

Systeme d'exploitation extensible de FirePOWER (FXOS) 2.2 : Authentification et autorisation de châssis pour la gestion à distance avec ACS utilisant RADIUS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurer le châssis FXOS](#)

[Configurer le serveur ACS](#)

[Vérifiez](#)

[Vérification de châssis FXOS](#)

[Vérification ACS](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification et l'autorisation de RADIUS pour le châssis du système d'exploitation extensible de FirePOWER (FXOS) par l'intermédiaire du serveur de contrôle d'accès (ACS).

Le châssis FXOS inclut les rôles de l'utilisateur suivants :

- Administrateur - Complete lecture-et-écrivent l'accès au système entier. Le compte par défaut d'admin est assigné ce rôle par défaut et il ne peut pas être changé.
- En lecture seule - Accès en lecture seule à la configuration de système sans des privilèges de modifier l'état du système.
- Des exécutions - Lecture-et-écrivez l'accès à la configuration de NTP, à la configuration de Smart Call Home pour l'autorisation intelligente, et aux logs système, y compris des serveurs de Syslog et des défauts. Accès en lecture au reste du système.
- AAA - Lecture-et-écrivez l'accès aux utilisateurs, aux rôles, et à la configuration d'AAA. Accès en lecture au reste du système.

Par l'intermédiaire du CLI ceci peut être vu comme suit :

```
fpr4120-TAC-A /security * # show role
```

Rôle :

Role name Priv

----- ----

AAA d'AAA

admin d'admin

exécutions d'exécutions

en lecture seule en lecture seule

Contribué par Ramirez élégant, Jose Soto, ingénieurs TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du système d'exploitation extensible de FirePOWER (FXOS)
- La connaissance de la configuration ACS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2.2 d'appareils de Sécurité de Cisco FirePOWER 4120
- Version 5.8.0.32 virtuelle de serveur de contrôle d'accès de Cisco

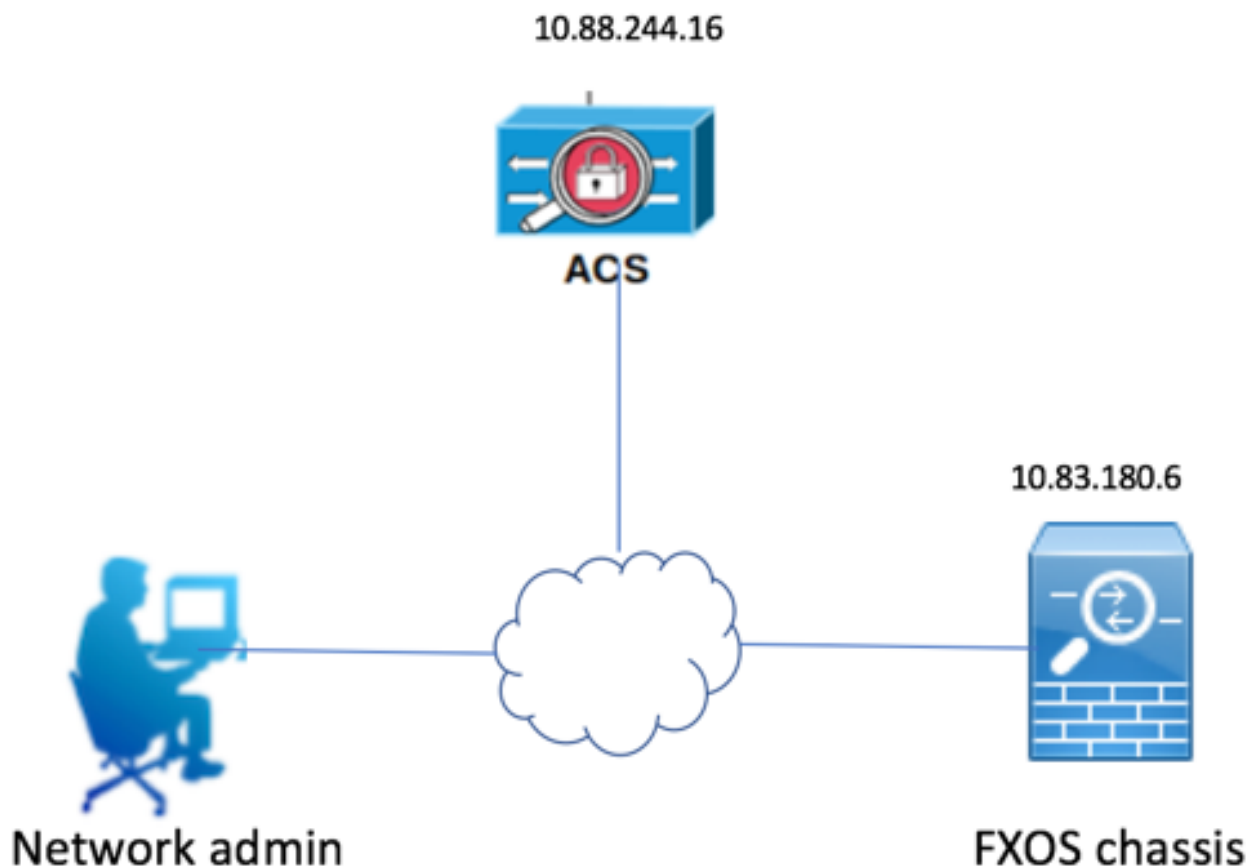
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Le but de la configuration est à :

- Authentifiez les utilisateurs se connectant dans le GUI du Web du FXOS et le SSH au moyen d'ACS.
- Autorisez les utilisateurs se connectant dans le GUI du Web du FXOS et le SSH selon leur rôle de l'utilisateur respectif au moyen d'ACS.
- Vérifiez le bon fonctionnement de l'authentification et de l'autorisation sur le FXOS au moyen d'ACS.

Diagramme du réseau



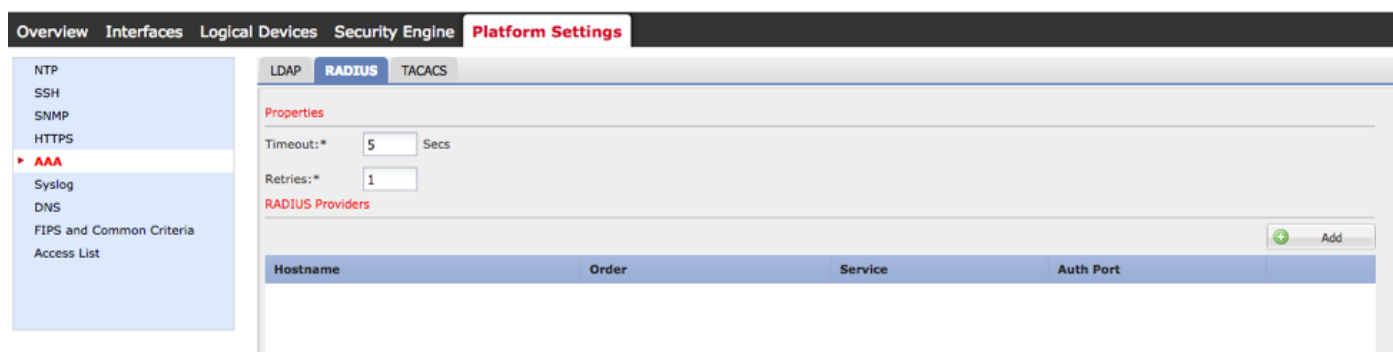
Configurations

Configurer le châssis FXOS

Création d'un fournisseur de RADIUS utilisant le gestionnaire de châssis

Étape 1. Naviguez vers des configurations > l'AAA de plate-forme.

Étape 2. Cliquez sur l'onglet de RADIUS.



Étape 3. Pour chaque fournisseur de RADIUS que vous voulez ajouter (jusqu'à 16 fournisseurs).

3.1. Dans la région de fournisseurs de RADIUS, cliquez sur Add.

3.2. Dans la boîte de dialogue de fournisseur de RADIUS d'ajouter, écrivez les valeurs requises.

3.3. Cliquez sur OK pour fermer la boîte de dialogue de fournisseur de RADIUS d'ajouter.

Add RADIUS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set:No

Confirm Key:

Authorization Port:*

Timeout:* Secs

Retries:*

Étape 4. Sauvegarde de clic.

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
▶ **AAA**
Syslog
DNS
FIPS and Common Criteria
Access List

LDAP **RADIUS** TACACS

Properties

Timeout:* Secs

Retries:*

RADIUS Providers

Hostname	Order	Service	Auth Port	
10.88.244.16	1	authorization	1812	

Étape 5. Naviguez vers le système > la gestion des utilisateurs > les configurations.

Étape 6. Sous l'authentification par défaut choisissez RADIUS.

Overview Interfaces Logical Devices Security Engine Platform Settings

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication: *Local is fallback authentication method

Console Authentication:

Remote User Settings

Remote User Role Policy: Assign Default Role No-Login

Création d'un fournisseur de RADIUS utilisant le CLI

Étape 1. Afin d'activer l'authentification de RADIUS, exécutez les commandes suivantes.

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # **par défaut-auth de portée**

fpr4120-TAC-A /security/default-auth # **a placé le rayon de royaume**

Étape 2. Utilisez la commande de **détail d'exposition** d'afficher les résultats.

fpr4120-TAC-A /security/default-auth # **détail d'exposition**

Authentification par défaut :

Royaume d'admin : **Radius**

Royaume opérationnel : **Radius**

La session Web régénèrent la période (en quelques sec) : 600

Délai d'attente de session (en quelques sec) pour le Web, ssh, sessions de telnet : 600

Délai d'attente de session absolu (en quelques sec) pour le Web, ssh, sessions de telnet : 3600

Délai d'attente de session de console série (en quelques sec) : 600

Délai d'attente de session absolu de console série (en quelques sec) : 3600

Groupe de serveurs d'authentification d'admin :

Groupe de serveurs opérationnel d'authentification :

Utilisation de 2ème facteur : Non

Étape 3. Afin de configurer des paramètres de serveur de RADIUS exécutez les commandes suivantes.

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # **rayon de portée**

fpr4120-TAC-A /security/radius # **présentent le serveur 10.88.244.16**

fpr4120-TAC-A /security/radius/server # **a placé le descr « serveur ISE »**

fpr4120-TAC-A /security/radius/server * # **placez la clé**

Introduisez la clé : *********

Confirmez la clé : *********

Étape 4. Utilisez la commande de **détail d'exposition** d'afficher les résultats.

```
fpr4120-TAC-A /security/radius/server * # détail d'exposition
```

Serveur de RADIUS :

Adresse Internet, FQDN ou adresse IP : 10.88.244.16

Descr :

Commande : 1

Port authentique : 1812

Clé : ****

Délai d'attente : 5

Configurer le serveur ACS

Ajouter le FXOS comme ressource de réseau

Étape 1. Naviguez vers des **ressources de réseau > des périphériques de réseau et des clients d'AAA**.

Étape 2. Le clic **créent**.

My Workspace

Network Resources

- Network Device Groups
 - Location
 - Device Type
 - Network Devices and AAA Clients**
 - Default Network Device
 - External Proxy Servers
 - OCSP Services
- Users and Identity Stores
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration

Network Resources > Network Devices and AAA Clients

Network Devices

Filter: Match if: Go

<input type="checkbox"/>	Name	IP Address	Description	NDG:Location	NDG:Device Type
<input type="checkbox"/>	APIC1P1	10.88.247.4/32		All Locations	All Device Types
<input type="checkbox"/>	APIC1P22	10.48.22.69/32		All Locations	All Device Types
<input type="checkbox"/>	ASA	10.88.244.12/32		All Locations	All Device Types
<input type="checkbox"/>	ASA_10.88.244.60	10.88.244.60/32	ASA_10.88.244.60	All Locations	All Device Types
<input type="checkbox"/>	Firesight	10.88.244.11/32		All Locations	All Device Types
<input type="checkbox"/>	FMC 6.1	10.88.244.51/32		All Locations	All Device Types
<input type="checkbox"/>	FXQS	10.83.180.6/32		All Locations	All Device Types

Create Duplicate Edit Delete | File Operations Export

Étape 3. Écrivez les valeurs requises (le nom, l'adresse IP, le type de périphérique et l'enable RADIUS et ajoutent la CLÉ).

Name:

Description:

Network Device Groups

Location

Device Type

IP Address

Single IP Address IP Subnets IP Range(s)

IP:

Authentication Options

▼ TACACS+

Shared Secret:

Single Connect Device

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

▼ RADIUS

Shared Secret:

CoA port:

Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format ASCII HEXADECIMAL

 = Required fields

Étape 4. Cliquez sur Submit.

