Firepower eXtensible Operating System (FXOS) 2.2: Chassis verificatie/autorisatie voor extern beheer met ISE met behulp van TACACS+

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram Configuraties Het FXOS-chassis configureren De ISE-server configureren Verifiëren Verificatie FXOS-chassis ISE 2.0 Verificatie Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u TACACS+ verificatie en autorisatie voor het FirePOWER Xtensible Operating System (FXOS) chassis via Identity Services Engine (ISE) kunt configureren.

Het FXOS-chassis bevat de volgende gebruikersrollen:

- Administrator volledige toegang tot het volledige systeem voor lezen en schrijven. De standaard admin-account krijgt deze rol standaard toegewezen en kan niet worden gewijzigd.
- Alleen-lezen alleen-lezen toegang tot de systeemconfiguratie zonder bevoegdheden om de systeemstatus te wijzigen.
- Operations lees-en-schrijftoegang tot de NTP-configuratie, Smart Call Home-configuratie voor slimme licenties en systeemlogbestanden, inclusief systeemservers en fouten. Lees de toegang tot de rest van het systeem.
- AAA lees-en-schrijf toegang tot gebruikers, rollen en AAA-configuratie. Lees de toegang tot de rest van het systeem.

Via CLI kan dit als volgt worden gezien:

fpr4120-TAC-A/security* # rol

Rol:

Functienaam Priv

Aa aaa

beheerder

operaties

alleen-lezen

Bijgedragen door Tony Remirez, Jose Soto, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER Xtensible Operating System (FXOS)
- Kennis van ISE-configuratie
- De licentie voor TACACS+ apparaatbeheer is vereist binnen ISE

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower 4120 security applicatie versie 2.2
- Virtual Cisco Identity Services Engine 2.2.0.470

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Het doel van de configuratie is:

- Verifieer gebruikers die zich aanmelden in de op het web gebaseerde GUI en SSH van FXOS met behulp van ISE
- Geef gebruikers toestemming om te loggen in de op het web gebaseerde GUI en SSH van FXOS overeenkomstig hun respectieve gebruikersrol door middel van ISE.
- Controleer de goede werking van de echtheidscontrole en de vergunning op de FXOS door middel van ISE

Netwerkdiagram



Configuraties

Het FXOS-chassis configureren

Een TACACS+ provider maken

Stap 1. Navigeer naar **platform instellingen > AAA**.

Stap 2. Klik op het tabblad **TACACS**.

Overview Interfaces Logic	al Devices Security Engine	Platform Settings		
NTP	LDAP RADIUS TACACS			
SSH				
SNMP	Properties			
HTTPS	Timeout:* 5 Secs			
► AAA				
Syslog	TACACS Providers			
DNS				O Add
FIPS and Common Criteria	Hostname	Order	Port	
Access List	nostiame	order	Port	

Stap 3. Voor elke TACACS+ provider die u wilt toevoegen (maximaal 16 providers).

3.1. Klik in het gebied TACACS Providers op Toevoegen.

3.2. Zodra het dialoogvenster TACACS-providers wordt geopend, voert u de gewenste waarden in.

3.3. Klik op **OK** om het dialoogvenster Add TACACS Provider te sluiten.

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

Stap 4. Klik op Opslaan.

Overview Interfaces Logi	ical Devices Security Engine Platform Setti	ngs				
NTP SSH	LDAP RADIUS TACACS					
SNMP HTTPS	Properties Timeout:* 5 Secs	rties nut:* 5 Secs				
> AAA Syslog	TACACS Providers	CS Providers				
DNS				Add		
FIPS and Common Criteria	Hostname	Order	Port			
Access List	10.88.244.50	1	49	<i>i</i>		
	Save Cancel					

Stap 5. Navigeer naar Systeem > Gebruikersbeheer > Instellingen.

Stap 6. Selecteer onder Standaardverificatie de optie **TACACS**.

Overview Interfaces	Logical Devices Security Engine Platform Settings			System Too	ls Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	TACACS v *Local is failback authentication method				
Console Authentication	Local v				
Remote User Settings Remote User Role Policy	🕒 Assign Detfuelt Role: 🔿 No-Login				

Een TACACS+ provider maken met CLI

Stap 1. Om TACACS-verificatie mogelijk te maken, voert u de volgende opdrachten uit.

voor de **beveiliging** van 4120-TAC-A# bereik

fpr4120-TAC-A/security #bereik: standaardinstelling

fpr4120-TAC-A/security/default-auth #set-realm-tac's

Stap 2. Gebruik de opdracht Details tonen om de configuratie te controleren.

fpr4120-TAC-A/security/default-auth # details laten zien

Standaardverificatie:

Admin Realm: Tacacs

Operationeel antwoord: Tacacs

Web sessie verfrissing periode (in seconden): 600

Session timeout (in s) voor web-, ssh-, telnet-sessies: 600

Absolute sessietijd (in seconden) voor web-, ssh-, telnet-sessies: 3600

Seriële console-sessietijd (in seconden): 600

Seriële console absolute sessietijd (in seconden): 3600

Admin-servergroep:

Vak Operationele verificatieserver:

Gebruik van de tweede factor: Nee

Stap 3. Om de TACACS-serverparameters te configureren voert u de volgende opdrachten uit.

voor de beveiliging van 4120-TAC-A# bereik

fr4120-TAC-A/security # tac-werkingssfeer

fpr4120-TAC-A/security/tacacs # server 10.8.244.50

fpr4120-TAC-A/security/tacacs/server # ingestelde "ACS-server"

fpr4120-TAC-A/security/tacacs/server* # ingestelde toets

Geef de toets op: ******

Bevestig de toets: ******

Stap 4. Gebruik de opdracht detail tonen om de configuratie te controleren.

fpr4120-TAC-A/security/tacacs/server* # details laten zien

TACACS+ server:

Hostname, FQDN of IP-adres: 10.88.244.50

Descr:

Volgorde: 1

Port: 49

Sleutel: ****

Time-out: 5

De ISE-server configureren

De FXOS als netwerkresource toevoegen

Stap 1. Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten.

Stap 2. Klik op ADD.



Stap 3. Voer de gewenste waarden in (Naam, IP-adres, Type apparaat en TACACS+ inschakelen en voeg de SLEUTEL toe) en klik op **Indienen.**

dentity Services Engine	Home +	Context Visibility	 Operations 	Policy	 Administration 	 Work Centers 		
System Identity Management	- Network Res	ources	Portal Managemen	nt pxGrid S	Services Feed S	ervice + Threat Centric I	NAC	
Network Devices Network Device 0	Groups Netwo	ork Device Profiles	External RADIU	S Servers	RADIUS Server Seq	uences NAC Managers	External MDM	Location Services
0	Network De							
Network devices	Network De	Devices						
Default Device			* Name FX	05				
Device Security Settings			Description					
	* IP	Address: 10.83.1	80.6	/ 32				
		• [Device Profile	Cisco 🔻 🕀				
		Soft	ware Version		:			
	* Netv	work Device Group						
	Device	FXOS	0	Set To Default	t			
	1	PSEC No	0	Set To Default	t			
	Lo	All Location	is 📀 📑	Set To Default	t			
	□ ▶R	ADIUS Authenticati	on Settings					
	V - T	ACACS Authenticat	on Settings					
		ACACS Autremicat	St Study Strategy St	nared Secret	Legacy Cisco Dr TACACS Draft C	Show svice	Support	
	□ • s	NMP Settings						
	□ ► A	dvanced TrustSec S	Settings					
	Save	Reset						

Identiteitsgroepen en gebruikers maken

Stap 1. Navigeer naar Administratie > identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen.

Stap 2. Klik op ADD.

-tisce Identity Services Engine Home	Context Visibility Operations Policy Admin	istration > Work Centers
System ✓ Identity Management Network Re	esources	Feed Service Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups	
<u>ج</u>	oser racinity croups	
⟨= + E +		
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
	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Stap 3. Voer de waarde voor Naam in en klik op Indienen.

den den	tity Services Engine	Home	Context Visibility	 Operations 	Policy	▼ Admir	nistration	Work Centers	
 System 	✓ Identity Management	Network R	esources + Devic	e Portal Managemen	t pxGrid S	ervices	Feed Serv	ice + Threat Centric NAC	
Identities	Groups External Ide	entity Sources	Identity Source Sec	quences + Setting	S				
Identity	r Groups	م ڇپ	User Identity Gro Identity Gro Name Description Submit	oups > New User Ide PROS ADMIN Cancel	entity Group				

Stap 4. Herhaal stap 3 voor alle vereiste gebruikersrollen.

titude dentity Services Engine Home	Context Visibility Operations Policy Adm	inistration Work Centers
► System Identity Management Network Re	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
	Employee	Default Employee User Group
	E AAA	
	FXOS ADMIN	
	E A FXOS OPER	
	FXOS Read Only	
		Differ to contract (differ the time contract

Stap 5. Navigeer naar Administratie > Identity Management > Identity > Gebruikers.

Stap 6. Klik op ADD.

-iltelia Identity Services Engine Home Context Visibility	Operations Policy Administration	▶ Work Centers	
System Identity Management Network Resources Device Point	tal Management pxGrid Services + Feed S	ervice	
Identities Groups External Identity Sources Identity Source Sequen	es		
0			
Users Network Access Users			
Latest Manual Network Scan Results	- Chalmoort Challerout	Duplicate	
	Contact Contraction		
Status Name	Description Fi	rst Name Last Name Email Address	User Identity Groups Admin
			No data available

Stap 7. Voer de gewenste waarden in (naam, gebruikersgroep, wachtwoord).

dentity Services Engine	Home
► System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
✓Identities Groups External Ident	ty Sources Identity Source Sequences
G	
Users	Network Access Users List > New Network Access User
Latest Manual Network Scan Results	* HELWORK ACCESS USER
	*Name fxosadmin
	Status 🖌 Enabled 👻
	Email
	▼ Passwords
	Password Type: Internal Users 💌
	Password Re-Enter Password
	Login Password Generate Password
	Enable Password Generate Password (i)
	▼ 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
	Exos admin 📀 — +
	Submit Cancel

Stap 8. Herhaal stap 6 voor alle vereiste gebruikers.

dentity Services Engine	Home + Conte	xt Visibility	Policy Administrat	on 🔹 Work Ce	nters			
System - Identity Management	Network Resources	s Device Portal Management	pxGrid Services + Fe	ed Service + The	eat Centric NAC			
- Identities Groups External Identity	y Sources Identity	Source Sequences	3					
0								
Users	Network Acce	ss Users						
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎥 Import	Export + X 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	2 fxosro					FXOS Read Only	

Het Shell-profiel maken voor elke gebruikersrol

Stap 1. Navigeer naar **werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen** en klik op **+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		

Stap 2. Voer de gewenste waarden in voor het TACACS-profiel

2.1. Voer de naam in.

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

2.2. Configureer in het TAB **RAW View** het volgende CISCO-AV-PAIR.

cisco-av-pair=shell:rollen="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. Klik op Indienen.

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile				
Ν	Aame FXOS_Admin_Profile			
Descri	ption			
Task Attribute View	Raw 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	it			¢-
О Туре	Name	Value		

Stap 3. Herhaal stap 2 voor de overige gebruikershandleidingen met behulp van de volgende Cisco-AV-paren.

shell:roles="admin"

C 🖻

Cancel Save

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

cisco-av-pair=shell:rollen="operaties"

cisco-av-pair=shell:rollen="alleen-lezen"

cisco-av-pair

Custom Attributes

MANDATORY

+ A	dd 🍵 Trash 🕶 🕑 E	dit		¢
	Туре	Name	Value	
	MANDATORY	cisco-av-pair	shell:roles="aaa"	6 🗊
			Cano	el Save

Custom Attributes

+ Ac	d 🛍 Trash 🕶 🕑 E	dit			¢-
	Туре	Name	Value		
	MANDATORY	cisco-av-pair	shell:r	oles="operations"	C' 🛍
Custor	n Attributes				
+ Ad	d 💼 Trash 🕶 🕑 E	dit			۰.
	Туре	Name	Value		
	MANDATORY	cisco-av-pair	shell:ro	les="read-only"	C' 🗊
TAC 0 Sel	ACS Profiles ected Refresh + Add	Duplicate 💼 Trash -	Rows	s/Page 8 ▼ M < 1 0 / 1 ► M Go	8 Total Rows er 🔹 🌣 🗸
	Name		Туре	Description	
	WLC ALL		WLC	WLC ALL	
	WLC MONITOR		WLC	WLC MONITOR	
	Deny All Shell Profil	e	Shell	Deny All Shell Profile	
	Default Shell Profile	•	Shell	Default Shell Profile	
	FXOS_Admin_Profi	le	Shell		
	FXOS_AAA_Shell		Shell		
	FXOS_Operations_	Shell	Shell		
	FXOS_ReadOnly_S	Shell	Shell		

Het Tacacs-machtigingsbeleid creëren

Stap 1. navigeren naar werkcentra > Apparaatbeheer > Apparaatbeheerset.

Cisco Identity Services Engine Home	Context Visibility + Operations + Policy + Administration Work Centers	(1) Q (0) Q (0)
Network Access Guest Access TrustSec Overview Identities User Identity Groups	BYOD + Profiler + Posture - Device Administration + PassiveID Ext Id Sources + Network Resources + Policy Elements Device Admin Policy Sets Reports Settings	Click here to do wireless setup and visibility setup Do not show this again. $\overset{\scriptstyle \times}{\times}$
Policy Sets Search policy rames & descriptions	Celle Goodeal * President resolution of the polarity of the p	
Tacace, Default Save Order Reset Order	Authentication 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, men Select Profile	Eði •

Stap 2. Zorg ervoor dat het verificatiebeleid op de interne gebruikersdatabase of de vereiste identiteitswinkel wijst.

Ŧ	Authent	ication Policy				
		Default Rule (If no match)	:	Allow Protocols : Default Device Admin	and use : All_User_ID_Stores	

Stap 3. Klik op de pijl aan het einde van het standaardbeleid voor autorisatie en klik op boven regels invoegen.

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

Stap 4. Voer de waarden voor de regel in met de vereiste parameters:

- 4.1. Naam van de regel: FXOS-beheerder.
- 4.2. Voorwaarden.

Indien : User Identity Group is FXOS ADMIN

Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles
FXOS Admin Rule	if Any Condition(s) 4 then Comman 4 and Select a Shell Prof
Zacacs_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)
Cruco	FXOS Read Only
Save	ALL_ACCOUNTS (default)

En apparaat: Apparaattype is gelijk aan alle apparaattypen #FXOS

Conditions (identity groups	and other conditions)	Command Sets She	ell Profiles			
if FX 💠 and D	EVICE:Devi 🗢 ther	Comman 🔶 and	Select a Shell Profile	\bigcirc		
o matches, then Selec	Add All Conditions Belo	w to Library				-
	Condition Name	Description DEVICE:Device Ty	📀 Equals 👻	All Device Types# 📀		ŵ .
					All Device Types All Device Types#EXOS	int Y
					aD	>
					DEVICE	>
					🚞 InternalUser	>
					Network Access	>
					Network Condition	>
					TACACS	>

Shell Profile : FXOS_Admin_Profiel

Select a Shell Profile	\bigcirc
	Shell Profile
	(م
	⟨= ▼ ■ ▼ 23.
	😪 Default Shell Profile
	😪 Deny All Shell Profile
	Generation FXOS_AAA_Shell
	General Stress FXOS_Admin_Profile
	Gerations_Shell
	Shell FXOS_ReadOnly_Shell
	See WLC ALL
	WLC MONITOR

Stap 5. Klik op Gereedschap.

Exceptions (0)		
Standard		
Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles	
🖉 🖉 👻 FXOS Admin Rule	If FX \diamond and DEVICE-Devi \diamond than Select an item \diamond and FXXS_Admin_Profile 📿	Done
Tacacs_Default	If no matches, then Soloct Profile(s) Deny Al Shell Profile	Edit 🕶
Save Reset		

Stap 6. Herhaal stap 3 en 4 voor de resterende gebruikersrollen en na het klaar zijn klikt u op **OPSLAAN**.

Except tandarc	ions (0)					
Stat	us 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
Ø 🔽	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 S	hell Pro	ofile	



Verifiëren

U kunt nu elke gebruiker testen en de toegewezen gebruikersrol controleren.

Verificatie FXOS-chassis

1. Telnet of SSH aan het FXOS-chassis en inloggen met behulp van een van de gemaakte gebruikers op ISE.

Username: fxosadmin

Wachtwoord:

Voor de **beveiliging** van de **FPR**4120-TAC-A#scope

fpr4120-TAC-A/security # geeft details voor externe gebruikers weer

Afstandsbediening door gebruiker:

Beschrijving:

Rol gebruiker:

Name: Aa

Name: alleen-lezen

Afstandsbediening door gebruiker fxosadmin:

Beschrijving:

Rol gebruiker:

Name: besturen

Name: alleen-lezen

Afstandsbediening door gebruiker:

Beschrijving:

Rol gebruiker:

Name: verrichting

Name: alleen-lezen

Afstandsbediening door gebruiker:

Beschrijving:

Rol gebruiker:

Name: alleen-lezen

Afhankelijk van de gebruikersnaam die in de FXOS-chassiscli is ingevoerd, worden alleen de opdrachten weergegeven die zijn geautoriseerd voor de gebruikersrol die is toegewezen.

Gebruiker beheren.

fpr4120-TAC-A/security #?

erkennen

duidelijke gebruikerssessies Wis gebruikerssessies

Maken beheerde objecten

Verwijdert beheerde objecten verwijderen

schakelt uitgeschakeld services uit

diensten mogelijk maken

Voer een beheerd object in

scope wijzigt de huidige modus

Vastgestelde waarden

Systeeminformatie weergeven

actieve cimc-sessies beëindigen

FPR4120-TAC-A#connect fxos

fpr4120-TAC-A (fxos)# debug Aa-verzoeken

fpr4120-TAC-A (FXS)#

Alleen-lezen gebruikersrol.

fpr4120-TAC-A/security #?

scope wijzigt de huidige modus

Vastgestelde waarden

Systeeminformatie weergeven

FPR4120-TAC-A#connect fxos

fpr4120-TAC-A (fxos)# debug Aa-verzoeken

% Toestemming geweigerd voor de rol

2. Bladeren naar het FXOS-chassis IP-adres en inloggen met behulp van een van de gemaakte gebruikers in ISE.

Gebruiker beheren.

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							

Alleen-lezen gebruikersrol.

Overview Interfaces Logical	I Devices Security Engine Platform Sett	ings				System T	xols He	1 0
NTP	LDAP RADUS TACACS							
SSH SNMP	Properties							
HTTPS	Timeout:* 5 Secs							
> AAA Syslog	TACACS Providen							
DNS				0 Add				
FIPS and Common Criteria	Hostname	Order	Port					
90000 L.N.	10.88.244.50	1	49	9,8				

Opmerking: Merk op dat de knop ADD gegraveerd is.

ISE 2.0 Verificatie

1. Navigeer naar **bewerkingen > TACACS-loggen.** Je zou succesvolle en mislukte pogingen moeten kunnen zien.

albah cisco	Identity Services Engine	Home + C	ontext Visibility	- Operations	Policy Admin	istration + Work Centers				۹. 😐	• •
►R	ADIUS Threat-Centric NAC Live L	ogs TACAC	S + Troubles	hoot + Adaptive Net	work Control Repo	orts		Click here to do wireles	s setup and visibility setup	to not show the	s again
Live Logs											
								lefresh Nover • Show Late	est 20 records - Within	Last 3 hours	s •
~	Defects										-
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			

Problemen oplossen

Om AAA-verificatie en -autorisatie te reinigen voert u de volgende opdrachten in de FXOS-cloud uit.

FPR4120-TAC-A#connect fxos

fpr4120-TAC-A (fxos)# debug Aa-verzoeken

fpr4120-TAC-A (fxos)# debug van gebeurtenis

fpr4120-TAC-A (FXS)# bug van fouten in de verwerking

fpr4120-TAC-A (FXS)# termijnmon

Na een succesvolle authenticatie poging, zult u de volgende output zien.

2018 jan 17 15:46:40.305247 aaa: aaa_req_process voor authenticatie. zitting nr. 0

2018 jan 17 15:46:40.305262 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: aanmelding appln_subtype: standaard

2018 jan 17 15:46:40.305271 aaa: probeer_next_aaa_methode

2018 jan 17 15:46:40.305285 aaa: in totaal zijn de methoden 1 , de huidige te beproeven index is 0

2018 jan 17 15:46:40.305294 aaa: handle_req_gebruikt_methode

2018 jan 17 15:46:40.305301 aaa: AAA_METHOD_SERVER_GROUP

2018 jan 17 15:46:40.305308 aaa: aaa_sg_handler groep = tacacs

2018 jan 17 15:46:40.305315 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 17 15:46:40.305324 aaa: Aanvraag naar TACACS-service verzenden

2018 jan 17 15:46:40.305384 aaa: Configureer methodegroep succesvol

2018 jan 17 15:46:40,554631 aaa: aaa_proces_fd_set

2018 jan 17 15:46:40,555229 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 17 15:46:40,555817 aaa: mts_message_response_handler: reactie op mts

2018 jan 17 15:46:40,556387 aaa: prot_daemon_reponse_handler

2018 jan 17 15:46:40,557042 aaa: zitting : 0x8df68c verwijderd uit de sessietabel 0

2018 jan 17 15:46:40,557059 aaa: is_a_rep_status_successtatus = 1

2018 jan 17 15:46:40,557066 aaa: is_a_rep_status_successie is TRUE

2018 jan 17 15:46:40,557075 aaa: aaa_send_client_response voor authenticatie. sessie->flags=21.aaa_resp->flags=0.

2018 jan 17 15:46:40,557083 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 17 15:46:40,557106 aaa: mts_send_response Succesvol

2018 jan 17 15:46:40,557364 aaa: aaa_req_process voor autorisatie. zitting nr. 0

2018 jan 17 15:46:40,557378 aaa: aaa_req_process aangeroepen met context vanaf appln: aanmelding appln_subtype: default authen_type:2, authen_ethode: 0

2018 jan 17 15:46:40,557386 aaa: aaa_send_req_use_context

2018 jan 17 15:46:40,557394 aaa: aaa_sg_handler groep = (nul)

2018 jan 17 15:46:40,557401 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 17 15:46:40,557408 aaa: op context gebaseerde of gerichte AAA-req (behalve: geen relaisverzoek). Kan geen kopie van een verzoek aannemen

2018 jan 17 15:46:40,557415 aaa: Aanvraag naar TACACS-service verzenden

2018 jan 17 15:46:40.801732 aaa: aaa_send_client_response voor autorisatie. sessie->flags=9. aaa_rep->flags=0.

2018 jan 17 15:46:40.801740 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 17 15:46:40.801761 aaa: mts_send_response Succesvol

2018 jan 17 15:46:40,848932 aaa: OUDE OPCODE: accounting_interim_update

2018 jan 17 15:46:40,848943 aaa: aaa_aangemaakt_local_acct_req: gebruiker=, sessie_id=, log=added gebruiker:fxosadmin aan de rol:admin

2018 jan 17 15:46:40,848963 aaa: aaa_req_process voor accounting. zitting nr. 0

2018 jan 17 15:46:40,848972 aaa: MTS aanvraag referentie is NULL. LOKALE AANVRAAG

2018 jan 17 15:46:40,848982 aaa: AAA_REQ_RESPONSE_NOT_NOED instellen

2018 jan 17 15:46:40,848992 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: standaard appln_subtype: standaard

2018 jan 17 15:46:40,849002 aaa: probeer_next_aaa_methode

2018 jan 17 15:46:40,849022 aaa: geen standaardinstellingen voor methoden

2018 jan 17 15:46:40,849032 aaa: geen configuratie beschikbaar voor dit verzoek

2018 jan 17 15:46:40,849043 aaa: probeert_fallback_ethode

2018 jan 17 15:46:40,849053 aaa: handle_req_gebruikt_methode

2018 jan 17 15:46:40,849063 aaa: local_methode_handler

2018 jan 17 15:46:40,849073 aaa: aaa_local_accounting_msg

2018 jan 17 15:46:40,849085 aaa: update::toegevoegde gebruiker:fxosadmin aan de rol:admin

Na een mislukte verificatiepoging ziet u de volgende uitvoer.

2018 jan 17 15:46:17,836271 aaa: aaa_req_process voor authenticatie. zitting nr. 0

2018 jan 17 15:46:17,836616 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: aanmelding appln_subtype: standaard

2018 jan 17 15:46:17,837063 aaa: probeer_next_aaa_methode

2018 jan 17 15:46:17,837416 aaa: in totaal zijn de methoden 1 , de huidige te beproeven index is 0

2018 jan 17 15:46:17,83776 aaa: handle_req_gebruikt_methode

2018 jan 17 15:46:17.838103 aaa: AAA_METHOD_SERVER_GROUP

2018 jan 17 15:46:17,83847 aaa: aaa_sg_handler groep = tacacs

2018 jan 17 15:46:17.83826 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 17 15:46:17.839-167 aaa: Aanvraag naar TACACS-service verzenden

2018 jan 17 15:46:17.840-225 aaa: Configureer methodegroep succesvol

2018 jan 17 15:46:18:043710 aaa: is_a_rep_status_successtatus = 2

2018 jan 17 15:46:18.044048 aaa: is_a_rep_status_successie is TRUE

2018 jan 17 15:46:18.044395 aaa: aaa_send_client_response voor authenticatie. sessie->flags=21.aaa_resp->flags=0.

2018 jan 17 15:46:18.044733 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 17 15:46:18:045096 aaa: mts_send_response Succesvol

2018 jan 17 15:46:18.04567 aaa: aaa_schoonmaak_sessie

2018 jan 17 15:46:18.045689 aaa: mts_drop-applicatie voor msg

2018 jan 17 15:46:18:045699 aaa: Aa_req moet worden vrijgelaten.

2018 jan 17 15:46:18.045715 aaa: aaa_proces_fd_set

2018 jan 17 15:46:18:045722 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 17 15:46:18.045732 aaa: aaa_wellicht_info_fig: GET_REQ voor ABBYY inlogfoutmelding

2018 jan 17 15:46:18.045738 aaa: terugkrijgen de retourwaarde van de configuratie:onbekend beveiligingsitem

Gerelateerde informatie

De opdracht van de Ethanalyzer op FX-OS CLI zal om een wachtwoord vragen wanneer TACACS/RADIUS-verificatie is ingeschakeld. Dit gedrag wordt veroorzaakt door een bug.

Eenmalig id: CSCvg875-18