Système d'exploitation extensible de FirePOWER (FXOS) 2.2 :

Authentification/autorisation de châssis pour la gestion à distance avec ISE utilisant RADIUS

Contenu

Introduction Conditions préalables Conditions requises Composants utilisés Configurez Diagramme du réseau Configurations Configurer le châssis FXOS Configurer le serveur ISE Vérifiez Vérification FXOS Chasis Vérification ISE 2.0 Dépannez Informations connexes

Introduction

Ce document décrit comment configurer l'authentification et l'autorisation de RADIUS pour le châssis du système d'exploitation extensible de FirePOWER (FXOS) par l'intermédiaire du Cisco Identity Services Engine (ISE).

Le châssis FXOS inclut les rôles de l'utilisateur suivants :

- Administrateur Complete lecture-et-écrivent l'accès au système entier. Le compte par défaut d'admin est assigné ce rôle par défaut et il ne peut pas être changé.
- En lecture seule Accès en lecture seule à la configuration de système sans des privilèges de modifier l'état du système.
- Des exécutions Lecture-et-écrivez l'accès à la configuration de NTP, à la configuration de Smart Call Home pour l'autorisation intelligente, et aux logs système, y compris des serveurs de Syslog et des défauts. Accès en lecture au reste du système.
- AAA Lecture-et-écrivez l'accès aux utilisateurs, aux rôles, et à la configuration d'AAA. Accès en lecture au reste du système.

Par l'intermédiaire du CLI ceci peut être vu comme suit :

fpr4120-TAC-A /security * # show role

Rôle :

Role name Priv

AAA d'AAA

admin d'admin

exécutions d'exécutions

en lecture seule en lecture seule

Contribué par Remirez élégant, Jose Soto, ingénieurs TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du système d'exploitation extensible de FirePOWER (FXOS)
- La connaissance de la configuration ISE

Composants utilisés

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

- Version 2.2 d'appareils de Sécurité de Cisco FirePOWER 4120
- Logiciel Cisco Identity Services Engine virtuel 2.2.0.470

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurezvous que vous comprenez l'effet potentiel de toute commande.

Configurez

Le but de la configuration est à :

- Authentifiez les utilisateurs se connectant dans le GUI du Web du FXOS et le SSH au moyen d'ISE
- Autorisez les utilisateurs se connectant dans le GUI du Web du FXOS et le SSH selon leur rôle de l'utilisateur respectif au moyen d'ISE.
- Vérifiez le bon fonctionnement de l'authentification et de l'autorisation sur le FXOS au moyen d'ISE

Diagramme du réseau



Configurations

Configurer le châssis FXOS

Création d'un fournisseur de RADIUS utilisant le gestionnaire de châssis

Étape 1. Naviguez vers des configurations > l'AAA de plate-forme.

Étape 2. Cliquez sur l'onglet de RADIUS.



Étape 3. Pour chaque fournisseur de RADIUS que vous voulez ajouter (jusqu'à 16 fournisseurs).

3.1. Dans la région de fournisseurs de RADIUS, cliquez sur Add.

3.2. Une fois la boîte de dialogue de fournisseur de RADIUS d'ajouter ouvre, écrit les valeurs exigées.

3.3. Cliquez sur OK pour fermer la boîte de dialogue de fournisseur de RADIUS d'ajouter.

ſ	Edit 10.88.244.50		?×
L	Hostname/FQDN(or IP Address):*	10.88.244.50	
L	Order:*	1	
L	Key:	•••••	Set:Yes
1	Confirm Key:	••••••	
L	Authorization Port:*	1812	
L	Timeout:*	5 Secs	
L	Retries:*	1	
Ľ		ок	ancel

Étape 4. Sauvegarde de clic.

Overview Interfaces Logic	cal Devices Security Engine	Platform Settings									
NTP	LDAP RADIUS TACACS										
SSH SNMP	Properties	Properties									
HTTPS	Timeout:* 5 Secs										
Syslog	Retries:* 1	Retries:* 1									
DNS	RADIUS Providers										
Access List					Add						
	Hostname	Order	Service	Auth Port							
	10.88.244.50	1	authorization	1812	J 🗇						
	Save										

Étape 5. Naviguez vers le système > la gestion des utilisateurs > les configurations.

Étape 6. Sous l'authentification par défaut choisissez RADIUS.

Overview Interfaces Log	cal Devices Security Engine Platform Settings		1	system Too	ls Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	RADIUS v "Local is failback authentication method				
Console Authentication	Local				
Remote User Settings					
Remote User Role Policy	G Assign Default Role ○No-Login				

Création d'un fournisseur de RADIUS utilisant le CLI

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

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # par défaut-auth de portée

fpr4120-TAC-A /security/default-auth # a placé le rayon de royaume

Étape 2. Utilisez la commande de détail d'exposition d'afficher les résultats.

fpr4120-TAC-A /security/default-auth # détail d'exposition

Authentification par défaut :

Royaume d'admin : Radius

Royaume opérationnel : Radius

La session Web régénèrent la période (en quelques sec) : 600

Délai d'attente de session (en quelques sec) pour le Web, ssh, sessions de telnet : 600

Délai d'attente de session absolu (en quelques sec) pour le Web, ssh, sessions de telnet : 3600

Délai d'attente de session de console série (en quelques sec) : 600

Délai d'attente de session absolu de console série (en quelques sec) : 3600

Groupe de serveurs d'authentification d'admin :

Groupe de serveurs opérationnel d'authentification :

Utilisation de 2ème facteur : Non

Étape 3. Afin de configurer des paramètres de serveur de RADIUS exécutez les commandes suivantes.

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # rayon de portée

fpr4120-TAC-A /security/radius # présentent le serveur 10.88.244.50

fpr4120-TAC-A /security/radius/server # a placé le descr « serveur ISE »

fpr4120-TAC-A /security/radius/server * # placez la clé

Introduisez la clé : ******

Confirmez la clé : ******

Étape 4. Utilisez la commande de détail d'exposition d'afficher les résultats.

fpr4120-TAC-A /security/radius/server * # détail d'exposition

Serveur de RADIUS :

Adresse Internet, FQDN ou adresse IP : 10.88.244.50

Descr :

Commande : 1

Port authentique : 1812

Clé : ****

Délai d'attente : 5

Configurer le serveur ISE

Ajouter le FXOS comme ressource de réseau

Étape 1. Naviguez vers la gestion > les ressources de réseau > les périphériques de réseau.

Étape 2. Cliquez sur Add

dentity Services Engine	Home + Contex	t Visibility ► Ope	rations Polic	Administration	 Work Centers 			
System Identity Management	 Network Resources 	Device Portal Ma	anagement pxGr	rid Services Feed Ser	vice + Threat Centric N	NAC		
Network Devices Network Device G	roups Network Dev	vice Profiles Extern	al RADIUS Servers	RADIUS Server Seque	nces NAC Managers	External MDM	Location Services	
0								
Network devices	Network Devi	ces						
Default Device								
Device Security Settings	🥖 Edit 🕂 Add	Duplicate 🛃 Imp	port 🔂 Export	Generate PAC X Dele	ete			
	Name	 IP/Mask 	Profile Name	Local	tion	Туре		Description
							No data a	available

Étape 3. Écrivez les valeurs requises (le nom, l'adresse IP, le type de périphérique et l'enable RADIUS et ajoutent la CLÉ), cliquez sur Submit.

cisco Identity Services Engine	Home	t Visibility	Policy ▼A	dministration	Vork Centers	
System Identity Management	 Network Resources 	Device Portal Management	t pxGrid Services	Feed Service	Threat Centric NAC	
Network Devices Network Device G	Froups Network Devi	ce Profiles External RADIUS	Servers RADIU	S Server Sequences	NAC Managers External MD	M Location Services
0						
Network devices	Network Devices Lis	SI > New Network Device				
Default Device	Network Device	t Name (Frid				
Device Security Settings		Description				
	* IP Address	: 10.83.180.6	32			
		* Device Profile 📩 C	Disco 🔻 🕀			
		Model Name	*			
		Software Version	Ţ			
	* Network Dev	vice Group				
	Hourse Bo					
	Device Type	FXOS 📀 S	et To Default			
	IPSEC	Is IPSEC Device 📀 🕓	et To Default			
	Location	All Locations 📀 S	et To Default			
	RADIUS /	Authentication Settings				
	RADIUS	UDP Settings				
			Protocol	RADIUS		
			 Shared Secret 	•••••	Show	
			CoA Port	1700	Set To Default	
	RADIUS	DTLS Settings (j)				
			DTLS Required			
			Shared Secret	radius/dtls	Ð	
			CoA Port	2083	Set To Default	
		Issuer CA of ISE 0	Certificates for CoA	Select if required (op	tional)	

Création des groupes et des utilisateurs d'identité

Étape 1. Naviguez vers la gestion > la Gestion de l'identité > les groupes > les groupes d'identité de l'utilisateur.

Étape 2. Cliquez sur Add.

altala cisco	Identity Services Engine	Home	Context Visibility	Operations	Policy	▼Adminis	tration	Work Centers				
Sys	tem Identity Management	Network R	esources	ortal Manageme	nt pxGrid S	Services +	Feed Ser	vice				
Ide	Identities Groups External Identity Sources Identity Source Sequences Settings											
Id	entity Groups		User Identity	Groups								
F		Q	ober adentity	Groups								
4	• E •	<u>i</u>	/ Edit 🕂 Add	🗙 Delete 👻	👔 Import	Export 👻						
•	Endpoint Identity Groups		Name				Descripti	on				
-	User Identity Groups		ALL_ACCOUNTS (default)				Default ALL_ACCOUNTS (default) User Group					
			Employee				Default Employee User Group					
			🗌 🧏 GROUP_	ACCOUNTS (de	efault)		Default GROUP_ACCOUNTS (default) User Group					
			GuestType_Contractor (default)				Identity group mirroring the guest type					
			🗌 🖉 GuestTyp	e_Daily (default)		Identity g	group mirroring the guest type				
			🗌 🖉 GuestTyp	e_Weekly (defa	ult)		Identity g	group mirroring the guest type				
			🗌 🔏 OWN_AC	COUNTS (defa	ult)		Default C	WN_ACCOUNTS (default) User Group				

Étape 3. Écrivez la valeur pour le nom et cliquez sur Submit.

cisco Iden	tity Services Engine	Home	Context Visibility	 Operations 	Policy	- Administration	Work Centers	
 System 	✓ Identity Management	Network R	esources + Devic	e Portal Management	pxGrid Ser	rices + Feed Ser	vice	
Identities	Groups External Ide	entity Sources	Identity Source Se	quences • Setting:	5			
Identity	y Groups	م ڇ-	User Identity Gr Identity Gro Name Description Submit	EXOS ADMIN	antity Group			

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

dentity Services Engine Home	Context Visibility Policy ✓ Adm	inistration Work Centers
► System	esources	Feed Service Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups	
	✓ Eait ♣Add ★ Delete ♥ @ Import Export ♥	
Endpoint Identity Groups	Name	 Description
 User Identity Groups 	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Ame: Currently Sorted	Default Employee User Group
	🗌 📲 FXOS AAA	
	FXOS ADMIN	
	E Pros Oper	
	FXOS Read Only	
		Diffult CROUR ACCOUNTS (Jefuith) Use Come

Étape 5. Naviguez vers la gestion > la Gestion de l'identité > l'identité > les utilisateurs.

Étape 6. Cliquez sur Add.

t Visibility	Administration Work 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									
s Users									
Change Status	V Delete								
Name Description	n First Name Last Name	Email Address User Identity Groups	Admin						
		No data available							
	t Visibility	t Visibility → Operations → Policy ~ Administration → Work Centers → Device Portal Management pxGrid Services → Feed Service → Threat Centric NA Source Sequences → Settings s Users Change Status Prof Prof.	t Visibility 						

Étape 7. Écrivez 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		(999)	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 Administrat	ion 🔹 Work Ce	nters				
System Identity 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	Users Network Access Users								
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎲 Impor	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	<u> f</u> xosro					FXOS Read Only		

Création du profil d'autorisation pour chaque rôle de l'utilisateur

Étape 1. Naviguez vers la stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation.

dentity Services Engine	Home → Context Visibility → C	Operations - Policy	► Administration ► Work Centers					
Authentication Authorization Profilin	ng Posture Client Provisioning	 Policy Elements 						
Dictionaries + Conditions - Results								
0								
Authentication Standard Authorization Profiles								
Authorization	For Policy Export go to Administra	tion > System > Backup &	Restore > Policy Export Page					
Plationation	/ Edit + Add DyDuplicate	XDelete						
Authorization Profiles	Name		Profile	Description				
Downloadable ACLs	Riackhole Wireless Access		the Cierco El	Default profile used to blacklist wireless devices. Ensu				
Profiling			and Class (D	Default profile used for Olean Dhanne				
	Cisco_IP_Phones			Default profile used for Lisco Phones.				
Posture	Cisco_WebAuth		atta 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				

Étape 2. Remplissez tous les attributs pour le profil d'autorisation.

2.1. Configurez le nom de profil.

Authentication Authorization Profil	ng Posture Client Provisioning Policy Elements
Dictionaries Conditions Result	3
0	
► Authentication	Authorization Profiles > FXOS-ADMIN-PROFILE Authorization Profile
- Authorization	Name FXOS-ADMIN-PROFILE
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT
▶ Profiling	Network Device Profile 🛛 🗯 Cisco 👻 🕀

2.2. Dans des attributs avancés les configurations configurent le CISCO-AV-PAIR suivant

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

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

2.3. Cliquez sur Save.



Étape 3. Répétez l'étape 2 pour les rôles de l'utilisateur restants utilisant les Cisco-POIDs du

commerce-paires suivantes

cisco-av-pair=shell : roles= " AAA »

cisco-av-pair=shell : roles= " exécutions »

cisco-av-pair=shell : roles= " en lecture seule »

▼ Advanced Attributes S	Settings	
Cisco:cisco-av-pair	shell:roles="aaa"	⊘ — +



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

titude Identity Services Engine	ome	
Authentication Authorization Profiling	Posture Client Provisioning Policy Elem	nents
Dictionaries + Conditions - Results		
G		
Authentication	Standard Authorization Profiles	
Authorization	For Policy Export go to Administration > System	n > Backup & Restore > Policy Export Page
Autorization	/ Edit + Add - Duplicate X Delete	
Authorization Profiles		Durch
Downloadable ACLs	Name	Profile
b Desfiller	Blackhole_Wireless_Access	
▶ Proming	Cisco_IP_Phones	disco 🕀
▶ Posture	Cisco_WebAuth	asta Cisco 🕀
	FXOS-AAA-PROFILE	ditto Cisco 🕀
Client Provisioning	FXOS-ADMIN-PROFILE	🔐 Cisco
	FXOS-OPER-PROFILE	🗰 Cisco 🕀
	FXOS-ReadOnly-PROFILE	😁 Cisco

Création de la stratégie d'authentification

Étape 1. Naviguez vers la **stratégie > l'authentification >** et cliquez sur la flèche à côté de éditent où vous voulez créer la règle.



Étape 2. L'installation est simple ; il peut être plus granulaire fait mais pour cet exemple nous utiliserons le type de périphérique :

Nom : RÈGLE D'AUTHENTIFICATION FXOS

SI nouveaux attribut/valeur choisis : **Périphérique : Le type de périphérique égale tous les types de périphériques #FXOS**

Permettez les protocoles : Accès au réseau par défaut

Utilisation : Utilisateurs internes

/ P 🔽		FXOS AUTHENTICATION RULE : If	DEVICE:Device Type EQUALS All Device Types#FXOSAllow Protocols : Default Network Access	and
	~	Default	:use Internal Users	

Création de la stratégie d'autorisation

Étape 1. Naviguez vers la **stratégie > l'autorisation >** et cliquez sur le net de flèche pour éditer où vous voulez créer la règle.



Étape 2. Écrivez les valeurs pour la règle d'autorisation avec les paramètres requis.

2.1. Nom de règle : Règle de Fxos <USER ROLE>.



2.2. Si : Groupes d'identité de l'utilisateur > <USER choisi ROLE>.

if FX and Condition(s) Image: AuthZ Pr ino ma FXOS ADMIN Image: AuthZ Pr Image: FXOS ADMIN Image: FXOS ADMIN Image: FXO	FX and Condition(s) Image: the mail of the mail	Conditions (id	dentity groups	and other condit	tions)	Perr	nissions	
FXOS ADMIN User Identity Groups User Identity Groups User Identity Groups Image: Ima	FXOS ADMIN Image: Constraint of the second seco	if FX	and	Condition(s)	¢	then	AuthZ Pr	
FXOS ADMIN User Identity Groups Image: State of the state of t	FXOS ADMIN User Identity Groups Image: State of the state of t	no ma						
User Identity Groups	User Identity Groups Image: Construction of the second s	FXO	IS ADMIN					
FXOS AAA GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS ADMIN Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default)	 FXOS AAA GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				User Identity Groups			
 FXOS AAA GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 FXOS AAA GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 					Q		
 FXOS AAA GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 FXOS AAA GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				↓ ■ .	÷		
 GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 GuestType_Weekly (default) OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				FXOS AAA			
 OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 OWN_ACCOUNTS (default) GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				GuestType_Weekly (default))		
 GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 GROUP_ACCOUNTS (default) FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				OWN_ACCOUNTS (default)			
 FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 FXOS ADMIN FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				GROUP_ACCOUNTS (default	t)		
 FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 FXOS OPER Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				EXOS ADMIN			
 Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 Employee GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				FXOS OPER			
 GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 GuestType_Daily (default) GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				Employee			
 GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 	 GuestType_Contractor (default) FXOS Read Only ALL_ACCOUNTS (default) 				GuestType_Daily (default)			
 FXOS Read Only ALL_ACCOUNTS (default) 	 FXOS Read Only ALL_ACCOUNTS (default) 				GuestType_Contractor (defa	ult)		
ALL_ACCOUNTS (default)	ALL_ACCOUNTS (default)				FXOS Read Only			
_ , ,					ALL_ACCOUNTS (default)			

2.3. ET : Créez le nouveaux état > périphérique : Le type de périphérique égale **tous les types de périphériques #FXOS**.

Conditions (identity groups a	and other conditions) Permissions	
if FX 🛟 and	DEVICE:Device Type EQUALS All 🗢 then Select an item 💠	
if no matches, then DenyAc	Add All Conditions Below to Library	
	Condition Name Description ↓ DEVICE:Device Ty ♥ Equals ▼ All Device Types# ♥	¥•
		P
		- <u>1</u>
	All Device Types	
(All Device Types#FXOS	
	AD	>
	Airespace	>
	Alcatel-Lucent	>
	🧰 Aruba	>
	🧰 Brocade	>
		>
	Cisco	>
	Cisco-BBSM	>
	Cisco-VPN3000	>
	СМА	>

2.4. Autorisations : La norme > choisissent le rôle de l'utilisateur de profil

Permissions		
then FXOS-A		
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	
	Generation FXOS-ReadOnly-PROFILE	
	😪 NSP_Onboard	
	Non_Cisco_IP_Phones	
	I PermitAccess	
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-PRO Types#FXOS	FILE

Étape 3. Répétez l'étape 2 pour tous les rôles de l'utilisateur.

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
	Fxos AAA Rule	FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
	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	





Vérifiez

Vous pouvez maintenant examiner chaque utilisateur et vérifier le rôle de l'utilisateur assigné.

Vérification FXOS Chasis

1. Telnet ou SSH au châssis FXOS et procédure de connexion utilisant les utilisateurs créés l'uns des sur l'ISE.

Nom d'utilisateur : fxosadmin

Mot de passe :

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # petit groupe d'utilisateur distant d'exposition

Fxosaaa d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : AAA

Nom : en lecture seule

Fxosadmin d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : admin

Nom : en lecture seule

Fxosoper d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : exécutions

Nom : en lecture seule

Fxosro d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : en lecture seule

Selon le nom d'utilisateur écrit le châssis FXOS le cli affichera seulement les commandes autorisées pour le rôle de l'utilisateur assigné.

Rôle de l'utilisateur d'admin.

fpr4120-TAC-A /security #?

reconnaissez reconnaissent

sessions de clear user de clair-utilisateur-sessions

créez les objets gérés Create

objets gérés par effacement d'effacement

le débronchement désactive des services

l'enable active des services

entrez écrit un objet géré

la portée change le mode courant

placez les valeurs d'une propriété réglées

affichez les informations de show system

terminez les sessions de l'Active cimc

fpr4120-TAC-A# connectent des fxos

fpr4120-TAC-A (fxos) # AAA-demandes de debug aaa

fpr4120-TAC-A (fxos) #

Rôle de l'utilisateur en lecture seule.

fpr4120-TAC-A /security #?

la portée change le mode courant

placez les valeurs d'une propriété réglées

affichez les informations de show system

fpr4120-TAC-A# connectent des fxos

fpr4120-TAC-A (fxos) # AAA-demandes de debug aaa

% d'autorisation refusée pour le rôle

2. Parcourez à l'adresse IP et à la procédure de connexion de châssis FXOS utilisant les utilisateurs créés l'uns des sur l'ISE.

Rôle de l'utilisateur d'admin.

Overview Interfaces Logica	Devices Security Engine Platform	Settings					Sys	tem Tools H	telp
NTP SSH SIMMP AAA Syslog DNS FUSE and Common Criteria Access List	LDAP RADIUS TACACS Properties Timeout:* 5 Secs Retries:* RADIUS Providers Hostname	Order	Add RADIUS Provider Hostname/FQDN(or IP Address):* Order:* Key:	lowest-available	(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	O Ad			
	10.88.244.16	1	Confirm Key: Authorization Port:* Timeout:* Retries:*	1812 5 Secs 1 OK Ce	ncel	/8			

Rôle de l'utilisateur en lecture seule.

Overview Interfaces Lo	gical Devices Security Engine	Platform Settings			
NTP	LDAP RADEUS TACACS				
SSH SNHP	Properties				
HTTPS	Timeout:* 5 Secs				
Syslog	Retries:* 1				
DNS FIPS and Common Criteria	RADOUS Providers				(a
Access List	Hostname	Order	Service	Auth Part	0 48
	10.88.244.16	1	authorization	1812	48

Note: Notez que le bouton d'AJOUTER est greyed.

Vérification ISE 2.0

1. Naviguez vers des **exécutions > RADIUS > vivent des logs.** Vous devriez pouvoir voir réussi et des essais ratés.

diala Ident	tity Services Engir	e Home	Context Visib	ilty • Operat	ions Po	olicy	Administration	Work Centers						0	A	0 C		
▼RADIUS	Threat-Centric NAC Live Logs + TACACS + Troubleshoot + Adaptive Network Control Reports													ss setup and visibility s	etup Do not	show this a	igain.	
Live Logs Live Sessions																		
		Misconfigured Supplicants ()			Misconfigured Network Devices			RADIUS Drops 🕲	Client	Client Stopped Responding O			Repeat Counter O					
	0			0			0		0		0							
										Refresh New	ver	• Show	Lat	test 20 records	Within La	st 3 hours	•	
C Refresh O Reset Repeat Counts 🕹 Export To -															۰.			
Time	3	Status	Details	Repeat C	Identity	/	Authentication Pol	licy	Authorization	Policy	Autho	orization Profile	s	Network Dev	Identity G	iroup		
×		-			Identity		Authentication Polic	У	Authorization P	folicy	Auth	orization Profiles		Network Device	Identity G	roup		
Jan 2	20, 2018 10:14:09		o.		fxosadmin	1	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos	Admin Rule	FXOS	-ADMIN-PROFIL	E	FXOS	User Ident	ty Groups:F	XOS	
Jan 2	20, 2018 10:13:59	۲	0		fxosadmin	1	Default >> FXOS AU	THENTICATION RULE >> Default						FXOS	User Ident	ity Groups:F	XOS	
Jan 2	20, 2018 10:09:01	1	O.		fxosro	1	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos	Read only Rule	FXOS	S-ReadOnly-PRO	FILE	FXOS	User Ident	ty Groups:F	XOS	
Jan 2	20, 2018 10:08:50	٥	0		fxosro	1	Default >> FXOS AU	THENTICATION RULE >> Default						FXOS	User Ident	ty Groups:F	xos	
Jan 2	20, 2018 10:06:17	٥	0		fxosro	1	Default >> FXOS AU	THENTICATION RULE >> Default						FXOS	User Ident	ty Groups:F	XOS	
Jan 2	20, 2018 10:05:15	٥	0		fxosro	1	Default >> FXOS AU	THENTICATION RULE >> Default						FXOS	User Ident	ty Groups:F	XOS	
Jan 2	20, 2018 10:04:23	2	0		fxosadmin	1	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos	Admin Rule	FXOS	S-ADMIN-PROFIL	E	FXOS	User Ident	ty Groups:F	xos	
Jan 2	20, 2018 10:02:59		à +		fxosadmin	÷ .	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos	Admin Rule	FXOS	S-ADMIN-PROFIL	E	FXOS	User Ident	ty Groups:F	xos	

Dépannez

Le debug aaa authentication et l'autorisation exécutent les commandes suivantes dans le FXOS cli.

fpr4120-TAC-A# connectent des fxos

fpr4120-TAC-A (fxos) # AAA-demandes de debug aaa

fpr4120-TAC-A (fxos) # événement de debug aaa

fpr4120-TAC-A (fxos) # erreurs de debug aaa

fpr4120-TAC-A (fxos) # terme lundi

Après qu'une tentative réussie d'authentification, vous voie la sortie suivante.

2018 AAAs du 20 janvier 17:18:02.410275 : aaa_req_process pour l'authentification. session No. 0

2018 AAAs du 20 janvier 17:18:02.410297 : aaa_req_process : Demande de général AAA d'appln : appln_subtype de procédure de connexion : par défaut

2018 AAAs du 20 janvier 17:18:02.410310 : try_next_aaa_method

2018 AAAs du 20 janvier 17:18:02.410330 : les méthodes totales configurées est 1, index en cours à essayer est 0

2018 AAAs du 20 janvier 17:18:02.410344 : handle_req_using_method

2018 AAAs du 20 janvier 17:18:02.410356 : AAA_METHOD_SERVER_GROUP

2018 AAAs du 20 janvier 17:18:02.410367 : groupe = rayon d'aaa_sg_method_handler

2018 AAAs du 20 janvier 17:18:02.410379 : Utilisant le sg_protocol qui est passé à cette fonction

2018 AAAs du 20 janvier 17:18:02.410393 : Envoi de la demande au service RADIUS

2018 AAAs du 20 janvier 17:18:02.412944 : mts_send_msg_to_prot_daemon : Longueur de charge utile = 374

2018 AAAs du 20 janvier 17:18:02.412973 : session : 0x8dfd68c ajouté au tableau 1 de session

2018 AAAs du 20 janvier 17:18:02.412987 : Groupe configuré de méthode réussi

2018 AAAs du 20 janvier 17:18:02.656425 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:18:02.656447 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:18:02.656470 : mts_message_response_handler : une réponse de mts

2018 AAAs du 20 janvier 17:18:02.656483 : prot_daemon_reponse_handler

2018 AAAs du 20 janvier 17:18:02.656497 : session : 0x8dfd68c retiré du tableau 0 de session

2018 AAAs du 20 janvier 17:18:02.656512 : état d'is_aaa_resp_status_success = 1

2018 AAAs du 20 janvier 17:18:02.656525 : les is_aaa_resp_status_success est VRAI

2018 AAAs du 20 janvier 17:18:02.656538 : aaa_send_client_response pour l'authentification. session->flags=21. aaa_resp->flags=0.

2018 AAAs du 20 janvier 17:18:02.656550 : AAA_REQ_FLAG_NORMAL

2018 AAAs du 20 janvier 17:18:02.656577 : mts_send_response réussi

2018 AAAs du 20 janvier 17:18:02.700520 : aaa_process_fd_set : mtscallback sur l'aaa_accounting_q

2018 AAAs du 20 janvier 17:18:02.700688 : VIEIL OPCODE : accounting_interim_update

2018 AAAs du 20 janvier 17:18:02.700702 : aaa_create_local_acct_req : user=, session_id=, fxosro log=added d'utilisateur

2018 AAAs du 20 janvier 17:18:02.700725 : aaa_req_process pour la comptabilité. session No. 0

2018 AAAs du 20 janvier 17:18:02.700738 : La référence de demande MTS est NULLE. Demande LOCALE

2018 AAAs du 20 janvier 17:18:02.700749 : Établissement d'AAA_REQ_RESPONSE_NOT_NEEDED

2018 AAAs du 20 janvier 17:18:02.700762 : aaa_req_process : Demande de général AAA d'appln : appln_subtype par défaut : par défaut

2018 AAAs du 20 janvier 17:18:02.700774 : try_next_aaa_method

2018 AAAs du 20 janvier 17:18:02.700798 : aucune méthodes configurées pour le par défaut de par défaut

2018 AAAs du 20 janvier 17:18:02.700810 : aucune configuration disponible pour ceci demande

2018 AAAs du 20 janvier 17:18:02.700997 : aaa_send_client_response pour la comptabilité. session->flags=254. aaa_resp->flags=0.

2018 AAAs du 20 janvier 17:18:02.701010 : la réponse pour la demande de comptabilité de la vieille bibliothèque sera envoyée comme SUCCÈS

2018 AAAs du 20 janvier 17:18:02.701021 : réponse non requise pour cette demande

2018 AAAs du 20 janvier 17:18:02.701033 : AAA_REQ_FLAG_LOCAL_RESP

2018 AAAs du 20 janvier 17:18:02.701044 : aaa_cleanup_session

2018 AAAs du 20 janvier 17:18:02.701055 : l'aaa_req devrait être libéré.

2018 AAAs du 20 janvier 17:18:02.701067 : Tombent de retour les gens du pays de méthode réussis

2018 AAAs du 20 janvier 17:18:02.706922 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:18:02.706937 : aaa_process_fd_set : mtscallback sur l'aaa_accounting_q

2018 AAAs du 20 janvier 17:18:02.706959 : VIEIL OPCODE : accounting_interim_update

2018 AAAs du 20 janvier 17:18:02.706972 : aaa_create_local_acct_req : user=, session_id=, utilisateur log=added : fxosro au rôle : en lecture seule

Après qu'une tentative d'authentification défaillante, vous voie la sortie suivante.

2018 AAAs du 20 janvier 17:15:18.102130 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102149 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102267 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102281 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102363 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102377 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102456 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102468 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102489 : mts_aaa_req_process

2018 AAAs du 20 janvier 17:15:18.102503 : aaa_req_process pour l'authentification. session No. 0

2018 AAAs du 20 janvier 17:15:18.102526 : aaa_req_process : Demande de général AAA d'appln : appln_subtype de procédure de connexion : par défaut

2018 AAAs du 20 janvier 17:15:18.102540 : try_next_aaa_method

2018 AAAs du 20 janvier 17:15:18.102562 : les méthodes totales configurées est 1, index en cours à essayer est 0

2018 AAAs du 20 janvier 17:15:18.102575 : handle_req_using_method

2018 AAAs du 20 janvier 17:15:18.102586 : AAA_METHOD_SERVER_GROUP

2018 AAAs du 20 janvier 17:15:18.102598 : groupe = rayon d'aaa_sg_method_handler

2018 AAAs du 20 janvier 17:15:18.102610 : Utilisant le sg_protocol qui est passé à cette fonction

2018 AAAs du 20 janvier 17:15:18.102625 : Envoi de la demande au service RADIUS

2018 AAAs du 20 janvier 17:15:18.102658 : mts_send_msg_to_prot_daemon : Longueur de charge utile = 371

2018 AAAs du 20 janvier 17:15:18.102684 : session : 0x8dfd68c ajouté au tableau 1 de session

2018 AAAs du 20 janvier 17:15:18.102698 : Groupe configuré de méthode réussi

2018 AAAs du 20 janvier 17:15:18.273682 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.273724 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.273753 : mts_message_response_handler : une réponse de mts

2018 AAAs du 20 janvier 17:15:18.273768 : prot_daemon_reponse_handler

2018 AAAs du 20 janvier 17:15:18.273783 : session : 0x8dfd68c retiré du tableau 0 de session

2018 AAAs du 20 janvier 17:15:18.273801 : état d'is_aaa_resp_status_success = 2

2018 AAAs du 20 janvier 17:15:18.273815 : les is_aaa_resp_status_success est VRAI

2018 AAAs du 20 janvier 17:15:18.273829 : aaa_send_client_response pour l'authentification. session->flags=21. aaa_resp->flags=0.

2018 AAAs du 20 janvier 17:15:18.273843 : AAA_REQ_FLAG_NORMAL

2018 AAAs du 20 janvier 17:15:18.273877 : mts_send_response réussi

2018 AAAs du 20 janvier 17:15:18.273902 : aaa_cleanup_session

2018 AAAs du 20 janvier 17:15:18.273916 : mts_drop des msg de demande

2018 AAAs du 20 janvier 17:15:18.273935 : l'aaa_req devrait être libéré.

2018 AAAs du 20 janvier 17:15:18.280416 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.280443 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.280454 : aaa_enable_info_config : GET_REQ pour le message d'erreur de procédure de connexion d'AAA

2018 AAAs du 20 janvier 17:15:18.280460 : obtenu de retour la valeur de retour de l'exécution de configuration : élément inconnu de Sécurité

Informations connexes

La commande d'Ethanalyzer sur FX-OS cli incitera pour le mot de passe pour un mot de passe quand l'authentification TACACS/RADIUS est activée. Ce comportement est provoqué par par une bogue.

Id de bogue : CSCvg87518