Firepower 拡張可能なオペレーティング システム(FXOS) 2.2: RADIUS を使用して ISE の遠 隔管理のためのシャーシ認証/許可

目次

<u>はじめに</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>設定</u> <u>ネットワーク図</u> <u>設定</u> FXOS シャーシの設定 ISE サーバの設定 確認 FXOS Chasis 確認 ISE 2.0 の検証 トラブルシューティング 関連情報

概要

この資料に Identity Services Engine (ISE)で Firepower 拡張可能なオペレーティング システム (FXOS)シャーシのための RADIUS認証および許可を設定する方法を記述されています。

FXOS シャーシは次のユーザの役割が含まれています:

- 管理者-システム全体に読み書きアクセスを完了して下さい。デフォルト管理者アカウントこのロールはデフォルトで割り当てられ、変更することができません。
- ・読み取り専用-システム状態を変更する特権無しのシステム構成への読み取り専用アクセス。
- オペレーション-スマートな認可のための NTP 設定、Smart Call Home 設定、および syslog サーバおよびエラーを含むシステムログへの読み書きアクセス。システムの他への読み取り アクセス。
- AAA: ユーザ、ロールおよび AAA設定への読み書きアクセス。 システムの他への読み取り アクセス。
- CLIによってこれは次の通り見られる場合があります:

fpr4120-TAC-A /security * #ロールを示して下さい

ロール:

ロール名 Priv

AAA AAA

admin admin

オペレーション オペレーション

読み取り専用読み取り専用

、ホセ Soto トニー Remirez によって貢献される、Cisco TAC エンジニア。

前提条件

要件

次の項目に関する知識が推奨されます。

- Firepower 拡張可能なオペレーティング システム(FXOS)のナレッジ
- ISE 設定のナレッジ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Firepower 4120 セキュリティ アプライアンス バージョン 2.2
- ・バーチャル Cisco Identity Services Engine 2.2.0.470

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメン トで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。 稼働中 のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してくだ さい。

設定

設定の目標はにあります:

- ISE によって FXOS の Webベース GUI および SSH にログイン して いるユーザを認証して 下さい
- ISE によってそれぞれユーザの役割に従って FXOS の Webベース GUI および SSH にログイ ン して いるユーザを許可して下さい。
- ISE によって FXOS の認証 および 権限の正しい動作を確認して下さい

ネットワーク図



設定

FXOS シャーシの設定

シャーシ マネージャを使用する RADIUS プロバイダの作成

ステップ 1.プラットフォーム設定 > AAA へのナビゲート。

ステップ 2. RADIUS タブをクリックして下さい。

Overview Interfaces Logi	vices Security Engine Platform Settings	
NTP	NAP RADIUS TACACS	
SSH	natias	
HTTPS	nonit* 5 Serc	
AAA		
Syslog	ines:* 1 DIUS Providers	
FIPS and Common Criteria		
Access List		
	ostname Order Service Auth Port	

ステップ3追加したいと思う各 RADIUS プロバイダに関しては(16 人までのプロバイダ)。

3.1. RADIUS プロバイダ エリアで、『Add』 をクリック して下さい。

3.2. 追加 RADIUS プロバイダ ダイアログボックスが開いたら、必要な値を入力して下さい。

3.3. 追加 RADIUS プロバイダ ダイアログボックスを閉じるために『OK』 をクリック し て下さい。

Í	Edit 10.88.244.50		?×
l	Hostname/FQDN(or IP Address):*	10.88.244.50	
1	Order:*	1	
	Key:	•••••	Set:Yes
1	Confirm Key:	•••••	
1	Authorization Port:*	1812	
1	Timeout:*	5 Secs	
l	Retries:*	1	
		ОКС	ancel

ステップ 4. 『SAVE』 をクリック して下さい。

Overview Interfaces Logic	al Devices Security Engine	Platform Settings			
NTP	LDAP RADIUS TACACS				
SSH	Properties				
HTTPS	Timeout:* 5 Secs				
► AAA					
Syslog	RADIUS Providers				
FIPS and Common Criteria					Add Add
Access List	Hostname	Order	Service	Auth Port	
	10.88.244.50	1	authorization	1812	08
	Save				

ステップ 5.**システム > ユーザマネージメント > 設定**へのナビゲート。

ステップ6デフォルトの認証の下で『RADIUS』 を選択 して下さい。

Overview Interfaces Logic	al Devices Security Engine Platform Settings			System Too	ols Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	RADIUS v "Local is failback authentication method				
Console Authentication	Local v				
Remote User Settings					
Remote User Role Policy	😪 Assign Default Role 🔿 No-Login				

CLI を使用する RADIUS プロバイダの作成

ステップ 1. RADIUS認証を有効に するために、次のコマンドを実行して下さい。

- fpr4120-TAC-A# スコープ セキュリティ
- fpr4120-TAC-A /security #スコープ デフォルトauth
- fpr4120-TAC-A /security/default-auth は#レルム半径を設定しました
- 呼び出します。結果を表示する提示 detail コマンドを使用して下さい。
- fpr4120-TAC-A /security/default-auth は#詳細を示します
- デフォルトの認証:
 - Admin レルム: Radius
 - 操作上レルム: Radius
 - Web セッション リフレッシュ期間(秒で):600
 - Web のためのセッション タイムアウト(秒で)、ssh、Telnetセッション: 600
 - Web のための絶対セッション タイムアウト(秒で)、ssh、Telnetセッション: 3600
 - シリアルコンソール セッション タイムアウト(秒で):600
 - シリアルコンソール絶対セッション タイムアウト(秒で):3600
 - Admin 認証サーバ グループ:
 - 操作上認証サーバ グループ:
 - 第2ファクタの使用:なし
- ステップ 3. RADIUSサーバ パラメータを設定するために次のコマンドを実行して下さい。
- fpr4120-TAC-A# スコープ セキュリティ
- fpr4120-TAC-A /security #スコープ半径
- fpr4120-TAC-A /security/radius は#サーバ 10.88.244.50 を入力します
- fpr4120-TAC-A /security/radius/server は#設定しました descr 「ISE サーバ」を
- fpr4120-TAC-A /security/radius/server * # Set a
- キーを入力して下さい: *******
- キーを確認して下さい:******
- ステップ 4 結果を表示する提示 detail コマンドを使用して下さい。
- fpr4120-TAC-A /security/radius/server * #詳細を示して下さい

RADIUSサーバ:

ホスト名、FQDN または IP アドレス: 10.88.244.50

descr :

- 発注: 1
- Auth ポート: 1812
- 凡例: ****
- タイムアウト:5

ISE サーバの設定

ネットワークリソースとして FXOS の追加

ステップ 1. Administration > ネットワークリソース > ネットワークデバイスへのナビゲート。

ステップ 2. 『Add』 をクリック して下さい

dentity Services Engine	Home	Operations Policy	Administration Work Centers					
System Identity Management Vetwork Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC								
Network Devices Network Device Gro	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences NAC Managers	External MDM Location Services				
0								
Network devices	Network Devices							
Default Device								
Device Security Settings	/ Edit 🕂 Add 🕞 Duplicate	🔂 Import 🚯 Export	Generate PAC X Delete					
	Name 🔺 IP/Ma	k Profile Name	Location	Type Description				
				No data available				

ステップ 3.必要な値を(名前、IP アドレス、デバイスの種類およびイネーブル RADIUS は KEY を追加します)入力し、『SUBMIT』 をクリック して下さい。

cisco Identity Services Engine	Home	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Network Devices Network Device	e Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
(0	
Network devices	Network Devices	
Default Device		
Device Security Settings	Passidies	
	* IP Address: 10.83.180.6 / 32	
	* Device Profile 🗰 Cisco 👻 🕀	
	Model Name	
	Software Version	
	* Network Device Group	
	Device Type FXOS Set To Default	
	All Locations 📀 Set To Default	
	✓ RADIUS Authentication Settings	
	RADIUS UDP Settings	
	Shared Secret	
	CoA Port 1700 Set To Default	
	RADIUS DTLS Settings (j)	
	DTLS Required 🔲 👔	
	Shared Secret radius/dtls (i)	
	CoA Port 2083 Set To Default	
	Issuer CA of ISE Certificates for CoA Select if required (optional)	

識別グループおよびユーザの作成

ステップ 1. Administration > アイデンティティ管理 > Groups > ユーザ識別グループにナビゲート して下さい。

ステップ 2. 『Add』 をクリック して下さい。

cisco Iden	tity Services Engine	Home	 Context Visibility 	▸ Operations	▶ Policy	- Administration	▶ Work Centers
 System 	✓ Identity Management	Network	Resources Dev	ce Portal Management	pxGrid S	Services Feed Se	Prvice Threat Centric NAC
Identities	Groups External Ide	ntity Sources	Identity Source So	equences Setting	s		

Identity Groups	User Identity Groups
	∠ Zelit - Add XDelete - Add KDelete - ZepImport - Export -
 Endpoint Identity Groups 	Name Description
User Identity Groups	ALL_ACCOUNTS (defauit) Defauit ALL_ACCOUNTS (defauit) User Group
	Employee Default Employee User Group
	GROUP_ACCOUNTS (default) Default GROUP_ACCOUNTS (default) User Group
	GuestType_Contractor (default) Identity group mirroring the guest type
	GuestType_Daily (default) Identity group mirroring the guest type
	GuestType_Weekly (default) Identity group mirroring the guest type
	ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group

ステップ 3.名前の値を入力し、『SUBMIT』 をクリック して下さい。

dentity Services Engine	Home +	Context Visibility	 Operations 	▶ Policy	- Administration	Work Centers
System Identity Management	Network Res	ources + Device	e Portal Managemen	t pxGrid S	ervices + Feed Ser	rvice
Identities Groups External Iden	ntity Sources I	Identity Source Seq	uences + Setting	S		
Identity Groups Identity Groups Image: Second Sec	م ڇ-	User Identity Gro Identity Gro Name [Description [Submit C	pups > New User Id up FXOS ADMIN ancel	entity Group		

ステップ 4.すべての必須ユーザの役割のためのステップ 3 を繰り返して下さい。

dent	tity Service:	s Engine	Home	Context Visibility	 Operations 	▶ Policy	- Administration	▸ Work Centers
System	✓ Identity N	lanagement	Network F	Resources Device	Portal Management	pxGrid S	ervices Feed Se	rvice
Identities	Groups	External Ider	tity Sources	Identity Source Sequ	ences Settings			

Identity Groups	P	User Identity Groups				
⟨= + E +	<u>نې</u>	✓ Edit ♣Add X Delete ▼ ♣Import ♣ Export	t *			
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 A FXOS ADMIN				
		E PROS OPER				
		FXOS Read Only				
			DEFUIL ODOLD ACCOUNTS (JEEUIL) USE COME			

ステップ 5. Administration > アイデンティティ管理 > 識別 > Users にナビゲート して下さい。

ステップ 6. 『Add』 をクリック して下さい。

-that- cisce Identity Services Engine	Home ► Context Visibility ► Op	erations Policy Administration	► Work Centers						
System Veldentity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC									
Identities Groups External Identity Sources Identity Source Sequences ▶ Settings									
0									
Users	Network Access Users								
Latest Manual Network Scan Results / Edit + Add Connge Status Depart Connge Status									
	Status Name	Description	irst Name Last Name Email Address	User Identity Groups Admin					
			,	No data available					

ステップ 7.必要な値(名前、ユーザグループ、パスワード)を入力して下さい。

cisco	Identity Sen	vices Engine	Home	 Context Visibility 	 Operations 	Policy	✓ Adm	inistration	Work Center	5
System	stem 🔽 Iden	tity Management	Network	Resources Devic	e Portal Management	pxGrid	Services	Feed Serv	ice + Threat	Centric NAC
▼ Ide	ntities Group	os External Ident	tity Sources	Identity Source Sec	uences					
		G	Networ	k Accase Lleare Liet > 1	New Network Access	Hear				
Users						User				
Latest I	Manual Networ	k Scan Results	* N	etwork access User						
			* Na	ame fxosadmin						
			St	atus 🔽 Enabled 👻]					
			-	mail						
			-	maii						
			* F	Passwords						
			Pa	assword Type: Intern	nal Users	Ŧ				
				Passy	vord		Re-Enter	Password		
			•	ogin Password	•••		•••••			Generate Password
			-							
			E	hable Password						Generate Password
			¥ t	Jser Information						
			Fi	rst Name						
				at Name		_				
			La	ast Name						
			× /	Account Options						
				Desc	ription					
			~							
			C	hange password on nex	a login 🗆					
			× 1	Account Disable Pol	icy					
				Disable account if da	ate exceeds 2018-0	3-01		(уууу-	mm-dd)	
			× t	Jser Groups						
			II (F	XOS ADMIN	<u> </u>					
				Canaal						
			Sub	Cancel						

ステップ 8.必要なすべてのユーザ向けのステップ 6 を繰り返して下さい。

dentity Services Engine	Home + Conte	xt Visibility	Policy Administra	ition 🔹 Work Ce	nters			
System - Identity Management	Network Resources	s	t pxGrid Services + Fe	eed Service + Th	reat Centric NAC			
	y Sources Identity	Source Sequences Setting	S					
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	2 fxosoper					FXOS OPER	
	🗌 🛃 Enabled	👷 fxosro					FXOS Read Only	

各ユーザの役割のための許可プロファイルの作成

ステップ 1.ポリシー > ポリシー要素へのナビゲートは > > 許可 > 許可プロファイル生じます。

dentity Services Engine	Home	 Operations Policy 	Administration Work Centers	
Authentication Authorization Profilin	ng Posture Client Provisioning			
Dictionaries + Conditions - Results	5			
0				
Authentication	Standard Authorization	n Profiles		
h Authorization	For Policy Export go to Admin	istration > System > Backup 8	Restore > Policy Export Page	
P Autorization	/ Edit + Add DyDuplicat	e XDelete		
Authorization Profiles	□ Name		Drofile	- Description
Downloadable ACLs			Prome	Description
b Des fille a	Blackhole_Wireless_Acc	2855	Sta Cisco 🖽	Default profile used to blacklist wireless devices. Ensu
Profiling	Cisco_IP_Phones		🗰 Cisco 🕀	Default profile used for Cisco Phones.
▶ Posture	Cisco_WebAuth		🗱 Cisco 🕀	Default Profile used to redirect users to the CWA port
	NSP_Onboard		🔐 Cisco 🕀	Onboard the device with Native Supplicant Provisioning
Client Provisioning	Non_Cisco_IP_Phones		🗰 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

ステップ 2.許可プロファイルのためのすべての属性を一杯にして下さい。

2.1. Profile Name を設定して下さい。

Authentication Authorization Profilir	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 🛛 🖽 Cisco 👻 🕀				

2.2. 高度属性設定で次の CISCO-AV-PAIR を設定して下さい

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

 Advanced Attributes Settings 		
Cisco:cisco-av-pair	= shell:roles="admin"	◎ - +

2.3. [Save] をクリックします。



ステップ 3.次の Cisco AVペアを使用して残りのユーザの役割のためのステップ 2 を繰り返して

```
下さい
```

cisco-av-pair=shell: roles= " AAA]

cisco-av-pair=shell: roles= "オペレーション」

cisco-av-pair=shell: 」読み取り専用 roles= "

 Advanced Attributes Settings 			
Cisco:cisco-av-pair] =	shell:roles="aaa"	⊘ — ∔

 Advanced Attributes Settings 		
Cisco:cisco-av-pair 📀	= shell:roles="operations"	○ — ⊥

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

-Identity Services Engine	ome Context Visibility Operations Policy	Administration
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 & Re-	store > Policy Export Page
	/ Edit + Add Duplicate	
Authorization Profiles	Name	Drofilo
Downloadable ACLs		Prolie
b Drofiller	Blackhole_wireless_Access	
• Proning	Cisco_IP_Phones	ditto Cisco 🕀
▶ Posture	Cisco_WebAuth	👑 Cisco 🕀
	FXOS-AAA-PROFILE	🚓 Cisco 🕀
Client Provisioning	FXOS-ADMIN-PROFILE	diste Cisco 🕀
	FXOS-OPER-PROFILE	🗱 Cisco 🕀
	FXOS-ReadOnly-PROFILE	disto Cisco 🕀

ステップ 1.**ポリシー > 認証**へのナビゲートは > およびルールをどこに作成したいと思うか矢印をの隣で編集しますクリックします。

relieder Identity Services Engine Hone + Context Vability + Opensions <mark>+ Petroy</mark> + Administration + Work Centers	(1) < 0 < 0 < 0
Authentication Authorization Profiling Posture Client Provisioning + Policy Elements	Click here to do wireless setup and visibility setup Do not show this again. ×
Authentication Policy Define the Authentication Policy Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Epoort ps to Administration > Signitum > Baduets & Restore > Policy Export Page Policy Type ③ Rule-Based	
Default Rule (If no match) : Allow Protocols : Default Network Access and use : DenyAccess	Insert new row above

呼び出します。 設定は簡単です; それはされた粒状である場合もありますが、この例のためにデ バイスの種類を使用します:

[Name]: FXOS 認証ルール

IF は属性/値を『New』 を選択 します: デバイス: デバイスの種類はすべての装置タイプ #FXOS に匹敵します

割り当てプロトコル: デフォルトネットワーク アクセス

使用: 内部ユーザ

 Image: State of the state

承認ポリシーの作成

ステップ 1.**ポリシー > 許可**へのナビゲートは > およびルールをどこに作成したいと思うか編集す るために矢印ネットをクリックします。



ステップ 2.必須パラメータの承認規則の値を入力して下さい。

2.1. [Rule Name]: Fxos <USER ROLE> ルール。



2.2. 条件 ユーザ識別グループ > 選定された <USER ROLE>。

conditions (identity groups and other cond	ditions) Permissions
FX and Condition(s)	수 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

2.3. および: 新しい状態 > デバイスを作成して下さい: デバイスの種類は**すべての装置タイプ** #FXOS に匹敵します。

Conditions (identity groups a	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 ◊ DEVICE:Device Ty ◊ Equals ▼ All Device Types# ◊	
	All Device Types	
(All Device Types#FXOS	
	AD >	
	Airespace >	
	Alcatel-Lucent >	
	Aruba >	
	Brocade >	
	CERTIFICATE >	
	Cisco >	
	Cisco-BBSM >	
	Cisco-VPN3000 >	
	☐ CWA >	

2.4. [Permissions]: 規格は > プロファイル ユーザの役割の選択します

Permissions		
then FXOS-A		
FXOS-ADMIN-PROFILE	o -	
	Standard	
	Blackhole_Wireless_Access	
	Gisco_IP_Phones	
	Cisco_WebAuth	
	C DenyAccess	
	S FXOS-AAA-PROFILE	
	S FXOS-ADMIN-PROFILE	
	S FXOS-OPER-PROFILE	
	STATES FXOS-ReadOnly-PROFILE	
	😪 NSP_Onboard	
	Non_Cisco_IP_Phones	
	PermitAccess	
Status Rule Name	Conditions (identity groups and other conditions) P	ermissions
Fxos Admin Rule If	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device then Types#FXOS	FXOS-ADMIN-PROFILE

ステップ 3.すべてのユーザの役割のためのステップ 2 を繰り返して下さい。

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
~	Fxos Admin Rule	if	FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then	FXOS-ADMIN-PROFILE
~	Fxos AAA Rule	if	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 n	o matches, then DenyAccess		

ステップ 4.ページの一番下に『SAVE』 をクリック して下さい。



確認

今各ユーザをテストし、割り当てられたユーザの役割を確認することができます。

FXOS Chasis 確認

1. FXOS シャーシへの Telnet か SSH および ISE の作成されたユーザの何れかを使用するログ オン。 ユーザ名: fxosadmin

パスワード:

fpr4120-TAC-A# スコープ セキュリティ

fpr4120-TAC-A /security は#リモートユーザ 詳細を示します

リモートユーザ fxosaaa:

説明:

ユーザの役割:

[Name] : AAA

[Name]: 読み取り専用

リモートユーザ fxosadmin:

説明:

ユーザの役割:

[Name] : admin

[Name]: 読み取り専用

リモートユーザ fxosoper:

説明:

ユーザの役割:

[Name]: 操作

[Name]: 読み取り専用

リモートユーザ fxosro:

説明:

ユーザの役割:

[Name]: 読み取り専用

FXOS シャーシ cli 入力されたユーザ名によっては割り当てられたユーザの役割のために承認され たコマンドだけを表示します。

管理者ユーザ ロール。

確認します確認して下さい

オフ ユーザ セッションはユーザセッションを解決します

作成します管理対象オブジェクトを作成して下さい

削除管理対象オブジェクトを削除して下さい

ディセーブル無効サービス

イネーブル有効サービス

入力します管理対象オブジェクトを入力して下さい

スコープは現在のモードを変更します

セットのプロパティ値を設定して下さい

Show system information を示して下さい

アクティブ cimc セッションを終了して下さい

fpr4120-TAC-A# は fxos を接続します

fpr4120-TAC-A (fxos) #デバッグ AAA AAA 要求

fpr4120-TAC-A (fxos) #

読み取り専用ユーザの役割。

fpr4120-TAC-A /security #**b** 。

スコープは現在のモードを変更します

セットのプロパティ値を設定して下さい

Show system information を示して下さい

fpr4120-TAC-A# は fxos を接続します

fpr4120-TAC-A (fxos) #デバッグ AAA AAA 要求

権限%のロールのために否定される

2. ISE の作成されたユーザの何れかを使用して FXOS シャーシ IP アドレスおよびログオンに 参照して下さい。

管理者ユーザ ロール。

Overview Interfaces Logical	I Devices Security Engine Platform	Settings					Syste	m Tools	Help fxosadmin
NTP SSH SNMP HTTPS	LDAP RADIUS TACACS Properties Timeout:* 5 Secs								
Syslog DNS FIPS and Common Criteria Access List	Retries:* 1 RADIUS Providers		Add RADIUS Provider Hostname/FQDN(or IP Address):* Order:*	kwest-available		O AM			
	10.88.244.15	1	Confirm Key: Authorization Pert:* Timeout:* Retries:*	1812 5 Secs 1 OK Cer	ncel	2 9			

読み取り専用ユーザの役割。

Overview In	nterfaces l	Logical C	vevices Security Engine	Platform Settings								
NTP			LDAP RADEUS TACACS									
SSH SNMP			Properties									
HTTPS			Timeout:* 5 Secs									
Syslog			Revise* 1									
FIPS and Come	umon Criteria							0 Add				
Access List			Hostname	Order		Service	Auth Port					
			10.88.244.16	1		authorization	1812	۹.8				

注: Add ボタンが選択不可能になることに注意して下さい。

ISE 2.0 の検証

1. **オペレーション > RADIUS** へのナビゲート **> ライブ ログ。**成功したおよび試行失敗を見ら れますはずです。

dentity Services Engi	ne Home → Context Visibility	y	Administration Work Centers			🚺 🤍 e e e
▼RADIUS Threat-Centric N	AC Live Logs + TACACS + Troubl	leshoot + Adaptive Network Contro	al Reports		Click here to do wireless setup and visibility	setup Do not show this again.
Live Logs Live Sessions						toonap be not onen one ogenn
	Misconfigured Supplicants O	Misconfigured Network Devi	ices 🛛 RADIUS Drops 🛈	Client Stopped Responding O	Repeat Counter O	
	0	0	0	0	0	
				Refresh Never	Show Latest 20 records	Within Last 3 hours
C Refresh O Reset Repe	at Counts 🔮 Export To 🗸					▼ Fiter • • •
Time	Status Details F	Repeat C Identity	Authentication Policy	Authorization Policy Auth	horization Profiles Network Dev	Identity Group
×	•	Identity	Authentication Policy	Authorization Policy Aut	thorization Profiles Network Device	Identity Group
Jan 20, 2018 10:14:09	2	fxosadmin (Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Admin Rule FXO	S-ADMIN-PROFILE FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:13:59	8 là	fxosadmin	Default >> FXOS AUTHENTICATION RULE >> Default		FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:09:01	2	fxosro (Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Read only Rule FXO	S-ReadOnly-PROFILE FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:08:50	o 💿 🚡	fxosro (Default >> FXOS AUTHENTICATION RULE >> Default		FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:06:17	 a 	fxosro (Default >> FXOS AUTHENTICATION RULE >> Default		FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:05:15	o 💿 🚡	fxosro (Default >> FXOS AUTHENTICATION RULE >> Default		FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:04:23	2	fxosadmin	Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Admin Rule FXO	S-ADMIN-PROFILE FXOS	User Identity Groups:FXOS
Jan 20, 2018 10:02:59	2 🔓 🔶	fxosadmin 💠 (Default >> FXOS AUTHENTICATION RULE >> Default	Default >> Fxos Admin Rule FXO	S-ADMIN-PROFILE FXOS	User Identity Groups:FXOS

トラブルシューティング

debug aaa authentication および許可は FXOS cli の次のコマンドを実行します。

fpr4120-TAC-A# は fxos を接続します

fpr4120-TAC-A (fxos) #デバッグ AAA AAA 要求

fpr4120-TAC-A (fxos) #デバッグ AAA イベント

fpr4120-TAC-A (fxos) #デバッグ AAA エラー

fpr4120-TAC-A (fxos) # term mon

認証の成功試みが、次の出力を見た後。

20 年 1 月 2018 日 17:18:02.410275 AAA: 認証のための aaa_req_process。 セッション 0 無し

20 年 1 月 2018 日 17:18:02.410297 AAA: aaa_req_process: appln からの一般 AAA 要求: ログオ ン appln_subtype: デフォルト

20 年 1 月 2018 日 17:18:02.410310 AAA: try_next_aaa_method

20 年 1 月 2018 日 17:18:02.410330 AAA: 設定される総方式は 1、試みられるべき現在のインデ ックスです 0 です

20 年 1 月 2018 日 17:18:02.410344 AAA: handle_req_using_method

20年1月2018日17:18:02.410356 AAA: AAA_METHOD_SERVER_GROUP

20 年 1 月 2018 日 17:18:02.410367 AAA: aaa_sg_method_handler グループ = 半径

20年1月2018日17:18:02.410379 AAA: この機能に通じる sg_protocol の使用

20 年 1 月 2018 日 17:18:02.410393 AAA: RADIUSサービスへ要求を送信 すること

20 年 1 月 2018 日 17:18:02.412944 AAA: mts_send_msg_to_prot_daemon: ペイロード長 = 374

20 年 1 月 2018 日 17:18:02.412973 AAA: セッション: セッション表 1 に追加される 0x8dfd68c

20 年 1 月 2018 日 17:18:02.412987 AAA: 成功する設定された方式グループ

20 年 1 月 2018 日 17:18:02.656425 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:18:02.656447 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:18:02.656470 AAA: mts_message_response_handler: mts 応答

20 年 1 月 2018 日 17:18:02.656483 AAA: prot_daemon_reponse_handler

20年1月2018日17:18:02.656497 AAA: セッション: セッション表0から取除かれる 0x8dfd68c

20 年 1 月 2018 日 17:18:02.656512 AAA: is_aaa_resp_status_success ステータス = 1

20 年 1 月 2018 日 17:18:02.656525 AAA: is_aaa_resp_status_success は TRUE です

20 年 1 月 2018 日 17:18:02.656538 AAA: 認証のための aaa_send_client_response。 session->flags=21. aaa_resp->flags=0.

20 年 1 月 2018 日 17:18:02.656550 AAA: AAA_REQ_FLAG_NORMAL

20 年 1 月 2018 日 17:18:02.656577 AAA: 正常な mts_send_response

20 年 1 月 2018 日 17:18:02.700520 AAA: aaa_process_fd_set: aaa_accounting_q の mtscallback

20 年 1 月 2018 日 17:18:02.700688 AAA: 古いオペレーション コード: accounting_interim_update

20 年 1 月 2018 日 17:18:02.700702 AAA: aaa_create_local_acct_req: user=、session_id=、 log=added ユーザ fxosro

20 年 1 月 2018 日 17:18:02.700725 AAA: 説明のための aaa_req_process。 セッション 0 無し

20 年 1 月 2018 日 17:18:02.700738 AAA: MTS 要求参照は NULL です。 ローカル要求

20 年 1 月 2018 日 17:18:02.700749 AAA: AAA_REQ_RESPONSE_NOT_NEEDED の設定

20 年 1 月 2018 日 17:18:02.700762 AAA: aaa_req_process: appln からの一般 AAA 要求: デフォ ルト appln_subtype: デフォルト

20 年 1 月 2018 日 17:18:02.700774 AAA: try_next_aaa_method

20 年 1 月 2018 日 17:18:02.700798 AAA: デフォルト デフォルトのために設定される方式無し

20 年 1 月 2018 日 17:18:02.700810 AAA: これのために利用可能な設定無し要求

20 年 1 月 2018 日 17:18:02.700997 AAA: 説明のための aaa_send_client_response。 session->flags=254. aaa_resp->flags=0.

20 年 1 月 2018 日 17:18:02.701010 AAA: 古いライブラリの説明要求のための応答は成功として 返されます

20 年 1 月 2018 日 17:18:02.701021 AAA: この要求のために必要とされない応答

20 年 1 月 2018 日 17:18:02.701033 AAA: AAA_REQ_FLAG_LOCAL_RESP

20 年 1 月 2018 日 17:18:02.701044 AAA: aaa_cleanup_session

20 年 1 月 2018 日 17:18:02.701055 AAA: aaa_req は解放する必要があります。

20 年 1 月 2018 日 17:18:02.701067 AAA: 成功するフォール バック方式ローカル

20 年 1 月 2018 日 17:18:02.706922 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:18:02.706937 AAA: aaa_process_fd_set: aaa_accounting_q の mtscallback

20 年 1 月 2018 日 17:18:02.706959 AAA: 古いオペレーション コード: accounting_interim_update

20 年 1 月 2018 日 17:18:02.706972 AAA: aaa_create_local_acct_req: user=、session_id=、 log=added ユーザ: ロールへの fxosro: 読み取り専用

失敗した認証試みが、次の出力を見た後。

20 年 1 月 2018 日 17:15:18.102130 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:15:18.102149 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:15:18.102267 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:15:18.102281 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:15:18.102363 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:15:18.102377 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:15:18.102456 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:15:18.102468 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:15:18.102489 AAA: mts_aaa_req_process

20 年 1 月 2018 日 17:15:18.102503 AAA: 認証のための aaa_req_process。 セッション 0 無し

20 年 1 月 2018 日 17:15:18.102526 AAA: aaa_req_process: appln からの一般 AAA 要求: ログオ ン appln_subtype: デフォルト

20 年 1 月 2018 日 17:15:18.102540 AAA: try_next_aaa_method

20 年 1 月 2018 日 17:15:18.102562 AAA: 設定される総方式は 1、試みられるべき現在のインデックスです 0 です

20 年 1 月 2018 日 17:15:18.102575 AAA: handle_req_using_method

20 年 1 月 2018 日 17:15:18.102586 AAA: AAA_METHOD_SERVER_GROUP

20 年 1 月 2018 日 17:15:18.102598 AAA: aaa_sg_method_handler グループ = 半径

20 年 1 月 2018 日 17:15:18.102610 AAA: この機能に通じる sg_protocol の使用

20 年 1 月 2018 日 17:15:18.102625 AAA: RADIUSサービスへ要求を送信 すること

20 年 1 月 2018 日 17:15:18.102658 AAA: mts_send_msg_to_prot_daemon: ペイロード長 = 371

20年1月2018日17:15:18.102684 AAA: セッション: セッション表1に追加される 0x8dfd68c

20 年 1 月 2018 日 17:15:18.102698 AAA: 成功する設定された方式グループ

20 年 1 月 2018 日 17:15:18.273682 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:15:18.273724 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:15:18.273753 AAA: mts_message_response_handler: mts 応答

20 年 1 月 2018 日 17:15:18.273768 AAA: prot_daemon_reponse_handler

20 年 1 月 2018 日 17:15:18.273783 AAA: セッション: セッション表 0 から取除かれる 0x8dfd68c

20 年 1 月 2018 日 17:15:18.273801 AAA: is_aaa_resp_status_success ステータス = 2

20 年 1 月 2018 日 17:15:18.273815 AAA: is_aaa_resp_status_success は TRUE です

20 年 1 月 2018 日 17:15:18.273829 AAA: 認証のための aaa_send_client_response。 session->flags=21. aaa_resp->flags=0.

20 年 1 月 2018 日 17:15:18.273843 AAA: AAA_REQ_FLAG_NORMAL

20 年 1 月 2018 日 17:15:18.273877 AAA: 正常な mts_send_response

20 年 1 月 2018 日 17:15:18.273902 AAA: aaa_cleanup_session

20 年 1 月 2018 日 17:15:18.273916 AAA: 要求メッセージの mts_drop

20 年 1 月 2018 日 17:15:18.273935 AAA: aaa_req は解放する必要があります。

20 年 1 月 2018 日 17:15:18.280416 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:15:18.280443 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:15:18.280454 AAA: aaa_enable_info_config: AAA Login エラーメッセージ のための GET_REQ

20 年 1 月 2018 日 17:15:18.280460 AAA: 設定 オペレーションの戻り値を取得される: 未知セキ ュリティ項目

関連情報

FX-OS cli の Ethanalyzer コマンドはパスワードのパスワードのために TACACS/RADIUS 認証が イネーブルになっているときプロンプト表示します。 この動作はバグによって引き起こされます 。

バグID: <u>CSCvg87518</u>