Firepower eXtensible Operating System (FXOS) 2.2: Autenticazione/autorizzazione dello chassis per la gestione remota con ISE tramite TACACS+

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete Configurazioni Configurazione dello chassis FXOS Configurazione del server ISE Verifica Verifica chassis FXOS Verifica ISE 2.0 Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento descrive come configurare l'autenticazione e l'autorizzazione TACACS+ per lo chassis Firepower eXtensible Operating System (FXOS) tramite Identity Services Engine (ISE).

Lo chassis FXOS include i seguenti ruoli utente:

- Amministratore: accesso completo in lettura e scrittura all'intero sistema. All'account amministratore predefinito viene assegnato questo ruolo per impostazione predefinita e non può essere modificato.
- Sola lettura Accesso in sola lettura alla configurazione del sistema senza privilegi per la modifica dello stato del sistema.
- Operazioni: accesso in lettura e scrittura alla configurazione NTP, alla configurazione di Smart Call Home per Smart Licensing e ai registri di sistema, inclusi i server syslog e i relativi errori. Accesso in lettura al resto del sistema.
- AAA: accesso in lettura e scrittura a utenti, ruoli e configurazione AAA. Accesso in lettura al resto del sistema.

Dalla CLI, questa condizione può essere vista come segue:

fpr4120-TAC-A /security* # show role

Ruolo:

Priv nome ruolo

aaa aaa

admin admin

operazioni

sola lettura

Contributo di Tony Remirez, Jose Soto, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Firepower eXtensible Operating System (FXOS)
- Conoscenza della configurazione ISE
- Per ISE, è richiesta la licenza TACACS+ Device Administration

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower 4120 Security Appliance versione 2.2
- Virtual Cisco Identity Services Engine 2.2.0.470

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

L'obiettivo della configurazione è:

- Autenticazione degli utenti che accedono alla GUI e SSH basata sul Web di FXOS tramite ISE
- Permette agli utenti di accedere alla GUI basata sul Web di FXOS e al protocollo SSH in base al loro ruolo con ISE.
- Verificare il corretto funzionamento dell'autenticazione e dell'autorizzazione su FXOS tramite ISE



Network admin

Configurazioni

Configurazione dello chassis FXOS

Creazione di un provider TACACS+

Passaggio 1. Passare a Impostazioni piattaforma > AAA.

Passaggio 2. Fare clic sulla scheda TACACS.

C	verview Interface	s Log	gical Device	s Secu	ity Engine	Platform Settings	s			
	NTP		LDAP	RADIUS	TACACS					
	SSH									
	SNMP		Propert	es						
	HTTPS		Timeou	.* 5	Secs					
	AAA									
	Syslog		TACACS	Providers						
	DNS								0	Add
	FIPS and Common Crite	eria	Hostr	ame		0	Order	Port		
	Access List		noaci							

Passaggio 3. Per ogni provider TACACS+ che si desidera aggiungere (fino a 16 provider).

3.1. Nell'area dei provider TACACS, fare clic su Add.

3.2. Una volta aperta la finestra di dialogo Aggiungi provider TACACS, immettere i valori richiesti.

3.3. Fare clic su **OK** per chiudere la finestra di dialogo Aggiungi provider TACACS.

Í	Add TACACS Provider			?×	
	Hostname/FQDN(or IP Address):*	10.88.24	4.50]	
l	Order:*	lowest-av	vailable]	
	Key:	•••••		Set:No	
l	Confirm Key:	•••••]	
l	Port:*	49			
l	Timeout:*	5	Secs		
			0K Car	sel	
l				icei	

Passaggio 4. Fare clic su Salva.

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

Passaggio 5. Passare a Sistema > Gestione utente > Impostazioni.

Passaggio 6. In Autenticazione predefinita scegliere TACACS.

Overview Interfaces Log	ical Devices Security Engine Platform Settings		5	iystem Tool	s Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	TACACS v Local is failback authentication method				
Console Authentication	Local				
Remote User Settings Remote User Role Policy	C Assign Default Role 🔿 No-Login				

Creazione di un provider TACACS+ tramite CLI

Passaggio 1. Per abilitare l'autenticazione TACACS, eseguire i seguenti comandi.

fpr4120-TAC-A# ambito sicurezza

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

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

Passaggio 2. Per verificare la configurazione, utilizzare il comando show detail.

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

Autenticazione predefinita:

Area di autenticazione amministrativa: Tacacacs

Area operativa: Tacacacs

Periodo di aggiornamento sessione Web (sec): 600

Timeout sessione (in sec) per sessioni Web, ssh e telnet: 600

Timeout sessione assoluta (in secondi) per sessioni Web, ssh e telnet: 3600

Timeout sessione console seriale (sec): 600

Timeout sessione assoluta console seriale (sec): 3600

Gruppo server Autenticazione amministratore:

Gruppo server di autenticazione operativo:

Utilizzo del secondo fattore: No

Passaggio 3. Per configurare i parametri del server TACACS, eseguire i seguenti comandi.

fpr4120-TAC-A# ambito sicurezza

fpr4120-TAC-A /security # ambito tacacs

fpr4120-TAC-A /security/tacacs # invio al server 10.88.244.50

fpr4120-TAC-A /security/tacacs/server # set descr "server ACS"

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

Immettere la chiave: *****

Confermare la chiave: *****

Passaggio 4. Per verificare la configurazione, usare il comando show detail.

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

Server TACACS+:

Nome host, FQDN o indirizzo IP: 10.88.244.50

Descr.:

Ordine: 1

Port: 49

Chiave: ****

Timeout: 5

Configurazione del server ISE

Aggiunta di FXOS come risorsa di rete

Passaggio 1. Passare a Amministrazione > Risorse di rete > Dispositivi di rete.

Passaggio 2. Fare clic su ADD.

dentity Services Engine	Home	Operations Policy	✓Administration	enters				
System Identity Management	Network Resources	Portal Management pxGrid	Services + Feed Service + Thr	reat Centric NAC				
Network Devices Network Device Gro	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences NAC	C Managers External MDM	rvices			
0								
Network devices	Network Devices							
Default Device								
Device Security Settings	🥖 Edit 🕂 Add 🕞 Duplicate	😭 Import 🚯 Export	Generate PAC 🔀 Delete					
	Name 🔺 IP/Mas	k Profile Name	Location	Туре	Description			
					No data available			

Passaggio 3. Immettere i valori richiesti (Nome, Indirizzo IP, Tipo di dispositivo, Abilita TACACS+ e aggiungere la CHIAVE), quindi fare clic su **Submit (Invia).**

dentity Services Engine	Home	 Context Visi 	Context Visibility → Operations → Policy → Administration → Work Centers					
System Identity Management	- Networ	k Resources	Device Portal Manageme	nt pxGrid Servic	es Feed Servi	ce + Threat Centric I	NAC	
▼ Network Devices Network Device	ce Groups	Network Device P	rofiles External RADIU	S Servers RAD	US Server Sequen	ces NAC Managers	External MDM	Location Services
	3							
Network devices	Netwo	work Devices List >	FXOS					
Default Device	i i cci	for perices	* Name FX	05	7			
Device Security Settings			Description					
		* IP Address:	10.83.180.6	/ 32				
			* Device Profile	Cisco 👻 🕀				
			Model Name	*				
			Software Version	Ţ				
	· ·	* Network Device	Group					
	t	Device Type FX0	s 📀	Set To Default				
		IPSEC No	o	Set To Default				
		Location All L	ocations 📀	Set To Default				
		RADIUS Auth	entication Settings					
	V	- TACACS Auth	entication Settings					
			Si Enable Single Co	hared Secret 🔐	••••	Show		
				•	egacy Cisco Devic ACACS Draft Com	e pliance Single Connect	Support	
		SNMP Setting	S					
		 Advanced Tru 	stSec Settings					
	Saw	e Reset						

Creazione di gruppi di identità e utenti

Passo 1: passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente.

Passaggio 2. Fare clic su ADD.

uluulu Identity Services Engine Home	Context Visibility Poperations Policy Admir	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 🕂 Add 🗙 Delete ▼ 👔 Import 😭 Export ▼			
Endpoint Identity Groups	Name	Description		
User Identity Groups	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group		
	Employee	Default Employee User Group		
	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group		
	GuestType_Contractor (default)	Identity group mirroring the guest type		
	GuestType_Daily (default)	Identity group mirroring the guest type		
	GuestType_Weekly (default)	Identity group mirroring the guest type		
	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group		

Passaggio 3. Immettere il valore per Nome e fare clic su Sottometti.

dentit	ty Services Engine	Home >	Context Visibility	 Operations 	► Policy -A	dministration	Work Centers	
 System 	 Identity Management 	Network Res	sources	e Portal Management	pxGrid Service	Feed Servi	ice	
Identities	Groups External Ide	ntity Sources	Identity Source Sec	quences > Settings	\$			
Identity (- - - Enc - - - - - - - - - - - - -	Groups	(م	User Identity Gro Identity Gro Name Description Submit	oups > New User Ide up FXOS ADMIN	intity Group			

Passaggio 4. Ripetere il passaggio 3 per tutti i ruoli utente richiesti.

tilitation Identity Services Engine Home	Context Visibility Operations Policy Adr	ninistration 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	
	/ Edit Add Delete - 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	
	FXOS ADMIN	
	E Pros Oper	
	FXOS Read Only	
		Diffult cooling accounts (diffult) line cours

Passaggio 5. Passare a Amministrazione > Gestione delle identità > Identità > Utenti.

Passaggio 6. Fare clic su ADD.

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

Passaggio 7. Inserire i valori richiesti (Nome, Gruppo di utenti, Password).

dentity Services Engine	Home	Operations Policy	 Administration 	Work Centers
System Identity Management	Network Resources Device Po	ortal Management pxGrid S	ervices Feed Ser	rvice
✓Identities Groups External Iden	ity Sources Identity Source Sequen	ices		
G				
Users	Network Access Users List > New	Network Access User		
Latest Manual Network Scan Results	Network Access User			
	* Name fxosadmin			
	Status 🔽 Enabled 👻			
	Email			
	▼ Passwords			
	Password Type: Internal L	Users 👻		
	Password	1 1	Re-Enter Password	
	Login Password		•••••	Generate Password (j)
	Enable Password			Generate Password (1)
	 User Information 			
	First Name			
	Last Name			
	Account Options			
	Description]
	Description	on		13
	Change password on next log	jin 🗅		
	▼ Account Disable Policy			
	Disable account if date e	exceeds 2018-03-01	())))	y-mm-dd)
	- 11			
	▼ User Groups			
	FXOS ADMIN	⊘ — +		
	Submit Cancel			

Passaggio 8. Ripetere il passaggio 6 per tutti gli utenti richiesti.

-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 Sources Identity Source Sequences Settings										
0	0									
Users	Users Network Access 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			

Creazione del profilo di shell per ogni ruolo utente

Passaggio 1. Passare a Work Center > Device Administration > Policy Elements > Results > TACACS Profiles e fare clic su +ADD.

cisco Identity Services Engine	Home Context Visibility Operations Pol	cy Administration Work Centers
Network Access Guest Access		e Administration PassiveID
Overview Identities User Ident	ty Groups Ext Id Sources + Network Resources - Po	icy Elements Device Admin Policy Sets Reports Settings
Conditions	TACACS Profiles 0 Selected	Rows/Page 4 - K 4 1 3 / 1 - K (Go) 4 Total Rows
Network Conditions	C Refresh	© Edit ŢFilter ▼ ♦ ▼
✓ Results	□ Name	Type Description
Allowed Protocols	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

Passaggio 2. Inserire i valori richiesti per il profilo TACACS

2.1. Inserire il nome.

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

2.2. Nella SCHEDA Visualizzazione RAW configurare la seguente coppia CISCO-AV.

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. Fare clic su Invia.

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile					
	Name	FXOS_Admin_Profile			
De	escription				
Task Attribute View	Raw	View			
Common Tasks					
Common Task Type Shell	•				
Default Privileg	e		0	(Select 0 to 15)	
Maximum Privil	ege		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	Edit				٥
🗆 Туре	Name		Value		
MANDATORY	cisco-a	v-pair	shell:roles="adm	nin"	医前

Passaggio 3. Ripetere il passaggio 2 per gli altri ruoli utente utilizzando le seguenti coppie Cisco-AV.

Cancel Save

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

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

```
cisco-av-pair=shell:roles="sola lettura"
```

```
Custom Attributes
```

+ 4	dd 🍵 Trash ▾ 🕑 E	dit		¢-
	Туре	Name	Value	
	MANDATORY	cisco-av-pair	shell:roles="aaa"	(j) (j)
			Cance	Save

Custom Attributes

+ Add	💼 Trash 🕶 🕑 E	dit			¢-
T	уре	Name	Va	lue	
	IANDATORY	cisco-av-pair	sh	ell:roles="operations"	C m
Custom	Attributes				Correct Correc
+ Add	💼 Trash 👻 🕑 E	dit			¢-
П	/pe	Name	Val	lue	
□ M	ANDATORY	cisco-av-pair	she	ell:roles="read-only"	C 🛍
0 Selec	ACS Profiles acted defresh + Add	Duplicate 💼 Trash	R C	ows/Page 8 ▼ 1 © / 1 ► ► Edit	Go 8 Total Rows
	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		

Creazione del criterio di autorizzazione TACACS

Passaggio 1. Passare a Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi.

cited Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	(1) Q (1) Q (1)
Network Access Guest Access TrustSec	BYOD Profiler Posture Postere Administration PassiveID	Click here to do wireless setup and visibility setup Do not show this again.
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 Placy Sport on Administration > System > Sections - Restore > Proteing Export Page Status - Name Decortorin	
*** 'C* * * X @	Default Tacacs, Default	
Summary of Policies A list of all your policies	Regular 🔿 Proxy Sequence 🔿	
Global Exceptions	Proxy Server Sequence	
Rules across entire deployment	Proxy server sequence:	
Default		
Tacacu_Default	* Authentication Policy	
Save Order Reset Order	Default Rule (if no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores	Edt =
	✓ Authorization Policy	
	Exceptions (0)	
	Standard	
	Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profiles	
	Tacecs_Default If no matches, then Solect Profile(3) Deny Al Shell Profile	Edt •

Passaggio 2. Verificare che il criterio di autenticazione punti al database Internal Users o

all'archivio identità richiesto.

•	Authenti	cation Policy		
		Default Rule (If no match)	: Allow Protocols : Default Device Admin and use : All_User_ID_Stores	

Passaggio 3. Fare clic sulla freccia alla fine del criterio di autorizzazione predefinito e fare clic su Inserisci regola.

 Authorization Policy 		
Exceptions (0)		
Standard		
Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Pro	les
Z Tacacs_Default	If no matches, then Select Profile(s) Deny All Shell Profile	Entit y

Passaggio 4. Inserire i valori per la regola con i parametri obbligatori:

- 4.1. Nome della regola: Regola di amministrazione FXOS.
- 4.2. Condizioni.

Se: Il gruppo di identità utente è FXOS ADMIN

FXOS Admin Rule If Any and Condition(s) & then Comman & and Select a Shell	
	rofile
Tacacs_Default if no ma	
User Identity Groups	
FXOS AAA	
GuestType_Weekly (default)	
OWN_ACCOUNTS (default)	
GROUP_ACCOUNTS (default)	
EXOS ADMIN	
FXOS OPER	
Employee	
GuestType_Daily (default)	
GuestType_Contractor (default)	
Excel Paset	
ave Reset	

E Dispositivo: Tipo di dispositivo è uguale a Tutti i tipi di dispositivo #FXOS

Conditions (identity groups and other conditions) C	Command Sets Shell Profiles
if FX 4 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# O Image: Control of the second s
	All Device Types All Device Types#FXOS
	ad >
	DEVICE >>
	ThternalUser >>
	Network Access >>
	Network Condition >
	TACACS >

Profilo shell: Profilo_amministrazione_FXOS

Shell Profile
(م
🖉 🕶 📃 🕶 🚳 🐳
Gerault Shell Profile
Carl Deny All Shell Profile
General Street FXOS_AAA_Shell
KOS_Admin_Profile
Generations_Shell
Generation FXOS_ReadOnly_Shell
Second WLC ALL
WLC MONITOR

Passaggio 5. Fare clic su Fine.

Except	ptions (0)		
Standa	rd		
St	atus Rule Name	Conditions (identify groups and other conditions) Command Sets Shell Profiles	
i 🖉 🗹	 FXOS Admin Rule 	FX 💠 and DEVICE-Devi 💠 and Select an item 💠 and FXOS Admin_Profile 💽	Done
<u>~</u>	Tacacs_Default	If no matches, then Select Profile(s) Dery Al Shell Profile	Edit 🔻
Save	Reset		

Passaggio 6. Ripetere i passaggi 3 e 4 per i ruoli utente rimanenti e al termine fare clic su SAVE.

Exceptions (0)	
Standard	
Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles
FXOS Admin Rule	if FXOS ADMIN AND DEVICE:Device Type then Select an item FXOS_Admin_Profile EQUALS All Device Types#FXOS
🖉 🗹 🛛 FXOS AAA Rule	If FXOS AAA AND DEVICE:Device Type then Select Profile(s) FXOS_AAA_Shell EQUALS All Device Types#FXOS
FXOS Operations Rule	if FXOS OPER AND DEVICE:Device Type then Select Profile(s) FXOS_Operations_Shell EQUALS All Device Types#FXOS
FXOS Read Only Rule	if FXOS Read Only AND DEVICE:Device Type then Select Profile(s) FXOS_ReadOnly_Shell EQUALS All Device Types#FXOS
Tacacs_Default	If no matches, then Select Profile(s) Deny All Shell Profile



Verifica

Èora possibile eseguire il test di ogni utente e verificare il ruolo utente assegnato.

Verifica chassis FXOS

1. Telnet o SSH sullo chassis FXOS ed effettuare il login utilizzando uno degli utenti creati sull'ISE.

Username: fxosadmin

Password:

fpr4120-TAC-A# scope security

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

Utente remoto fxosaaa:

Descrizione:

Ruoli utente:

Nome: aaa

Nome: read-only

Utente remoto fxosadmin:

Descrizione:

Ruoli utente:

Nome: admin

Nome: read-only

Fxosoper utente remoto:

Descrizione:

Ruoli utente:

Nome: operazioni

Nome: read-only

Fxosro utente remoto:

Descrizione:

Ruoli utente:

Nome: read-only

A seconda del nome utente immesso, nella cli dello chassis FXOS verranno visualizzati solo i comandi autorizzati per il ruolo utente assegnato.

Ruolo utente amministratore.

fpr4120-TAC-A /security #?

conferma conferma conferma

clear-user-session Cancella sessioni utente

creazione Creazione di oggetti gestiti

delete Elimina oggetti gestiti

disabilita Disabilita i servizi

abilita Abilita i servizi

enter Immette un oggetto gestito

scope Modifica la modalità corrente

impostare i valori delle proprietà

show Mostra informazioni di sistema

termina sessioni Active Cisco

fpr4120-TAC-A#connect fxos

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

fpr4120-TAC-A (fxos)#

Ruolo Utente Di Sola Lettura.

fpr4120-TAC-A /security #?

scope Modifica la modalità corrente

impostare i valori delle proprietà

show Mostra informazioni di sistema

fpr4120-TAC-A#connect fxos

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

% Autorizzazione negata per il ruolo

2. Individuare l'indirizzo IP dello chassis FXOS e accedere usando uno degli utenti creati sull'ISE.

Ruolo utente amministratore.

Overview Interfaces Logical	Devices Security Engine Platform Settin	igs								
NTP	LDAP RADIUS TACACS									
SSH	Properties									
HTTPS	Timeout:* 5 Secs									
AAA	TACACS Providers	CACS Providers								
DNS		Add TACACS Provider			Add					
FIPS and Common Criteria	Hostname	Order	Hostname/FQDN(or IP Address):*							
Access List	10.88.244.50	1	Order:*	lowest-available		a 🖉 🗊				
			Key:		Set:No					
			Confirm Key:]					
			Port:*	49						
			Timeout:*	5 Secs						
				ок с	ancel					
	Save Cancel									

Ruolo utente di sola lettura.

Overview Interfaces Logic	al Devices Security Engine Platform	n Settings				System T	ools H	ielp f	10570
NTP	LDAP RADIUS TACACS								
SNMP	Properties								
HTTPS	Treevit* 5 Sea								
Sysiog	TACACS Providers								
DNS FIRS and Common Oritoria				O Add					
Access List	Hostname	Order	Port						
	10.88.244.50	1	49	9,8					
	1								

Nota: Il pulsante ADD è disattivato.

Verifica ISE 2.0

1. Passare a **Operazioni > TACACS Livelog.** Dovrebbe essere possibile visualizzare i tentativi riusciti e quelli non riusciti.

ubalu Identi	y Services Engine	Home + Co	ntext Visibility	- Operations	Policy + Admin	istration			3	۹ و	o o
RADIUS	Threat-Centric NAC Live L	ogs - TACACS	Troublesh	ioot + Adaptive Netw	ork Control Repo	rts		Click here to do wireles	s setup and visibility setup [to not show this	again. ×
Live Logs											
Refresh Never Show Latest 20 records • Within Last 3 hours •											
C Refresh	A Export To -									¥ Filter -	۰.
Logge	d 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		ò	fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admin	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_ReadO	Jnly_S
Jan 17	2018 08:57:00.825 PM	1	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			

Risoluzione dei problemi

Per eseguire il debug dell'autenticazione e dell'autorizzazione AAA, eseguire i seguenti comandi nella cli di FXOS.

fpr4120-TAC-A#connect fxos

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

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

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

fpr4120-TAC-A (fxos)# termine mon

Dopo un tentativo di autenticazione riuscito, verrà visualizzato l'output seguente.

2018 Gen 17 15:46:40,305247 aaa: aaa_req_process per l'autenticazione. sessione n. 0

2018 Gen 17 15:46:40,305262 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn: login sottotipo_applicazione: predefinito

2018 Gen 17 15:46:40,305271 aaa: try_next_aaa_method

2018 Gen 17 15:46:40,305285 aaa: il numero totale di metodi configurati è 1, l'indice corrente da provare è 0

2018 gen 17 15:46:40,305294 aaa: handle_req_using_method

2018 Gen 17 15:46:40,305301 aaa: AAA_METHOD_SERVER_GROUP

2018 Gen 17 15:46:40,305308 aaa: gruppo aaa_sg_method_handler = tacacs

2018 Gen 17 15:46:40,305315 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 Gen 17 15:46:40,305324 aaa: Invio della richiesta al servizio TACACS

2018 Gen 17 15:46:40,305384 aaa: Gruppo di metodi configurato completato

2018 Gen 17 15:46:40,554631 aaa: aaa_process_fd_set

2018 Gen 17 15:46:40,555229 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 Gen 17 15:46:40,55817 aaa: mts_message_response_handler: risposta mts

2018 Gen 17 15:46:40,556387 aaa: gestore_risposta_daemon

2018 gen 17 15:46:40,557042 aaa: sessione: 0x8dfd68c rimosso dalla tabella delle sessioni 0

2018 Gen 17 15:46:40,557059 aaa: is_aaa_resp_status_success status = 1

2018 Gen 17 15:46:40,557066 aaa: is_aaa_resp_status_success è TRUE

2018 gen 17 15:46:40,557075 aaa: aaa_send_client_response per l'autenticazione. session->flags=21. aaa_resp->flags=0.

2018 gen 17 15:46:40,557083 aaa: AAA_REQ_FLAG_NORMAL

2018 Gen 17 15:46:40,557106 aaa: mts_send_response riuscito

2018 Gen 17 15:46:40,557364 aaa: aaa_req_process per l'autorizzazione. sessione n. 0

2018 Gen 17 15:46:40,557378 aaa: aaa_req_process richiamato con contesto da appln: login sottotipo_applicazione: auto_type:2, auto_method: 0

2018 Gen 17 15:46:40,557386 aaa: aaa_send_req_using_context

2018 gen 17 15:46:40,557394 aaa: gruppo aaa_sg_method_handler = (null)

2018 Gen 17 15:46:40,557401 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 Gen 17 15:46:40,557408 aaa: richiesta AAA basata sul contesto o diretta(eccezione: non è una richiesta di inoltro). Non riceve copia della richiesta aaa

2018 Gen 17 15:46:40,557415 aaa: Invio della richiesta al servizio TACACS

2018 gen 17 15:46:40,801732 aaa: aaa_send_client_response per l'autorizzazione. session->flags=9. aaa_resp->flags=0.

2018 Gen 17 15:46:40,801740 aaa: AAA_REQ_FLAG_NORMAL

2018 Gen 17 15:46:40,801761 aaa: mts_send_response riuscito

2018 gen 17 15:46:40,848932 aaa: CODICE OPERATIVO PRECEDENTE: accounting_interim_update

2018 gen 17 15:46:40,848943 aaa: aaa_create_local_acct_req: user=, session_id=, log=aggiunto user:fxosadmin al ruolo:admin

2018 gen 17 15:46:40,848963 aaa: aaa_req_process per l'accounting. sessione n. 0

2018 gen 17 15:46:40,848972 aaa: Il riferimento alla richiesta MTS è NULL. richiesta LOCALE

2018 gen 17 15:46:40,848982 aaa: Impostazione di AAA_REQ_RESPONSE_NOT_NEEDED

2018 gen 17 15:46:40,848992 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn: default appln_subtype: predefinito

2018 gen 17 15:46:40,849002 aaa: try_next_aaa_method

2018 gen 17 15:46:40,849022 aaa: nessun metodo configurato per l'impostazione predefinita

2018 gen 17 15:46:40,849032 aaa: nessuna configurazione disponibile per questa richiesta

2018 gen 17 15:46:40,849043 aaa: try_fallback_method

2018 gen 17 15:46:40,849053 aaa: handle_req_using_method

2018 gen 17 15:46:40,849063 aaa: gestore_metodo_locale

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

2018 gen 17 15:46:40,849085 aaa: update::added user:fxosadmin to the role:admin

Dopo un tentativo di autenticazione non riuscito, verrà visualizzato l'output seguente.

2018 gen 17 15:46:17,836271 aaa: aaa_req_process per l'autenticazione. sessione n. 0

2018 gen 17 15:46:17,836616 aaa: aaa_req_process: Richiesta generale AAA da parte dell'appn: login sottotipo_applicazione: predefinito

2018 gen 17 15:46:17,837063 aaa: try_next_aaa_method

2018 gen 17 15:46:17,837416 aaa: il numero totale di metodi configurati è 1, l'indice corrente da provare è 0

2018 gen 17 15:46:17,837766 aaa: handle_req_using_method

2018 gen 17 15:46:17,838103 aaa: AAA_METHOD_SERVER_GROUP

2018 gen 17 15:46:17,838477 aaa: gruppo aaa_sg_method_handler = tacacs

2018 gen 17 15:46:17,838826 aaa: Utilizzo di sg_protocol passato a questa funzione

2018 gen 17 15:46:17,839167 aaa: Invio della richiesta al servizio TACACS

2018 gen 17 15:46:17,840225 aaa: Gruppo di metodi configurato completato

2018 Gen 17 15:46:18,043710 aaa: is_aaa_resp_status_success status = 2

2018 Gen 17 15:46:18,044048 aaa: is_aaa_resp_status_success è TRUE

2018 Gen 17 15:46:18,044395 aaa: aaa_send_client_response per l'autenticazione. session->flags=21. aaa_resp->flags=0.

2018 Gen 17 15:46:18,044733 aaa: AAA_REQ_FLAG_NORMAL

2018 Gen 17 15:46:18,045096 aaa: mts_send_response riuscito

2018 Gen 17 15:46:18,045677 aaa: sessione_pulizia_aaa

2018 Gen 17 15:46:18,045689 aaa: mts_drop del messaggio di richiesta

2018 Gen 17 15:46:18,045699 aaa: aaa_req deve essere liberato.

2018 Gen 17 15:46:18,045715 aaa: aaa_process_fd_set

2018 Gen 17 15:46:18,045722 aaa: aaa_process_fd_set: mtscallback su aaa_q

2018 Gen 17 15:46:18,045732 aaa: aaa_enable_info_config: GET_REQ per il messaggio di errore di accesso aaa

2018 Gen 17 15:46:18,045738 aaa: è stato restituito il valore restituito dell'operazione di configurazione:elemento di sicurezza sconosciuto

Informazioni correlate

Il comando Ethanalyzer sulla cli di FX-OS richiederà una password quando l'autenticazione TACACS/RADIUS è abilitata. Questo comportamento è causato da un bug.

ID bug: CSCvg87518