FirePOWER eXtensible Operating System (FXOS) 2.2: Chassis-Authentifizierung/-Autorisierung für Remote-Management mit ISE unter Verwendung von TACACS+

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Konfigurationen Konfigurieren des FXOS-Chassis Konfigurieren des ISE-Servers Überprüfen Überprüfen Überprüfung der FXOS-Chassis ISE 2.0-Verifizierung Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie die TACACS+-Authentifizierung und -Autorisierung für das FirePOWER eXtensible Operating System (FXOS)-Chassis über die Identity Services Engine (ISE) konfiguriert wird.

Das FXOS-Chassis umfasst die folgenden Benutzerrollen:

- Administrator Vollständiger Lese- und Schreibzugriff auf das gesamte System. Dem Standard-Administratorkonto wird diese Rolle standardmäßig zugewiesen, und es kann nicht geändert werden.
- Schreibgeschützt: Schreibgeschützter Zugriff auf die Systemkonfiguration ohne Berechtigung zum Ändern des Systemstatus.
- Betrieb Lese- und Schreibzugriff auf die NTP-Konfiguration, Smart Call Home-Konfiguration für Smart Licensing und Systemprotokolle, einschließlich Syslog-Server und -Fehler. Lesezugriff auf den Rest des Systems.
- AAA Lese- und Schreibzugriff auf Benutzer, Rollen und AAA-Konfiguration. Lesezugriff auf den Rest des Systems.

Über die CLI kann dies wie folgt angezeigt werden:

fpr4120-TAC-A /security* # Rolle anzeigen

Rolle:

Rollenname Priv.

Aaa

Administrator

Betriebsabläufe

schreibgeschützt

Mitarbeiter: Tony Remirez, Jose Soto, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis des FirePOWER eXtensible Operating System (FXOS)
- Kenntnis der ISE-Konfiguration
- In der ISE ist eine Lizenz für die TACACS+-Geräteadministration erforderlich.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco FirePOWER 4120 Security Appliance Version 2.2
- Virtuelle Cisco Identity Services Engine 2.2.0.470

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Ziel der Konfiguration ist es,

- Authentifizierung von Benutzern, die sich über die webbasierte GUI und SSH von FXOS anmelden, mithilfe der ISE
- Autorisieren Sie Benutzer, die sich über die ISE in die webbasierte Benutzeroberfläche und SSH von FXOS einloggen, entsprechend ihrer jeweiligen Benutzerrolle.
- Überprüfung des ordnungsgemäßen Betriebs der Authentifizierung und Autorisierung auf dem FXOS mithilfe der ISE

Netzwerkdiagramm



Network admin

Konfigurationen

Konfigurieren des FXOS-Chassis

Erstellen eines TACACS+-Anbieters

Schritt 1: Navigieren Sie zu Plattformeinstellungen > AAA.

Schritt 2: Klicken Sie auf die Registerkarte TACACS.

Overview	Interfaces	Logical	Devices	Secur	ity Engine	Platform Settings	S		
NTP			LDAP	RADIUS	TACACS				
SSH									
SNMP			Propertie	s					
HTTPS			Timeout:	* 5	Secs				
AAA				-					
Syslog			TACACS	Providers					
DNS									🔕 Add
FIPS and C	Common Criteria	3	Hostna	me		o	Order	Port	
Access List									

Schritt 3: Für jeden TACACS+-Anbieter, den Sie hinzufügen möchten (bis zu 16 Anbieter).

3.1 Klicken Sie im Bereich TACACS Providers (TACACS-Anbieter) auf Add (Hinzufügen).

3.2 Geben Sie nach dem Öffnen des Dialogfelds TACACS-Anbieter hinzufügen die erforderlichen Werte ein.

3.3 Klicken Sie auf OK, um das Dialogfeld TACACS-Anbieter hinzufügen zu schließen.

Í	Add TACACS Provider		?×
	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		ОК Са	incel

Schritt 4: Klicken Sie auf Speichern.

Overview Interfaces Logic	al Devices Security Engine Platform Setting	gs		
NTP				
SNMP	Properties			
HTTPS	Timeout:* 5 Secs			
Syslog	TACACS Providers			
DNS				Add
FIPS and Common Criteria	Hostname	Order	Port	
Access List	10.88.244.50	1	49	28
	Save Cancel			

Schritt 5: Navigieren Sie zu System > User Management > Settings.

Schritt 6: Wählen Sie unter Standardauthentifizierung die Option TACACS aus.

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				

Erstellen eines TACACS+-Anbieters mithilfe der CLI

Schritt 1: Führen Sie die folgenden Befehle aus, um die TACACS-Authentifizierung zu aktivieren.

fpr4120-TAC-A# Bereichssicherheit

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

fpr4120-TAC-A /security/default-auth # Festlegen des Bereichstakkus

Schritt 2: Verwenden Sie den Befehl show detail, um die Konfiguration zu überprüfen.

fpr4120-TAC-A /security/default-auth # Details anzeigen

Standardauthentifizierung:

Admin-Bereich: Taktiken

Operativer Bereich: Taktiken

Aktualisierungszeitraum für Websitzungen (in Sekunden): 600

Sitzungs-Timeout (in Sekunden) für Web-, SSH-, Telnet-Sitzungen: 600

Absolutes Sitzungs-Timeout (in Sekunden) für Web-, SSH- und Telnet-Sitzungen: 3600

Timeout für serielle Konsolensitzung (in Sekunden): 600

Absolutes Sitzungs-Timeout für die serielle Konsole (in Sekunden): 3600

Servergruppe "Admin Authentication":

Operational Authentication Server-Gruppe:

Anwendung des zweiten Faktors: Nein

Schritt 3: Führen Sie zum Konfigurieren der TACACS-Serverparameter die folgenden Befehle aus.

fpr4120-TAC-A# Bereichssicherheit

fpr4120-TAC-A/Security # Scope-Taks

fpr4120-TAC-A /security/tacacs # Server 10.88.244.50 eingeben

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

fpr4120-TAC-A /security/tacacs/server* # Schlüssel festlegen

Geben Sie den Schlüssel ein: *******

Schlüssel bestätigen: *******

Schritt 4: Verwenden Sie den Befehl show detail, um die Konfiguration zu überprüfen.

fpr4120-TAC-A /security/tacacs/server* # Details anzeigen

TACACS+-Server:

Hostname, FQDN oder IP-Adresse: 10,88,244,50

Beschreibung:

Bestellung: 1

Port: 49

Schlüssel: *****

Timeout: 5

Konfigurieren des ISE-Servers

Hinzufügen des FXOS als Netzwerkressource

Schritt 1: Navigieren Sie zu Administration > Network Resources > Network Devices.

Schritt 2: Klicken Sie auf HINZUFÜGEN.

dentity Services Engine	Home	Operations Policy	✓Administration	ns	
System Identity Management	Network Resources	Portal Management pxGrid	Services + Feed Service + Threat	Centric NAC	
Network Devices Network Device Green	oups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences NAC Ma	anagers External MDM + Location Se	ervices
G					
Network devices	Network Devices				
Default Device					
Device Security Settings	/ Edit 🕂 Add 🖓 Duplicat	e 🎲 Import 🚯 Export 🔘	Generate PAC 🔀 Delete		
	Name 🔺 IP/Ma	sk Profile Name	Location	Туре	Description
					No data available

Schritt 3: Geben Sie die erforderlichen Werte ein (Name, IP-Adresse, Gerätetyp und TACACS+ aktivieren), und klicken Sie dann auf **Senden.**

dentity Sen	vices Engine	Home	 Context 	Visibility • Operation	ns Policy	- Administratio	n 🕨	/ork Centers		
► System ► Ident	ity Management	- Networ	rk Resources	Device Portal Manag	ement pxGrid	Services + Fee	d Service	Threat Centric N	NAC	
✓ Network Devices	Network Device	Groups	Network Devi	ce Profiles External R	ADIUS Servers	RADIUS Server S	equences	NAC Managers	External MDM	Location Services
	6	Notur	ork Douisse Li							
Network devices		Netwo	work Devices Lis	st > PXOS						
Default Device				* Name	FXOS					
Device Security Settin	gs			Description						
			* IP Address	8: 10.83.180.6	/ 32					
				Device Profile	ttt: Cisco 👻	Ð				
						_				
				Model Name		<u>.</u>				
				Software version		<u>*</u>				
		•	* Network Dev	vice Group						
			Device Type	EXOS C	Set To Defau	alt				
			IPSEC		Set To Defai	dł.				
			Location		Set To Defa	dt				
			► RADIUS	Authentication Settings						
			TACACS	Authentication Settings						
			111011001	automodulor octango						
					Shared Secret	•••••		Show		
				Enable Sing	le Connect Mode					
						Legacy Cisco TACACS Dra	Device ft Complian	ce Single Connect	Support	
			SNMP Se	ttings						
			 Advanced 	TrustSec Settings						
		Sav	Reset							
		- uan								

Erstellen von Identitätsgruppen und Benutzern

Schritt 1: Navigieren Sie zu Administration > Identity Management > Groups > User Identity Groups (Administration > Identitätsverwaltung > Gruppen > Benutzeridentitätsgruppen).

Schritt 2: Klicken Sie auf HINZUFÜGEN.

tisce Identity Services Engine Home	Context Visibility Poperations Policy Admin	istration Work Centers
► System Identity Management Network R	esources	Feed Service Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups	
	/ Edit Takad K Delete + Epithport P 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

Schritt 3: Geben Sie den Wert für Name ein, und klicken Sie auf Senden.

diale Ider	ntity Services Engine	Home	Context Visibility	 Operations 	Policy	Administration	Work Centers	
 System 	- Identity Management	Network Re	esources + Devic	e Portal Management	pxGrid Servi	es I Feed Ser	rvice + Threat Centric NAC	
Identities	Groups External Ide	entity Sources	Identity Source Sec	quences + Settings	5			
Identit v v · · · ·	y Groups	م پ	User Identity Gro Identity Gro Name Description Submit	oups > New User Ide up FXOS ADMIN	antity Group			

Schritt 4: Wiederholen Sie Schritt 3 für alle erforderlichen Benutzerrollen.

tilitilitie Identity 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			
⟨= • E •	/ Edit 🕂 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		
	E AAA			
	E A FXOS ADMIN			
	E Pros Oper			
	FXOS Read Only			
		D.S. & COOLINE ACCOUNTS (J.S. & U.S. C.S.		

Schritt 5: Navigieren Sie zu Administration > Identity Management > Identity > Users.

Schritt 6: Klicken Sie auf HINZUFÜGEN.

-thele Identity Services Engine	Home ► Context Visibility ► Op	verations Policy Administration	n Work Centers						
System Identity Management	Network Resources	Management pxGrid Services + Fee	d Service						
◄ Identities Groups External Identity	Hantities Groups External Identity Sources Identity Source Sequences → Settings								
0									
Users	Network Access Users								
Latest Manual Network Scan Results	Latest Manual Network Scan Results / Edit 🕂 Add 📴 Change Status 😥 Import 🎲 Export 🛠 Delete 🏠 Duplicate								
	Status Name	 Description 	First Name Last Name Email Add	dress User Identity Groups Admin					
				No data available					

Schritt 7: Geben Sie die erforderlichen Werte ein (Name, Benutzergruppe, Passwort).

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
◄ Identities Groups External Identi	y Sources Identity Source Sequences
0	Network Assess Lists New Network Assess Lists
Users	Network Access Users List > New Network Access User
Latest Manual Network Scan Results	• Network Access oser
	*Name fxosadmin
	Status Cabled -
	Email
	▼ Passwords
	Password Type: Internal Users 👻
	Password Re-Enter Password
	Login Password Generate Password
	Enable Password Generate Password (
	✓ User Information
	First Name
	Last Name
	▼ Account Options
	Description
	Change password on next login
	Account Disable Policy
	Disable account if date exceeds 2018-03-01 (yyyy-mm-dd)
	▼ User Groups
	FXOS ADMIN 📀 — +
	Submit Cancel

Schritt 8: Wiederholen Sie Schritt 6 für alle erforderlichen Benutzer.

Identity Services Engine	Home Conte	xt Visibility	Policy Administrati	on 🔹 Work Ce	nters			
System - Identity Management	Network Resources	s Device Portal Managemen	t pxGrid Services + Fee	ed Service + Thr	eat Centric NAC			
- Identities Groups External Identity	y Sources Identity	Source Sequences Setting	5					
0	Not set a set							
Users	Network Acce	ss Users						
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎲 Import	🕞 Export 👻 🗙 Delete 👻	Duplicate				
	Status	Name	 Description 	First Name	Last Name	Email Address	User Identity Groups	Admin
	Enabled	👤 fxosaaa					FXOS AAA	
	Enabled	👤 fxosadmin					FXOS ADMIN	
	🗌 🛃 Enabled	9 fxosoper					FXOS OPER	
	🗌 🛃 Enabled	9 fxosro					FXOS Read Only	

Erstellen des Shell-Profils für jede Benutzerrolle

Schritt 1: Navigieren Sie zu **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles** und klicken Sie auf **+ADD**.

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 → Conditions 0 Selected Rows/Page 4 → 1 0 / 1 → 1 Go 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		

Schritt 2: Geben Sie die erforderlichen Werte für das TACACS-Profil ein.

2.1 Geben Sie den Namen ein.

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

2.2 Konfigurieren Sie auf der REGISTERKARTE **RAW View** (RAW-Ansicht) den folgenden CISCO-AV-PAIR.

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 Klicken Sie auf Senden.

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile				
Name	e FXOS_Admin_Profile			
Description	n			
Task Attribute View Ra	aw View			
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		0	(Select true or false)	
Timeout		0	Minutes (0-9999)	
Idle Time		0	Minutes (0-9999)	
Custom Attributes				
+ Add 📋 Trash - 🕑 Edit				۰-
Type Nar	me	Value		
MANDATORY cisc	co-av-pair	shell:roles="adr	min"	C 🛍

Schritt 3: Wiederholen Sie Schritt 2 für die verbleibenden Benutzerrollen mit den folgenden Cisco-AV-Paaren.

Cancel

Save

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

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

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

Custom Attributes

+ A	dd 🍵 Trash 👻 🖸 E	idit		۰.
	Туре	Name	Value	
	MANDATORY	cisco-av-pair	shell:roles="aaa"	C' 🗊
			Cance	I Save

Custom Attributes

+ Add	d 💼 Trash ▾ 🖸 B	Edit			¢-
	Туре	Name	Value	9	
	MANDATORY	cisco-av-pair	shell:	roles="operations"	C 🛍
Custom	Attributes				Course
+ Add	🗎 🗂 Trash 👻 🕑 E	dit			÷-
	Гуре	Name	Value		
	MANDATORY	cisco-av-pair	shell:r	oles="read-only"	C 🗎
TAC	ACS Profiles		Row	s/Page 8 ▼ M < 1 ⓒ / 1 ► ► Go	8 Total Rows
S	Refresh 🕂 Add	Duplicate 🛍 Trash -	C Ed	dit 🔻 Filt	er 🕶 🌣 🕶
	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	•	Shell	Default Shell Profile	
	FXOS_Admin_Prof	ile	Shell		
	FXOS_AAA_Shell		Shell		
	FXOS_Operations_	Shell	Shell		
	FXOS_ReadOnly_S	Shell	Shell		

Erstellen der TACACS-Autorisierungsrichtlinie

Schritt 1: Navigieren Sie zu Work Center > Device Administration > Device Admin Policy Sets (Geräteverwaltung > Geräte-Admin-Richtliniensätze).

cisco Identity Services Engine Home	+ Context Vability + Operations + Policy + Administration + Work Centers	(1) Q (1)
Network Access Guest Access TrustSec	BYOD Profiler Posture Posture PossiveID	Click here to do wireless setup and visibility setup Do not show this again. X
Overview Identities User Identity Groups	Ext Id Sources + Network Resources + Policy Elements Device Admin Policy Sets Reports Settings	
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 Export go to Administration > System > Backup & Restore > Policy Export Page Status Name Description	
Summary of Policies	Default Tacacs_Default Regular (> Provy Sequence (>	
Global Exceptions Rules across entire deployment	Proxy Server Sequence Proxy server sequence	
Default Taxas Default	a kokastiostis Beller	
Seve Order Reset Order	Autometrocation Policy 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 (dentity groups and other conditions) Command Sets Shell Profiles Tacace Default If no matches then Saled Profile/II Denv at Shell Profile	Edit =
		Refer 1

Schritt 2: Stellen Sie sicher, dass die Authentifizierungsrichtlinie auf die Datenbank für interne

Benutzer oder den erforderlichen Identitätsspeicher verweist.



Schritt 3: Klicken Sie am Ende der standardmäßigen Autorisierungsrichtlinie auf den Pfeil, und klicken Sie oben auf Regel einfügen.

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

Schritt 4: Geben Sie die Werte für die Regel mit den erforderlichen Parametern ein:

- 4.1 Regelname: FXOS-Admin-Regel.
- 4.2 Bedingungen.

Wenn : Benutzeridentitätsgruppe: FXOS ADMIN

Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles	
🖉 🖉 👻 FXOS Admin Rule	if Any and Condition(s) 💠 then Comman 💠 and Select a Shell Prof	ile
Tacacs_Default	if no ma	
	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)	
Cours	FXOS Read Only	
Save	ALL_ACCOUNTS (default)	

Und Gerät: Der Gerätetyp ist gleich allen Gerätetypen #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 >

Shell-Profil: FXOS_Admin_Profile

Select a Shell Profile	\bigcirc
	Shell Profile
	Se Verault Shell Profile
	🥁 Deny All Shell Profile
	G FXOS_AAA_Shell
	KOS_Admin_Profile
	Store Store Street Street Store Street Store Sto
	Generation FXOS_ReadOnly_Shell
	😪 WLC ALL
	WLC MONITOR

Schritt 5: Klicken Sie auf Fertig.

Exc	eptions (0)		
Stand	land		
5	Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles	
i 🖉 🖥	 FXOS Admin Rule 	If FX	Done
	Tacacs_Default	if no matches, then Select Profile(s) Deny Al Shell Profile	Edit 🕶
Save	Reset		

Schritt 6: Wiederholen Sie die Schritte 3 und 4 für die übrigen Benutzerrollen, und klicken Sie abschließend auf **SPEICHERN**.

Exceptio	ons (0)					
Standard						
Status	s Rule Name		Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
ø 🗹	FXOS Admin Rule	if	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select an item	FXOS_Admin_Profile
Ø 🗹	FXOS AAA Rule	if	FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select Profile(s)	FXOS_AAA_Shell
# 🗹	FXOS Operations Rule	if	FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	Select Profile(s)	FXOS_Operations_Shell
Ø 🗹	FXOS Read Only Rule	if	FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS			FXOS_ReadOnly_Shell
~	Tacacs_Default	if n	o matches, then Select Profile(s) Deny All	Shell Pr	ofile	



Überprüfen

Sie können jetzt jeden Benutzer testen und die zugewiesene Benutzerrolle überprüfen.

Überprüfung der FXOS-Chassis

1. Telnet oder SSH zum FXOS-Chassis und melden Sie sich mit einem der erstellten Benutzer auf der ISE an.

Benutzername: Fxosadmin

Kennwort:

fpr4120-TAC-A# Scope Security

fpr4120-TAC-A/security # Details für Remote-Benutzer anzeigen

Remote-Benutzer fxosaa:

Beschreibung:

Benutzerrollen:

Name: Aaa

Name: schreibgeschützt

Remote-Benutzer fxosadmin:

Beschreibung:

Benutzerrollen:

Name: Administrator

Name: schreibgeschützt

Remote-Benutzer-Faxgerät:

Beschreibung:

Benutzerrollen:

Name: Betrieb

Name: schreibgeschützt

Remote User FXOTOR:

Beschreibung:

Benutzerrollen:

Name: schreibgeschützt

Je nach dem eingegebenen Benutzernamen werden in der FXOS-Chassis-CLI nur die Befehle angezeigt, die für die zugewiesene Benutzerrolle autorisiert wurden.

Administratorbenutzerrolle.

fpr4120-TAC-A /security #?

Bestätigung

Benutzersitzungen löschen

Erstellen verwalteter Objekte

Löschen verwalteter Objekte

Deaktivierung von Diensten

Aktivieren von Services

Geben Sie ein verwaltetes Objekt ein.

Bereich Ändert den aktuellen Modus

Festlegen von Eigenschaftenwerten

Systeminformationen anzeigen

Aktive CMC-Sitzungen beenden

fpr4120-TAC-A# Connect-FXOS

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

fpr4120-TAC-A (fxos)#

Reiner Lesezugriff auf Benutzerrollen.

fpr4120-TAC-A /security #?

Bereich Ändert den aktuellen Modus

Festlegen von Eigenschaftenwerten

Systeminformationen anzeigen

fpr4120-TAC-A# Connect-FXOS

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

% Berechtigung verweigert für die Rolle

2. Navigieren Sie zur IP-Adresse des FXOS-Chassis, und melden Sie sich mit einem der erstellten Benutzer auf der ISE an.

Administratorbenutzerrolle.

Overview Interfaces Logica	I Devices Security Engine Platform Setti	ngs								
NTP	LDAP RADIUS TACACS									
SSH SNMP HTTPS	Properties Timeout:* 5 Secs									
> AAA	TACACS Providers									
Syslog DNS			Add TACACS Provider			Add				
FIPS and Common Criteria Access List	Hostname	Order	Hostname/FQDN(or IP Address):*]					
	10.88.244.50	1	Order:*	lowest-available		d 🗇 🗇				
			Key:		Set:No					
			Confirm Key:							
			Port:*	49						
			Timeout:*	5 Secs						
				ОКС	ancel					
	Save Cancel									

Schreibgeschützte Benutzerrolle.

riew Interfaces	Logical I	Devices Security Engine	Platform Settings					
9		LDAP RADUS TACACS						
SH NHP		Properties						
HTTPS		Timout* 5 Secs						
Syslog		TACACS Providers						
DNS						0	Add	
Access List		Hostname	On	der	Port			
		10.88.244.50	1		49	۹. ۵		

Hinweis: Beachten Sie, dass die Schaltfläche ADD deaktiviert ist.

ISE 2.0-Verifizierung

1. Navigieren Sie zu Operations > TACACS Livelog. Erfolgreiche und fehlgeschlagene Versuche sollten angezeigt werden.

altalt cisco	Identity Services Engine	Home + Co	ntext Visibility	- Operations	Policy Admir	istration + Work Centers				۹. 😐	• •
RADIUS Threat-Centric NAC Live Logs TrackCS Trackieshoot Adaptive Network Control Reports											
Live Logs											
								Refresh Never + Show Late	est 20 records · Within	Last 3 hours	s •
0	Defects									¥	-
2	Remean Z Export to *									f Piller •	••
	Logged Time	Status	Details	Username	Туре	Authentication Policy	Authorization Policy	Failure Reason	Matched Comma	Shell Profile	•
×]	Username	•	Authentication Policy	Authorization Policy	Failure Reason	Matched Command S	Shell Profile	
	Jan 17, 2018 08:57:23.272 PM	e	.0	fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admir	_Profile
	Jan 17, 2018 08:57:22.852 PM	•	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default					
	Jan 17, 2018 08:57:10.829 PM	۰	0	fxosadmin	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared			
	Jan 17, 2018 08:57:01.069 PM	~		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			

Fehlerbehebung

Führen Sie zum Debuggen der AAA-Authentifizierung und -Autorisierung die folgenden Befehle in der FXOS-CLI aus.

fpr4120-TAC-A# Connect-FXOS

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

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

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

fpr4120-TAC-A (fxos)# term mon

Nach einem erfolgreichen Authentifizierungsversuch wird die folgende Ausgabe angezeigt.

17.01.2018 15:46:40.305247 aaa: aa_req_process für die Authentifizierung. Sitzung Nr. 0

17.01.2018 15:46:40.305262 aaa: aaa_req_process: Allgemeine AAA-Anfrage von Anwendung: login appln_subtype: Standard

17.01.2018 15:46:40.305271 aaa: try_next_aaa_method

17.01.2018 15:46:40.305285 aaa: Die konfigurierten Methoden gesamt sind 1, der aktuelle Index ist 0.

17.01.2018 15:46:40.305294 aaa: Handle_req_using_method

17. Januar 2018 15:46:40.305301 aaa: AAA_METHODE_SERVER_GRUPPE

17. Januar 2018 15:46:40.305308 aaa: aa_sg_method_handler group = takacs

17. Januar 2018 15:46:40.305315 aaa: Verwenden des an diese Funktion übergebenen sg_protocol

17.01.2018 15:46:40.305324 aaa: Anfrage an TACACS-Dienst senden

17.01.2018 15:46:40.305384 aaa: Konfigurierte Methodengruppe erfolgreich

17. Januar 2018 15:46:40:554631 aaa: aaa_process_fd_set

17. Januar 2018 15:46:40:555229 aaa: aa_process_fd_set: mtscallback auf aaa_q

17. Januar 2018 15:46:40:555817 aaa: mts_message_response_handler: eine MTS-Antwort

17. Januar 2018 15:46:40:556387 aaa: prot_daemon_response_handler

17. Januar 2018 15:46:40:557042 aaa: Sitzung: 0x8dfd68c aus Sitzungstabelle 0 entfernt

17. Januar 2018 15:46:40:557059 aaa: is_aaa_resp_status_Succ= 1

17. Januar 2018 15:46:40:557066 aaa: is_aa_resp_status_Success ist TRUE

17. Januar 2018 15:46:40:557075 aaa: aa_send_client_response für die Authentifizierung. session->flags=21. aa_resp->flags=0.

17. Januar 2018 15:46:40:557083 aaa: AAA_REQ_FLAG_NORMAL

17. Januar 2018 15:46:40:557106 aaa: mts_send_response erfolgreich

17. Januar 2018 15:46:40:557364 aaa: aa_req_process für die Autorisierung. Sitzung Nr. 0

17. Januar 2018 15:46:40:557378 aaa: aaa_req_process called with context from appln: login appln_subtype: default authen_type:2, authen_method: 0

17. Januar 2018 15:46:40:557386 aaa: aaa_send_req_using_context

17. Januar 2018 15:46:40:557394 aaa: aa_sg_method_handler group = (null)

17. Januar 2018 15:46:40:557401 aaa: Verwenden des an diese Funktion übergebenen sg_protocol

17. Januar 2018 15:46:40:557408 aaa: kontextbasiertes oder gerichtetes AAA req (Ausnahme: keine Relay-Anfrage). Keine Kopie einer Anforderung wird übernommen.

17. Januar 2018 15:46:40:557415 aaa: Anfrage an TACACS-Dienst senden

17. Januar 2018 15:46:40.801732 aaa: aa_send_client_response für die Autorisierung. session->flags=9. aa_resp->flags=0.

17. Januar 2018 15:46:40:801740 aaa: AAA_REQ_FLAG_NORMAL

17. Januar 2018 15:46:40.801761 aaa: mts_send_response erfolgreich

17. Januar 2018 15:46:40.848932 aaa: ALTER OPCODE: accounting_interim_update_update

17.01.2018 15:46:40.848943 aaa: aa_create_local_acct_req: user=, session_id=, log=added user:fxosadmin to role:admin

17. Januar 2018 15:46:40.848963 aaa: aa_req_process for accounting. Sitzung Nr. 0

17. Januar 2018 15:46:40.848972 aaa: Die MTS-Anforderungsreferenz lautet NULL. LOKALE Anforderung

17.01.2018 15:46:40.848982 aaa: Festlegen von AAA_REQ_RESPONSE_NOT_NEEED

17.01.2018 15:46:40.848992 aaa: aaa_req_process: Allgemeine AAA-Anfrage von Anwendung: default appln_subtype: Standard

17. Januar 2018 15:46:40.849002 aaa: try_next_aaa_method

17. Januar 2018 15:46:40.849022 aaa: Keine Standardmethoden konfiguriert

17. Januar 2018 15:46:40.849032 aaa: Keine Konfiguration für diese Anforderung verfügbar

17. Januar 2018 15:46:40.849043 aaa: try_fallback_method

17. Januar 2018 15:46:40.849053 aaa: Handle_req_using_method

17. Januar 2018 15:46:40.849063 aaa: local_method_handler

17. Januar 2018 15:46:40.849073 aaa: aaa_local_accounting_msg

17. Januar 2018 15:46:40.849085 aaa: Aktualisieren::Benutzer:fxosadmin zur Rolle hinzugefügt:admin

Nach einem fehlgeschlagenen Authentifizierungsversuch wird die folgende Ausgabe angezeigt.

17.01.2018 15:46:17.836271 aaa: aa_req_process für die Authentifizierung. Sitzung Nr. 0

17.01.2018 15:46:17.83616 aaa: aaa_req_process: Allgemeine AAA-Anfrage von Anwendung: login appln_subtype: Standard

17.01.2018 15:46:17.837063 aaa: try_next_aaa_method

17.01.2018 15:46:17.837416 aaa: Die konfigurierten Methoden gesamt sind 1, der aktuelle Index ist 0.

17.01.2018 15:46:17.83766 aaa: Handle_req_using_method

17.01.2018 15:46:17.838103 aaa: AAA_METHODE_SERVER_GRUPPE

17.01.2018 15:46:17.83847 aaa: aa_sg_method_handler group = takacs

17.01.2018 15:46:17.83826 aaa: Verwenden des an diese Funktion übergebenen sg_protocol

17.01.2018 15:46:17.839167 aaa: Anfrage an TACACS-Dienst senden

17. Januar 2018 15:46:17.840225 aaa: Konfigurierte Methodengruppe erfolgreich

17. Januar 2018 15:46:18.043710 aaa: is_aa_resp_status_Success status = 2

17. Januar 2018 15:46:18.044048 aaa: is_aa_resp_status_Success ist TRUE

17. Januar 2018 15:46:18.044395 aaa: aa_send_client_response für die Authentifizierung. session->flags=21. aa_resp->flags=0.

17. Januar 2018 15:46:18.04473 aaa: AAA_REQ_FLAG_NORMAL

17.01.2018 15:46:18.045096 aaa: mts_send_response erfolgreich

17. Januar 2018 15:46:18.04567 aaa: aaa_cleanup_session

17. Januar 2018 15:46:18.045689 aaa: mts_drop der Anfrage msg

17.01.2018 15:46:18.04569 aaa: aaa_req sollte freigegeben werden.

17. Januar 2018 15:46:18.045715 aaa: aaa_process_fd_set

17. Januar 2018 15:46:18.045722 aaa: aa_process_fd_set: mtscallback auf aaa_q

17. Januar 2018 15:46:18.045732 aaa: aa_enable_info_config: GET_REQ für eine Anmeldefehlermeldung

17. Januar 2018 15:46:18.045738 aaa: Rückgabewert des Konfigurationsvorgangs zurückerhalten:Unbekannter Sicherheitsaspekt

Zugehörige Informationen

Der Ethanalyzer-Befehl in der FX-OS-CLI fordert Sie zur Eingabe des Kennworts auf, wenn die

TACACS/RADIUS-Authentifizierung aktiviert ist. Dieses Verhalten wird durch einen Fehler verursacht.

Bug-ID: CSCvg87518