Sistema operacional Firepower eXtensible (FXOS) 2.2: Autenticação/autorização do chassi para gerenciamento remoto com ISE usando TACACS+

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Diagrama de Rede Configurações Configurações Configuração do servidor ISE Verificar Verificação de chassi FXOS Verificação do ISE 2.0 Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como configurar a autenticação e autorização TACACS+ para o chassi do Firepower eXtensible Operating System (FXOS) através do Identity Services Engine (ISE).

O chassi FXOS inclui as seguintes funções de usuário:

- Administrador Acesso completo de leitura e gravação a todo o sistema. A conta admin padrão recebe essa função por padrão e não pode ser alterada.
- Somente leitura Acesso somente leitura à configuração do sistema sem privilégios para modificar o estado do sistema.
- Operações Acesso de leitura e gravação à configuração do NTP, configuração do Smart Call Home para Smart Licensing e registros do sistema, incluindo servidores de syslog e falhas. Leia o acesso ao restante do sistema.
- AAA acesso de leitura e gravação a usuários, funções e configuração de AAA. Leia o acesso ao restante do sistema.

Através da CLI, isso pode ser visto da seguinte maneira:

fpr4120-TAC-A /security* # show role

Função:

Nome da função Priv

aaa aaa

admin admin

operações operacionais

somente leitura

Contribuído por Tony Remirez, José Soto, engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firepower eXtensible Operating System (FXOS)
- Conhecimento da configuração do ISE
- A licença TACACS+ Device Administration é necessária no ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Firepower 4120 Security Appliance versão 2.2
- Cisco Identity Services Engine 2.2.0.470 virtual

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

Configurar

O objetivo da configuração é:

- Autentique os usuários que fazem login na GUI baseada na Web e no SSH do FXOS por meio do ISE
- Autorize os usuários a fazer login na GUI baseada na Web e no SSH do FXOS de acordo com sua respectiva função de usuário por meio do ISE.
- Verificar a operação adequada de autenticação e autorização no FXOS por meio do ISE

Diagrama de Rede



Configurações

Configurando o chassi FXOS

Criando um provedor TACACS+

Etapa 1. Navegue até **Configurações da plataforma > AAA**.

Etapa 2. Clique na guia 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	Hestname	Order	Deat	
Access List	Hostname	order	Port	

Etapa 3. Para cada provedor TACACS+ que você deseja adicionar (até 16 provedores).

3.1. Na área TACACS Providers, clique em Add.

3.2. Quando a caixa de diálogo Add TACACS Provider for aberta, insira os valores necessários.

3.3. Clique em **OK** para fechar a caixa de diálogo Adicionar Provedor TACACS.

Í	Add TACACS Provider		?×	
	Hostname/FQDN(or IP Address):*	10.88.244.50		6
l	Order:*	lowest-available		
I	Key:	•••••	Set:No	
l	Confirm Key:	•••••		
l	Port:*	49		
l	Timeout:*	5 Secs		
l		OK Car	ncel	

Etapa 4. Click Save.

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

Etapa 5. Navegue até **System > User Management > Settings**.

Etapa 6. Em Autenticação padrão, escolha TACACS.

Overview In	nterfaces Logical	Devices Security Engine Platform Settings			iystem Too	is Help fxosadmin
			Configuration	Licensing	Updates	User Management
Local Users	ettings					
Default Authent	tication	TACACS v *Local is falback authentication method				
Console Auther	ntication	Local V				
Remote User S	Settings tole Policy	Assign Default Role 🔿 No-Login				

Criando um provedor TACACS+ usando CLI

Etapa 1. Para habilitar a autenticação TACACS, execute os seguintes comandos.

segurança de escopo fpr4120-TAC-A#

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

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

Etapa 2. Use o comando show detail para verificar a configuração.

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

Autenticação padrão:

Domínio administrativo: TACACS

Domínio operacional: TACACS

Período de atualização da sessão da Web (em segundos): 600

Tempo limite da sessão (em segundos) para sessões web, ssh, telnet: 600

Tempo limite da sessão absoluta (em segundos) para sessões web, ssh, telnet: 3600

Tempo limite da sessão do console serial (em segundos): 600

Tempo limite da sessão absoluta do console serial (em segundos): 3600

Grupo de servidores de Autenticação do Administrador:

Grupo de servidores de Autenticação Operacional:

Uso do segundo fator: No

Etapa 3. Para configurar os parâmetros do servidor TACACS, execute os seguintes comandos.

segurança de escopo fpr4120-TAC-A#

fpr4120-TAC-A /segurança # táticas de escopo

fpr4120-TAC-A /security/tacacs # entre no servidor 10.88.244.50

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

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

Digite a chave: ******

Confirme a chave: ******

Etapa 4. Use o comando show detail para verificar a configuração.

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

Servidor TACACS+:

Nome do host, FQDN ou endereço IP: 10.88.244.50

Descr:

Pedido: 1

Porta: 49

Chave: ****

tempo limite: 5

Configuração do servidor ISE

Adicionando o FXOS como um recurso de rede

Etapa 1. Navegue até Administration > Network Resources > Network Devices.

Etapa 2. Clique em Add.



Etapa 3. Insira os valores necessários (Nome, Endereço IP, Tipo de dispositivo e Habilitar TACACS+ e adicione a CHAVE), clique em **Enviar.**

dentity Services Engine	Home	 Context \ 	Visibility	Policy	 Administration 	 Work Centers 		
System Identity Management	- Network	k Resources	Device Portal Managem	ent pxGrid Se	rvices + Feed Serv	vice	IAC	
Network Devices Network Device	Groups	Network Device	e Profiles External RADI	US Servers R	ADIUS Server Sequer	nces NAC Managers	External MDM	Location Services
(3							
Network devices	Netv	vork Devices List	I > FXOS					
Default Device			* Name F	YOS				
Device Security Settings			Description					
		* IP Address:	10.83.180.6	/ 32				
			* Device Profile	Cisco 👻 🕀				
			Model Name	Ţ]			
			Software Version	Ţ]			
	•	Network Devi	ce Group					
	C	Device Type	FXOS 📀	Set To Default	1			
		IPSEC	No 📀	Set To Default	Ì			
		Location	All Locations	Set To Default	Ì			
					-			
		RADIUS A	uthentication Settings					
	✓	- TACACS A	uthentication Settings					
			Enable Single (Shared Secret Connect Mode	Legacy Cisco Devi TACACS Draft Cor	Ce npliance Single Connect S	Support	
		SNMP Sett	tings					
		Advanced	TrustSec Settings					
	Save	Reset						

Criando grupos de identidade e usuários

Etapa 1. Navegue até Administration > Identity Management > Groups > User Identity Groups.

Etapa 2. Clique em Add.

titudie Identity 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	
[م		
⟨= + 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
	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

Etapa 3. Insira o valor para Nome e clique em Enviar.

diale Identity	/ Services Engine	Home >	Context Visibility	 Operations 	▶ Policy	- Administration	► Work Centers
System	 Identity Management 	Network Res	sources + Device	e Portal Managemer	t pxGrid S	ervices + Feed	Service
Identities	Groups External Id	entity Sources	Identity Source Seq	uences	S		
Identity G v V End S Uso	iroups . . point Identity Groups r Identity Groups	م ڇ-	User Identity Gro Identity Gro Name [Description [Submit C	Dups > New User Id up FXOS ADMIN ancel	entity Group]	

Etapa 4. Repita a etapa 3 para todas as funções de usuário necessárias.

dentity Services Engine Home	Context Visibility Operations 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	
<	/ 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	
	EXOS ADMIN	
	E A FXOS OPER	
	FXOS Read Only	
		D-5-14 CROUP ACCOUNTS (J-5-14) U-1 Court

Etapa 5. Navegue até Administration > Identity Management > Identity > Users.

Etapa 6. Clique em Add.

-that- cisce Identity Services Engine	Home ► Context Visibility ► Op	erations Policy Administration	► Work Centers		
System Identity Management	Network Resources	Management pxGrid Services + Feed	Service		
◄ Identities Groups External Identity	Identities Groups External Identity Sources Identity Source Sequences Settings				
0					
Users	Network Access Users				
Latest Manual Network Scan Results	/ Edit Add 📴 Change Status	🕞 Import 😭 Export 🗙 Delete 🛱	Duplicate		
	Status Name	Description	irst Name Last Name Email Address	User Identity Groups Admin	
			,	No data available	

Passo 7. Insira os valores necessários (Nome, Grupo de usuários, Senha).

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

Etapa 8. Repita a etapa 6 para todos os usuários necessários.

Identity Services Engine	Home + Conte	xt Visibility	Policy Administrat	ion 🔹 Work Ce	nters			
System Identity Management	Network Resources	s Device Portal Managemen	nt pxGrid Services + Fe	ed Service + Thr	eat Centric NAC			
- Identities Groups External Identit	y Sources Identity	Source Sequences	15					
0								
Users	Network Acce	ss 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	

Criando o perfil de shell para cada função de usuário

Etapa 1. Navegue até Centros de trabalho > Administração do dispositivo > Elementos de política > Resultados > Perfis TACACS e clique em +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 0 Selected Rows/Page 4 1 0 / 1 D 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			

Etapa 2. Insira os valores necessários para o perfil TACACS

2.1. Digite o nome.

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

2.2. Na guia **RAW View**, configure o CISCO-AV-PAIR a seguir.

cisco-av-pair=shell:funções="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. Clique em Submit.

TACACS Profiles > FXOS_Admin_Profile

TACACS Profile					
	Name	FXOS_Admin_Profile			
Des	cription				
Task Attribute View	Raw	View			
Common Tasks					
Common Task Type Shell	-				
, · · · · ·	-				
Default Privilege			0	(Select 0 to 15)	
Maximum Privile	ge		0	(Select 0 to 15)	
Access Control L	ist		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				¢-
□ Туре	Name		Value		

Etapa 3. Repita a etapa 2 para as funções de usuário restantes usando os seguintes pares Cisco-AV.

shell:roles="admin"

C 🖻

Cancel

Save

cisco-av-pair=shell:funções="aaa"

cisco-av-pair=shell:funções="operações"

cisco-av-pair=shell:funções="somente leitura"

cisco-av-pair

Custom Attributes

MANDATORY

+ Add	Z Edit		¢ •
□ Туре	Name	Value	
MANDATORY	cisco-av-pair	shell:roles="aaa"	C 🗊
			Cancel Save

Custom Attributes

+ Add	💼 Trash 👻 🖸 🛙	Edit			¢-			
	Гуре	Name	Value	Value				
	MANDATORY	cisco-av-pair	shell:r	oles="operations"	ش ک			
Custom	Attributes				6 mm			
+ Add	💼 Trash 🕶 🕑 E	Edit			¢-			
П	уре	Name	Value					
	IANDATORY	cisco-av-pair	shell:ro	es="read-only"	c 🗊			
TAC/ 0 Sele	ACS Profiles		Row	S/Page 8 ▼ M < 1 0 /1 ► ► Go	8 Total Rows			
SF	Refresh 🕂 Add	Duplicate 🗂 Trash 🗸	C Ed	it T 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	э	Shell	Default Shell Profile				
	FXOS_Admin_Prof	ile	Shell					
	FXOS_AAA_Shell		Shell					
	FXOS_Operations_	Shell	Shell					
	FXOS_ReadOnly_S	Shell	Shell					

Criando a política de autorização TACACS

Etapa 1. Navegue até Centros de trabalho > Administração do dispositivo > Conjuntos de políticas de administração do dispositivo.

cited In Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	() < 0 < 0 < 0						
Network Access Guest Access TrustSec	BYOD + Profiler + Posture - Device Administration + PassiveID	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 Definut Tecace_Refut							
Summary of Policies	Regular Proxy Sequence							
Global Exceptions Rules across entire deployment								
🖸 Default								
Tacacs_Default	 Authentication Policy 							
Save Order Reset Order	Default Rule (If no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores							
	✓ Authorization Policy							
	Standard							
	Status Rule Name Conditions (identity groups and other conditions) Command Sets Shell Profiles							
	Tecacs_Default If no matches, than Select Profile(1) Deny At Shell Profile	Edit						

Etapa 2. Certifique-se de que a Política de Autenticação aponte para o banco de dados de

Usuários Internos ou para o Repositório de Identidades necessário.



Etapa 3. Clique na seta ao final da diretiva de autorização padrão e clique em inserir regra acima.



Etapa 4. Insira os valores da regra com os parâmetros necessários:

- 4.1. Nome da regra: Regra de administração FXOS.
- 4.2. Condições.

Se: O grupo de identidade do usuário é ADMIN FXOS

Status Rule Name	Co	nditions (id	lentity g	roups and other	conditions)	Command Set	ts She	ell Profiles
🖉 🗹 👻 FXOS Admin Rule	if	Any	[⊖] a	nd Condition(5) 🔶	then Comman	4 and	Select a Shell Profile
Tacacs_Default	f no ma	Any				- 4		
					Use	er Identity Groups	5	
					4	•	م نیز	•
						FXOS AAA		
						GuestType_Weekly (d	lefault)	
						OWN_ACCOUNTS (de	efault)	
		\square				GROUP_ACCOUNTS ((default)	
						FXOS ADMIN		
						FXOS OPER		
						Employee		
						GuestType_Daily (def	ault)	
						GuestType_Contracto	r (default)	
Cours						FXOS Read Only		
Save						ALL_ACCOUNTS (def	ault)	

E dispositivo: Tipo de dispositivo é igual a todos os tipos de dispositivo #FXOS

Conditions (identity groups and other con	nditions) Command Sets Shell Profiles
if FX \Leftrightarrow and DEVICE:Devi	🗢 then Comman 💠 and Select a Shell Profile 📀
o matches, then Selet Add All C	Conditions Below to Library
Condition	Description Device Ty 📀 Equals 🔹 All Device Types# 📀
	All Device Types
	AD >
	DEVICE >>
	InternalUser >
	Network Access
	TACACS >

Perfil da Shell: FXOS_Admin_Profile

Select a Shell Profile	
	Shell Profile
	🔄 🕶 📃 🕶 🔯 🕁
	Q Default Shell Profile
	😪 Deny All Shell Profile
	GA FXOS_AAA_Shell
	G FXOS_Admin_Profile
	Gerations_Shell
	Generation FXOS_ReadOnly_Shell
	WLC ALL
	WLC MONITOR

Etapa 5. Clique em Concluído.

Exc	eptions (0)		
Stand	fard		
1	Status Rule Name	Conditions (identity groups and other conditions) Command Sets Shell Profiles	
i 🖉 🖥	FXOS Admin Rule	If FX \diamondsuit and DEVICE:Devi \diamondsuit Then Select an item \diamondsuit and FXOS Admin Profile	Done
1	 Tacacs_Default 	If no matches, then Select Profile(s) Deny Al Shell Profile	Edit 🔻
Save	Reset		

Etapa 6. Repita as etapas 3 e 4 para as funções de usuário restantes e, quando terminar, clique em SALVAR.

Excepti	ons (0)					
Stanuaru						
Statu	Is 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
ør 🔽	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 r	no matches, then Select Profile(s) Deny All S	hell Pr	ofile	



Verificar

Agora você pode testar cada usuário e verificar a função de usuário atribuída.

Verificação de chassi FXOS

1. Faça Telnet ou SSH para o chassi FXOS e faça login usando qualquer um dos usuários criados no ISE.

Nome de usuário: fxosadmin

Senha:

fpr4120-TAC-A# segurança de escopo

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

Arquivo de usuário remoto:

Descrição:

Funções de usuário:

Nome: aaa

Nome: somente leitura

Usuário remoto fxosadmin:

Descrição:

Funções de usuário:

Nome: admin

Nome: somente leitura

Usuário remoto operacional:

Descrição:

Funções de usuário:

Nome: operações

Nome: somente leitura

Fxosor do usuário remoto:

Descrição:

Funções de usuário:

Nome: somente leitura

Dependendo do nome de usuário inserido, a cli do chassi do FXOS exibirá apenas os comandos autorizados para a função de usuário atribuída.

Função de Usuário Admin.

fpr4120-TAC-A /security #?

Reconhecer

clear-user-sessions Clear User Sessions

criar objetos gerenciados

excluir excluir objetos gerenciados

desabilitar desabilita serviços

enable Habilita serviços

inserir um objeto gerenciado

escopo Altera o modo atual

definir valores de propriedade

show system information

terminar sessões cimc ativas

fpr4120-TAC-A# connect fxos

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

fpr4120-TAC-A (fxos)#

Função de usuário somente leitura.

fpr4120-TAC-A /security #?

escopo Altera o modo atual

definir valores de propriedade

show system information

fpr4120-TAC-A# connect fxos

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

% Permissão negada para a função

2. Navegue até o endereço IP do chassi FXOS e faça login usando qualquer um dos usuários criados no ISE.

Função de Usuário Admin.

Overview Interfaces	Logical	Devices	Secur	ity Engine	Platform Settin	ngs				
NTP		LDAP	RADIUS	TACACS						
SSH SNMP HTTPS		Propertie	s	Sect						
> AAA		TACACS	Providers	Secs						
Syslog DNS			in overall in the second secon				Add TACACS Provider		? ×	O Add
FIPS and Common Criteria	3	Hostna	ime			Order	Hostname/FQDN(or IP Address):*]	
Access List		10.88.2	44.50			1	Order:*	lowest-available		J 🗍
							Key:		Set:No	
							Confirm Key:]	
							Port:*	49		
							Timeout:*	5 Secs		
								ОКС	ancel	
		Save	Cancel							

Função de usuário somente leitura.

iew Int	erfaces	Logical C	Vevices	Securit	ty Engine	Platform 5	iettings						
NTP			LDAP	RADOUS	TACACS								
SSH SNMP			Properties										
HTTPS			Timewit* 5 Becs										
Syslog	Syslog			roviders									
ONS	I Common Criteria ist										0	Add	
FIPS and Comm Access List			Hostnar				On	der	Port				
PECCES L'AL			10.88.24	4.50			1		49		48		

Note: Observe que o botão ADD está acinzentado.

Verificação do ISE 2.0

1. Navegue até Operations > TACACS Livelog. Você deve ser capaz de ver tentativas bem-sucedidas e com falha.

ultuda cisco	Identity Services Engine	Home + Co	intext Visibility	- Operations	Policy Admir	istration + Work Centers			•	۹ 😐	• •		
RADIUS Threat-Centric NAC Live Logs Trubleshoot Adaptive Network Control Reports Click base to do witeless calue and vielability-calue Do not about this													
Live Logs													
								lefresh Nover • Show Late	est 20 records · Within	Last 3 hours	s •		
~	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	2		fxosadmin	Authorization		Tacacs_Default >> FXOS Admin Rule			FXOS_Admir	_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	•		fxosro	Authorization		Tacacs_Default >> FXOS Read Only			FXOS_Read	Only_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	٠	.0	fxosro	Authentication	Tacacs_Default >> Default >> Default		22040 Wrong password or invalid shared					

Troubleshoot

Para depurar a autenticação e a autorização AAA, execute os seguintes comandos na cli do FXOS.

fpr4120-TAC-A# connect fxos

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

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

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

fpr4120-TAC-A (fxos)#term mon

Após uma tentativa de autenticação bem-sucedida, você verá a seguinte saída.

2018 Jan 17 15:46:40.305247 aaa: aaa_req_process para autenticação. session no 0

2018 Jan 17 15:46:40.305262 aaa: aaa_req_process: Solicitação geral de AAA do appln: login appln_subtype: padrão

2018 Jan 17 15:46:40.305271 aaa: try_next_aaa_method

2018 Jan 17 15:46:40.305285 aaa: total de métodos configurados é 1, índice atual a ser tentado é 0

2018 Jan 17 15:46:40.305294 aaa: fp_req_using_method

2018 Jan 17 15:46:40.305301 aaa: AAA_METOD_SERVER_GROUP

2018 Jan 17 15:46:40.305308 aaa: aaa_sg_method_handler group = tacacs

2018 Jan 17 15:46:40.305315 aaa: Usando sg_protocol que é passado para esta função

2018 Jan 17 15:46:40.305324 aaa: Enviando solicitação para o serviço TACACS

2018 Jan 17 15:46:40.305384 aaa: Grupo de métodos configurado com êxito

2018 Jan 17 15:46:40.554631 aaa: aaa_process_fd_set

2018 Jan 17 15:46:40.555229 aaa: aaa_process_fd_set: mtscallback em aaa_q

2018 Jan 17 15:46:40.555817 aaa: mts_message_response_handler: uma resposta mts

2018 Jan 17 15:46:40.556387 aaa: prot_daemon_reponse_handler

2018 Jan 17 15:46:40.557042 aaa: sessão: 0x8dfd68c removido da tabela de sessão 0

2018 Jan 17 15:46:40.557059 aaa: is_aaa_resp_status_successful status = 1

2018 Jan 17 15:46:40.557066 aaa: is_aaa_resp_status_successful é TRUE

2018 Jan 17 15:46:40.557075 aaa: aaa_send_client_response para autenticação. session->flags=21. aaa_resp->flags=0.

2018 Jan 17 15:46:40.557083 aaa: AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:40.557106 aaa: mts_send_response Bem-sucedido

2018 Jan 17 15:46:40.557364 aaa: aaa_req_process para autorização. session no 0

2018 Jan 17 15:46:40.557378 aaa: aaa_req_process chamado com o contexto do appln: login appln_subtype: default authen_type:2, authen_method: 0

2018 Jan 17 15:46:40.557386 aaa: aaa_send_req_using_context

2018 Jan 17 15:46:40.557394 aaa: aaa_sg_method_handler group = (nulo)

2018 Jan 17 15:46:40.557401 aaa: Usando sg_protocol que é passado para esta função

2018 Jan 17 15:46:40.557408 aaa: solicitação AAA baseada em contexto ou direcionada(exceção: não uma solicitação de retransmissão). Não receberá cópia da solicitação aaa

2018 Jan 17 15:46:40.557415 aaa: Enviando solicitação para o serviço TACACS

2018 Jan 17 15:46:40.801732 aaa: aaa_send_client_response para autorização. session->flags=9. aaa_resp->flags=0.

2018 Jan 17 15:46:40.801740 aaa: AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:40.801761 aaa: mts_send_response Bem-sucedido

2018 Jan 17 15:46:40.848932 aaa: CÓDIGO ANTIGO: accounting_mid_update

2018 Jan 17 15:46:40.848943 aaa: aaa_create_local_acct_req: user=, session_id=, log=adicionou user:fxosadmin à função:admin

2018 Jan 17 15:46:40.848963 aaa: aaa_req_process para contabilidade. session no 0

2018 Jan 17 15:46:40.848972 aaa: A referência de solicitação MTS é NULL. solicitação LOCAL

2018 Jan 17 15:46:40.848982 aaa: Definindo AAA_REQ_RESPONSE_NOT_NEEDED

2018 Jan 17 15:46:40.848992 aaa: aaa_req_process: Solicitação geral de AAA do appln: appln_subtype padrão: padrão

2018 Jan 17 15:46:40.849002 aaa: try_next_aaa_method

2018 Jan 17 15:46:40.849022 aaa: nenhum método configurado para o padrão

2018 Jan 17 15:46:40.849032 aaa: nenhuma configuração disponível para esta solicitação

2018 Jan 17 15:46:40.849043 aaa: try_fallback_method

2018 Jan 17 15:46:40.849053 aaa: fp_req_using_method

2018 Jan 17 15:46:40.849063 aaa: local_method_handler

2018 Jan 17 15:46:40.849073 aaa: aaa_local_accounting_msg

2018 Jan 17 15:46:40.849085 aaa: atualização:::usuário adicionado:fxosadmin à função:admin

Após uma tentativa de autenticação com falha, você verá a seguinte saída.

2018 Jan 17 15:46:17.836271 aaa: aaa_req_process para autenticação. session no 0

2018 Jan 17 15:46:17.836616 aaa: aaa_req_process: Solicitação geral de AAA do appln: login appln_subtype: padrão

2018 Jan 17 15:46:17.837063 aaa: try_next_aaa_method

2018 Jan 17 15:46:17.837416 aaa: total de métodos configurados é 1, índice atual a ser tentado é 0

2018 Jan 17 15:46:17.837766 aaa: fp_req_using_method

2018 Jan 17 15:46:17.838103 aaa: AAA_METOD_SERVER_GROUP

2018 Jan 17 15:46:17.838477 aaa: aaa_sg_method_handler group = tacacs

2018 Jan 17 15:46:17.838826 aaa: Usando sg_protocol que é passado para esta função

2018 Jan 17 15:46:17.839167 aaa: Enviando solicitação para o serviço TACACS

2018 Jan 17 15:46:17.840225 aaa: Grupo de métodos configurado com êxito

2018 Jan 17 15:46:18.043710 aaa: is_aaa_resp_status_successful status = 2

2018 Jan 17 15:46:18.044048 aaa: is_aaa_resp_status_successful é TRUE

2018 Jan 17 15:46:18.044395 aaa: aaa_send_client_response para autenticação. session->flags=21. aaa_resp->flags=0.

2018 Jan 17 15:46:18.044733 aaa: AAA_REQ_FLAG_NORMAL

2018 Jan 17 15:46:18.045096 aaa: mts_send_response Bem-sucedido

2018 Jan 17 15:46:18.045677 aaa: aaa_cleanup_session

2018 Jan 17 15:46:18.045689 aaa: mts_drop de msg de solicitação

2018 Jan 17 15:46:18.045699 aaa: aaa_req deve ser liberada.

2018 Jan 17 15:46:18.045715 aaa: aaa_process_fd_set

2018 Jan 17 15:46:18.045722 aaa: aaa_process_fd_set: mtscallback em aaa_q

2018 Jan 17 15:46:18.045732 aaa: aaa_enable_info_config: GET_REQ para uma mensagem de erro de login

2018 Jan 17 15:46:18.045738 aaa: recuperou o valor de retorno da operação de configuração:item de segurança desconhecido

Informações Relacionadas

O comando Ethanalyzer na cli do FX-OS solicitará uma senha quando a autenticação TACACS/RADIUS estiver habilitada. Esse comportamento é causado por um bug.

ID do bug: CSCvg87518