Système d'exploitation extensible de FirePOWER (FXOS) 2.2 : Authentification et autorisation de châssis pour la gestion à distance avec ACS utilisant TACACS+.

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 TACACS+ 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 Remirez 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

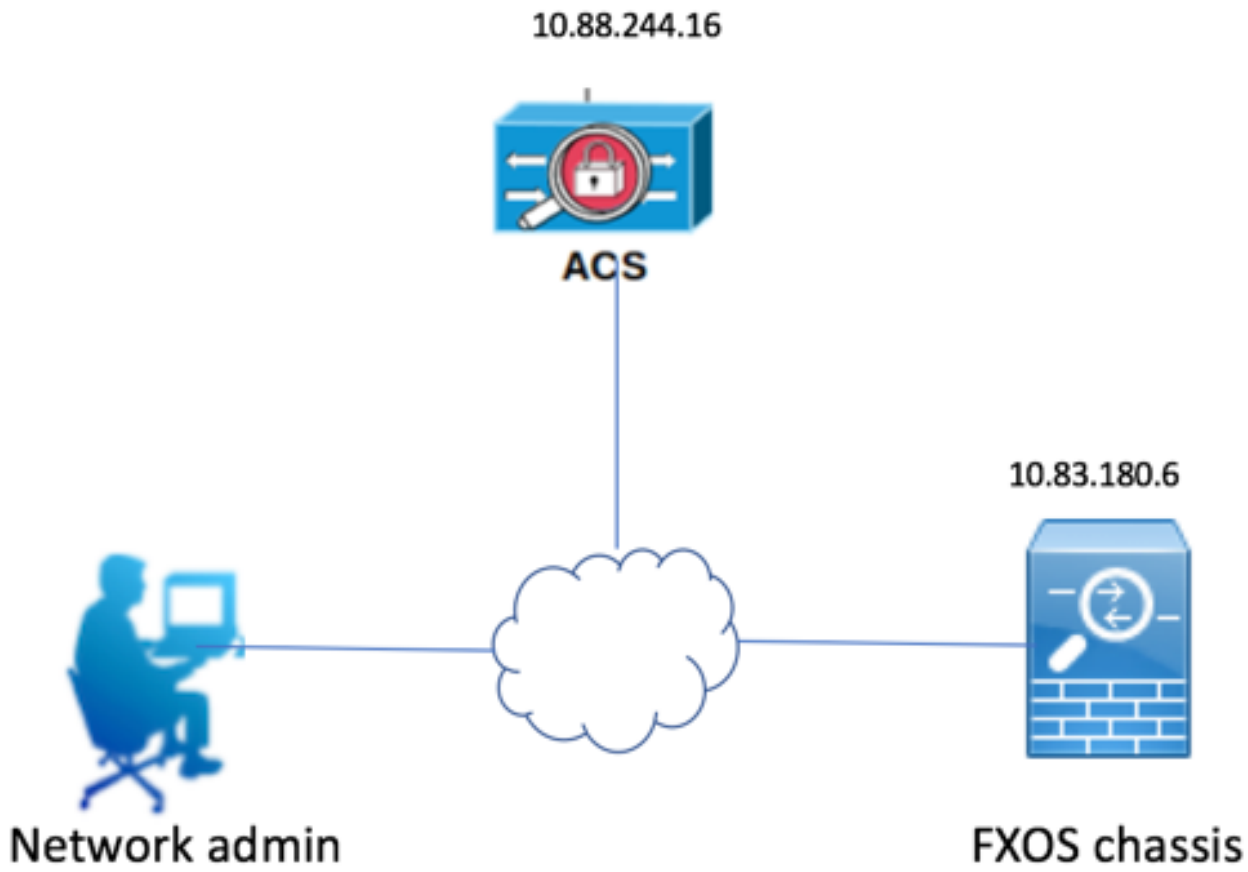
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez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



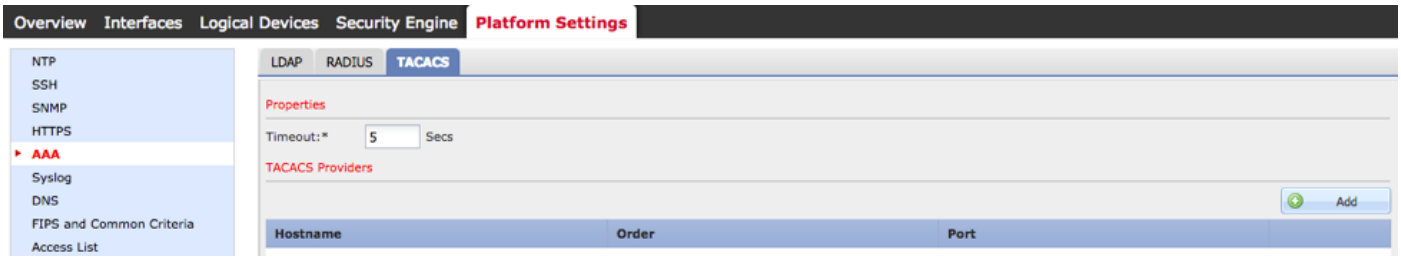
Configurations

Configurer le châssis FXOS

Création d'un fournisseur TACACS utilisant le gestionnaire de châssis

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

Étape 2. Cliquez sur l'onglet **TACACS**.

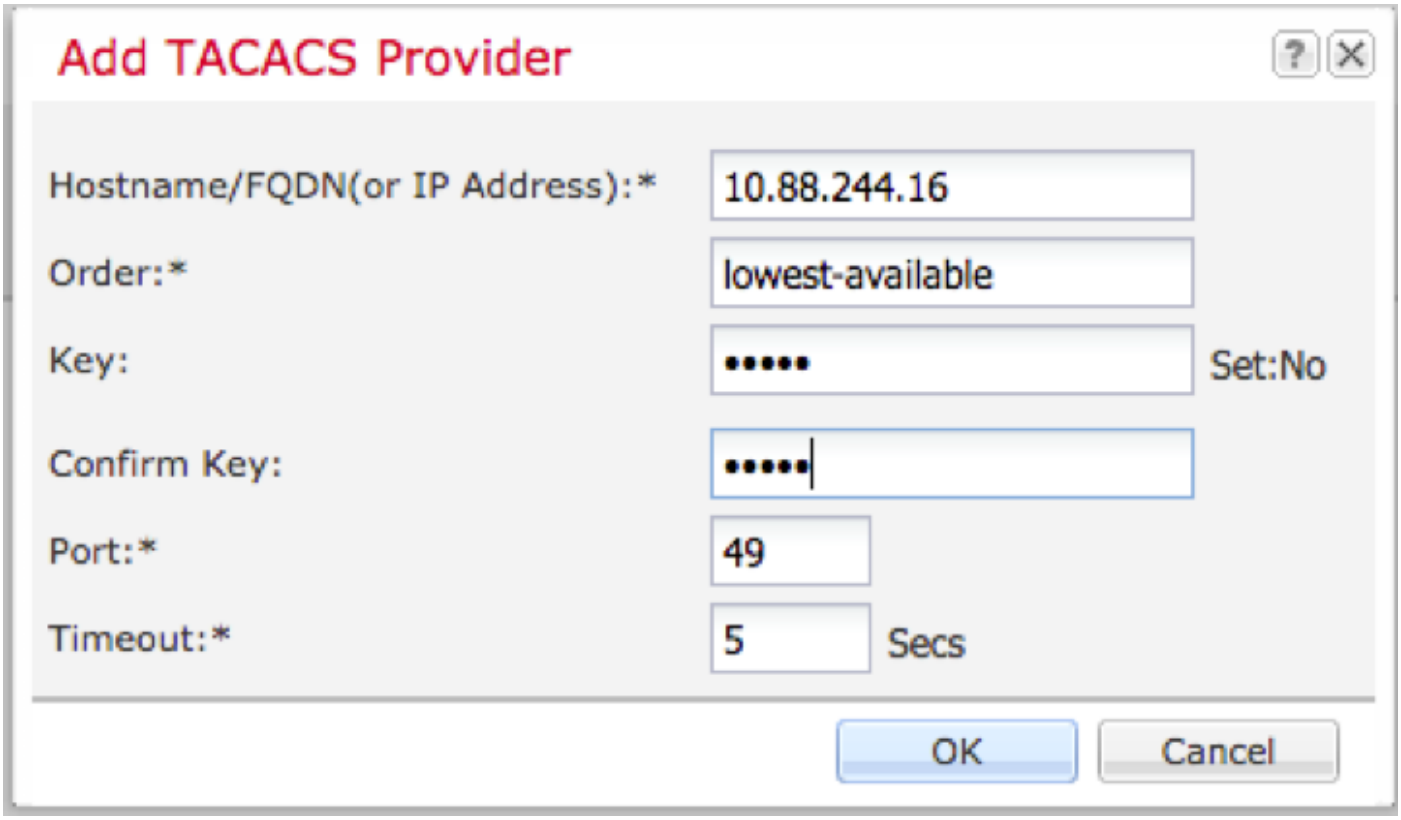


Étape 3. Pour chaque fournisseur TACACS+ que vous voulez ajouter (jusqu'à 16 fournisseurs).

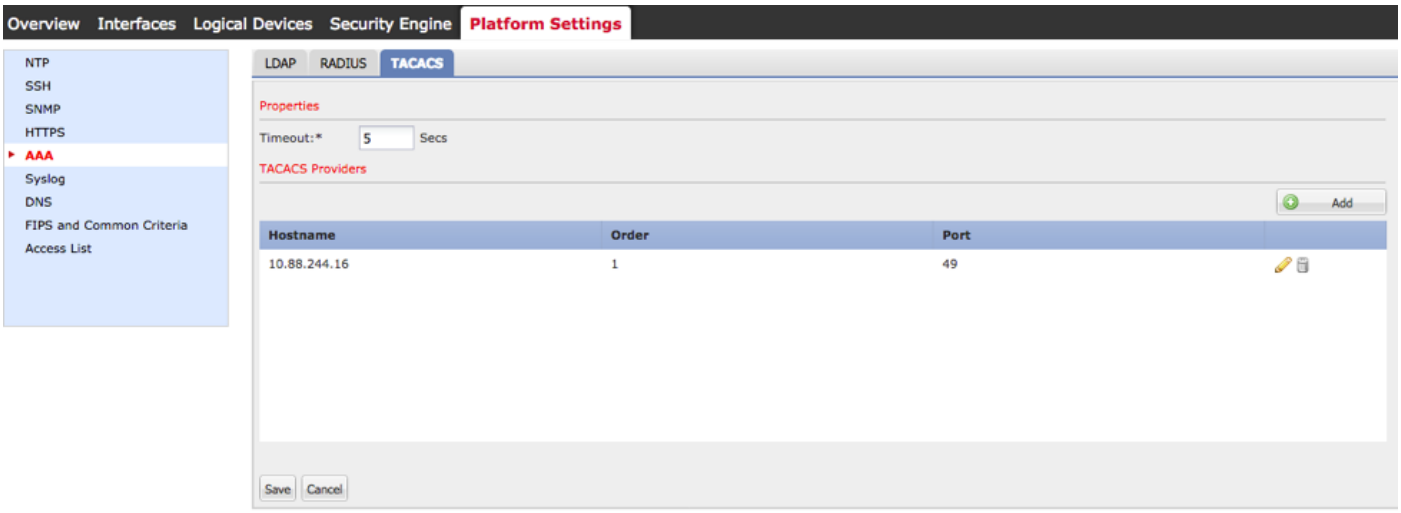
3.1. Dans la région de fournisseurs TACACS, cliquez sur Add.

3.2. Dans la boîte de dialogue de fournisseur de l'ajouter TACACS, écrivez les valeurs requises.

3.3. Cliquez sur OK pour fermer la boîte de dialogue de fournisseur de l'ajouter TACACS.

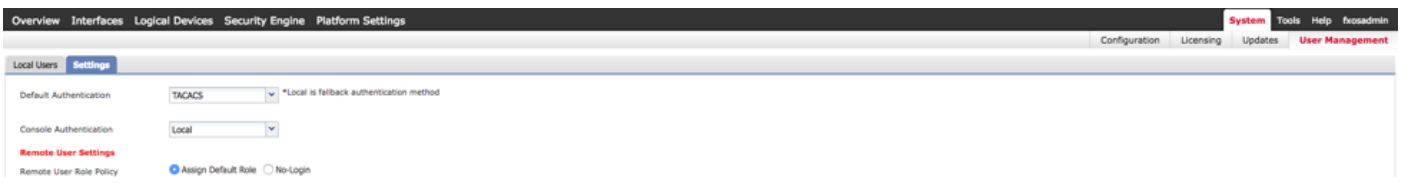


Étape 4. **Sauvegarde de** clic.



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

Étape 6. Sous l'authentification par défaut choisissez **TACACS**.



Création d'un fournisseur TACACS+ utilisant le CLI

Étape 1. Afin d'activer l'authentification TACACS 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 des tacacs 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 : **Tacacs**

Royaume opérationnel : **Tacacs**

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 TACACS exécutez les commandes suivantes.

Sécurité de portée fpr4120-TAC-A#

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

fpr4120-TAC-A /security/tacacs # **présentent le serveur 10.88.244.50**

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

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

Serveur TACACS+ :

Adresse Internet, FQDN ou adresse IP : 10.88.244.50

Descr :

Commande : 1

Port : 49

Clé : ****

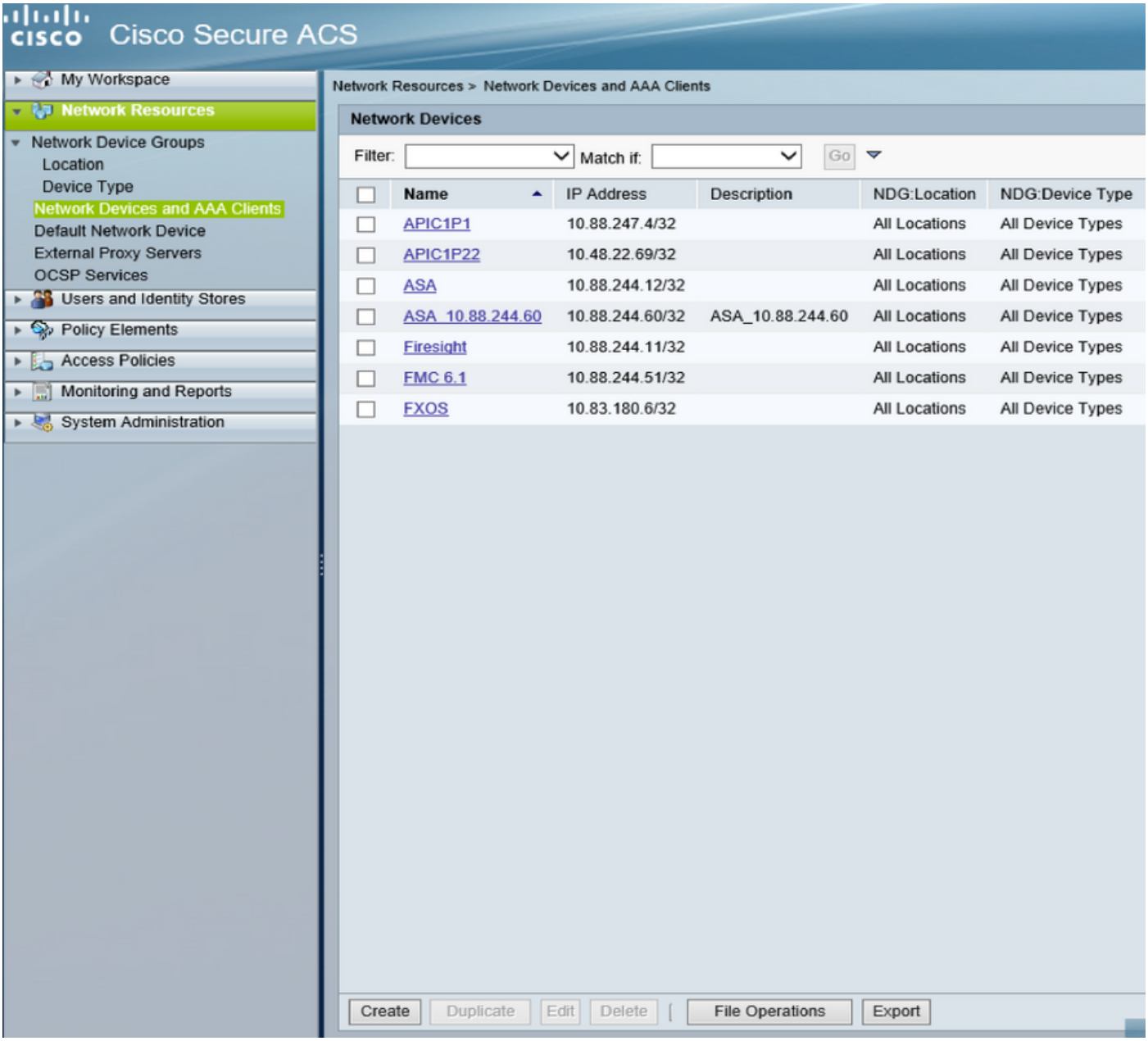
Délai d'attente : 5

Configurer le serveur ACS

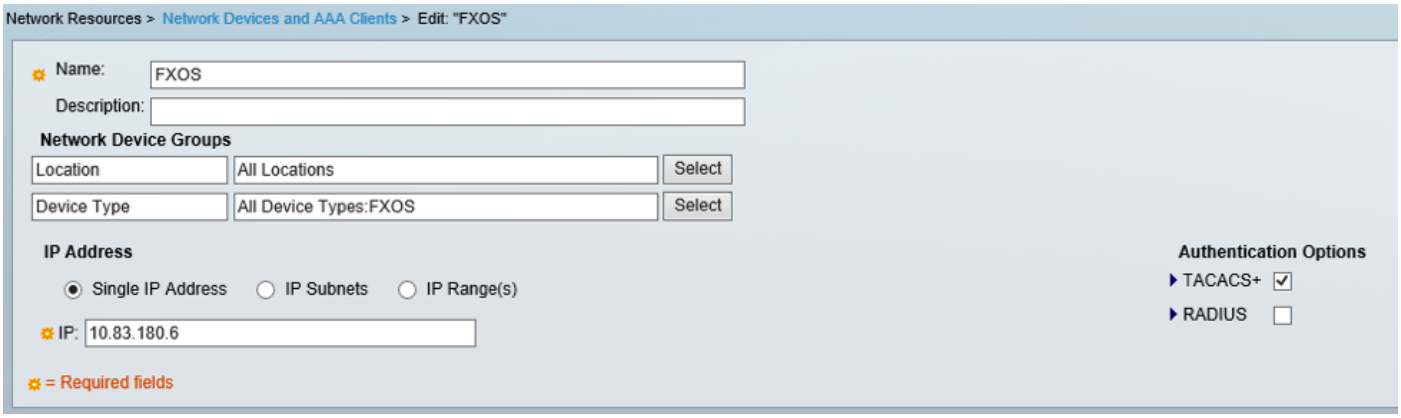
Ajouter le FXOS comme ressource de réseau

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

Étape 2. Le clic **créent.**



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



Étape 4. Cliquez sur Submit.