Firepower可擴展作業系統(FXOS)2.2:使用 TACACS+通過ISE進行遠端管理的機箱身份驗證 /授權

目錄

簡介

本檔案介紹如何透過身分識別服務引擎(ISE)設定Firepower可擴充作業系統(FXOS)機箱的 TACACS+驗證和授權。

FXOS機箱包括以下使用者角色:

- Administrator 對整個系統的完全讀寫訪問許可權。預設情況下為預設管理員帳戶分配此角色 ,並且無法更改。
- 只讀 對系統配置的只讀訪問許可權,無修改系統狀態的許可權。
- 操作 對NTP配置、智慧許可的Smart Call Home配置以及系統日誌(包括系統日誌伺服器和 故障)的讀寫訪問許可權。對系統其餘部分的讀取訪問許可權。

• AAA — 對使用者、角色和AAA配置的讀寫訪問。對系統其餘部分的讀取訪問許可權。 通過CLI可以看到,如下所示:

fpr4120-TAC-A /security* # show role

角色:

角色名稱Priv

----- ----

aaa aaa

admin

運營運營

唯讀唯讀

作者:Tony Remirez、Jose Soto、Cisco TAC工程師。

必要條件

需求

思科建議您瞭解以下主題:

- Firepower可擴展作業系統(FXOS)知識
- ISE配置知識
- ISE中需要TACACS+裝置管理許可證

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco Firepower 4120安全裝置版本2.2
- 虛擬思科身分識別服務引擎2.2.0.470

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

此組態的目的是:

- 通過ISE驗證登入到FXOS基於Web的GUI和SSH的使用者
- 通過ISE根據使用者角色授權使用者登入FXOS基於Web的GUI和SSH。
- 通過ISE驗證FXOS上的身份驗證和授權操作是否正確

網路圖表



組態

配置FXOS機箱

建立TACACS+提供程式

步驟1.導覽至Platform Settings > AAA。

步驟2.按一下TACACS索引標籤。

Overview Interfaces Logi	cal Devices Security Engine	atform Settings							
NTP	LDAP RADIUS TACACS								
SSH									
SNMP	Properties	verties (Construction)							
HTTPS	Timeout:* 5 Secs	imeout:* 5 Secs							
► AAA									
Syslog	TACACS Providers								
DNS				O Add					
FIPS and Common Criteria	Hostaame	Order	Port						
Access List	nostiane	order	For						

步驟3.對於要新增的每個TACACS+提供程式(最多16個提供程式)。

3.1.在TACACS提供程式區域中,按一下Add。

3.2. 開啟「新增TACACS提供程式」對話方塊後,輸入所需的值。

3.3.按一下OK關閉「新增TACACS提供程式」對話方塊。

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

步驟4.按一下「Save」。

Overview Interfaces Logic	al Devices Security Engine Platform Setting	gs								
NTP SSH	LDAP RADIUS TACACS									
SNMP	Properties	verties International Internat								
HTTPS AAA	Timeout:* 5 Secs	eout:" Secs								
Syslog	TACACS Providers									
FIPS and Common Criteria			-	Add						
Access List	10.88.244.50	1	49	28						
		-		<i>~</i> u						
	Save Cancel									

步驟5.導覽至System > User Management > Settings。

步驟6.在Default Authentication下選擇TACACS。

Overview Interfaces	.ogical Devices Security Engine Platform Settings		5	iystem Too	ls Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	TACACS v tucal is fallback authentication method				
Console Authentication	Loai v				
Remote User Settings Remote User Role Policy	C Assign Default Role O No-Login				

使用CLI建立TACACS+提供程式

步驟1.要啟用TACACS身份驗證,請運行以下命令。

fpr4120-TAC-A#作用域**安全性**

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

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

步驟2.使用show detail命令驗證設定。

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

預設身份驗證:

管理領域:Tacacs

操作領域:Tacacs

Web會話刷新期間(秒):600

Web、ssh、telnet會話的會話超時(秒):600

Web、ssh、telnet會話的絕對會話超時(秒):3600

串列控制檯會話超時(秒):600

串列控制檯絕對會話超時(秒):3600

管理員身份驗證伺服器組:

操作身份驗證伺服器組:

使用第二個因素:否

步驟3.要配置TACACS伺服器引數,請運行以下命令。

fpr4120-TAC-A#作用域安全性

fpr4120-TAC-A /security # scope tacacs

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

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

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

輸入金鑰:******

確認金鑰:******

步驟4.使用show detail命令驗證設定。

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

TACACS+伺服器:

主機名、FQDN或IP地址:10.88.244.50

描述:

訂購:1

連接埠:49

主要:****

逾時:5

配置ISE伺服器

將FXOS新增為網路資源

步驟1.導覽至Administration > Network Resources > Network Devices。

步驟2.按一下ADD。



步驟3.輸入所需的值(名稱、IP地址、裝置型別和啟用TACACS+並新增金鑰),然後點選提交。

dentity Services Engine	Home	 Context Visibility 	 Operations 	Policy	 Administration 	 Work Centers 		
System Fidentity Management	- Network Re	esources Device	Portal Managemer	nt pxGrid Se	ervices + Feed S	ervice	AC	
Network Devices Network Device 0	Groups Net	twork Device Profiles	External RADIUS	S Servers F	RADIUS Server Seq	uences NAC Managers	External MDM	Location Services
0	Network 7							
Network devices	Network	k Devices						
Default Device			* Name FX	25				
Device Security Settings			Description					
	•1	P Address: 10.83.1	80.6	/ 32				
		• c	Device Profile	Cisco 👻 🕀				
			Model Name	*	1			
		Soft	ware Version	•]			
	* Ne	etwork Device Group						
	Devi	ice Type FXOS	o	Set To Default				
		IPSEC No	0	Set To Default				
	ı	Location All Location	is 📀	Set To Default				
		DADIUS Authentiesti	on Cottingo					
		RADIUS Authenticatio	on Settings					
	•	TACACS Authenticati	on Settings					
			Sh	nared Secret	•••••	Show		
			Enable Single Co	nnect Mode (🔄			
					TACACS Draft (Compliance Single Connect	Support	
		SNMP Settings						
	□,	Advanced TrustSec S	Settings					
	Save	Reset						

建立身份組和使用者

步驟1.導航到管理>身份管理>組>使用者身份組。

步驟2.按一下ADD。

cisco Ident	tity Service:	s Engine	Home	Context Visibility	 Operations 	Policy	- Administration	Work Centers	
System	✓ Identity N	lanagement	Network	Resources	Portal Managemer	nt pxGrid S	Services Feed Se	rvice	
Identities	Groups	External Ider	ntity Sources	Identity Source Sequ	uences + Setting	IS			

Identity Groups	User Identity Groups	User Identity Groups							
⟨= • E • §	/ 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							

步驟3.輸入Name的值,然後按一下**Submit。**

den cisco	tity Services Engine	Home	Context Visibility	 Operations 	▶ Policy	- Administration	Work Centers	
 System 	✓ Identity Management	Network Re	esources + Devic	e Portal Managemen	t pxGrid S	ervices + Feed S	ervice	
Identities	Groups External Ide	ntity Sources	Identity Source Sec	quences + Setting	S			
Identity	r Groups	م چ	User Identity Gr Identity Gro Name Description Submit	oups > New User Ide NUP FXOS ADMIN	entity Group]		

步驟4.對所有所需的使用者角色重複步驟3。

cisco Ident	tity Services Engine	Home	Context Visibility	 Operations 	Policy	- Administration	▶ Work Centers
 System 	- Identity Management	Network	Resources Device	Portal Management	pxGrid S	ervices + Feed Se	ervice
Identities	Groups External Ide	ntity Sources	Identity Source Sequ	uences			

Identity Groups	P	User Identity Groups						
↓ E •	<u>نې</u>	✓ Edit ♣Add X 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					
		🗌 💐 FXOS AAA						
		E A FXOS ADMIN						
		E PROS OPER						
		FXOS Read Only						
			Defects oppoint accountry (defects) there cause					

步驟5.導航到管理>身份管理>身份>使用者。

步驟6.按一下ADD。

-thata Identity Services Engine	Home Context	Visibility	Policy	- Administration	Work Center	8				
System Identity Management	Network Resources	Device Portal Managemen	t pxGrid Ser	rvices + Feed Se	rvice + Threat	Centric NAC				
Identities Groups External Identity	Identities Groups External Identity Sources Identity Source Sequences ▶ Settings									
0										
Users	Network Access	s Users								
Latest Manual Network Scan Results	Latest Manual Network Scan Results									
	Status	Name	 Description 	Firs	t Name La	ast Name	Email Address	User Identity Groups	Admin	
							,	No data available		

步驟7.輸入所需的值(名稱、使用者組和密碼)。

cisco Id	entity Service	es Engine	Home	 Context Visi 	ibility 🕨	Operations	Policy	▼ Adm	inistration	• Work C	enters
 System 	n 🔽 Identity I	Management	Network	Resources >	Device Port	tal Managemen	t pxGrid	Services	Feed Ser	rvice + Th	reat Centric NAC
- Identiti	es Groups	External Identi	ty Sources	Identity Sour	ce Sequence	es	S				
		0	Notword		Lint a Marca M						
Users			Network	twork Access	LISt > New P	Tetwork Access	s User				
Latest Mar	nual Network So	can Results	• 110	LWOIR ACCESS	soser						
			• Na	me fxosadmir	n						
			Sta	itus 🔽 Enab	oled +						
			Er	nail							
			• P	asswords							
			Pa	ssword Type:	Internal Us	sers	•				
					Password			Re-Enter	Password		
			·	ogin Password	•••••			•••••			Generate Password (1)
			En	able Password							Generate Password
)
			- U	lser Informat	ion						
			Fir	st Name							
			La	st Name							
			▼ A	ccount Optio	ns						
					Description	n					
			Ch	ange password	on next logir	n 🗆					
			T A	ccount Disab	le Policy						
				count bisub	ic roney				_		
				Disable accou	unt if date ex	ceeds 2018-0	03-01		()))))	y-mm-dd)	
				lser Groups							
			E	XOS ADMIN		<u>o</u> – -					
			Sub	mit Cancel)						
			300	Cancel	J						

步驟8.對所有必需使用者重複步驟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		
- Identities Groups External Identity	y Sources Identity	Source Sequences	3				
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	

為每個使用者角色建立外殼配置檔案

步驟1。導覽至工作中心>裝置管理>原則元素>結果> TACACS設定檔,然後按一下+ADD。

dentity Services Engine	Home Context Visibility Operations Po	Nicy Administration Work Centers			
Network Access Guest Access	TrustSec BYOD Profiler Posture Devi	ce Administration PassiveID			
Overview Identities User Identi	y Groups Ext Id Sources + Network Resources - Pa	olicy Elements Device Admin Policy Sets Reports Settings			
Conditions TACACS Profiles 0 Selected Rows/Page 4 1 0 / 1 Go 4 Total Rows					
Network Conditions	C Refresh + Add Duplicate 🗂 Trash	 ✓ Edit ✓ Filter < ♦ 			
✓ Results	□ Name	Type Description			
Allowed Protocols	WLC ALL	WLC WLC ALL			
TACACS Command Sets	WLC MONITOR	WLC WLC MONITOR			
TACACS Profiles	Deny All Shell Profile	Shell Deny All Shell Profile			
	Default Shell Profile	Shell Default Shell Profile			

步驟2.輸入TACACS配置檔案所需的值

2.1.輸入名稱。

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

2.2.在**原始檢視**頁籤中,配置以下CISCO-AV配對。

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

TACACS Profiles > New

TACACS Profile

Name	FXOS_Admin_Profile
Description	
Task Attribute View Raw	View
Profile Attributes	
<u>cisco-av-pair</u> =shell:roles="admin"	

Cancel Submit

2.3.按一下**Submit**。

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile		
Name	FXOS_Admin_Profile	
Description		
Task Attribute View Raw	View	
Common Tasks		
Common Task Type Shell		
Default Privilege	٢	(Select 0 to 15)
Maximum Privilege	0	(Select 0 to 15)
Access Control List	0	
Auto Command	0	
No Escape	0	(Select true or false)
Timeout	0	Minutes (0-9999)
Idle Time	0	Minutes (0-9999)
Custom Attributes		

+ /	Add 🍵 Trash 🗸 🕑 E	dit		۰.
	Туре	Name	Value	
	MANDATORY	cisco-av-pair	shell:roles="admin"	C 🛍
			Ca	ncel Save

步驟3.使用以下Cisco-AV配對對其餘使用者角色重複步驟2。

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

cisco-av-pair=shell:roles="只讀"

Custom Attributes

+ Add	dit		۰.
🗆 Туре	Name	Value	
MANDATORY	cisco-av-pair	shell:roles="aaa"	C 🗊
		Cance	Save

Custom Attributes

+ Add	🕑 Edit			¢-
□ Туре	Name	Value		
MANDATORY	cisco-av-pair	shell:ro	les="operations"	C 🗇
ustom Attributes				Const.
+ Add 💼 Trash -	C Edit			٥-
□ Туре	Name	Value		
MANDATORY	cisco-av-pair	shell:ro	es="read-only"	G. 🗒
0 Selected	Add Duplicate 💼	Rows Trash ▼	/Page 8 🔽 M < 1 🔅 /	1 ► ► Go 8 Total Rows
Name		Туре	Description	
U WLC ALL		WLC	WLC ALL	
	TOR	WLC	WLC MONITOR	
Deny All She	ell Profile	Shell	Deny All Shell Profile	
Default Shel	Il Profile	Shell	Default Shell Profile	
FXOS_Adm	in_Profile	Shell		
FXOS_AAA	_Shell	Shell		
FXOS_Oper	rations_Shell	Shell		
FXOS_Read	dOnly_Shell	Shell		

建立TACACS授權策略

步驟1.導航到工作中心>裝置管理>裝置管理策略集。

ext Vability + Operations + Policy + Administration + Work Centers	① < 0 < 0
00 + Profiler + Posture + Device Administration + PassiveID	Click here to do wireless setup and visibility setup Do not show this again.
Sources + Network Resources + Policy Elements Device Admin Policy Sets Reports Settings	
ne the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. Patcy Export go to Administration > System > Backup & Resource > Policy Export Rege	
Status Name Description	
Ler O Prany Sequence O	
Proxy Server Sequence	
Authentication Policy	
Default Rule (If no match) : Allow Protocols : Default Device Admin and use : All_User_10_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(0) Deny Al Shell Profile	Edit •
	Mukhatity • Overdoors • More Centers 200 • Potators • Potators • Potators 200 • Potators • Potators • Potators 200 • Potators • Potators • Potators 200 • Potators • Potators • Potators 200 • Potators • Potators • Potators 200 • Potators • Potators • Potators 200 • Potators • Potators • Potators 200 • Potators • Description • Description 200 • Detators

步驟2.確保身份驗證策略指向內部使用者資料庫或所需的身份庫。

Ŧ	Authenti	cation Policy				
		Default Rule (If no match)	:	Allow Protocols : Default Device Admin	and use : All_User_ID_Stores	

步驟3.按一下預設授權策略末尾的箭頭,然後按一下上面的插入規則。

▼ 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	FAI	1.4
		Insert New Rule Above	

步驟4.輸入具有所需引數的規則值:

4.1.規則名稱:FXOS管理規則。

4.2.條件。

如果:使用者身份組為FXOS管理員

Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Prof	iles
FXOS Admin Rule	if Any Condition(s) 💠 then Comman 💠 and Selection	t a Shell Profile
Tacacs_Default	if no ma	
	User Identity Groups	
	FXOS AAA	
	GuestType_Weekly (default)	
	OWN_ACCOUNTS (default)	
	GROUP_ACCOUNTS (default)	
	L FXOS ADMIN	
	FXOS OPER	
	Employee	
	GuestType_Daily (default)	
	GuestType_Contractor (default)	
	FXOS Read Only	
Save	ALL_ACCOUNTS (default)	

和裝置:裝置型別等於所有裝置型別#FXOS

Conditions (identity groups	and other conditions)	Command Sets She	Il Profiles			
if FX 💠 and [DEVICE:Devi 🗢 ther	Comman 🔶 and	Select a Shell Profile	0		
o matches, then Selec	Add All Conditions Belo	w to Library				
	Condition Name	Description DEVICE:Device Ty	📀 Equals 👻	All Device Types# 📀]	ġ ₊
					(→ = .	م
					All Device Types All Device Types#FXOS	
					AD	>
					DEVICE	>
					InternalUser	>
					Network Access	>
					Network Condition	>
					TACACS	>

外殼配置檔案:FXOS_Admin_Profile

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

Exceptions (0)	
Standard	
Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profiles	
🛛 🖉 🗸 FXDS Admin Rule 🔰 🕅 FX 💠 ind DEVICE:Devi	Done
Tacaca_Default If no matches, then Select Profile(s) Deny Al Shetl Profile	Edit 🕶
Sive Reset	

步驟6.對其餘使用者角色重複步驟3和步驟4,並在完成後按一下SAVE。

 Authorization Policy 										
Exceptions (0)										
Standard										
Status	Rule Name		Conditions (identity groups and other conditions)		Command Sets	Shell Profiles				
i 🖉 🗹	FXOS Admin Rule	if	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select an item	FXOS_Admin_Profile				
1	FXOS AAA Rule	if	FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select Profile(s)	FXOS_AAA_Shell				
i in 🔽	FXOS Operations Rule	if	FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select Profile(s)	FXOS_Operations_Shell				
1	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 Pro	ofile					



驗證

現在,您可以測試每個使用者並驗證分配的使用者角色。

FXOS機箱驗證

1.通過Telnet或SSH訪問FXOS機箱,然後使用ISE上任何建立的使用者登入。

使用者名稱:fxosadmin

密碼:

fpr4120-TAC-A#scope安全

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

遠端使用者fxosaa:

說明:

使用者角色:

名稱:aaa

名稱:**唯讀**

遠端使用者fxosadmin:

說明:

使用者角色:

名稱:admin

名稱:**唯讀**

遠端使用者fxosper:

說明:

使用者角色:

名稱:**操作**

名稱:**唯讀**

遠端使用者fxosro:

說明:

使用者角色:

名稱:**唯讀**

根據輸入的使用者名稱,FXOS機箱cli將僅顯示已分配使用者角色的授權命令。

管理員使用者角色。

fpr4120-TAC-A /security #?

確認確認

clear-user-sessions Clear User Sessions

建立建立託管對象

刪除刪除託管對象

禁用禁用服務

啟用啟用服務

輸入輸入託管對象

作用域更改當前模式

set Set屬性值

顯示顯示系統資訊

終止活動的cimc會話

fpr4120-TAC-A#connect fxos

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

fpr4120-TAC-A(fxos)#

只讀使用者角色。

fpr4120-TAC-A /security #?

作用域更改當前模式

set Set屬性值

顯示顯示系統資訊

fpr4120-TAC-A#connect fxos

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

%角色許可權被拒絕

2.瀏覽到FXOS機箱IP地址,並使用ISE上任何建立的使用者登入。

管理員使用者角色。

Overview Interfaces Logic	al Devices Security Engine Platform Security	ettings				
NTP SSH SNMP HTTPS AAA	LDAP RADIUS TACACS Properties Timeout:* 5 Secs TACACS Browiders					
Syslog DNS FIPS and Common Criteria			Add TACACS Provider		?×	Add
Access List	Hostname	Order	Hostname/FQDN(or IP Address):*	lowest susibility		4.9
	10.00144.30		Confirm Key: Port:* Timeout:*	49 5 Secs	Set:No	~ 0
	Save Cancel			ОКСС	ancel	

只讀使用者角色。

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help (
NTP LDAP RADOUS YACACS	
SSH SAND Properties	
HTTPS Timeout:* 5 Secs	
Systep TACACS Providers	
DNS	O Add
FIDS and Common Criteria Hostname Order Port	
10.88.244.50 1 49	4 8

附註:請注意, ADD按鈕呈灰色顯示。

ISE 2.0

1. Operations > TACACS Livelog

cisco	Identity Services Engine	Home + Cont	text Visibility	Operations	Policy + Admin	istration + Work Centers			•	۹ 0	0
▶ F	ADIUS Threat-Centric NAC Live L	ogs TACACS	Troublesh	oot + Adaptive Netw	ork Control Repo	orts		Click here to do wireles	s sahun and visihility satun l	to not show this ar	X
Like Logs											Berr
							R	tefresh Nover • Show Late	est 20 records • Within	Last 3 hours	•
C	Refresh 💆 Export To 🕶									Filter -	÷.
	Logged Time	Status	Details	Username	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	2	0	fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admin_P	Profile
	Jan 17, 2018 08:57:22.852 PM		0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default					
	Jan 17, 2018 08:57:10.829 PM	۰	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			
	Jan 17, 2018 08:57:01.069 PM	2		fxosro	Authorization		Tacacs_Default >> FXOS Read Only			FXOS_ReadOnl	ly_S
	Jan 17, 2018 08:57:00.825 PM	2	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			

疑難排解

為了調試AAA身份驗證和授權,請在FXOS cli中運行以下命令。

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)# term mon

成功嘗試身份驗證後,您將看到以下輸出。

2018年1月17日15:46:40.305247 aaa:用於身份驗證的aaa_req_process。會話編號0

2018年1月17日15:46:40.305262 aaa:aaa_req_process:來自裝置的常規AAA請求:login appn_subtype:預設

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:配置的方法總數為1,要嘗試的當前索引為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:使用傳遞到此函式的sg_protocol

2018年1月17日15:46:40.305324 aaa:正在向TACACS服務傳送請求

2018年1月17日15:46:40.305384 aaa:配置的方法組成功

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響應

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

2018年1月17日15:46:40.557042 aaa:會話: 0x8dfd68c已從會話表0中刪除

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

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

2018年1月17日15:46:40.557075 aaa:用於身份驗證的aaa_send_client_response。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:用於授權的aaa_req_process。會話編號0

2018年1月17日15:46:40.557378 aaa:使用來自應用程式的上下文呼叫aaa_req_process:login appn_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 group = (空)

2018年1月17日15:46:40.557401 aaa:使用傳遞到此函式的sg_protocol

2018年1月17日15:46:40.557408 aaa:基於上下文或定向AAA請求(異常:不是中繼請求)。 將不獲取 aaa請求的副本

2018年1月17日15:46:40.557415 aaa:正在向TACACS服務傳送請求

2018年1月17日15:46:40.801732 aaa:用於授權的aaa_send_client_response。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:舊操作碼: 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 the role:admin

2018年1月17日15:46:40.848963 aaa:aaa_req_process用於記帳。會話編號0

2018年1月17日15:46:40.848972 aaa:MTS請求引用為空。LOCAL請求

2018年1月17日15:46:40.848982 aaa:設定AAA_REQ_RESPONSE_NOT_NEEDED

2018年1月17日15:46:40.848992 aaa:aaa_req_process:來自裝置的常規AAA請求:default appln_subtype:預設

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:沒有針對預設預設配置的方法

2018年1月17日15:46:40.849032 aaa:沒有可用於此請求的配置

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:update:::added user:fxosadmin至role:admin

身份驗證嘗試失敗後,您將看到以下輸出。

2018年1月17日15:46:17.836271 aaa:用於身份驗證的aaa_req_process。會話編號0

2018年1月17日15:46:17.836616 aaa:aaa_req_process:來自裝置的常規AAA請求:login appn_subtype:預設

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:配置的方法總數為1,要嘗試的當前索引為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:使用傳遞到此函式的sg_protocol

2018年1月17日15:46:17.839167 aaa:正在向TACACS服務傳送請求

2018年1月17日15:46:17.840225 aaa:配置的方法組成功

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

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

2018年1月17日15:46:18.044395 aaa:用於身份驗證的aaa_send_client_response。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:請求消息的mts_drop

2018年1月17日15:46:18.045699 aaa:應釋放aaa_req。

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登入錯誤消息

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

相關資訊

啟用TACACS/RADIUS身份驗證後,FX-OS cli上的Ethanalyzer命令將提示密碼輸入密碼。此行為 是由錯誤引起的。

錯誤id: <u>CSCvg87518</u>