Context Visibility	 Operations 	Policy	→ Adm	inistration	Work Cent	ers
System ▼ Ident	ity Management Network	Resources Device	e Portal Management	pxGrid \$	Services	Feed Ser	vice I Thre	at Centric NAC
◄ Identities Group	es External Identity Sources	Identity Source Sequ	uences					
	()		and the second second					
Users	Netwo	atwork Access Users List > N	iew network Access	User				
Latest Manual Network	k Scan Results	etwork Access User						
	• N	ame fxosadmin						
	St	atus 🔽 Enabled 👻]					
	E	mail						
	×1	Passwords						
	P	assword Type: Intern	al Users	•				
		Passw	vord		Re-Enter	Password		
		Login Password	•••		•••••			Generate Password (
	E	nable Password						Generate Password
	~ 1	Jser Information						
	F	rst Name						
	L.	ast Name						
		and and and and						
	• /	Account Options						
		Descr	ription					
	c	hange password on next	t login					
		Account Disable Poli	icy					
] Disable account if da	te exceeds 2018-0	3-01		(уууу	-mm-dd)	
	¥.	User Groups						
		FXOS ADMIN	<mark>0</mark> — -					
	Sut	Cancel						

步骤8.对所有必需用户重复步骤6。

dentity Services Engine	Home + Conte	xt Visibility	Policy Administrat	on Work Centers						
System - Identity Management	Network Resources	s Device Portal Management	pxGrid Services + Fe	ed Service + Threat Cen	tric NAC					
0										
Users	Network Acce	ss Users								
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎲 Import	🕞 Export 👻 🗙 Delete 👻	Duplicate						
	Status	Name	Description	First Name Last N	ame Email Address	User Identity Groups	Admin			
	🗌 🛃 Enabled	👤 fxosaaa				FXOS AAA				
	Enabled	👤 fxosadmin				FXOS ADMIN				
	🗌 🛃 Enabled	9 fxosoper				FXOS OPER				
	🗌 🛃 Enabled	2 fxosro				FXOS Read Only				

为每个用户角色创建外壳配置文件

步骤1.导航至工作中心(Work Centers)>**设备管理(Device Administration)>策略元素(Policy** Elements)>**结果(Results)> TACACS配置文件(TACACS Profiles)**,然后单击**+添加(ADD)。**

dentity Services Engine	Home	licy Administration Work Centers				
Network Access Guest Access	TrustSec BYOD Profiler Posture Devi	ce Administration PassiveID				
Overview Identities User Identit	y Groups Ext Id Sources + Network Resources + Pe	blicy Elements Device Admin Policy Sets Reports Settings				
Conditions	0 Selected	Rows/Page 4 - Rows Go 4 Total Rows				
Network Conditions						
	🗘 Refresh 🕂 Add Duplicate 🏛 Trash	r Ø Edit Trilter - ♥ -				
✓ Results	□ Name	Type Description				
Allowed Protocols	WLC ALL	WLC WLC ALL				
TACACS Command Sets	U WLC MONITOR	WLC WLC MONITOR				
TACACS Profiles	Deny All Shell Profile	Shell Deny All Shell Profile				
	Default Shell Profile	Shell Default Shell Profile				

步骤2.输入TACACS配置文件所需的值

2.1.输入名称。

TACACS Profiles > New	
TACACS Profile	
Name	FXOS_Admin_Profile
Description	
Task Attribute View Raw	View

2.2.在"原始视图"选项卡中,配置以下CISCO-AV-PAIR。

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

TACACS Profiles > New

TACACS Profile

Name	FXOS_Admin_Profile
Description	
Task Attribute View Raw Profile Attributes	View
cisco-ay-pair=shell:roles="admin"	

Cancel Submit

2.3.单击"提**交"**。

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile		
Name	FXOS_Admin_Profile	
Description		
Task Attribute View Raw	v View	
Common Tasks		
Common Task Type Shell 🔹		
Default Privilege	0	(Select 0 to 15)
Maximum Privilege	0	(Select 0 to 15)
Access Control List	0	
Auto Command		
No Escape	©	(Select true or false)
	•	Minutes (0-9999)
	v	
Idle Time	0	Minutes (0-aaaa)
Custom Attributes		

🕇 Add 🍵 Trash 👻 🕑 E	Edit		۰- ۵
О Туре	Name	Value	
MANDATORY	cisco-av-pair	shell:roles="admin"	じ 前
			Cancel Save

步骤3.使用以下Cisco-AV-Pair对剩余的用户角色重复步骤2。

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

cisco-av-pair=shell:roles="只读"

Custom Attributes

🕇 Add 🍵 Trash 🗸 🖸	Edit		¢-
□ Туре	Name	Value	
MANDATORY	cisco-av-pair	shell:roles="aaa"	c 🗊
			Cancel Save

Custom Attributes

+ Ad	d 💼 Trash 🕶 🕑 E	dit			٥
	Туре	Name	Value		
	MANDATORY	cisco-av-pair	shell:ro	ies="operations"	C' 🗇
Custom	Attributes				
+ Add	i 💼 Trash ▾ 🖸 E	dit			¢ •
	Гуре	Name	Value		
	MANDATORY	cisco-av-pair	shell:rol	es="read-only"	C' 🗎
0 Sele	ACS Profiles	Duolicata 🚔 Trash	Rows	/Page 8 . M < 1 0 / 1 ► H Go	8 Total Rows
	Name	Dupildate i Itasii .	Type	Description	
	WLC ALL		WLC	WLC ALL	
	WLC MONITOR		WLC	WLC MONITOR	
	Deny All Shell Profil	e	Shell	Deny All Shell Profile	
	Default Shell Profile	1	Shell	Default Shell Profile	
	FXOS_Admin_Profi	le	Shell		
	FXOS_AAA_Shell		Shell		
	FXOS_Operations_	Shell	Shell		
	FXOS_ReadOnly_S	Shell	Shell		

创建TACACS授权策略

步骤1.导航至Work Centers > Device Administration > Device Admin Policy Sets。

cisco Identity Services Engine Home	Context Visibility + Operations + Policy + Administration Work Centers	③ ④ ● ●
Network Access Guest Access TrustSec	BYOD + Profiler + Posture + Device Administration + PassiveID	Click here to do wireless setup and visibility setup Do not show this again. X
Overview + Identities User Identity Groups	Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings	
Policy Sets Search policy names & descriptions.	Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration - System - Backup & Restore - Policy Export Page	
+-P- ++ X 2	Status Name Description	
Summary of Policies	Default Tacaka_Default Regular (Pray Sequence)	
Global Exceptions	✓ Proxy Server Sequence	
Rules across entire deployment	Proxy server sequence:	
Default Tacacs_Default	* Authentication Policy	
Save Order Reset Order	Default Rule (If no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores	Edt +
	Authorization Policy	
	Exceptions (0)	
	Standard	
	Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profiles	
	Tacacs, Default if no matches, then Select Profile (a) Deny At Shell Profile	Edit •

步骤2.确保身份验证策略指向内部用户数据库或所需的身份库。

•	Authent	ication Policy				
		Default Rule (If no match)	:	Allow Protocols : Default Device Admin	and use : All_User_ID_Stores	

步骤3.点击默认授权策略末尾的箭头,然后点击上方的插入规则。

 Authorization Policy 			
Exceptions (0)			
Standard			
Status Rule Name	Conditions (identity groups and other conditions) Command Sets	Shell Profiles	
Tacacs_Default	If no matches, then Select Profile(s) Deny All Shell Profile		Fritt
			Insert New Rule Above

步骤4.输入具有所需参数的规则值:

- 4.1.规则名称:FXOS管理规则。
- 4.2.条件。

如果:用户身份组为FXOS ADMIN

Status Rule Name	Cond	litions (ide	ntity grou	ps and other co	nditions)	Command Set	s She	Il Profiles
🖉 🗹 👻 FXOS Admin Rule	if	Any	^{Co} and	Condition(s)	÷	then Comman	🔶 and	Select a Shell Profile
Tacacs_Default	if no ma	Any			0	- +		
					Us	er Identity Groups	;	
						• = •	م انت)
						FXOS AAA	14	
						GuestType_Weekly (d	efault)	
						OWN_ACCOUNTS (de	fault)	_
	Ç				-	GROUP_ACCOUNTS (default)	
						FXOS ADMIN		
						FXOS OPER		
						Employee		
						GuestType_Daily (def	ault)	
						GuestType_Contractor	r (default)	
Caup Decat						FXOS Read Only		
Save						ALL_ACCOUNTS (defa	ult)	

设备:设备类型等于所有设备类型#FXOS

Conditions (identity group	os and other conditions)	Command Sets Sh	ell Profiles			
if FX 🛟 and	DEVICE:Devi 🗢 the	n Comman 🔶 and	Select a Shell Profile	\odot		
o matches, then Selec	Add All Conditions Be	ow to Library				-
	Condition Name	Description DEVICE:Device	Ty 😋 Equals 👻	All Device Types# 😋]	ŵ ₊
						þ
					All Device Types	₹ <u>0</u> 5
					All Device Types#FXOS	>
					DEVICE	>
					InternalUser Network Access	>
					Network Condition	>
					TACACS	>

外壳配置文件:FXOS_Admin_Profile

Shell Profile Shell Profile Shell Profile Image: Constraint of the state of the

步骤5.单击"**完成**"。

Exceptions (0)		
Standard		
Status Rule Name Conditions (identity	y groups and other conditions) Command Sets Shell Profiles	
🖉 🖌 🛃 🔹 FXOS Admin Rule 👘 FX 🔶	and DEVICE-Devi \diamondsuit then Select an item \diamondsuit and PXOS_Admin_Profile O	0
Tacacs_Default if no matches, then	Saloct Profile(s) Deny Al Shell Profile Edit	t •
Save Reset		

步骤6.对其余用户角色重复步骤3和4,完成后单击SAVE。

Authoriza	tion Policy					
Exception	ns (0)					
Standard						
Status	Rule Name		Conditions (identity groups and other conditions)		Command Sets	Shell Profiles
P 🔽	FXOS Admin Rule	if	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select an item	FXOS_Admin_Profile
ø 🔽	FXOS AAA Rule	if	FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select Profile(s)	FXOS_AAA_Shell
Ø 🗹	FXOS Operations Rule	if	FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select Profile(s)	FXOS_Operations_Shell
Ø 🗹	FXOS Read Only Rule	if	FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS			FXOS_ReadOnly_Shell
~	Tacacs_Default	if n	o matches, then Select Profile(s) Denv All S	hell P	rofile	



Save Reset

您现在可以测试每个用户并验证分配的用户角色。

FXOS机箱验证

1. Telnet或SSH至FXOS机箱,并使用ISE上任何已创建的用户登录。

username : fxosadmin

密码:

fpr4120-TAC-A#范围**安全**

fpr4120-TAC-A /security # show remote-user detail

远程用户fxosaa:

描述:

用户角色:

名称:**aaa**

名称:**只读**

远程用户fxosadmin:

描述:

用户角色:

名称:admin

名称:**只读**

远程用户fxosoper:

描述:

用户角色:

名称:**运营**

名称:**只读**

远程用户fxosro:

描述:

用户角色:

名称:**只读**

根据输入的用户名,FXOS机箱cli将仅显示为分配的用户角色授权的命令。

管理员用户角色。

fpr4120-TAC-A /security #?

确认确认

clear-user-sessionsclear User Sessions

创建托管对象

删除托管对象

禁用禁用服务

启用服务

输入管理对象

范围更改当前模式

设置属性值

显示系统信息

终止活动CIMC会话

fpr4120-TAC-A#connect fxos

fpr4120-TAC-A(fxos)# debug aaa aaa-requests

fpr4120-TAC-A(fxos)#

只读用户角色。

fpr4120-TAC-A /security #?

范围更改当前模式

设置属性值

显示系统信息

fpr4120-TAC-A#connect fxos

fpr4120-TAC-A(fxos)# debug aaa aaa-requests

拒绝角色的权限百分比

2.浏览到FXOS机箱IP地址,然后使用ISE上任何已创建的用户登录。

管理员用户角色。

Overview Interfaces Logic	cal Devices Security Engine Platform	Settings				
NTP SSH SNMP HTTPS AAA Syslog	LDAP RADIUS TACACS Properties Timeout:* 5 Secs TACACS Providers		Add TACACS Provider		() X	
FIPS and Common Criteria Access List	Hostname	Order	Hostname/FQDN(or IP Address):*			Add
	10.88.244.50	1	Order:" Key: Confirm Key: Port:" Timeout:"	lowest-available 49 5 Secs OK C	Set:No	
	Save Cancel					

只读用户角色。

Overview Interfaces Logi	cal Devices Security Engine Platfo	rm Settings			System T	ols Helj	p fxosro
NTP	LDAP RADIUS TACACS						
SSH SNMP	Properties						
HTTPS	Timeout:* 5 Secs						
Syslog	TACACS Providers						
ONS				OAdd			
FIPS and Common Criteria Access List	Hostname	Order	Port				
	10.88.244.50	1	49	9.8			

注意:请注意,"添加"按钮呈灰色显示。

ISE 2.0

1."">"TACACS"

altala j	dentity Services Engine	Home + Co	ntext Visibility	- Operations	Policy + Admin	istration + Work Centers			•	۹ 0	0
+ RAD	IUS Threat-Centric NAC Live L	.ogs TACACS	Troublest	ioot + Adaptive Netw	ork Control Repo	rts		Click here to do wireles	s setun and visibility setun (to not show this or	X
Live Lo	gs								a setup and tisking actup (o not anon une al	yan.
								tefresh Never • Show Late	est 20 records • Within	Last 3 hours	•
									_		
C Ref	resh 💆 Export To 🕶									¥ Filter •	۰۰
1	logged Time	Status	Details	Usemame	Туре	Authentication Policy	Authorization Policy	Failure Reason	Matched Comma	Shell Profile	
×				Username		Authentication Policy	Authorization Policy	Failure Reason	Matched Command S	Shell Profile	
	Jan 17, 2018 08:57:23.272 PM		0	fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admin_P	Profile
	Jan 17, 2018 08:57:22.852 PM	2	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default					
	Jan 17, 2018 08:57:10.829 PM	•	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			
	Jan 17, 2018 08:57:01.069 PM		9	fxosro	Authorization		Tacacs_Default >> FXOS Read Only			FXOS_ReadOnl	ly_S
	Jan 17, 2018 08:57:00.825 PM		0	fxosro	Authentication	Tacacs_Default >> Default >> Default					
	Jan 17, 2018 08:56:50.888 PM	۰	0	fxosro	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			

故障排除

要调试AAA身份验证和授权,请在FXOS cli中运行以下命令。

fpr4120-TAC-A#connect fxos

- fpr4120-TAC-A(fxos)# debug aaa aaa-requests
- fpr4120-TAC-A(fxos)# debug aaa event
- fpr4120-TAC-A(fxos)# debug aaa errors

fpr4120-TAC-A(fxos)#期限监控器

身份验证尝试成功后,您将看到以下输出。

2018年1月17日15:46:40.305247 aaa:aaa_req_process进行身份验证。session no 0

2018年1月17日15:46:40.305262 aaa:aaa_req_process:来自应用的常规AAA请求:login appln_subtype:默认

2018年1月17日15:46:40.305271 aaa:try_next_aaa_method

2018年1月17日15:46:40.305285 aaa:配置的方法总数为1,当前要尝试的索引为0

2018年1月17日15:46:40.305294 aaa:handle_req_using_method

2018年1月17日15:46:40.305301 aaa:AAA_METHOD_SERVER_GROUP

2018年1月17日15:46:40.305308 aaa:aaa_sg_method_handler group = tacacs

2018年1月17日15:46:40.305315 aaa:使用传递给此函数的sg_protocol

2018年1月17日15:46:40.305324 aaa:正在向TACACS服务发送请求

2018年1月17日15:46:40.305384 aaa:已成功配置方法组

2018年1月17日15:46:40.554631 aaa:aaa_process_fd_set

2018年1月17日15:46:40.555229 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月17日15:46:40.555817 aaa:mts_message_response_handler:MTS响应

2018年1月17日15:46:40.556387 aaa:prot_daemon_reponse_handler

2018年1月17日15:46:40.557042 aaa:会话: 0x8dfd68c已从会话表0中删除

2018年1月17日15:46:40.557059 aaa:is_aaa_resp_status_success状态= 1

2018年1月17日15:46:40.557066 aaa:is_aaa_resp_status_success为TRUE

2018年1月17日15:46:40.557075 aaa:aaa_send_client_response以进行身份验证。session->flags=21。aaa_resp->flags=0。

2018年1月17日15:46:40.557083 aaa:AAA_REQ_FLAG_NORMAL

2018年1月17日15:46:40.557106 aaa:mts_send_response成功

2018年1月17日15:46:40.557364 aaa:aaa_req_process进行授权。session no 0

2018年1月17日15:46:40.557378 aaa:aaa_req_process通过来自应用的上下文调用:login appln_subtype:default authen_type:2, authen_method:0

2018年1月17日15:46:40.557386 aaa:aaa_send_req_using_context

2018年1月17日15:46:40.557394 aaa:aaa_sg_method_handler组=(空)

2018年1月17日15:46:40.557401 aaa:使用传递给此函数的sg_protocol

2018年1月17日15:46:40.557408 aaa:基于情景或定向AAA请求(例外:不是中继请求)。 不会复制 AAA请求

2018年1月17日15:46:40.557415 aaa:正在向TACACS服务发送请求

2018年1月17日15:46:40.801732 aaa:aaa_send_client_response以进行授权。session->flags=9。 aaa_resp->flags=0。

2018年1月17日15:46:40.801740 aaa:AAA_REQ_FLAG_NORMAL

2018年1月17日15:46:40.801761 aaa:mts_send_response成功

2018年1月17日15:46:40.848932 aaa:旧操作码:accounting_interim_update

2018年1月17日15:46:40.848943 aaa:aaa_create_local_acct_req:user=, session_id=, log=added user:fxosadmin to role:admin

2018年1月17日15:46:40.848963 aaa:aaa_req_process,用于记帐。session no 0

2018年1月17日15:46:40.848972 aaa:MTS请求引用为NULL。本地请求

2018年1月17日15:46:40.848982 aaa:设置AAA_REQ_RESPONSE_NOT_NEEDEDED

2018年1月17日15:46:40.848992 aaa:aaa_req_process:来自应用的常规AAA请求:default appln_subtype:默认

2018年1月17日15:46:40.849002 aaa:try_next_aaa_method

2018年1月17日15:46:40.849022 aaa:没有默认配置方法

2018年1月17日15:46:40.849032 aaa:此请求没有可用的配置

2018年1月17日15:46:40.849043 aaa:try_fallback_method

2018年1月17日15:46:40.849053 aaa:handle_req_using_method

2018年1月17日15:46:40.849063 aaa:local_method_handler

2018年1月17日15:46:40.849073 aaa:aaa_local_accounting_msg

2018年1月17日15:46:40.849085 aaa:更新:::已添加用户:fxosadmin到角色:admin

身份验证尝试失败后,您将看到以下输出。

2018年1月17日15:46:17.836271 aaa:aaa_req_process进行身份验证。session no 0

2018年1月17日15:46:17.836616 aaa:aaa_req_process:来自应用的常规AAA请求:login appln_subtype:默认

2018年1月17日15:46:17.837063 aaa:try_next_aaa_method

2018年1月17日15:46:17.837416 aaa:配置的方法总数为1,当前要尝试的索引为0

2018年1月17日15:46:17.837766 aaa:handle_req_using_method

2018年1月17日15:46:17.838103 aaa:AAA_METHOD_SERVER_GROUP

2018年1月17日15:46:17.838477 aaa:aaa_sg_method_handler group = tacacs

2018年1月17日15:46:17.838826 aaa:使用传递给此函数的sg_protocol

2018年1月17日15:46:17.839167 aaa:正在向TACACS服务发送请求

2018年1月17日15:46:17.840225 aaa:已成功配置方法组

2018年1月17日15:46:18.043710 aaa:is_aaa_resp_status_success状态= 2

2018年1月17日15:46:18.044048 aaa:is_aaa_resp_status_success为TRUE

2018年1月17日15:46:18.044395 aaa:aaa_send_client_response以进行身份验证。session->flags=21。aaa_resp->flags=0。

2018年1月17日15:46:18.044733 aaa:AAA_REQ_FLAG_NORMAL

2018年1月17日15:46:18.045096 aaa:mts_send_response成功

2018年1月17日15:46:18.045677 aaa:aaa_cleanup_session

2018年1月17日15:46:18.045689 aaa:mts_drop request msg

2018年1月17日15:46:18.045699 aaa:aaa_req应被释放。

2018年1月17日15:46:18.045715 aaa:aaa_process_fd_set

2018年1月17日15:46:18.045722 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月17日15:46:18.045732 aaa:aaa_enable_info_config:GET_REQ for aaa login错误消息

2018年1月17日15:46:18.045738 aaa:返回配置操作的返回值:未知安全项

相关信息

启用TACACS/RADIUS身份验证时,FX-OS CLI上的Ethanalyzer命令将提示输入密码。此行为由 Bug引起。

Bug ID: CSCvg87518