Firepower Système d'exploitation extensible (FXOS) 2.2 : Authentification/autorisation du châssis pour la gestion à distance avec ISE à l'aide de TACACS+

Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Diagramme du réseau Configurations Configuration du châssis FXOS Configuration du serveur ISE Vérification Vérification du châssis FXOS Vérification ISE 2.0 Dépannage Informations connexes

Introduction

Ce document décrit comment configurer l'authentification et l'autorisation TACACS+ pour le châssis Firepower eXtensible Operating System (FXOS) via Identity Services Engine (ISE).

Le châssis FXOS comprend les rôles d'utilisateur suivants :

- Administrateur : accès complet en lecture-écriture à l'ensemble du système. Ce rôle est attribué par défaut au compte d'administration par défaut et il ne peut pas être modifié.
- Lecture seule : accès en lecture seule à la configuration du système sans privilèges permettant de modifier l'état du système.
- Opérations : accès en lecture-écriture à la configuration NTP, à la configuration Smart Call Home pour Smart Licensing et aux journaux système, y compris les serveurs syslog et les pannes. Accès en lecture au reste du système.
- AAA : accès en lecture-écriture aux utilisateurs, aux rôles et à la configuration AAA. Accès en lecture au reste du système.

Par l'intermédiaire de l'interface de ligne de commande, ceci peut être vu comme suit :

fpr4120-TAC-A /security* # show role

Rôle :

Nom du rôle Priv.

aaa aaa

admin admin

opérations opérationnelles

lecture seule

Contribué par Tony Remirez, Jose Soto, Ingénieurs TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de Firepower eXtensible Operating System (FXOS)
- Connaissance de la configuration ISE
- La licence TACACS+ Device Administration est requise dans ISE

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité Cisco Firepower 4120 version 2.2
- Cisco Identity Services Engine virtuel 2.2.0.470

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

L'objectif de la configuration est de :

- Authentifier les utilisateurs qui se connectent à l'interface utilisateur graphique Web et à SSH de FXOS via ISE
- Autoriser les utilisateurs à se connecter à l'interface utilisateur graphique Web et à SSH de FXOS en fonction de leur rôle d'utilisateur respectif au moyen de ISE.
- Vérifier le bon fonctionnement de l'authentification et de l'autorisation sur FXOS par le biais de ISE

Diagramme du réseau



Configurations

Configuration du châssis FXOS

Création d'un fournisseur TACACS+

Étape 1. Accédez à Paramètres de la plate-forme > AAA.

Étape 2. Cliquez sur l'onglet **TACACS**.



Étape 3. Pour chaque fournisseur TACACS+ à ajouter (jusqu'à 16 fournisseurs).

3.1. Dans la zone Fournisseurs TACACS, cliquez sur Ajouter.

3.2. Une fois la boîte de dialogue Ajouter un fournisseur TACACS ouverte, saisissez les valeurs requises.

3.3. Cliquez sur **OK** pour fermer la boîte de dialogue Ajouter un fournisseur TACACS.

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	ncel	

Étape 4. Click Save.

Overview Interfaces Logic	cal Devices Security Engine Platform Settin	gs		
NTP	LDAP RADIUS TACACS			
SNMP	Properties			
HTTPS	Timeout:* 5 Secs			
AAA Sucion	TACACS Providers			
DNS				Add
FIPS and Common Criteria	Hostname	Order	Port	
Access List	10.88.244.50	1	49	28
				P 0
	Save Cancel			

Étape 5. Accédez à System > User Management > Settings.

Étape 6. Sous Authentification par défaut, sélectionnez TACACS.

Overview Interfaces	Logical Devices Security Engine Platform Settings	l i		System Too	ls Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	TACACS v fulcal is fallback authentication method				
Console Authentication	Local				
Remote User Settings Remote User Role Policy	S Assign Default Role 🔿 No-Login				

Création d'un fournisseur TACACS+ à l'aide de l'interface de ligne de commande

Étape 1. Afin d'activer l'authentification TACACS, exécutez les commandes suivantes.

fpr4120-TAC-A# scope security

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

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

Étape 2. Utilisez la commande show detail pour vérifier la configuration.

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

Authentification par défaut :

Domaine d'administration : Tacas

Domaine opérationnel : Tacas

Période d'actualisation de la session Web (en secondes) : 600

Délai d'attente de session (en secondes) pour les sessions web, ssh, telnet : 600

Délai d'attente de session absolue (en secondes) pour les sessions Web, ssh et telnet : 3600

Délai d'expiration de la session de la console série (en secondes) : 600

Délai d'attente de session absolue de la console série (en secondes) : 3600

Groupe de serveurs Admin Authentication :

Groupe de serveurs d'authentification opérationnelle :

Utilisation du deuxième facteur : Non

Étape 3. Afin de configurer les paramètres du serveur TACACS, exécutez les commandes suivantes.

fpr4120-TAC-A# scope security

fpr4120-TAC-A /security # scope tacacs

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

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

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

Saisissez la clé : ******

Confirmez la clé : ******

Étape 4. Utilisez la commande **show detail** pour vérifier la configuration.

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

Serveur TACACS+ :

Nom d'hôte, nom de domaine complet ou adresse IP : 10.88.244.50

Description :

Commande : 1

Port: 49

Clé : ****

timeout : 5

Configuration du serveur ISE

Ajout du FXOS en tant que ressource réseau

Étape 1. Accédez à Administration > Network Resources > Network Devices.

Étape 2. Cliquez sur Add.



Étape 3. Entrez les valeurs requises (Nom, Adresse IP, Type de périphérique et Activer TACACS+ et ajoutez la CLÉ), cliquez sur **Envoyer.**

dentity Services	s Engine Ho	me	/isibility > Operations	Policy Adr	ninistration 🔹 🕨	ork Centers		
System Identity M	fanagement - Ne	twork Resources	Device Portal Managemen	nt pxGrid Services	Feed Service	Threat Centric N	AC	
	etwork Device Group	Network Device	e Profiles External RADIU	S Servers RADIUS	Server Sequences	NAC Managers	External MDM	Location Services
	G							
Network devices	N	Network Devices List	s FXOS					
Default Device			Name EV	05				
Device Security Settings			Description					
		* IP Address:	10.83.180.6	/ 32				
			* Device Profile	Cisco 💌 🕀				
			Model Name	Ţ				
			Software Version	Ť				
		* Network Devi	ce Group					
		Device Type	xos 📀 🗄	Set To Default				
		IPSEC	ło 📀 🗄	Set To Default				
		Location A	All Locations 📀	Set To Default				
		RADIUS A	uthentication Settings					
		✓ TACACS A	uthentication Settings					
			Sł Enable Single Co	nared Secret	acy Cisco Device	Show	Support	
		SNMP Sett	ings					
		Advanced	TrustSec Settings					
		Save Reset						

Création des groupes d'identités et des utilisateurs

Étape 1. Accédez à Administration > Identity Management > Groups > User Identity Groups.

Étape 2. Cliquez sur Add.

Context Visibility > Operations > Policy - Admir	histration Work Centers
esources	Feed Service Threat Centric NAC
Identity Source Sequences	
User Identity Groups	
🖋 Edit 🕂 Add 🗙 Delete 👻 🎼 Import 😭 Export 👻	
Name	Description
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
	Context Visibility > Operations > Policy ~ Administrative context of the services Isources > Device Portal Management pxGrid Services Identity Source Sequences > Settings User Identity Groups

Étape 3. Entrez la valeur de Name et cliquez sur Submit.

den cisco	tity Services Engin	e Home	Context Visibility	 Operations 	Policy	Administration	► Work Centers
 System 	- Identity Manager	ent Network R	tesources + Devic	e Portal Managemen	t pxGrid Servi	ces + Feed Servic	ce
Identities	Groups Extern	al Identity Sources	Identity Source Se	quences + Setting	s		
Identity	y Groups	(م +@	User Identity Gr Identity Gr Name Description Submit	roups > New User Id Dup FXOS ADMIN Cancel	entity Group		

Étape 4. Répétez l'étape 3 pour tous les rôles utilisateur requis.

dentity Services Engine Home	Context Visibility Operations Policy Adr	ninistration
► System	esources	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
	E AAA	
	E Pros Admin	
	E Pros Oper	
	FXOS Read Only	
		Default cholin Accountry (default) liese come

Étape 5. Accédez à Administration > Identity Management > Identity > Users.

Étape 6. Cliquez sur Add.

-that- cisce Identity Services Engine	Home	ibility Operations I	Policy - Administration	► Work Centers			
System Identity Management	Network Resources	Device Portal Management	pxGrid Services Feed	Service			
◄ Identities Groups External Identity	Identities Groups External Identity Sources Identity Source Sequences ▶ Settings						
0							
Users	Network Access U	sers					
Latest Manual Network Scan Results	/ Edit 🕂 Add 📴 🛛	Change Status	Export X Delete	Duplicate			
	Status Nar	me 🔺 D	Description	First Name Last Name	Email Address	User Identity Groups	Admin
						No data available	

Étape 7. Saisissez les valeurs requises (Nom, Groupe d'utilisateurs, Mot de passe).

cisco Ident	ity Service	s Engine	Home	Context V	lsibility	 Operations 	Policy	▼ Adm	inistration	Work Ce	nters
System	- Identity I	Management	Network	Resources	Device F	Portal Managemen	t pxGrid	Services	Feed Se	rvice I Thr	reat Centric NAC
- Identities	Groups	External Identi	ty Sources	Identity So	urce Seque	ences	S				
		G	Matural								
Users			Netwon	Access User	s List > Ne	W Network Acces	s User				
Latest Manual	Network So	an Results	• Ne	LWORK ACCE	ss user						
			• Na	me fxosadm	nin						
			Sta	tus 🔽 Ena	abled 💌						
			En	nail							
			▼ P	asswords							
			Pa	ssword Type:	Internal	Users	Ŧ				
					Passwor	rd		Re-Enter	Password		
			•	ogin Passwor	d	•		•••••			Generate Password (i)
			En	able Passwor	d						Generate Password (
			ΨU	ser Informa	ation						
			Fin	st Name							
			La	st Name							
			▼ A	ccount Opti	ions						
					Descrip	tion					
			Ch	ange passwor	rd on next lo	ogin 🗆					
			▼ A	ccount Disa	ble Polic	У					
				Disable acc	ount if date	exceeds 2018-	03-01		())))	y-mm-dd)	
			× 11	ser Groupe							
				voc Annual							
			:: (E	NOS ADMIN							
			Subr	nit Cance	el						

Étape 8. Répétez l'étape 6 pour tous les utilisateurs requis.

Identity Services Engine	Home + Conte:	xt Visibility	Policy Administration	on 🔹 Work Cer	iters				
> System videntity Management > Network Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC									
Identities Groups External Identity Sources Identity Source Sequences ▶ Settings									
0	0								
Users	Network Acces	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	2 fxosoper					FXOS OPER		
	🗌 🗹 Enabled	9 fxosro					FXOS Read Only		

Création du profil Shell pour chaque rôle utilisateur

Étape 1. Accédez à Centres de travail > Administration des périphériques > Eléments de stratégie > Résultats > Profils TACACS et cliquez sur +AJOUTER.

dentity Services Engine	Home Context Visibility Operations Poli	cy Administration Work Centers					
Network Access Guest Access	TrustSec BYOD Profiler Posture Device	Administration PassiveID					
Overview Identities User Ident	ty Groups Ext Id Sources + Network Resources - Pol	cy Elements Device Admin Policy Sets Reports Settings					
Conditions TACACS Profiles 0 Selected Rows/Page 4 1 0 / 1 0 0 4 Total Rows							
Network Conditions	C Refresh + Add Duplicate 🛍 Trash -	G' Edit					
✓ 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					

Étape 2. Saisissez les valeurs requises pour le profil TACACS

2.1. Saisissez le nom.

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

2.2. Dans l'ONGLET Vue RAW, configurez CISCO-AV-PAIR suivant.

cisco-av-pair=shell : rôles=« 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. Cliquez sur Submit.

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile				
	Name FXOS_Admin_Profile			
Des	cription			
Task Attribute View	Raw View			
Common Tasks				
Common Task Type Shell	•			
Default Privilege		(Select 0 to 15)		
Maximum Privileg	ge	(Select 0 to 15)		
Access Control Li	ist	0		
Auto Command		0		
No Escape		Select true or f	alse)	
Timeout		O Minutes (0-9999)	
Idle Time		Minutes (0-9999)	
Custom Attributos				
Custom Attributes				
				+
Add Trash C E	Edit			Q
🗆 Туре	Name	Value		

Étape 3. Répétez l'étape 2 pour les autres rôles d'utilisateur à l'aide des paires Cisco-AV suivantes.

shell:roles="admin"

C 🖻

Save

Cancel

cisco-av-pair=shell : rôles=« aaa »

cisco-av-pair=shell : rôles=« opérations »

cisco-av-pair=shell : rôles=« lecture seule »

cisco-av-pair

Custom Attributes

MANDATORY

+ A	dd 🍵 Trash ▾ 🕑 E	dit		۰.
	Туре	Name	Value	
	MANDATORY	cisco-av-pair	shell:roles="aaa"	G 🗊
			Cance	I Save

Custom Attributes

+ Ad	ld 💼 Trash ▾ 🕑 B	Edit			¢-
	Туре	Name	Value	3	
	MANDATORY	cisco-av-pair	shell:r	oles="operations"	C 🛍
Custor	n Attributes				
+ Ad	d 💼 Trash 🕶 🕑 E	dit			¢-
	Туре	Name	Value		
	MANDATORY	cisco-av-pair	shell:ro	ples="read-only"	C' 🛍
TAC 0 Sel	ACS Profiles ected		Row	s/Page 8 ▼ M < 1 ⓒ /1 ► ► Go	8 Total Rows
C	Refresh 🕂 Add	Duplicate 🛍 Trash 🗸	C Ed	jit T Fil	ter 🕶 🌣 👻
	Name		Туре	Description	
	WLC ALL		WLC	WLC ALL	
	WLC MONITOR		WLC	WLC MONITOR	
	Deny All Shell Profi	le	Shell	Deny All Shell Profile	
	Default Shell Profile	9	Shell	Default Shell Profile	
	FXOS_Admin_Prof	ile	Shell		
	FXOS_AAA_Shell		Shell		
	FXOS_Operations_	Shell	Shell		
	FXOS_ReadOnly_S	Shell	Shell		

Création de la stratégie d'autorisation TACACS

Étape 1. Accédez à Centres de travail > Administration des périphériques > Jeux de stratégies d'administration des périphériques.

National Access & Justifice & BNOD + Profiler & Pasture - Device Administration + PassiveD Device Administration - PassiveD Device Administrati	cited In Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	(1) Q (1)
Verview * identifies User looking Groups Ext id Sources * Network Resources * Policy Extenses Device Admin Policy Sets Settings Policy Sets Sector backor names & Sector stores Sector backor names Sector backor names & Sector stores Sector backor names Sector backor names	Network Access Guest Access TrustSec	BYOD + Profiler + Posture Cevice Administration + PassiveID	Click here to do wireless setup and visibility setup Do not show this again. X
Paticy Sets Set or planes & description. Image: Paticy Experies Set or points in the basicy of planes and drop sets on the list had side to drange the order. Image: Paticy Experies Set or planes in the basicy of planes and drop sets on the list had side to drange the order. Image: Paticy Experies Set order drange the products Description Image: Paticy Experies Set order drange the order. Set or the list in the basicy Set on conditions. Dags and drop sets on the list had side to drange the order. Image: Paticy Experies Set order drange the products Description Image: Paticy Experies Set order drange the order. Set or the list in the basicy Set on conditions. Dags and drop sets on the list had side to drange the order. Image: Paticity Experies Set order Prove Set order Prove Set order Image: Paticity Experies Set order Image: Paticity Experies Set order Image: Paticity Experies Set order Image: Paticity Experies Set order Image: Paticity Experies Set order Image: Paticity Experies Set order Image: Paticity Experies Set order Image: Paticity Experies Set order Image: Paticity Experime Set order Image: Paticity Experime Experiment Set or drange the order order order order order order order order Image: Paticity Experiment Set order Image: Paticity Experiment Set order Image: Paticity Experiment Set order Image: Paticity Experiment Set order	Overview Identities User Identity Groups	Ext Id Sources + Network Resources + Policy Elements Device Admin Policy Sets Reports Settings	
Summary of Policies Orfault Tecast_Default A tot of all your policies Regular Proxy Sequence Regular Proxy Sequence Reduct constraint deployment Proxy Server Sequence Proxy Server Sequence * Authentication Policy Default Rule (if no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores Edit = * Authentication Policy Default Rule (if no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores Edit = * Authorization Policy Default Rule (if no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores Edit = * Status Rule Name Conditions (denthy groups and other conditions) Command Bes Shell Profiles	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 Suppring to A Administration > System > Buckup & Realow = > Policy Export Page Status > Name = ==================================	
Alse of all your polinics Is do bit all coop polinics Is all coop polinics </td <th>Summary of Policies</th> <td>Default Tacacs_Default</td> <td></td>	Summary of Policies	Default Tacacs_Default	
Global Exceptions Proxy Server Sequence Nate screatering deployment Proxy Server Sequence Serve Order Reset Order Serve Order Reset Order Obsault Rule (In n match): Allow Protocols: Default Device Admin and use: All_User_ID_Stores Edit • • Authonization Policy • Authonization Policy • Standard Standard Standard Standard	A list of all your policies	Regular 🔿 Proxy Sequence 🔿	
Note scores ether deployment Pracy server sequence: • Authentication Policy • Serve Order	Global Exceptions	* Proxy Server Sequence	
Contract Reset Circler Authentication Policy Authentication Policy Authentication Policy Authentication Policy Authorization Policy Authorization Policy Standard Stand	Rules across entire deployment	Proxy server sequence:	
Konce, Unitant Kence, U	Default		
Save Order Reset Order Default Rule (in o match) : Allow Protocols : Default Device Admin and use : All_User_10_Stores Edd + Authorization Policy Exceptions (0) Standard Standard Standard Conditions (dentify groups and other conditions) Command Ses Shell Profiles Interview Shell Profiles Shell	Tacacu_Default	* Authentication Policy	
Authorization Policy Exceptions (0) Standard Stalus Rule Name Conditons (dentify groups and other conditions) Command Sets Shell Profiles	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 Conditors (dentity groups and other conditions) Command Sets Shell Profiles			
Exceptions (0) Standard Status Rule Name Conditons (dentity 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	
Tacace_Default If no matches, than Salect Profile Edit +		Tacacs_Default if no matches, then Select Profile(8) Deny Al Shell Profile	Edit •

Étape 2. Assurez-vous que la stratégie d'authentification pointe vers la base de données

Utilisateurs internes ou vers le magasin d'identités requis.



Étape 3. Cliquez sur la flèche à la fin de la stratégie d'autorisation par défaut et cliquez sur Insérer une règle ci-dessus.

Authorization Policy			
Exceptions (0)			
Standard			
Status Rule Name	Conditions (identity groups and other conditions) Command 5	Sets Shell Profiles	
Tacacs_Default	If no matches, then Select Profile(s) Deny All Shell Profile		Insert New Rule Above

Étape 4. Entrez les valeurs de la règle avec les paramètres requis :

- 4.1. Nom de la règle : Règle d'administration FXOS.
- 4.2. Conditions.

Si : Le groupe d'identités utilisateur est FXOS ADMIN



Et Périphérique : Type de périphérique égal à tous les types de périphériques #FXOS

Conditions (identity group	os and other conditions) Command Sets Shell Profiles	
if FX 💠 and	DEVICE:Devi 🗢 then Comman 💠 and Select a Shell Profile 📀	
o matches, then Selec	Add All Conditions Below to Library	
	Condition Name Description DEVICE:Device Ty O Equals All Device Types	# 🧿 🖓 🗸
		All Device Types All Device Types#FXOS
		AD >
		DEVICE >
		InternalUser >
		Network Access >
		Network Condition >
		TACACS >

Profil Shell : Profil_Admin_FXOS

Select a Shell Profile	
	Shell Profile
	🔄 🕶 📃 🕶 🚳 🖓 🖓 🗸
	🥁 Default Shell Profile
	Seny All Shell Profile
	General FXOS_AAA_Shell
	S FXOS_Admin_Profile
	Generations_Shell
	FXOS_ReadOnly_Shell
	Se WLC ALL
	SA WLC MONITOR

Étape 5. Cliquez sur Done.

Forceptions (d) Status Status Status Rufe Name Conditions (dentify groups and other conditions) Contrand Sets Status PXOS Admin Rufe PXOS Admin Rufe				
Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profiles V V FXOS Admin Rule IFX I and DEVICE-Devi I and DEVICE-Devi I and Device-Devi I and PXOS, Admin, Profile I and	Excel	eptions (0)		
Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profile Done PXDS Admin Rule If FX If Done Select an item Ind FXDS Admin Profile Done Tacace_Default If no matches, then Select Profile(s) Deny Al Shell Profile Edit +	Stand	lard		
Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profile Done You S. Admin Rule If IND matches, then Select Profile(s) Deny All Shell Profile Select Profile(s) Select Profile(
PXOS Admin Rude If PX and Device:Devi Intermediate Done Tacaca_Default If no matches, then Select Profile(s) Deny All Shell Profile Edit +	٤	Status Rule Name	Conditions (idensity groups and other conditions) Command Sets Shell Profiles	
Tacace_Default If no matches, then Select Profile(s) Deny Al Shell Profile Edit •	i 🖉 🖪	 FXOS Admin Rule 	I FX 🔷 and DEVICE-Devi 🔷 final Select an item 🔷 and FXOS, Admin Profile 💽	Done
		Tacacs_Default	If no matches, then Soloct Profile(s) Deny Al Shell Profile	Edit 🕶
Save Reset	Save	Reset		

Étape 6. Répétez les étapes 3 et 4 pour les autres rôles d'utilisateur et, lorsque vous avez terminé, cliquez sur **ENREGISTRER**.

Exceptions (0) Standard Status Rule Na FXOS Admi	me n Rule if	Conditions (identity groups and o	ther conditions)	Command Sala	
Status Rule Na	me n Rule i f	Conditions (identity groups and o	ther conditions)	Command Cata	
		FXOS ADMIN AND DEVICE:Dev EQUALS All Device Types#FXOS	ice Type then	Select an item	Shell Profiles FXOS_Admin_Profile
FXOS AAA	Rule if	FXOS AAA AND DEVICE:Device EQUALS All Device Types#FXOS	Type then	Select Profile(s)	FXOS_AAA_Shell
FXOS Oper	ations Rule if	FXOS OPER AND DEVICE:Device EQUALS All Device Types#FXOS	ce Type then	Select Profile(s)	FXOS_Operations_Shell
🖉 🗹 🛛 FXOS Read	Only Rule if	FXOS Read Only AND DEVICE: EQUALS All Device Types#FXOS	Device Type then		FXOS_ReadOnly_Shell
Tacacs_Def	ault if r	no matches, then Select Profile	(S) Deny All Shell P	rofile	



Vérification

Vous pouvez maintenant tester chaque utilisateur et vérifier le rôle d'utilisateur assigné.

Vérification du châssis FXOS

1. Établissez une connexion Telnet ou SSH au châssis FXOS et connectez-vous à l'aide de l'un des utilisateurs créés sur l'ISE.

username (nom d'utilisateur) : fxosadmin

Mot de passe :

fpr4120-TAC-A# sécurité de portée

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

Utilisateur distant fxosaaa :

Description:

Rôles utilisateur :

Name : aaa

Name : en lecture seule

Utilisateur distant fxosadmin :

Description:

Rôles utilisateur :

Name : admin

Name : en lecture seule

Utilisateur distant fxosoper :

Description:

Rôles utilisateur :

Name : opérations

Name : en lecture seule

Utilisateur distant fxosro :

Description:

Rôles utilisateur :

Name : en lecture seule

En fonction du nom d'utilisateur saisi, l'interface de ligne de commande du châssis FXOS affiche uniquement les commandes autorisées pour le rôle d'utilisateur attribué.

Rôle utilisateur Admin.

fpr4120-TAC-A /security #?

reconnaître

clear-user-sessions Clear User Sessions

créer des objets gérés

supprimer les objets managés

désactiver les services Désactive

activer les services

Entrez un objet managé

étendue Modifie le mode actuel

définir les valeurs de propriété

show show system information

terminer les sessions cimc actives

fpr4120-TAC-A# connect fxos

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

fpr4120-TAC-A (fxos)#

Rôle utilisateur en lecture seule.

fpr4120-TAC-A /security #?

étendue Modifie le mode actuel

définir les valeurs de propriété

show show system information

fpr4120-TAC-A# connect fxos

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

% Autorisation refusée pour le rôle

2. Accédez à l'adresse IP du châssis FXOS et connectez-vous à l'aide de l'un des utilisateurs créés sur l'ISE.

Rôle utilisateur Admin.

Overview Interfaces Logic	al Devices Security Engine	latform Settings				
NTP	LDAP RADIUS TACACS					
SSH SNMP HTTPS	Properties Timeout:* 5 Secs					
AAA Suclea	TACACS Providers					
DNS			Add TACACS Provider		? ×	O Add
FIPS and Common Criteria Access List	Hostname	Order	Hostname/FQDN(or IP Address):*			
	10.88.244.50	1	Order:*	lowest-available		<i>d</i>
			Key:		Set:No	
			Confirm Key:			
			Port:*	49		
			Timeout:*	5 Secs		
				ОК Са	incel	
	Save					

Rôle utilisateur en lecture seule.

iew Int	erfaces	Logical G	Devices	Securit	ty Engine	Platform 5	iettings				
NTP			LDAP	RADOUS	TACACS						
SSH SNMP			Properties								
HTTPS			Timeout:	5	Secs						
Syslog			TACACS P	roviders							
ONS										0	Add
FIPS and Comm Access List	non Criberia		Hostnar				On	der	Port		
PECCES L'AL			10.88.24	4.50			1		49	48	

Note: Notez que le bouton ADD est grisé.

Vérification ISE 2.0

1. Accédez à Opérations > TACACS Livelog. Vous devriez être en mesure de voir des tentatives réussies et échouées.

albah cisco	Identity Services Engine	Home + C	ontext Visibility	- Operations	Policy Admin	istration + Work Centers				۹. 😐	• •
RADIUS Threat-Centric NAC Live Logs TruckCS Truckets by Metwork Control Reports											s again
Live Logs											
	Refresh Never • Show Latest 20 records • Within									Last 3 hours	s •
Colore J Court De											-
2	Remean Z Export to •									f riter+	••
	Logged Time	Status	Details	Username	Туре	Authentication Policy	Authorization Policy	Failure Reason	Matched Comma	Shell Profile	3
×			·	Username	•	Authentication Policy	Authorization Policy	Failure Reason	Matched Command S	Shell Profile	
	Jan 17, 2018 08:57:23.272 PM	1	ò	fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admir	n_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	۰	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			
	Jan 17, 2018 08:57:01.069 PM	2	.0	fxosro	Authorization		Tacacs_Default >> FXOS Read Only			FXOS_Read	Only_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			

Dépannage

Pour déboguer l'authentification et l'autorisation AAA, exécutez les commandes suivantes dans l'interface de ligne de commande FXOS.

fpr4120-TAC-A# connect fxos

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

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

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

fpr4120-TAC-A (fxos)# term mon

Après une tentative d'authentification réussie, le résultat suivant s'affiche.

17 janvier 2018 15:46:40.305247 aaa : aaa_req_process pour l'authentification. session no 0

17 janvier 2018 15:46:40.305262 aaa : aaa_req_process : Demande AAA générale de l'application : login appln_subtype : par défaut

17 janvier 2018 15:46:40.305271 aaa : try_next_aaa_méthode

17 janvier 2018 15:46:40.305285 aaa : total des méthodes configurées est 1, l'index actuel à essayer est 0

17 janvier 2018 15:46:40.305294 aaa : handle_req_using_méthode

17 janvier 2018 15:46:40.305301 aaa : GROUPE_SERVEURS_MÉTHODE_AAA

17 janvier 2018 15:46:40.305308 aaa : aaa_sg_method_handler groupe = tacacs

17 janvier 2018 15:46:40.305315 aaa : Utilisation de sg_protocol passé à cette fonction

17 janvier 2018 15:46:40.305324 aaa : Envoi de la demande au service TACACS

17 janvier 2018 15:46:40.305384 aaa : Groupe de méthodes configuré Réussite

17 janvier 2018 15:46:40.554631 aaa : aaa_process_fd_set

17 janvier 2018 15:46:40.555229 aaa : aaa_process_fd_set : mtscallback sur aaa_q

17 janvier 2018 15:46:40.555817 aaa : mts_message_response_handler : réponse mts

17 janvier 2018 15:46:40.556387 aaa : prot_daemon_reponse_handler

17 janvier 2018 15:46:40.557042 aaa : session : 0x8dfd68c supprimé de la table de session 0

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

17 janvier 2018 15:46:40.557066 aaa : is_aaa_resp_status_success est TRUE

17 janvier 2018 15:46:40.557075 aaa : aaa_send_client_response pour l'authentification. session->flags=21. aaa_resp->flags=0.

17 janvier 2018 15:46:40.557083 aaa : AAA_REQ_FLAG_NORMAL

17 janvier 2018 15:46:40.557106 aaa : mts_send_response Réussite

17 janvier 2018 15:46:40.557364 aaa : aaa_req_process pour autorisation. session no 0

17 janvier 2018 15:46:40.557378 aaa : aaa_req_process appelé avec contexte à partir de appln : login appln_subtype : type_auteur par défaut : 2, méthode_auteur : 0

17 janvier 2018 15:46:40.557386 aaa : aaa_send_req_using_contexte

17 janvier 2018 15:46:40.557394 aaa : groupe aaa_sg_method_handler = (null)

17 janvier 2018 15:46:40.557401 aaa : Utilisation de sg_protocol passé à cette fonction

17 janvier 2018 15:46:40.557408 aaa : demande AAA basée sur le contexte ou dirigée(exception : pas une requête de relais). Ne prendra pas copie de la demande aaa

17 janvier 2018 15:46:40.557415 aaa : Envoi de la demande au service TACACS

17 janvier 2018 15:46:40.801732 aaa : aaa_send_client_response pour autorisation. session->flags=9. aaa_resp->flags=0.

17 janvier 2018 15:46:40.801740 aaa : AAA_REQ_FLAG_NORMAL

17 janvier 2018 15:46:40.801761 aaa : mts_send_response Réussite

17 janvier 2018 15:46:40.848932 aaa : ANCIEN OPCODE : mise à jour_intermédiaire_comptable

17 janvier 2018 15:46:40.848943 aaa : aaa_create_local_acct_req : user=, session_id=, log=ajouté utilisateur:fxosadmin au rôle:admin

17 janvier 2018 15:46:40.848963 aaa : aaa_req_process pour la comptabilité. session no 0

17 janvier 2018 15:46:40.848972 aaa : La référence de la demande MTS est NULL. Demande LOCALE

17 janvier 2018 15:46:40.848982 aaa : Définition de AAA_REQ_RESPONSE_NOT_NEEDED

17 janvier 2018 15:46:40.848992 aaa : aaa_req_process : Demande AAA générale de l'application : appln_subtype par défaut : par défaut

17 janvier 2018 15:46:40.849002 aaa : try_next_aaa_méthode

17 janvier 2018 15:46:40.849022 aaa : Aucune méthode configurée pour la valeur par défaut

17 janvier 2018 15:46:40.849032 aaa : aucune configuration disponible pour cette demande

17 janvier 2018 15:46:40.849043 aaa : try_fallback_méthode

17 janvier 2018 15:46:40.849053 aaa : handle_req_using_méthode

17 janvier 2018 15:46:40.849063 aaa : gestionnaire_méthode_locale

17 janvier 2018 15:46:40.849073 aaa : aaa_local_accounting_msg

17 janvier 2018 15:46:40.849085 aaa : mettre à jour::utilisateur ajouté:fxosadmin au rôle:admin

Après une tentative d'authentification échouée, le résultat suivant s'affiche.

17 janvier 2018 15:46:17.836271 aaa : aaa_req_process pour l'authentification. session no 0

17 janvier 2018 15:46:17.836616 aaa : aaa_req_process : Demande AAA générale de l'application : login appln_subtype : par défaut

17 janvier 2018 15:46:17.837063 aaa : try_next_aaa_méthode

17 janvier 2018 15:46:17.837416 aaa : total des méthodes configurées est 1, l'index actuel à essayer est 0

17 janvier 2018 15:46:17.837766 aaa : handle_req_using_méthode

17 janvier 2018 15:46:17.838103 aaa : GROUPE_SERVEURS_MÉTHODE_AAA

17 janvier 2018 15:46:17.838477 aaa : aaa_sg_method_handler groupe = tacacs

17 janvier 2018 15:46:17.838826 aaa : Utilisation de sg_protocol passé à cette fonction

17 janvier 2018 15:46:17.839167 aaa : Envoi de la demande au service TACACS

17 janvier 2018 15:46:17.840225 aaa : Groupe de méthodes configuré Réussite

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

17 janvier 2018 15:46:18.044048 aaa : is_aaa_resp_status_success est TRUE

17 janvier 2018 15:46:18.044395 aaa : aaa_send_client_response pour l'authentification. session->flags=21. aaa_resp->flags=0.

17 janvier 2018 15:46:18.044733 aaa : AAA_REQ_FLAG_NORMAL

17 janvier 2018 15:46:18.045096 aaa : mts_send_response Réussite

17 janvier 2018 15:46:18.045677 aaa : aaa_cleanup_session

17 janvier 2018 15:46:18.045689 aaa : mts_drop de la requête msg

17 janvier 2018 15:46:18.045699 aaa : aaa_req doit être libéré.

17 janvier 2018 15:46:18.045715 aaa : aaa_process_fd_set

17 janvier 2018 15:46:18.045722 aaa : aaa_process_fd_set : mtscallback sur aaa_q

17 janvier 2018 15:46:18.045732 aaa : aaa_enable_info_config : GET_REQ pour un message d'erreur de connexion aaa

17 janvier 2018 15:46:18.045738 aaa : récupération de la valeur de retour de l'opération de configuration:élément de sécurité inconnu

Informations connexes

La commande Ethanalyzer sur le cli FX-OS vous invite à saisir un mot de passe lorsque l'authentification TACACS/RADIUS est activée. Ce comportement est causé par un bogue.

ID de bogue: CSCvg87518