Firepower eXtensible Operating System(FXOS)2.2:TACACS+を使用したISEによ るリモート管理のためのシャーシ認証/許可

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 設定

 ネットワーク図

 設定

 FXOSシャーシの設定

 ISEサーバの設定

 確認

 FXOSシャーシ検証

 ISE 2.0 の検証

 トラブルシュート

 関連情報

概要

このドキュメントでは、Identity Services Engine(ISE)を介してFirepower eXtensible Operating System(FXOS)シャーシのTACACS+認証および認可を設定する方法について説明します。

FXOSシャーシには、次のユーザロールが含まれます。

- 管理者:システム全体への読み取り/書き込みアクセスを完了します。デフォルトの管理者ア カウントにはデフォルトでこのロールが割り当てられ、変更できません。
- ・読み取り専用:システムの状態を変更する権限のない、システム設定への読み取り専用アクセス。
- 操作:NTP設定、スマートライセンス用のSmart Call Home設定、システムログ(syslogサー バと障害を含む)への読み取りと書き込みのアクセス。システムの残りの部分への読み取り アクセス。
- AAA:ユーザ、ロール、およびAAA設定への読み取りおよび書き込みアクセス。システムの 残りの部分への読み取りアクセス。

CLIでは、次のように表示できます。

fpr4120-TAC-A /security* # show role

ロール:

ロール名の特権

aaa

admin admin

運用業務

読み取り専用

著者: Cisco TACエンジニア、Tony Remirez、Jose Soto

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower eXtensible Operating System(FXOS)に関する知識
- ISE設定に関する知識
- TACACS+デバイス管理ライセンスがISE内に必要

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower 4120セキュリティアプライアンスバージョン2.2
- 仮想Cisco Identity Services Engine(ISE)2.2.0.470

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

設定の目的は次のとおりです。

- ・ISEを使用して、FXOSのWebベースGUIおよびSSHにログインするユーザを認証します
- ISEを使用して、FXOSのWebベースGUIおよびSSHにログインするユーザを、それぞれのユ ーザロールに従って許可します。
- ISEを使用したFXOSでの認証と認可の適切な動作の確認

ネットワーク図



設定

FXOSシャーシの設定

TACACS+プロバイダーの作成

ステップ1:[Platform Settings] > [AAA]に移動します。

ステップ2:[TACACS]タブを**クリック**します。

Overview Interfaces Log	cal 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	nostname	order	Port	

ステップ3:追加する各TACACS+プロバイダー(最大16プロバイダー)について。

3.1. [TACACS Providers]領域で、[Add]をクリックします。

3.2. [Add TACACS Provider]ダイアログボックスが開いたら、必要な値を入力します。

3.3.「**OK**」をクリック**し**、「TACACSプロバイダーの追加」ダイアログ・ボックスを閉じ ます。

Í	Add TACACS Provider		?×	
I	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	icel	

ステップ4:[Save]をクリ**ックします**。

Overview Interfaces Log	cal Devices Security Engine Plat	form Settings		
NTP SSH SNMP HTTPS AAA Syslog DNS	LDAP RADIUS TACACS Properties Timeout:* 5 Secs TACACS Providers			Add
FIPS and Common Criteria	Hostname	Order	Port	
Access List	10.88.244.50	1	49	2
	Save			

ステップ5:[System] > [User Management] > [Settings]に移動します。

ステップ6:[Default Authentication]で[**TACACS**]を選択します。

Overview	Interfaces	Logical Devices Security Engine Platform Settings		1	System Too	ıls Help fxosadmin
			Configuration	Licensing	Updates	User Management
Local Users	Settings					
Default Aut	hentication	TACACS v *Local is falback authentication method				
Console Au	thentication	Local v				
Remote Us	er Settings					
Remote Us	er Role Policy	Assign Default Role No-Login				

CLIを使用したTACACS+プロバイダーの作成

ステップ1:TACACS認証を有効にするには、次のコマンドを実行します。

fpr4120-TAC-A#スコープセ**キュリティ**

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

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

ステップ2:show detailコマンドを使用して設定を確認します。

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

デフォルト認証:

管理レルム:**TACACS**

動作領域:TACACS

Webセッションの更新間隔(秒):600

Web、ssh、telnetセッションのセッションタイムアウト(秒):600

Web、ssh、telnetセッションの絶対セッションタイムアウト(秒):3600

シリアルコンソールセッションのタイムアウト(秒):600

シリアルコンソールの絶対セッションタイムアウト(秒):3600

管理認証サーバグループ:

動作認証サーバグループ:

2次係数の使用:No

ステップ3:TACACSサーバパラメータを設定するには、次のコマンドを実行します。

fpr4120-TAC-A#スコープセキュリティ

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

キーを入力します。******

キーを確認します。******

ステップ4:show detailコマンドを使用して設定を確認します。

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

TACACS+サーバ:

ホスト名、FQDN、またはIPアドレス: 10.88.244.50

descr :

発注:1

[Port]: 49

ポイント:****

タイムアウト:5

ISEサーバの設定

ネットワークリソースとしてのFXOSの追加

ステップ1:[Administration] > [Network Resources] > [Network Devices]の順に移動します。

ステップ2:[ADD]をクリッ**クします。**

dentity Services Engine	Home	Operations Policy	✓ Administration > W	fork Centers	
System Identity Management	Network Resources Device	Portal Management pxGrid	Services Feed Service	Threat Centric NAC	
Network Devices Network Device Gr	roups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers External MDM	Location Services
0					
Network devices	Network Devices				
Default Device					
Device Security Settings	/ Edit 🕂 Add 🕞 Duplicate	Export	Generate PAC X Delete		
	Name IP/Mas	sk Profile Name	Location	Туре	Description
					No data available

ステップ3:必要な値([Name]、[IP Address]、[Device Type]、[Enable TACACS+])を入力し、 [Submit]をクリックします。

dentity Services Engine	Home	 Context Visibility 	 Operations 	Policy	 Administration 	 Work Centers 		
System Identity Management	- Network R	esources Device	Portal Managemen	nt pxGrid Se	rvices Feed Se	rvice	NAC	
✓ Network Devices Network Device G	Broups Ne	twork Device Profiles	External RADIU	S Servers R	ADIUS Server Sequ	ences NAC Managers	External MDM	 Location Services
0	Mahurak	Devices Lists EVER						
Network devices	Network	rk Devices						
Default Device			* Name FX	ns				
Device Security Settings			Description					
	·	IP Address: 10.83.1	80.6	/ 32				
		• 0	Device Profile	Cisco 🔻 🕀				
		Soft	Model Name	ť				
		001		Ť				
	* N	letwork Device Group						
	Dev	vice Type FXOS	0	Set To Default	1			
		IPSEC No		Set To Default	,)			
		Location All Location		Set To Default)			
		All Cocado	ы <u> </u>		J			
	Ο,	RADIUS Authentication	on Settings					
	v	TACACS Authenticati	on Settings					
		monoo numentioati	on ootungo					
			Sł Enable Single Co	nared Secret	······	Show		
					 Legacy Cisco Der TACACS Draft Co 	vice ompliance Single Connect	Support	
	□,	SNMP Settings						
		Advanced TrustSec S	Settings					
	Save	Reset						

アイデンティティグループとユーザの作成

ステップ1:[Administration] > [**Identity Management] > [Groups] > [User Identity Groups]に移動しま** す。

ステップ2:[ADD]をクリッ**クします。**

cisco Identi	ity Service	s Engine	Home	Context Visib	ity • Operation	ons	Policy	▼ Admi	nistration	
System	- Identity M	lanagement	Network	Resources F	evice Portal Mana	igement	pxGrid S	ervices	Feed Se	ervice
Identities	Groups	External Ider	ntity Sources	Identity Source	Sequences +	Settings				

Identity Groups	User Identity Groups
(E - Q.	/ 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

ステップ3:[Name]に値を入力し、[Submit]をクリックします。

dentity	Services Engine	Home +	Context Visibility	 Operations 	▶ Policy	- Administration	Work Centers	
System	Identity Management	 Network Res 	sources + Device	e Portal Managemen	t pxGrid Ser	vices + Feed Ser	vice	
Identities	Groups External Ider	tity Sources	Identity Source Seq	uences • Setting	S			
Identity G v Identity G Endy G User	voups	م ڇ.	User Identity Gro Identity Gro Name [Description [Submit C	Pups > New User Ide up FXOS ADMIN	antity Group			

ステップ4:必要なすべてのユーザロールについて、ステップ3を繰り返します。

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

Identity Groups	٩	User Identity Groups				
↓ E +	<u>نې</u>	🖋 Edit 🕂 Add 🗙 Delete 👻 🎲 Import 🞲 Export	t v			
Endpoint Identity Groups		Name	Description			
User Identity Groups		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group			
		Employee	Default Employee User Group			
		E 🖉 FXOS AAA				
		FXOS ADMIN				
		E A FXOS OPER				
		FXOS Read Only				
			D.E. & CROUR ACCOUNTS (J.E. &) U.E. C			

ステップ5:[Administration] > [Identity Management] > [Identity] > [Users]に移動します。

ステップ6:[ADD]をクリッ**クします。**

lome → Context Visibility → Op	erations Policy Administrat	on Vork Centers							
System Veldentity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC									
✓Identities Groups External Identity Sources Identity Source Sequences > Settings									
0									
Network Access Users									
/ Edit + Add RChange Status	Export Export	Duplicate							
Status Name	 Description 	First Name Last Name	Email Address	User Identity Groups	Admin				
			N	lo data available					
	ome Contaxt Visibility Op letwork Resources Device Portal I ources Identity Source Sequences Network Access Users	ome > Context Visibility > Operations > Policy ~ Administration letwork Resources > Device Portal Management pxGrid Services > Fee ources Identity Source Sequences > Settings Network Access Users ✓ Edit — Add @ Change Status @ Import > Export > Delete Status Name > Description	Operations > Policy > Work Centers letwork Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC ources Identity Source Sequences > Settings Network Access Users	Operation > Policy ~ Administration > Work Centers letwork Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC ources Identity Source Sequences > Settings Network Access Users	• Context Visibility • Operations • Policy • Administration • Work Centers • Mork Centers • Mork Centers • Device Portal Management pxGrid Services • Feed Service • Threat Centric NAC • Ources Identity Source Sequences • Settings • Centers • Device Portal Management pxGrid Services • Feed Service • Threat Centric NAC • Centers • Ce				

ステップ7:必要な値(名前、ユーザグループ、パスワード)を入力します。

cisco	Identit	y Service	es Engine	Home	F Cor	ntext Visibility	y • Operations	Policy	✓ Adm	inistration	Work Cent	ers
Sys	tem	 Identity 	Management	Netwo	rk Resourc	ces Dev	vice Portal Managemer	nt pxGrid	Services	Feed Serv	vice • Threa	at Centric NAC
- Iden	ntities	Groups	External Ide	ntity Sourc	es Iden	tity Source S	Sequences	S				
				3 Note	ork Acces	e Lleore Liet	> New Network Acces	e Heer				
Users				Netw	OIK ACCES	S USEIS LISU	> New Network Acces	s User				
Latest M	Manual N	Network S	can Results	•	Network	Access Us	ser					
				•	Name fo	osadmin						
					Status	Enabled	•					
					Email							
					Passwo	rds						
					Password	Type: Int	ternal Users	-				
						Pag	eeword		Re-Enter	Password		
							554010		rte-Linter	103511010		
					 Login Pa 	ssword ••	•••••		•••••			Generate Password (i)
					Enable Pa	ssword						Generate Password (1)
				•	User In	formation						
					First Name	•						
					Last Name	•						
					Account	t Options						
						De	escription					
					Change pa	assword on r	next login					
					Account	t Disable P	Policy					
					Disat	e account if	f date exceeds 2018-	03-01		(7777-	-mm-dd)	
					User Gr	oups						
					FXOS AD	MIN	<u> </u>					
				S	ubmit	Cancel						

ステップ8:必要なすべてのユーザに対してステップ6を繰り返します。

Context Visibility		cy Administration	Work Center	15						
ork Resources + Device	Portal Management px0	Grid Services + Feed Se	ervice + Threat	Centric NAC						
Hdentities Groups External Identity Sources Identity Source Sequences → Settings										
0										
WORK ACCESS USERS										
idit 🕂 Add 🐻 Change S	tatus 👻 🎲 Import 👔 Ex	port + 🗙 Delete + 🖻	Duplicate							
Status Name	 Desc 	cription Fi	rst Name L	ast Name	Email Address	User Identity Groups	Admin			
🗹 Enabled 🛛 👤 fxosaaa						FXOS AAA				
🗹 Enabled 🛛 👤 fxosadm	in					FXOS ADMIN				
Enabled 9 fxosoper	r					FXOS OPER				
Enabled 9 fxosro						FXOS Read Only				
	Context Visibility rk Resources Device es Identity Source Sequ work Access Users dit	Contaxt Visibility Operations Poi rk Resources Device Portal Management pxi pxi	Context Visibility Operations Policy Administration rk Resources Device Portal Management pxGrid Services Feed S Identity Source Sequences Settings work Access Users It Change Status Name Description Fi Enabled fxosaaa Enabled fxosoper Enabled fxosoper Enabled fxosoper Enabled fxosoper Enabled fxosoper fxosoper				Contaxt Visibility Poperations Policy * Administration * Work Centers rrk Resources * Device Portal Management pxGrid Services * Feed Service * Threat Centric NAC es ldentity Source Sequences * Settings work Access Users sit * Policy profile sit * Partice profile vork Access sit * Partice profile reable status Name proscription First Name Last Name procos admin procos admin Procos oper procos oper procos oper procos oper procos oper			

各ユーザロールのシェルプロファイルの作成

ステップ1:[Work Centers] > [**Device Administration] > [Policy Elements] > [Results] > [TACACS** Profiles]に移動し、[+ ADD]をクリックします。

cisco Identity Services Engine	Home Context Visibility Operations Policy	y ► Administration
Network Access Guest Access	TrustSec + BYOD + Profiler + Posture	Administration PassiveID
Overview Identities User Identit	Groups Ext Id Sources + Network Resources - Police	y Elements Device Admin Policy Sets Reports Settings
Conditions	TACACS Profiles 0 Selected	Rows/Page 4 - I 3 / 1 D I Go 4 Total Rows
Network Conditions	C Refresh + Add Duplicate	© Edit ŢFilter → ♦ →
✓ Results	Name	Type Description
Allowed Protocols	U 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

ステップ2:TACACSプロファイルに必要な値を入力します

2.1. [Name]を入力します。

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

2.2. [RAW View]**タブで**、次のCISCO-AV-PAIRを設定します。

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

TACACS Profiles > New

TACACS Profile

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

Cancel Submit

2.3. [送信]をクリッ**クします**。

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile										
Nam	e FXOS_Admin_Profile									
Descriptio	n									
Task Attribute View R	aw View									
Common Tasks	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	0									
No Escape	٢	(Select true or false)								
Timeout	0	Minutes (0-9999)								
Idle Time	0	Minutes (0-9999)								
Custom Attributes										

+ Add	C Edit		¢-
□ Туре	Name	Value	
MANDATORY	cisco-av-pair	shell:roles="admin"	じ 副
			Cancel Save

ステップ3:次のCisco-AV-Pairsを使用して、残りのユーザロールについてステップ2を繰り返します。

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

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

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

Custom Attributes

+ Add	C Edit		٥
□ Туре	Name	Value	
MANDATORY	cisco-av-pair	shell:roles="aaa"	C 🗎
			Cancel Save

Custom Attributes

+ Ac	dd 💼 Trash 🕶 🕑 E	dit			¢-
	Туре	Name	Value		
	MANDATORY	cisco-av-pair	shell:ro	eles="operations"	ش ال
Custor	n Attributes				0
+ Ad	ld 🏛 Trash ▼ 🕑 E	dit			¢-
	Туре	Name	Value		
	MANDATORY	cisco-av-pair	shell:rol	es="read-only"	C 💼
0 Sel	ected Refresh + Add	Duplicate 🗂 Trash -	Rows	/Page 8 ▼ 1 € / 1 ► ► Go	8 Total Rows ter • • •
	Name		Туре	Description	
	WLC ALL		WLC	WLC ALL	
	WLC MONITOR		WLC	WLC MONITOR	
	Deny All Shell Profil	e	Shell	Deny All Shell Profile	
	Default Shell Profile	•	Shell	Default Shell Profile	
	FXOS_Admin_Profi	le	Shell		
	FXOS_AAA_Shell		Shell		
	FXOS_Operations_	Shell	Shell		
	FXOS_ReadOnly_S	Shell	Shell		

TACACS認可ポリシーの作成

ステップ1:[Work Centers] > [Device Administration] > [Device Admin Policy Sets]に移動します。

titude Identity Services Engine Home	Context Vability + Openations + Palicy + Administration + Work Centers	① < 0 < 0 < 0				
Network Access Guest Access TrustSec	BYOD + Profiler + Posture = Device Administration + PassiveID	Click here to do wireless setup and visibility setup Do not show this apain. X				
Overview Hentities User Identity Groups	Ext Id Sources + Network Resources + Policy Elements Device Admin Policy Sets Reports Settings					
Policy Sets Search policy names & descriptions. ,O	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					
++B+ ↑ ↓ × ⊕	Status Name Description					
Summary of Policies	Regular O Proxy Sequence O					
Global Exceptions Rules across entire deployment	Proxy Server Sequence 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					
	Tabacs_Default (in or matches, then Setter Profile) Deny Al Shell Profile	Edt •				

ステップ2:認証ポリシーが内部ユーザデータベースまたは必要なIDストアを指していることを確認します。

▼ Authentication Policy						
		Default Rule (If no match)	:	Allow Protocols : Default Device Admin	and use : All_User_ID_Stores	

ステップ3:デフォルトの認可ポリシーの最後にある矢印をクリックし、上の[Insert rule]をクリッ クします。

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

ステップ4:必要なパラメータを使用して、ルールの値を入力します。

4.1.ルール名:FXOS管理規則。

4.2条件

条件ユーザIDグループはFXOS ADMINです

Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles	
FXOS Admin Rule	if Any Condition(s) 💠 then Comman 💠 and Select a	Shell Profile
Zacacs_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)	
Cause Depart	FXOS Read Only	
Save Reset	ALL_ACCOUNTS (default)	



Conditions (identity groups and other conditions)	Command Sets Shell Profiles	
If FX 💠 and DEVICE:Devi 🗢 then	Comman 💠 and Select a Shell Profile 📀	
a matches, then Select Add All Conditions Below	to Library	
Condition Name	Description DEVICE:Device Ty 📀 Equals 🔹 All Device Types# 😒	ŵ .
		م بق • ا
		All Device Types
	U	All Device Types#FXOS
	E	AD >
	-	DEVICE >
	E	InternalUser >
	=	Network Access >
	E	Network Condition >
	•	TACACS >

シェルプロファイル:FXOS_Admin_Profile

Shell Profile Control Control	Shall Brofile
↓ ↓ <th>Shell Profile</th>	Shell Profile
 Control Control Contr	[م]
Default Shell Profile Deny All Shell Profile FXOS_AAA_Shell FXOS_Admin_Profile FXOS_Operations_Shell FXOS_ReadOnly_Shell WLC ALL WLC MONITOR	⟨= ▼ ■ ▼ ↔
Deny All Shell Profile FXOS_AAA_Shell FXOS_Admin_Profile FXOS_Operations_Shell FXOS_ReadOnly_Shell WLC ALL WLC MONITOR	Sefault Shell Profile
State State </td <td>S Deny All Shell Profile</td>	S Deny All Shell Profile
FXOS_Admin_Profile FXOS_Operations_Shell FXOS_ReadOnly_Shell WLC ALL WLC MONITOR	FXOS_AAA_Shell
State FXOS_Operations_Shell FXOS_ReadOnly_Shell WLC ALL WLC MONITOR WLC MONITOR	KOS_Admin_Profile
SeadOnly_Shell WLC ALL WLC MONITOR	FXOS_Operations_Shell
WLC ALL WLC MONITOR	FXOS_ReadOnly_Shell
WLC MONITOR	😪 WLC ALL
	WLC MONITOR

ステップ5:[完了]をクリ**ックします**。

► Exce	eptions (0)		
Stand	lawl		
Starra			
S	Itatus Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles	
i 🖉 🛃	▼ FXOS Admin Rule	FX 💠 and DEVICE-Devi 💠 that Select an Item 💠 and FXOS, Admin, Profile 🔘	Done
E	Tacacs_Default	if no matches, then Select Profile(s) Deny Al Shell Profile	Edit 🔻
_			
Save	Reset		

ステップ6:残りのユーザロールについてステップ3と4を繰り返し、完了したら[**SAVE**]をクリック**します**。

Except	ions (0)					
Standard						
Statu 🖌 🖉	IS Rule Name FXOS Admin Rule	Conditions (identii if FXOS ADMIN AN EQUALS All Devic	y groups and other conditions) DEVICE:Device Type the Types#FXOS	C then	Command Sets Select an item	Shell Profiles FXOS_Admin_Profile
ø 🔽	FXOS AAA Rule	if FXOS AAA AND I EQUALS All Device	DEVICE:Device Type ce Types#FXOS	then	Select Profile(s)	FXOS_AAA_Shell
Ø 🔽	FXOS Operations Rule	if FXOS OPER AND EQUALS All Device	DEVICE:Device Type e Types#FXOS	then	Select Profile(s)	FXOS_Operations_Shell
Ø 🗹	FXOS Read Only Rule	If FXOS Read Only EQUALS All Device	AND DEVICE:Device Type ce Types#FXOS			FXOS_ReadOnly_Shell
~	Tacacs_Default	if no matches, then	Select Profile(s) Deny All Si	hell Profi	ile	



確認

各ユーザをテストし、割り当てられたユーザロールを確認できます。

FXOSシャーシ検証

1. FXOSシャーシにTelnetまたはSSHで接続し、ISEで作成したユーザのいずれかを使用してログ インします。

ユーザ名:fxosadmin

パスワード:

fpr4120-TAC-A#スコープセ**キュリティ**

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

リモートユーザーfxosa:

説明:

ユーザ ロール:

[Name] : **[AAA]**

[Name]: 読み取り専用

リモートユーザーfxosadmin:

説明:

ユーザ ロール:

[Name] : admin

[Name]: 読み取り専用

リモートユーザーフ**ソッパー**:

説明:

- ユーザ ロール:
 - [Name]: 運用

[Name]: 読み取り専用

- リモートユー**ザーfxosro**:
 - 説明:

ユーザ ロール:

[Name]: 読み取り専用

FXOSシャーシのcliに入力したユーザ名に応じて、割り当てられたユーザロールに対して許可されたコマンドだけが表示されます。

管理者ユーザロール。

fpr4120-TAC-A /security #?

確認応答

clear-user-sessions Clear User Sessions

管理対象オブジェクトの作成

管理オブジェクトの削除

disableサービスを無効にします

サービスの有効化

入力マネージオブジェクトを入力

scope現在のモードを変更する

プロパティ値の設定

show system information

アクティブなcimcセッションの終了

fpr4120-TAC-A#connect fxos

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

fpr4120-TAC-A(fxos)#

読み取り専用ユーザロール。

fpr4120-TAC-A /security #?

scope現在のモードを変更する

プロパティ値の設定

show system information

fpr4120-TAC-A#connect fxos

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

%権限が拒否されました

2. FXOSシャーシのIPアドレスを参照し、ISEで作成したユーザのいずれかを使用してログインします。

管理者ユーザロール。



読み取り専用ユーザロール。

¢	iverview Interfaces Log	gical	Devices Security Engine	Platform Settings				System	Tools	Help	fxosro
	NTP SSH		LDAP RADIUS TACACS							_	_
	SNMP HTTPS		Properties Timeout:* 5 Secs								
ľ	Syslog		TACACS Providers								
	DNS FIPS and Common Criteria		Hostname	Orde	er	Port	0 44				
	PLACES LIFE		10.88.244.50	1		42	9,8				

注: [ADD]ボタンがグレー表示されていることに注意してください。

ISE 2.0

1. [Operations] > [TACACS Livelog]

dentity s	ervices Engine	Home + C	Context Visibility	- Operations	Policy + Admin	istration			3	۹ و	o o
RADIUS TI	reat-Centric NAC Live L	.ogs • TACAO	CS Troublesh	hoot + Adaptive Net	vork Control Repo	rts		Click here to do wirelet	is setup and visibility setup [o not show this	s again. ×
Live Logs											
								Refresh Nover Show Lat	est 20 records 🚽 Within	Last 3 hours	•
C Refresh	Export To -									¥ Filter •	۰۰
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, 2	018 08:57:23.272 PM	1	à	fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admin	_Profile
Jan 17, 2	018 08:57:22.852 PM	~	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default					
Jan 17, 2	018 08:57:10.829 PM	۰	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			
Jan 17, 2	018 08:57:01.069 PM	1	.0	fxosro	Authorization		Tacacs_Default >> FXOS Read Only			FXOS_Read(Dnly_S
Jan 17, 2	018 08:57:00.825 PM	1	0	fxosro	Authentication	Tacacs_Default >> Default >> Default					
Jan 17, 2	018 08:56:50.888 PM	۰	0	fxosro	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			

トラブルシュート

AAA認証と認可をデバッグするには、FXOS CLIで次のコマンドを実行します。

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

認証に成功すると、次の出力が表示されます。

2018 Jan 17 15:46:40.305247 aaa:aaa_req_processを使用します。session no 0

2018 Jan 17 15:46:40.305262 aaa:aaa_req_process:applnからの一般的なAAA要求:login appln_subtype:default

2018 Jan 17 15:46:40.305271 aaa:try_next_aaa_method

2018 Jan 17 15:46:40.305285 aaa:設定されたメソッドの総数は1、試行される現在のインデック スは0

2018 Jan 17 15:46:40.305294 aaa:handle_req_using_method

2018 Jan 17 15:46:40.305301 aaa:AAA_METHOD_SERVER_GROUP

2018 Jan 17 15:46:40.305308 aaa:aaa_sg_method_handler group = tacacs

2018 Jan 17 15:46:40.305315 aaa:この関数に渡されるsg_protocolの使用

2018 Jan 17 15:46:40.305324 aaa:TACACSサービスへの要求の送信

2018 Jan 17 15:46:40.305384 aaa:構成されたメソッドグループが成功しました

2018 Jan 17 15:46:40.554631 aaa:aaa_process_fd_set

2018 Jan 17 15:46:40.555229 aaa:aaa_process_fd_set:aaa_qのmtscallback

2018 Jan 17 15:46:40.555817 aaa:mts_message_response_handler:mts応答

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

2018 Jan 17 15:46:40.557042 aaa:session:0x8dfd68cがセッションテーブル0から削除されました

2018 Jan 17 15:46:40.557059 aaa:is_aaa_resp_status_success status = 1

2018 Jan 17 15:46:40.557066 aaa:is_aaa_resp_status_successはTRUEです

2018年1月17 15:46:40.557075 aaa:aaa_send_client_responseを使用します。session->flags=21. aaa_resp->flags=0.

2018 Jan 17 15:46:40.557083 aaa:AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:40.557106 aaa:mts_send_response成功

2018 Jan 17 15:46:40.557364 aaa:aaa_req_processを使用します。session no 0

2018 Jan 17 15:46:40.557378 aaa:aaa_req_process called with context from appln:login appln_subtype:default authen_type:2, authen_method:0

2018 Jan 17 15:46:40.557386 aaa:aaa_send_req_using_context

2018 Jan 17 15:46:40.557394 aaa:aaa_sg_method_handler group = (null)

2018 Jan 17 15:46:40.557401 aaa:この関数に渡されるsg_protocolの使用

2018 Jan 17 15:46:40.557408 aaa:コンテキストベースまたはダイレクトAAA要求(例外:リレー 要求ではありません)。 AAA要求のコピーを取らない

2018 Jan 17 15:46:40.557415 aaa:TACACSサービスへの要求の送信

2018 Jan 17 15:46:40.801732 aaa:aaa_send_client_response(認可用)。session->flags=9. aaa_resp->flags=0

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

2018 Jan 17 15:46:40.801761 aaa:mts_send_response成功

2018 Jan 17 15:46:40.848932 aaa:古いOPCODE:accounting_interim_update

2018 Jan 17 15:46:40.848943 aaa:aaa_create_local_acct_req:user=、session_id=、log=added user:fxosadmin to role:admin

2018 Jan 17 15:46:40.848963 aaa:aaa_req_process(アカウンティング用)。session no 0

2018 Jan 17 15:46:40.848972 aaa:MTS要求参照がNULLです。ローカル要求

2018 Jan 17 15:46:40.848982 aaa:AAA_REQ_RESPONSE_NOT_NEEDEDの設定

2018 Jan 17 15:46:40.848992 aaa:aaa_req_process:applnからの一般的なAAA要求:デフォルト のappln_subtype:default

2018 Jan 17 15:46:40.849002 aaa:try_next_aaa_method

2018 Jan 17 15:46:40.849022 aaa:デフォルトで設定されている方法はありません

2018 Jan 17 15:46:40.849032 aaa:この要求に使用できる構成がありません

2018 Jan 17 15:46:40.849043 aaa:try_fallback_method

2018 Jan 17 15:46:40.849053 aaa:handle_req_using_method

2018 Jan 17 15:46:40.849063 aaa:local_method_handler

2018 Jan 17 15:46:40.849073 aaa:aaa_local_accounting_msg

2018 Jan 17 15:46:40.849085 aaa:update:::added user:fxosadmin to role:admin

認証に失敗すると、次の出力が表示されます。

2018 Jan 17 15:46:17.836271 aaa:aaa_req_processを使用します。session no 0

2018 Jan 17 15:46:17.836616 aaa:aaa_req_process:applnからの一般的なAAA要求:login appln_subtype:default

2018 Jan 17 15:46:17.837063 aaa:try_next_aaa_method

2018 Jan 17 15:46:17.837416 aaa:設定されたメソッドの総数は1、試行される現在のインデック スは0

2018 Jan 17 15:46:17.837766 aaa:handle_req_using_method

2018 Jan 17 15:46:17.838103 aaa:AAA_METHOD_SERVER_GROUP

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

2018 Jan 17 15:46:17.838826 aaa:この関数に渡されるsg_protocolの使用

2018 Jan 17 15:46:17.839167 aaa:TACACSサービスへの要求の送信

2018 Jan 17 15:46:17.840225 aaa:構成されたメソッドグループが成功しました

2018 Jan 17 15:46:18.043710 aaa:is_aaa_resp_status_success status = 2

2018 Jan 17 15:46:18.044048 aaa:is_aaa_resp_status_successはTRUEです

2018 Jan 17 15:46:18.044395 aaa:aaa_send_client_responseを使用します。session->flags=21. aaa_resp->flags=0.

2018 Jan 17 15:46:18.044733 aaa:AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:18.045096 aaa:mts_send_response成功

2018 Jan 17 15:46:18.045677 aaa:aaa_cleanup_session

2018 Jan 17 15:46:18.045689 aaa:要求メッセージのmts_drop

2018 Jan 17 15:46:18.045699 aaa:aaa_reqは解放される必要があります。

2018 Jan 17 15:46:18.045715 aaa:aaa_process_fd_set

2018 Jan 17 15:46:18.045722 aaa:aaa_process_fd_set:aaa_qのmtscallback

2018 Jan 17 15:46:18.045732 aaa:aaa_enable_info_config:GET_REQ for aaa loginエラーメッセ ージ

2018 Jan 17 15:46:18.045738 aaa:設定操作の戻り値を取得しました:不明なセキュリティ項目

関連情報

TACACS/RADIUS認証が有効な場合、FX-OS CLIでEthanalyzerコマンドを実行すると、パスワードの入力を求めるプロンプトが表示されます。この動作はバグが原因です。

Bug ID: <u>CSCvg87518</u>