Firepower可擴展作業系統(FXOS)2.2:使用 RADIUS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 RADIUS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

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

使用機箱管理器建立RADIUS提供程式

步驟1.導覽至Platform Settings > AAA。

步驟2.按一下RADIUS索引標籤。

Overview Interfaces Logi	cal Devices Security Engine Pla	tform Settings			
NTP	LDAP RADIUS TACACS				
SSH SNMP	Properties				
HTTPS	Timeout:* 5 Secs				
	Retries:* 1				
DNS	RADIUS Providers				
FIPS and Common Criteria					O Add
Access List	Hostname	Order	Service	Auth Port	

步驟3.對於要新增的每個RADIUS提供程式(最多16個提供程式)。

3.1.在RADIUS提供程式區域中,按一下Add。

3.2. 開啟「新增RADIUS提供程式」對話方塊後,輸入所需的值。

3.3.按一下確定關閉「新增RADIUS提供程式」對話方塊。

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

步驟4.按一下「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	RADIUS Providers				
FIPS and Common Criteria Access List					O Add
	Hostname	Order	Service	Auth Port	
	10.88.244.50	1	authorization	1812	<i>i</i>
	Save Cancel				

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

步驟6.在Default Authentication下選擇RADIUS。

Overview Interfaces	Logical Devices Security Engine Platform Settings			System To:	ols Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	RADIUS Vical is failback authentication method				
Console Authentication	Local V				
Remote User Settings					
Remote User Role Policy	SAssign Default Role ON-Login				

使用CLI建立RADIUS提供程式

步驟1。若要啟用RADIUS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 radius

步驟2.使用show detail命令顯示結果。

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

預設身份驗證:

管理領域:Radius

操作領域:Radius

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RADIUS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 radius

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

fpr4120-TAC-A /security/radius/server # set descr "ISE Server"

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

輸入金鑰:******

確認金鑰:******

步驟4.使用show detail命令顯示結果。

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

RADIUS伺服器:

主機名、FQDN或IP地址:10.88.244.50

描述:

訂購:1

身份驗證埠:1812

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RADIUS並新增金鑰),然後點選提交。

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	
0	8	
Network devices	Network Devices	
Default Device		
Device Security Settings		
	Description	
	* IP Address: 10.83.180.6 / 32	
	Device Profile det Cisco The Cisco	
	Model Name 👻	
	Software Version	
	Network Device Group	
	Device Type Exoc	
	Is IPSEC Device 💟 Set To Default	
	Location All Locations 📀 Set To Default	
	✓ RADIUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS	
	Shared Secret Show	
	CoA Port 1700 Set To Default	
	RADIUS DTLS Settings ①	
	DTLS Required 🔲 🕡	
	Shared Secret radius/dtls (1)	
	CoA Port 2083 Set To Default	
	Issuer CA of ISE Certificates for CoA Select if required (optional)	

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。

dent	ity Services Engine	Home 🕨	Context Visibility	▸ Operations	▶ Policy	- Administration	Work Centers
System	- Identity Management	Network Reso	ources Device	Portal Management	pxGrid S	ervices Feed Set	rvice
Identities	Groups External Ide	ntity Sources Ic	dentity Source Sequ	ences > Settings			

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								
	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 Sources Identity Source Sequences Settings									
0									
Users	Network Access Users								
Latest Manual Network Scan Results	/ Edit 🕂 Add	Change Status	Export	X Delete	uplicate				
	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)。

dentity Services Engine	tome Context Visibility Operations Policy Administration Work Centers	
System Identity Management	Network Resources	
✓Identities Groups External Identi	Sources Identity Source Sequences	
0	Network Assess Lister Mary Network Assess Lister	
Users	Network Access User List > new network Access User	_
Latest Manual Network Scan Results	* Network Access User	
	* Name fxosadmin	
	Status 🔽 Enabled 👻	
	Email	
	▼ Passwords	
	Password Type: Internal Users 💌	
	Password Re-Enter Password	
	Login Password Generate Password ()	
	Enable Password Generate Password ()	
	* User Information	_
	First Name	
	Last Name	
	▼ Account Options	
	Description	
	Change password on next login	
	- Assume Disable Dellar	
	✓ Account Disable Policy	
	Disable account if date exceeds 2018-03-01 (yyyy-mm-dd)	
	▼ User Groups	
	FXOS ADMIN 📀 — +	
	Submit Cancel	

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	ion 🔹 Work Ce	nters					
System Identity Management	Network Resources	s Device Portal Managemen	t pxGrid Services + Fe	ed Service + Th	reat Centric NAC					
- Identities Groups External Identity	Sources Identity	Source Sequences	5							
0	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 Name	Email Address	User Identity Groups	Admin		
	Enabled	👤 fxosaaa					FXOS AAA			
	Enabled	👤 fxosadmin					FXOS ADMIN			
	🗌 🗹 Enabled	9 fxosoper					FXOS OPER			
	🗌 🛃 Enabled	9 fxosro					FXOS Read Only			

為每個使用者角色建立授權配置檔案

步驟1。導覽至Policy > Policy Elements > Results > Authorization > Authorization Profiles。

dentity Services Engine	Home	Operations Policy	► Administration ► Work Centers	
Authentication Authorization Profilin	ng Posture Client Provisioning			
Dictionaries + Conditions - Results	5			
0				
Authentication	Standard Authorization	n Profiles		
Authorization	For Policy Export go to Admin	istration > System > Backup &	& Restore > Policy Export Page	
Plationation	/ Edit + Add Duplicat	e XDelete		
Authorization Profiles	Name		Profile	Description
Downloadable ACLs		2020	Ht Cierce (D)	Desurption Default profile used to blacklict wirelass devices. Engl
b Profiling		2055	350 CISCO (D	Delaur, prome used to blacklist wireless devices. Elist
Froming	Cisco_IP_Phones		atta Cisco ⊕	Default 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 Provisioning
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

步驟2.填充授權配置檔案的所有屬性。

2.1.配置配置檔名稱。

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 2th Cisco 👻 🕀

2.2.在進階屬性設定中,設定以下CISCO-AV-PAIR

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

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

2.3.按一下**儲存。**



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="aaa"
```

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

cisco-av-pair=shell:roles="只讀"





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

dentity Services Engine	Home → Context Visibility → Operations → Policy	Administration Work Centers							
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements								
Dictionaries Conditions - Results									
0									
▶ Authentication	Standard Authorization Profiles	Standard Authorization Profiles							
Authorization	For Policy Export go to Administration > System > Backup & F	<pre>kestore > Policy Export Page</pre>							
	/ Edit + Add C Duplicate								
Authorization Profiles		Profile							
Downloadable ACLs		Holie							
▶ Profiling	Blackhole_wireless_Access	esse Cisco (5							
, i ronning	Cisco_IP_Phones	diste Cisco ⊕							
▶ Posture	Cisco_WebAuth	🔐 Cisco 🕀							
	FXOS-AAA-PROFILE	disto Cisco 🕀							
Client Provisioning	FXOS-ADMIN-PROFILE	dete Cisco 🕀							
	FXOS-OPER-PROFILE	號 Cisco 🕀							
	FXOS-ReadOnly-PROFILE	deb Cisco 🕀							

建立身份驗證策略

步驟1。導覽至Policy > Authentication >, 然後點選要建立規則的位置旁邊的箭頭。



步驟2.設定簡單;可以更精細地完成,但在本範例中,我們將使用裝置型別:

名稱:FXOS驗證規則

IF選擇新屬性/值:裝置:裝置型別等於所有裝置型別#FXOS

允許協定:預設網路訪問

使用:內部使用者

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

 Default
 :use Internal Users

建立授權策略

步驟1。導覽至Policy > Authorization >, 然後點選箭頭網以編輯您要建立規則的位置。

cisce Identity	Services Engin	Home + Context Visibility + Operations Policy + Administration + Work	k Centers	🕕 q e o o
Authentication	Authorization	Profiling Posture Client Provisioning + Policy Elements		Click here to do wireless setup and visibility setup Do not show this again. \times
Authorizatio	n Policy			
Define the Author For Policy Expor	rization Policy by a t go to Administrat	onfiguring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. on > System > Backup & Restore > Policy Export Page		
First Matched R	ule Applies	×		
Exception	s (0)			
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
	Default	If no matches, then DenyAccess		Insert New Rule Above

步驟2.使用所需引數輸入授權規則的值。

2.1.規則名稱: Fxos < USER ROLE>規則。



2.2.如果:使用者身份組>選擇<使用者角色>。

conditions (identity groups and other condition	ons) Permissions
FX Condition(s)	🔶 then AuthZ Pr
na	
FXOS ADMIN	
	User Identity Groups
	FXOS AAA
	GuestType_Weekly (default)
	OWN_ACCOUNTS (default)
	GROUP_ACCOUNTS (default)
	E FXOS ADMIN
	FXOS OPER
	Employee
	GuestType_Daily (default)
	GuestType_Contractor (default)
	ALL_ACCOUNTS (default)

2.3.和: Create New Condition > Device:Device type Equals All Devices Types #FXOS。

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

2.4.許可權:標準>選擇使用者角色配置檔案

Permissions	
then FXOS-A ^{CD}	
FXOS-ADMIN-PROFILE	
	Standard
	Blackhole_Wireless_Access
	Cisco_IP_Phones
	🨪 Cisco_WebAuth
	C DenyAccess
	S FXOS-AAA-PROFILE
	S FXOS-ADMIN-PROFILE
	S FXOS-OPER-PROFILE
	KOS-ReadOnly-PROFILE
	SP_Onboard
	San Non_Cisco_IP_Phones
	RermitAccess
Status Rule Name	Conditions (identity groups and other conditions) Permissions
🖉 🗹 🛛 Fxos Admin Rule	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device then FXOS-ADMIN-PROFILE Types#FXOS

步驟3.對所有使用者角色重複步驟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	then FXOS-ADMIN-PROFILE
1		Fxos AAA Rule	FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
1		Fxos Oper Rule	FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-OPER-PROFILE
		Fxos Read only Rule	FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ReadOnly-PROFILE
	~	Default	no matches, then DenyAccess	

步驟4.按一下頁面底部的Save。



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連線到FXOS機箱,並使用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. 瀏覽至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 Logical	Devices Security Engine Platform S	ettings						System 1	Tools Help	fxosadmin
NTP SSH SNMP HTTPS	LDAP RADIUS TACADS Properties Tacada Sale						 			
AAA Syslog DNS FIPS and Common Criteria	Retries:* 1 RADIUS Providers		Add RADIUS Provider Hostname/FQDN(or IP Address):*	laund a silable	**	0				
Access List	Hostname	Order	Key:	KNWESK GVANADIE	Set:No	0 100				
	10.88.244.16	1	Confirm Key: Authorization Port:* Timeaut:* Retries:*	1812 5 Secs 1 OK Can	cel	2 8				

只讀使用者角色。

Overview In	interfaces	Logical D	Devices Security	Ingine Platform Sett	ings							
NTP			LDAP RADEUS	ACACS								
SSH			Propries									
HTTPS			Timeout:* 5 Secs									
Syslog			Retries*									
DNS			ALODS Providers									
FIPS and Com	d Common Criteria Jat							O A66				
PROESS LOS			Hostname		Order	Service	Auth Port					
			10.88.244.16		1	authorization	1812	9.8				

附註:請注意, ADD按鈕呈灰色顯示。

ISE 2.0驗證

1. 導覽至Operations > RADIUS > Live logs。您應該能夠看到成功和失敗的嘗試。

cisco	Identity Services Engi	ne Home	 Context Visi 	bility • Operatio	ns Polic	y Administration	Work Centers				🚺 🤉 e e e		
RADIUS Threat-Centric NAC Live Logs + TACACS + Troubleshoot + Adaptive Network Control Reports Click here to do wireless setup and visibility setup Do not show this again													
Live L	ogs Live Sessions												
		Misconfigured S	upplicants O	Misconfi	nfigured Network Devices 🔁		RADIUS Drops 💿	Client Stopped Respor	ding O	Repeat Counter O			
		0			0		0	0		0			
								Refresh N	aver • Sho	w Latest 20 records	Within Last 3 hours		
C Refresh O Reset Repeat Counts Z Export To - ▼ Filter -													
	Time	Status	Details	Repeat C	dentity	Authentication Po	blicy	Authorization Policy	Authorization Prof	iles Network Dev	Identity Group		
×]		Identity	Authentication Polis	cy	Authorization Policy	Authorization Profile	Network Device	Identity Group		
	Jan 20, 2018 10:14:09	1	0		fxosadmin	Default >> FXOS AL	UTHENTICATION RULE >> Default	Default >> Fxos Admin Rule	FXOS-ADMIN-PROF	ILE FXOS	User Identity Groups:FXOS		
	Jan 20, 2018 10:13:59	•	0	1	fxosadmin	Default >> FXOS Al	JTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS		
	Jan 20, 2018 10:09:01		0	1	fxosro	Default >> FXOS Al	JTHENTICATION RULE >> Default	Default >> Fxos Read only Rule	FXOS-ReadOnly-PR	OFILE FXOS	User Identity Groups:FXOS		
	Jan 20, 2018 10:08:50	•	0	1	fxosro	Default >> FXOS AU	JTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS		
	Jan 20, 2018 10:06:17	•	0	1	fxosro	Default >> FXOS AL	UTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS		
	Jan 20, 2018 10:05:15	•	0	1	fxosro	Default >> FXOS AL	JTHENTICATION RULE >> Default			FXOS	User Identity Groups:FXOS		
	Jan 20, 2018 10:04:23	1	0		fxosadmin	Default >> FXOS AL	UTHENTICATION RULE >> Default	Default >> Fxos Admin Rule	FXOS-ADMIN-PROF	ILE FXOS	User Identity Groups:FXOS		
	Jan 20, 2018 10:02:59		à +		fxosadmin 🔸	Default >> FXOS AL	UTHENTICATION RULE >> Default	Default >> Fxos Admin Rule	FXOS-ADMIN-PROF	ILE FXOS	User Identity Groups:FXOS		

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20日17:18:02.410275 aaa:用於身份驗證的aaa_req_process。會話編號0

2018年1月20日17:18:02.410297 aaa:aaa_req_process:來自裝置的常規AAA請求:login appn_subtype:預設

2018年1月20日17:18:02.410310 aaa:try_next_aaa_method

2018年1月20日17:18:02.410330 aaa:配置的方法總數為1,要嘗試的當前索引為0

2018年1月20日17:18:02.410344 aaa:handle_req_using_method

2018年1月20日17:18:02.410356 aaa:AAA_METHOD_SERVER_GROUP

2018年1月20日17:18:02.410367 aaa:aaa_sg_method_handler group = radius

2018年1月20日17:18:02.410379 aaa:使用傳遞到此函式的sg_protocol

2018年1月20日17:18:02.410393 aaa:正在向RADIUS服務傳送請求

2018年1月20日17:18:02.412944 aaa:mts_send_msg_to_prot_daemon:負載長度= 374

2018年1月20日17:18:02.412973 aaa:會話: 0x8dfd68c已新增到會話表1

2018年1月20日17:18:02.412987 aaa:配置的方法組成功

2018年1月20日17:18:02.656425 aaa:aaa_process_fd_set

2018年1月20日17:18:02.656447 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月20日17:18:02.656470 aaa:mts_message_response_handler:mts響應

2018年1月20日17:18:02.656483 aaa:prot_daemon_response_handler

2018年1月20日17:18:02.656497 aaa:會話: 0x8dfd68c已從會話表0中刪除

2018年1月20日17:18:02.656512 aaa:is_aaa_resp_status_success status = 1

2018年1月20日17:18:02.656525 aaa:is_aaa_resp_status_success為TRUE

2018年1月20日17:18:02.656538 aaa:用於身份驗證的aaa_send_client_response。session->flags=21. aaa_resp->flags=0。 2018年1月20日17:18:02.656550 aaa:AAA_REQ_FLAG_NORMAL

2018年1月20日17:18:02.656577 aaa:mts_send_response成功

2018年1月20日17:18:02.700520 aaa:aaa_process_fd_set:aaa_accounting_q上的mtscallback

2018年1月20日17:18:02.700688 aaa:舊操作碼:accounting_interim_update

2018年1月20日17:18:02.700702 aaa:aaa_create_local_acct_req:user=, session_id=, log=added user fxosro

2018年1月20日17:18:02.700725 aaa:aaa_req_process用於記帳。會話編號0

2018年1月20日17:18:02.700738 aaa:MTS請求引用為空。LOCAL請求

2018年1月20日17:18:02.700749 aaa:設定AAA_REQ_RESPONSE_NOT_NEEDED

2018年1月20日17:18:02.700762 aaa:aaa_req_process:來自裝置的常規AAA請求:default appln_subtype:預設

2018年1月20日17:18:02.700774 aaa:try_next_aaa_method

2018年1月20日17:18:02.700798 aaa:沒有針對預設預設配置的方法

2018年1月20日17:18:02.700810 aaa:沒有可用於此請求的配置

2018年1月20日17:18:02.700997 aaa:aaa_send_client_response用於記帳。session->flags=254. aaa_resp->flags=0。

2018年1月20日17:18:02.701010 aaa:舊庫記帳請求的響應將作為SUCCESS傳送

2018年1月20日17:18:02.701021 aaa:此請求不需要響應

2018年1月20日17:18:02.701033 aaa:AAA_REQ_FLAG_LOCAL_RESP

2018年1月20日17:18:02.701044 aaa:aaa_cleanup_session

2018年1月20日17:18:02.701055 aaa:應釋放aaa_req。

2018年1月20日17:18:02.701067 aaa:回退方法本地成功

2018年1月20日17:18:02.706922 aaa:aaa_process_fd_set

2018年1月20日17:18:02.706937 aaa:aaa_process_fd_set:aaa_accounting_q上的mtscallback

2018年1月20日17:18:02.706959 aaa:舊操作碼: accounting_interim_update

2018年1月20日17:18:02.706972 aaa:aaa_create_local_acct_req:user=, session_id=, log=added user:fxosr to the role:read-only

身份驗證嘗試失敗後,您將看到以下輸出。

2018年1月20日17:15:18.102130 aaa:aaa_process_fd_set

2018年1月20日17:15:18.102149 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月20日17:15:18.102267 aaa:aaa_process_fd_set

2018年1月20日17:15:18.102281 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月20日17:15:18.102363 aaa:aaa_process_fd_set

2018年1月20日17:15:18.102377 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月20日17:15:18.102456 aaa:aaa_process_fd_set

2018年1月20日17:15:18.102468 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月20日17:15:18.102489 aaa:mts_aaa_req_process

2018年1月20日17:15:18.102503 aaa:用於身份驗證的aaa_req_process。會話編號0

2018年1月20日17:15:18.102526 aaa:aaa_req_process:來自裝置的常規AAA請求:login appn_subtype:預設

2018年1月20日17:15:18.102540 aaa:try_next_aaa_method

2018年1月20日17:15:18.102562 aaa:配置的方法總數為1,要嘗試的當前索引為0

2018年1月20日17:15:18.102575 aaa:handle_req_using_method

2018年1月20日17:15:18.102586 aaa:AAA_METHOD_SERVER_GROUP

2018年1月20日17:15:18.102598 aaa:aaa_sg_method_handler group = radius

2018年1月20日17:15:18.102610 aaa:使用傳遞到此函式的sg_protocol

2018年1月20日17:15:18.102625 aaa:正在向RADIUS服務傳送請求

2018年1月20日17:15:18.102658 aaa:mts_send_msg_to_prot_daemon:負載長度= 371

2018年1月20日17:15:18.102684 aaa:會話: 0x8dfd68c已新增到會話表1

2018年1月20日17:15:18.102698 aaa:配置的方法組成功

2018年1月20日17:15:18.273682 aaa:aaa_process_fd_set

2018年1月20日17:15:18.273724 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月20日17:15:18.273753 aaa:mts_message_response_handler:mts響應

2018年1月20日17:15:18.273768 aaa:prot_daemon_response_handler

2018年1月20日17:15:18.273783 aaa:會話: 0x8dfd68c已從會話表0中刪除

2018年1月20日17:15:18.273801 aaa:is_aaa_resp_status_success status = 2

2018年1月20日17:15:18.273815 aaa:is_aaa_resp_status_success為TRUE

2018年1月20日17:15:18.273829 aaa:用於身份驗證的aaa_send_client_response。session->flags=21. aaa_resp->flags=0。

2018年1月20日17:15:18.273843 aaa:AAA_REQ_FLAG_NORMAL

2018年1月20日17:15:18.273877 aaa:mts_send_response成功

2018年1月20日17:15:18.273902 aaa:aaa_cleanup_session

2018年1月20日17:15:18.273916 aaa:請求消息的mts_drop

2018年1月20日17:15:18.273935 aaa:應釋放aaa_req。

2018年1月20日17:15:18.280416 aaa:aaa_process_fd_set

2018年1月20日17:15:18.280443 aaa:aaa_process_fd_set:aaa_q上的mtscallback

2018年1月20日17:15:18.280454 aaa:aaa_enable_info_config:GET_REQ for aaa登入錯誤消息

2018年1月20日17:15:18.280460 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>