Sistema operacional elástico de FirePOWER (FXO) 2.2: Autenticação/autorização do chassi para o Gerenciamento remoto com ISE usando o RAIO

Índice

Introdução Pré-requisitos Requisitos Componentes Utilizados Configurar Diagrama de Rede Configurações Configurando o chassi FXO Configurando o server ISE Verificação FXO Chasis Verificação FXO Chasis Verificação ISE 2.0 Troubleshooting Informações Relacionadas

Introdução

Este documento descreve como configurar a autenticação RADIUS e a autorização para o chassi elástico do sistema operacional de FirePOWER (FXO) através do Identity Services Engine (ISE).

O chassi FXO inclui os seguintes papéis de usuário:

- Administrador Termine o acesso de leitura e gravação ao sistema inteiro. A conta admin do padrão é atribuída este papel à revelia e não pode ser mudada.
- Read-Only Acesso somente leitura à configuração de sistema sem privilégios alterar o estado de sistema.
- Operações Acesso de leitura e gravação à configuração de NTP, à configuração esperta do Call Home para Smart que licencia, e aos log de sistema, incluindo servidores de SYSLOG e falhas. Acesso de leitura ao resto do sistema.
- AAA Acesso de leitura e gravação aos usuários, aos papéis, e à configuração de AAA. Acesso de leitura ao resto do sistema.

Através do CLI isto pode ser visto como segue:

fpr4120-TAC-A /security * # papel da mostra

Papel:

Priv do nome do papel

aaa aaa

admin admin

operações das operações

de leitura apenas de leitura apenas

Contribuído por Tony Remirez, Jose Soto, engenheiros de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do sistema operacional elástico de FirePOWER (FXO)
- Conhecimento da configuração ISE

Componentes Utilizados

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

- Versão 2.2 da ferramenta de segurança de Cisco FirePOWER 4120
- Cisco Identity Services Engine virtual 2.2.0.470

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

O objetivo da configuração está a:

- Autentique os usuários que registram no GUI com base na Web e no SSH do FXOS por meio do ISE
- Autorize os usuários que registram no GUI com base na Web e no SSH do FXOS de acordo com seu papel de usuário respectivo por meio do ISE.
- Verifique a operação apropriada da authentication e autorização nos FXO por meio do ISE

Diagrama de Rede



Configurações

Configurando o chassi FXO

Criando um fornecedor do RAIO que usa o gerente do chassi

Etapa 1. Navegue aos ajustes da plataforma > ao AAA.

Etapa 2. Clique a aba do RAIO.



Etapa 3. Para cada fornecedor do RAIO que você quer adicionar (até 16 fornecedores).

3.1. Na área dos fornecedores do RAIO, o clique adiciona.

3.2. Uma vez a caixa de diálogo do fornecedor do RAIO adicionar abre, incorpora os valores exigidos.

3.3. Clique a **APROVAÇÃO** para fechar a caixa de diálogo do fornecedor do RAIO adicionar.

Edit 1	0.88.244.50				?×
Hostnam	ne/FQDN(or IP Address):*	10.88.24	4.50		
Order:*		1			
Key:		•••••			Set:Yes
Confirm	Key:	••••••			
Authoriz	ation Port:*	1812			
Timeout	*	5	Secs		
Retries:*	ĸ	1			
			ок) [c	ancel

Etapa 4. Salvaguarda do clique.

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

Etapa 5. Navegue ao sistema > ao gerenciamento de usuário > aos ajustes.

Etapa 6. Sob a autenticação padrão escolha o RAIO.

Overview Interfaces	ogical Devices Security Engine Platform Settings			System To	ols Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	RADIUS v *Local is fallback authentication method				
Console Authentication	Local				
Remote User Settings Remote User Role Policy	S Assign Default Role 🔿 No-Login				

Criando um fornecedor do RAIO que usa o CLI

Etapa 1. A fim permitir a autenticação RADIUS, execute os comandos seguintes.

Segurança do espaço fpr4120-TAC-A#

fpr4120-TAC-A /security # padrão-AUTH do espaço

fpr4120-TAC-A /security/default-auth # ajustou o raio do reino

Etapa 2. Use o comando detail da mostra indicar os resultados.

fpr4120-TAC-A /security/default-auth # detalhe da mostra

Autenticação padrão:

Reino Admin: Radius

Reino operacional: Radius

A sessão da web refresca o período (nos segundos): 600

Timeout de sessão (nos segundos) para a Web, ssh, sessões de Telnet: 600

Timeout de sessão absoluto (nos segundos) para a Web, ssh, sessões de Telnet: 3600

Timeout de sessão do console serial (nos segundos): 600

Timeout de sessão absoluto do console serial (nos segundos): 3600

Grupo de servidor da Autenticação de admin:

Grupo de Authentication Server operacional:

Uso do ò fator: No

Etapa 3. A fim configurar parâmetros do servidor Radius execute os comandos seguintes.

Segurança do espaço fpr4120-TAC-A#

fpr4120-TAC-A /security # raio do espaço

fpr4120-TAC-A /security/radius # entram no server 10.88.244.50

fpr4120-TAC-A /security/radius/server # ajustou o descr "server ISE"

fpr4120-TAC-A /security/radius/server * # ajuste a chave

Incorpore a chave: ******

Confirme a chave: ******

Etapa 4. Use o comando detail da mostra indicar os resultados.

fpr4120-TAC-A /security/radius/server * # detalhe da mostra

Servidor Radius:

Hostname, FQDN ou endereço IP de Um ou Mais Servidores Cisco ICM NT: 10.88.244.50

Descr:

Ordem: 1

Porta do AUTH: 1812

Chave: ****

Intervalo: 5

Configurando o server ISE

Adicionando os FXO como uns recursos de rede

Etapa 1. Navegue à administração > aos recursos de rede > aos dispositivos de rede.

Etapa 2. O clique ADICIONA

dentity Services Engine	Home	✓ ♦ Operations ♦ Policy	y → Administration → W	/ork Centers	
System Identity Management	Network Resources Dev	rice Portal Management pxGr	id Services Feed Service	Threat Centric NAC	
Network Devices Network Device Gr	roups Network Device Profile	es External RADIUS Servers	RADIUS Server Sequences	NAC Managers External MDM	Location Services
0					
Network devices	Network Devices				
Default Device					
Device Security Settings	/ Edit 🕂 Add 🖓 Duplic	cate 🛃 Import 🕞 Export	Generate PAC X Delete		
	Name A IP/	Mask Profile Name	Location	Туре	Description
					No data available

Etapa 3. Incorpore os valores exigidos (o nome, endereço IP de Um ou Mais Servidores Cisco ICM NT, tipo de dispositivo e permite o RAIO e adiciona a CHAVE), clique **submetem-se**.

cisco Identity Services Engine	Home + Co	ontext Visibility	► Policy ▼A	dministration	ork Centers		
System Identity Management	- Network Resource	Device Portal Manageme	ent pxGrid Services	Feed Service	Threat Centric NAC		
Network Devices Network Device	Groups Network	Device Profiles External RADI	JS Servers RADIU	S Server Sequences	NAC Managers Externa	MDM Location Services	
G	•						
Network devices	Network Device	es List > New Network Device					
Default Device	Network De	avices					
Device Security Settings		Name F	KOS				
		Description					
	• IP Add	dress: 10.83.180.6	/ 32				
							1
		Device Profile	Cisco 🔻 🕀				
		Model Name	*				
		Software Version					
	* Network	k Device Group					
	Device Tv	700 muco	CHT D.C. B				
	Device Ty	Pe FXOS	Set to Default				
	IPSE	EC Is IPSEC Device 📀	Set To Default				
	Location	All Locations	Set To Default				
	✓ RADI	IUS Authentication Settings					
	RAD	DIUS UDP Settings					
			Protocol	RADIUS			
			* Shared Secret	•••••	Show		
			CoA Port	1700	Set To Default]	
	RAD	DIUS DTLS Settings (i)					
			DTLS Required	1			
			Shared Secret	radius/dtls	(i)		
			CoA Port	2083	Set To Default		
		Issuer CA of ISE	E Certificates for CoA	Select if required (opt	tional)] 🕡	
					•	-	

Criando os grupos e os usuários da identidade

Etapa 1. Navegue à administração > ao Gerenciamento de identidades > aos grupos > aos grupos da identidade do usuário.

Etapa 2. O clique ADICIONA.

-Indentity Services Engine Home	Context Visibility Operations Policy Administration Work Centers
System Identity Management Network	Resources
Identities Groups External Identity Sources	Identity Source Sequences
Identity Groups	User Identity Groups
٩	
<	/ 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
	GONN_ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group

Etapa 3. Incorpore o valor para o nome e o clique submete-se.

cisco Iden	tity Services Engine	Home	Context Visibility	 Operations 	▶ Policy	→ Administra	ation 🕠	Work Centers	
 System 	✓ Identity Management	Network Re	esources + Devic	e Portal Managemen	t pxGrid Se	rvices F	eed Service	Threat Centric NAC	
Identities	Groups External Id	entity Sources	Identity Source Sec	quences + Setting	S				
Identity v i v i c i v i c i v i c i v i v i v i v i v i v i v i v	r Groups	م ڇ	User Identity Gro Identity Gro Name Description Submit	oups > New User Ide PROS ADMIN Cancel	entity Group]			

Etapa 4. Repita etapa 3 para todos os papéis de usuário exigidos.

dentity Services Engine Home	Context Visibility → Operations → Policy → Ad	dministration Work Centers
► System	esources	S Feed Service F Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups	
	/ Edit - Add X 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
	🗌 👰 FXOS AAA	
	E FXOS ADMIN	
	FXOS OPER	
	FXOS Read Only	
		D-5-14 CROUD ACCOUNTS (J-5-14) II C

Etapa 5. Navegue à administração > ao Gerenciamento de identidades > à identidade > aos usuários.

Etapa 6. O clique ADICIONA.

dentity Services Engine	Home Context	Visibility	ns Policy	- Administration	▶ Work Centers				
System Vetwork Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC									
- Identities Groups External Identity	Sources Identity S	ource Sequences + S	Settings						
G									
Users	Network Access	Users							
Latest Manual Network Scan Results	/ Edit 🕂 Add	Change Status	Import 🔀 Export	X Delete	uplicate				
	Status	Name	 Descript 	ion Fir	st Name Last Name	Email Address	User Identity Groups	Admin	
							No data available		

Etapa 7. Incorpore os valores exigidos (nome, grupo de usuário, 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 exigidos.

dentity Services Engine	Home + Conte	xt Visibility	Policy Administrati	on 🔹 Work Ce	nters					
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC										
✓Identities Groups External Identity Sources Identity Source Sequences → Settings										
0	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			

Criando o perfil da autorização para cada papel de usuário

Etapa 1. Navegue à **política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização.**

dentity Services Engine	Home	Operations Policy	Administration Work Centers						
Authentication Authorization Profilir	ng Posture Client Provisionir	Policy Elements							
Dictionaries + Conditions - Results	3								
0									
Authentication	Authentication Standard Authorization Profiles								
Authorization	For Policy Export go to Adm	inistration > System > Backup	& Restore > Policy Export Page						
Plationzation	/ Edit + Add C Duplic	ate X Delete							
Authorization Profiles	Name		Profile	Description					
Downloadable ACLs	Blackhole_Wireless_A	ccess	itto Cisco ⊕	Default profile used to blacklist wireless devices. Ensu					
▶ Profiling	Cisco_IP_Phones		atta Clisco 🕀	Default profile used for Cisco Phones.					
Posture	Cisco_WebAuth		🗰 Cisco 🕀	Default Profile used to redirect users to the CWA port					
	NSP_Onboard		atta Cisco ⊕	Onboard the device with Native Supplicant Provisionin					
Client Provisioning	Non_Cisco_IP_Phone	s	🗰 Cisco 🕀	Default Profile used for Non Cisco Phones.					
	DenyAccess			Default Profile with access type as Access-Reject					
	PermitAccess			Default Profile with access type as Access-Accept					

Etapa 2. Encha todos os atributos para o perfil da autorização.

2.1. Configurar o nome de perfil.

Authentication Authorization Profilin	g Posture Client Provisioning - Policy Elements
Dictionaries Conditions Results	
0	
Authentication	Authorization Profiles > FXOS-ADMIN-PROFILE Authorization Profile
- Authorization	* Name FXOS-ADMIN-PROFILE
Authorization Profiles	Description
Downloadable ACLs	Access Type ACCESS_ACCEPT T
▶ Profiling	Network Device Profile dtt Cisco 👻 🕀

2.2. Em ajustes avançados dos atributos configurar o seguinte CISCO-AV-PAIR

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

 Advanced Attributes Setting 	s	
Cisco:cisco-av-pair	shell:roles="admin"	⊘ — +

2.3. Click Save.



Etapa 3. Repita etapa 2 para os papéis de usuário restantes usando os seguintes pares Cisco AV

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

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

cisco-av-pair=shell: roles= " de leitura apenas"





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

dentity Services Engine	Home → Context Visibility → Operations → Policy →	Administration + Work Centers						
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements							
Dictionaries + Conditions - Results								
0								
Authentication	Standard Authorization Profiles							
Authorization	For Policy Export go to Administration > System > Backup & Rest	tore > Policy Export Page						
	/ Edit + Add D Duplicate X Delete							
Authorization Profiles	Name	Profile						
Downloadable ACLs		He Cieco F						
▶ Profiling								
		CISCO C						
▶ Posture	Cisco_WebAuth	🔐 Cisco 🕀						
	FXOS-AAA-PROFILE	atte Cisco 🕀						
Client Provisioning	FXOS-ADMIN-PROFILE	🚟 Cisco 🕀						
	FXOS-OPER-PROFILE	💼 Cisco 🕀						
	FXOS-ReadOnly-PROFILE	este Cisco 🕀						

Criando a política de autenticação

Etapa 1. Navegue à **política > à autenticação >** e clique a seta ao lado de editam onde você quer criar a regra.



Etapa 2. A instalação é simples; pode ser mais granulada feito mas para este exemplo nós usaremos o tipo de dispositivo:

Nome: REGRA DA AUTENTICAÇÃO FXO

SE atributo/valor novos seletos: **Dispositivo: O tipo de dispositivo iguala todos os tipos de dispositivos #FXOS**

Permita protocolos: Acesso de rede padrão

Uso: Usuários internos



Criando a política da autorização

Etapa 1. Navegue à **política > à autorização >** e clique a rede da seta para editar onde você quer criar a regra.

cisce Identity Serv	vices Engine	Home + Context Visibility + Operations Policy + Administration + Work C	Centers		🙂 🤍 🔍 🔍 🔍								
Authentication Au	uthorization	Profiling Posture Client Provisioning + Policy Elements	Click here to do wireless setup and visibility setup Do not show this again. $\stackrel{\scriptstyle \times}{\times}$										
Authorization Po	Authorization Policy												
Define the Authorizatio For Policy Export go to	Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drep rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page												
First Matched Rule Ap	oplies	•											
Exceptions (0))												
Standard													
Status Rul	Je Name	Conditions (identity groups and other conditions)	Permissions										
Def	rfault	If no matches, then DenyAccess			Insert New Rule Above								
Seve Reset													

Etapa 2. Incorpore os valores para a regra da autorização com os parâmetros requerido.

2.1. Nome da regra: Regra de Fxos <USER ROLE>.



2.2. Se: Grupos da identidade do usuário > <USER seleto ROLE>.

Conditions (identity groups and other co	nditions) Permissions
f FX and Condition(s) 🗇 then AuthZ Pr
ma	
FXOS ADMIN	
	User Identity Groups
	↓ ■ ↓ ♀ ♀↓
	FXOS AAA
	GuestType_Weekly (default)
	OWN_ACCOUNTS (default)
	GROUP_ACCOUNTS (default)
	FXOS ADMIN
	FXOS OPER
	Employee
	GuestType_Daily (default)
	GuestType_Contractor (default)
	FXOS Read Only
	ALL_ACCOUNTS (default)

2.3. E: Crie a condição nova > o dispositivo: O tipo de dispositivo iguala **todos os tipos de dispositivos #FXOS**.

Conditions (identity groups	and other conditions) Permissions	
if FX 💠 and	DEVICE:Device Type EQUALS All 🗢 then Select an item 💠	
if no matches, then DenyAc	Add All Conditions Below to Library	
	Condition Name Description Image: Device Ty Image: Device Ty Image: Device Ty Image: Device Ty	≩
		P
	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	£î.
	All Device Types#FXOS	
	AD Alexandr	>
		>
		,
	Brorade	<u> </u>
	Cisco	
	Cisco-BBSM	
	Cisco-VPN3000	>
	Сия	>

2.4. Permissões: O padrão > escolhe o **papel de usuário do perfil**

Permissions		
then FXOS-A		
FXOS-ADMIN-PROFILE	o	
	Standard	
	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	
	Blackhole_Wireless_Access	
	Cisco_IP_Phones	
	Cisco_WebAuth	
	2 DenyAccess	
	S FXOS-AAA-PROFILE	
	FXOS-ADMIN-PROFILE	
	STATE FXOS-OPER-PROFILE	
	VSP. Ophoard	
	Non Cisco IP Phones	
Status Rule Name	Conditions (identity groups and other conditions) Permissi	ons
Fxos Admin Rule	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device then FXOS- Types#FXOS	ADMIN-PROFILE

Etapa 3. Repita etapa 2 para todos os papéis de usuário.

Status	Rule Name		Conditions (identity groups and other conditions)	I	Permissions
~	Fxos Admin Rule	if	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-ADMIN-PROFILE
	Fxos AAA Rule	lf	FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-AAA-PROFILE
~	Fxos Oper Rule	if	FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-OPER-PROFILE
	Fxos Read only Rule	if	FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-ReadOnly-PROFILE
~	Default	if r	o matches, then DenyAccess		

Etapa 4. Salvaguarda do clique na parte inferior da página.



Verificar

Você pode agora testar cada usuário e verificar o papel de usuário atribuído.

Verificação FXO Chasis

1. Telnet ou SSH ao chassi e ao início de uma sessão FXO usando alguns dos usuários criados no ISE.

Nome de usuário: fxosadmin

Senha:

Segurança do espaço fpr4120-TAC-A#

fpr4120-TAC-A /security # detalhe do usuário remoto da mostra

Fxosaaa do usuário remoto:

Descrição:

Papéis de usuário:

Nome: aaa

Nome: somente leitura

Fxosadmin do usuário remoto:

Descrição:

Papéis de usuário:

Nome: admin

Nome: somente leitura

Fxosoper do usuário remoto:

Descrição:

Papéis de usuário:

Nome: operações

Nome: somente leitura

Fxosro do usuário remoto:

Descrição:

Papéis de usuário:

Nome: somente leitura

Segundo o username incorporado o chassi FXO o CLI indicará somente os comandos autorizados para o papel de usuário atribuído.

Papel de usuário admin.

fpr4120-TAC-A /security #?

reconheça reconhecem

as claro-USER-sessões cancelam sessões do usuário

crie criam objetos gerenciado

suprima de objetos gerenciado da supressão

serviços das inutilizações do desabilitação

permita permite serviços

entre incorpora um objeto gerenciado

o espaço muda o modo atual

ajuste valores do proprietário ajustados

mostre a informação de sistema da mostra

termine sessões do Active cimc

fpr4120-TAC-A# conectam fxos

fpr4120-TAC-A (fxos) # debugam AAA-pedidos aaa

fpr4120-TAC-A (fxos) #

Papel de usuário de leitura apenas.

fpr4120-TAC-A /security #?

o espaço muda o modo atual

ajuste valores do proprietário ajustados

mostre a informação de sistema da mostra

fpr4120-TAC-A# conectam fxos

fpr4120-TAC-A (fxos) # debugam AAA-pedidos aaa

% da permissão negada para o papel

2. Consulte ao endereço IP de Um ou Mais Servidores Cisco ICM NT e ao início de uma sessão do chassi FXO usando alguns dos usuários criados no ISE.

Papel de usuário admin.

Overview Interfaces Logica	I Devices Security Engine Platf	orm Settings						System Tool	s Help fxosadmin
NTP SSH SNMP HTTPS AAA	LDAP RADIUS TACACS Properties Timeout:* \$ Secs		Add RADIUS Provider		T K		 		
Syslog DNS FIPS and Common Criteria Access List	Retries:* 1 RADIUS Providers		Hostname/FQDN(or IP Address):* Order:* Newest-available			O Add			
	Hostname 10.89.244.16	Order 1	Confirm Key: Authorization Port:* Timeout:*	1812 5 Secs	SIELINO	/ 9			
			Retries:*	0K Can	cel				

Papel de usuário de leitura apenas.

Overview	Interfaces	Logical I	Devices	Security Engine	Platform Settings				
NTP			LDAP	ADEUS TACACS					
SSH			Properties						
HTTPS			Timeout:*	5 Secs					
Syslog			Retries:*	1					
DNS FIPS and C	Common Criteria		KADEUS PR	propers					
Access List	t							0	A00
			Hostnam	Me .	Order	Service	Auth Port		
			10.88.24	4.16	1	authorization	1812	۹.8	

Note: Observe que o botão Add é desabilitada para fora.

Verificação ISE 2.0

1. Navegue às **operações > ao RAIO > logs vivos.** Você deve poder ver bem sucedido e falhas de tentativa.

disce Iden	tity Services Engir	e Home	Context Visibi	ity - Operati	ions Po	olicy	Administration	Work Centers					1) 🤍 () o (
→ RADIUS	Threat-Centric NA	C Live Logs 🔹 🕨 1	TACACS + Trou	ibleshoot + Ad	aptive Networ	rk Contro	ol Reports				Click here to do y	vireless setup an	d visibility s	tup Do not sho	w this again.
Live Logs	Live Sessions							_				,			
		Misconfigured St	upplicants	Miscont	figured Netwo	ork Dev	ices O	RADIUS Drops O	Client Sto	pped Responding	0	Repeat Counte	er O		
		0			0			0		0		0			
										Refresh Never	• Show	Latest 20 reco	rds 🔹 V	/ithin Last 3	hours •
C Refresh O Reset Repeat Counts 差 Export To - ▼ Filter												iter • • •			
Tim	0	Status	Details	Repeat C	Identity	/	Authentication Pol	icy	Authorization Po	licy	Authorization Profiles	s Network	k Dev	Identity Grou	qu
×		-			Identity		Authentication Policy	1	Authorization Polic	ay	Authorization Profiles	Network	k Device	Identity Grou	p
Jan	20, 2018 10:14:09		0		fxosadmin	1	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Ad	lmin Rule	FXOS-ADMIN-PROFILE	FXOS		User Identity (Groups:FXOS
Jan	20, 2018 10:13:59	۰	0		fxosadmin	1	Default >> FXOS AU	THENTICATION RULE >> Default				FXOS		User Identity (Groups:FXOS
Jan	20, 2018 10:09:01	V	0		fxosro	1	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Re	ad only Rule	FXOS-ReadOnly-PROF	ILE FXOS		User Identity (Broups:FXOS
Jan	20, 2018 10:08:50	۲	O.		fxosro		Default >> FXOS AU	THENTICATION RULE >> Default				FXOS		User Identity (Groups:FXOS
Jan	20, 2018 10:06:17	۲	0		fxosro	1	Default >> FXOS AU	THENTICATION RULE >> Default				FXOS		User Identity (Groups:FXOS
Jan	20, 2018 10:05:15	٥	0		fxosro	1	Default >> FXOS AU	THENTICATION RULE >> Default				FXOS		User Identity (Broups:FXOS
Jan	20, 2018 10:04:23	1	0		fxosadmin	1	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Ad	Imin Rule	FXOS-ADMIN-PROFILE	FXOS		User Identity (Groups:FXOS
Jan	20, 2018 10:02:59		à +		fxosadmin	÷ 1	Default >> FXOS AU	THENTICATION RULE >> Default	Default >> Fxos Ad	Imin Rule	FXOS-ADMIN-PROFILE	FXOS		User Identity (Groups:FXOS

Troubleshooting

A fim debugar a autenticação de AAA e a autorização execute os comandos seguintes nos FXO CLI.

fpr4120-TAC-A# conectam fxos

fpr4120-TAC-A (fxos) # debugam AAA-pedidos aaa

fpr4120-TAC-A (fxos) # debugam o evento aaa

fpr4120-TAC-A (fxos) # debugam erros aaa

fpr4120-TAC-A (fxos) # termo segunda-feira

Depois que uma tentativa da autenticação bem sucedida, você considerará a seguinte saída.

2018 o 20 de janeiro 17:18:02.410275 aaa: aaa_req_process para a autenticação. sessão nenhum 0

2018 o 20 de janeiro 17:18:02.410297 aaa: aaa_req_process: Pedido geral AAA do appln: appln_subtype do início de uma sessão: padrão

2018 o 20 de janeiro 17:18:02.410310 aaa: try_next_aaa_method

2018 o 20 de janeiro 17:18:02.410330 aaa: os métodos totais configurados são 1, deslocamento predeterminado atual a ser tentado são 0

2018 o 20 de janeiro 17:18:02.410344 aaa: handle_req_using_method

2018 o 20 de janeiro 17:18:02.410356 aaa: AAA_METHOD_SERVER_GROUP

2018 o 20 de janeiro 17:18:02.410367 aaa: grupo = raio do aaa_sg_method_handler

2018 o 20 de janeiro 17:18:02.410379 aaa: Usando o sg_protocol que é passado a esta função

2018 o 20 de janeiro 17:18:02.410393 aaa: Enviando o pedido ao serviço de raio

2018 o 20 de janeiro 17:18:02.412944 aaa: mts_send_msg_to_prot_daemon: Comprimento de carga útil = 374

2018 o 20 de janeiro 17:18:02.412973 aaa: sessão: 0x8dfd68c adicionado à tabela 1 da sessão

2018 o 20 de janeiro 17:18:02.412987 aaa: Grupo configurado do método sucedido

2018 o 20 de janeiro 17:18:02.656425 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:18:02.656447 aaa: aaa_process_fd_set: mtscallback no aaa_q

2018 o 20 de janeiro 17:18:02.656470 aaa: mts_message_response_handler: uma resposta dos mts

2018 o 20 de janeiro 17:18:02.656483 aaa: prot_daemon_reponse_handler

2018 o 20 de janeiro 17:18:02.656497 aaa: sessão: 0x8dfd68c removido da tabela 0 da sessão

2018 o 20 de janeiro 17:18:02.656512 aaa: estado dos is_aaa_resp_status_success = 1

2018 o 20 de janeiro 17:18:02.656525 aaa: os is_aaa_resp_status_success são VERDADEIROS

2018 o 20 de janeiro 17:18:02.656538 aaa: aaa_send_client_response para a autenticação. session->flags=21. aaa_resp->flags=0.

2018 o 20 de janeiro 17:18:02.656550 aaa: AAA_REQ_FLAG_NORMAL

2018 o 20 de janeiro 17:18:02.656577 aaa: mts_send_response bem sucedido

2018 o 20 de janeiro 17:18:02.700520 aaa: aaa_process_fd_set: mtscallback no aaa_accounting_q

2018 o 20 de janeiro 17:18:02.700688 aaa: OPCODE VELHO: accounting_interim_update

2018 o 20 de janeiro 17:18:02.700702 aaa: aaa_create_local_acct_req: user=, session_id=, fxosro log=added do usuário

2018 o 20 de janeiro 17:18:02.700725 aaa: aaa_req_process para explicar. sessão nenhum 0

2018 o 20 de janeiro 17:18:02.700738 aaa: A referência do pedido MTS é NULA. Pedido LOCAL

2018 o 20 de janeiro 17:18:02.700749 aaa: Ajustando AAA_REQ_RESPONSE_NOT_NEEDED

2018 o 20 de janeiro 17:18:02.700762 aaa: aaa_req_process: Pedido geral AAA do appln: appln_subtype do padrão: padrão

2018 o 20 de janeiro 17:18:02.700774 aaa: try_next_aaa_method

2018 o 20 de janeiro 17:18:02.700798 aaa: nenhuns métodos configurados para o padrão do padrão

2018 o 20 de janeiro 17:18:02.700810 aaa: nenhuma configuração disponível para esta pedido

2018 o 20 de janeiro 17:18:02.700997 aaa: aaa_send_client_response para explicar. session->flags=254. aaa_resp->flags=0.

2018 o 20 de janeiro 17:18:02.701010 aaa: a resposta para o pedido explicando da biblioteca velha será enviada como o SUCESSO

2018 o 20 de janeiro 17:18:02.701021 aaa: resposta não necessária para este pedido

2018 o 20 de janeiro 17:18:02.701033 aaa: AAA_REQ_FLAG_LOCAL_RESP

2018 o 20 de janeiro 17:18:02.701044 aaa: aaa_cleanup_session

2018 o 20 de janeiro 17:18:02.701055 aaa: o aaa_req deve ser livrado.

2018 o 20 de janeiro 17:18:02.701067 aaa: Recuar o local do método sucedido

2018 o 20 de janeiro 17:18:02.706922 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:18:02.706937 aaa: aaa_process_fd_set: mtscallback no aaa_accounting_q

2018 o 20 de janeiro 17:18:02.706959 aaa: OPCODE VELHO: accounting_interim_update

2018 o 20 de janeiro 17:18:02.706972 aaa: aaa_create_local_acct_req: user=, session_id=, usuário log=added: fxosro ao papel: somente leitura

Depois que uma tentativa da autenticação falha, você considerará a seguinte saída.

2018 o 20 de janeiro 17:15:18.102130 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:15:18.102149 aaa: aaa_process_fd_set: mtscallback no aaa_q

2018 o 20 de janeiro 17:15:18.102267 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:15:18.102281 aaa: aaa_process_fd_set: mtscallback no aaa_q

2018 o 20 de janeiro 17:15:18.102363 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:15:18.102377 aaa: aaa_process_fd_set: mtscallback no aaa_q

2018 o 20 de janeiro 17:15:18.102456 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:15:18.102468 aaa: aaa_process_fd_set: mtscallback no aaa_q

2018 o 20 de janeiro 17:15:18.102489 aaa: mts_aaa_req_process

2018 o 20 de janeiro 17:15:18.102503 aaa: aaa_req_process para a autenticação. sessão nenhum 0

2018 o 20 de janeiro 17:15:18.102526 aaa: aaa_req_process: Pedido geral AAA do appln: appln_subtype do início de uma sessão: padrão

2018 o 20 de janeiro 17:15:18.102540 aaa: try_next_aaa_method

2018 o 20 de janeiro 17:15:18.102562 aaa: os métodos totais configurados são 1, deslocamento predeterminado atual a ser tentado são 0

2018 o 20 de janeiro 17:15:18.102575 aaa: handle_req_using_method

2018 o 20 de janeiro 17:15:18.102586 aaa: AAA_METHOD_SERVER_GROUP

2018 o 20 de janeiro 17:15:18.102598 aaa: grupo = raio do aaa_sg_method_handler

2018 o 20 de janeiro 17:15:18.102610 aaa: Usando o sg_protocol que é passado a esta função

2018 o 20 de janeiro 17:15:18.102625 aaa: Enviando o pedido ao serviço de raio

2018 o 20 de janeiro 17:15:18.102658 aaa: mts_send_msg_to_prot_daemon: Comprimento de carga útil = 371

2018 o 20 de janeiro 17:15:18.102684 aaa: sessão: 0x8dfd68c adicionado à tabela 1 da sessão

2018 o 20 de janeiro 17:15:18.102698 aaa: Grupo configurado do método sucedido

2018 o 20 de janeiro 17:15:18.273682 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:15:18.273724 aaa: aaa_process_fd_set: mtscallback no aaa_q

2018 o 20 de janeiro 17:15:18.273753 aaa: mts_message_response_handler: uma resposta dos mts

2018 o 20 de janeiro 17:15:18.273768 aaa: prot_daemon_reponse_handler

2018 o 20 de janeiro 17:15:18.273783 aaa: sessão: 0x8dfd68c removido da tabela 0 da sessão

2018 o 20 de janeiro 17:15:18.273801 aaa: estado dos is_aaa_resp_status_success = 2

2018 o 20 de janeiro 17:15:18.273815 aaa: os is_aaa_resp_status_success são VERDADEIROS

2018 o 20 de janeiro 17:15:18.273829 aaa: aaa_send_client_response para a autenticação. session->flags=21. aaa_resp->flags=0.

2018 o 20 de janeiro 17:15:18.273843 aaa: AAA_REQ_FLAG_NORMAL

2018 o 20 de janeiro 17:15:18.273877 aaa: mts_send_response bem sucedido

2018 o 20 de janeiro 17:15:18.273902 aaa: aaa_cleanup_session

2018 o 20 de janeiro 17:15:18.273916 aaa: mts_drop de msg do pedido

2018 o 20 de janeiro 17:15:18.273935 aaa: o aaa_req deve ser livrado.

2018 o 20 de janeiro 17:15:18.280416 aaa: aaa_process_fd_set

2018 o 20 de janeiro 17:15:18.280443 aaa: aaa_process_fd_set: mtscallback no aaa_q

2018 o 20 de janeiro 17:15:18.280454 aaa: aaa_enable_info_config: GET_REQ para o Mensagem de Erro do início de uma sessão aaa

2018 o 20 de janeiro 17:15:18.280460 aaa: recebido de volta o valor do retorno da operação da configuração: artigo desconhecido da Segurança

Informações Relacionadas

O comando de Ethanalyzer em FX-OS CLI alertará para a senha para uma senha quando a autenticação TACACS/RADIUS é permitida. Este comportamento é causado por um erro.

Bug ID: <u>CSCvg87518</u>