Firepower可扩展操作系统(FXOS)2.2:使用TACACS+的ACS进行远程管理的机箱身份验证和授权。

目录

简介

本文档介绍如何通过访问控制服务器(ACS)为Firepower可扩展操作系统(FXOS)机箱配置TACACS+身份验证和授权。

FXOS机箱包括以下用户角色：

- 管理员 — 完成对整个系统的读写访问。默认管理员帐户默认分配此角色，且无法更改。
- 只读 — 对系统配置的只读访问，无权修改系统状态。
- 操作 — 对NTP配置、智能许可的Smart Call Home配置和系统日志（包括系统日志服务器和故障）的读写访问。读取系统其余部分的访问权限。
- AAA — 对用户、角色和AAA配置的读写访问。读取系统其余部分的访问权限。

通过CLI，可以看到如下内容：

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

角色：

角色名称优先级

—

aaa

管理员

运营

只读只读只读

作者：Tony Remirez、Jose Soto，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower可扩展操作系统(FXOS)知识
- ACS配置知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Firepower 4120安全设备版本2.2
- 虚拟思科访问控制服务器版本5.8.0.32

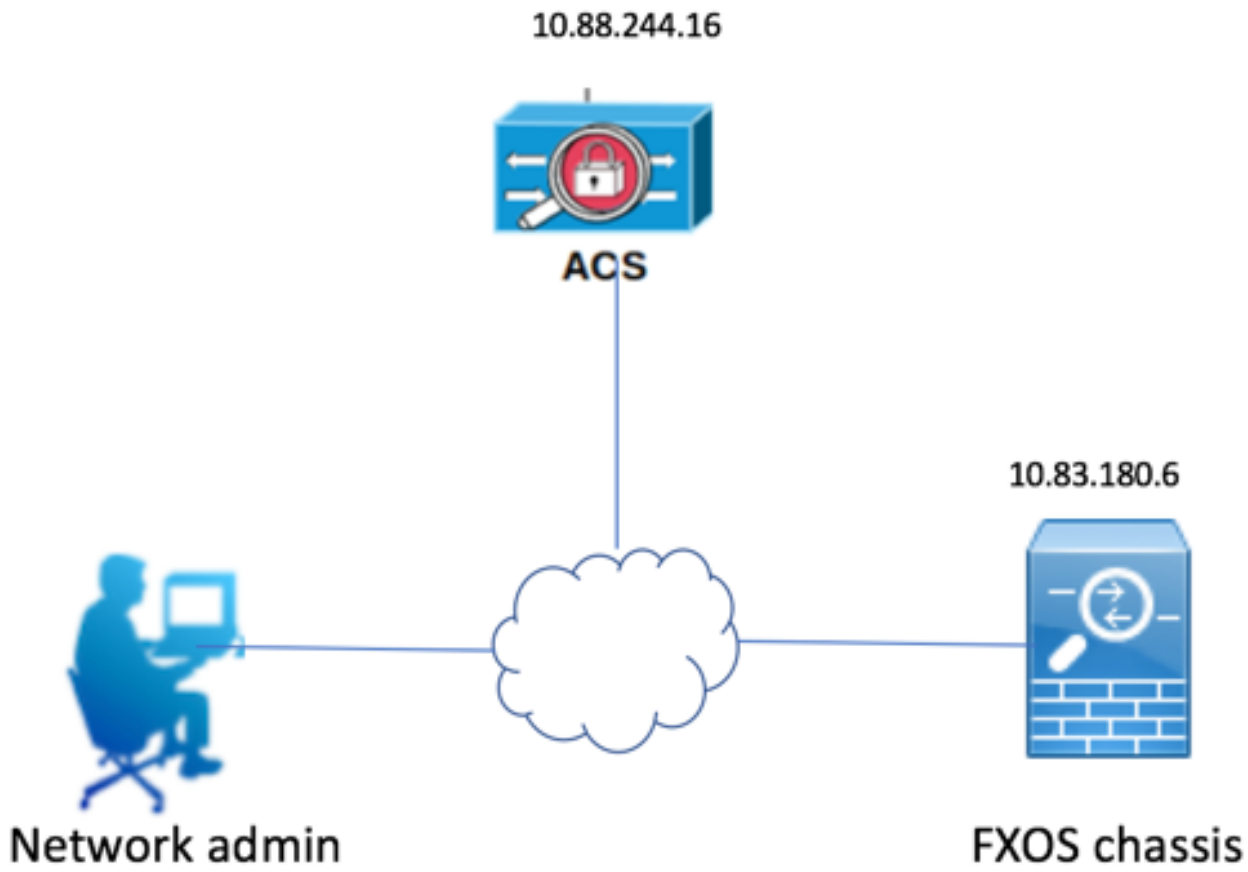
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

配置的目标是：

- 通过ACS对登录FXOS基于Web的GUI和SSH的用户进行身份验证。
- 通过ACS根据用户角色，授权用户登录FXOS基于Web的GUI和SSH。
- 通过ACS验证FXOS上身份验证和授权的正确操作。

网络图



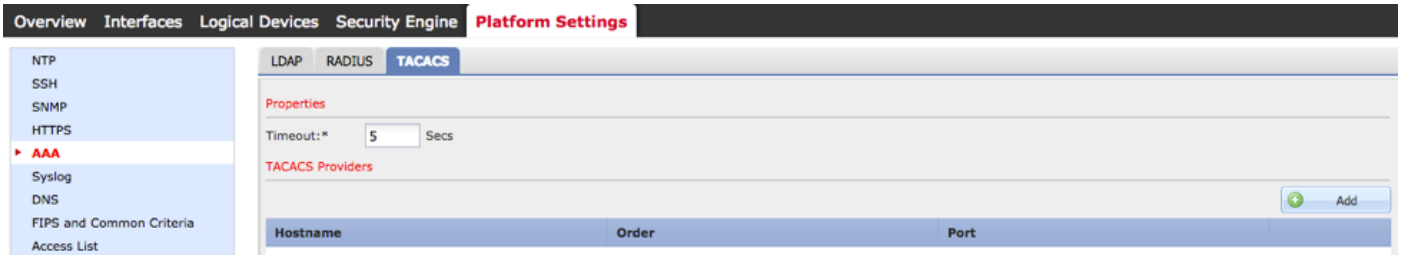
配置

配置FXOS机箱

使用机箱管理器创建TACACS提供程序

步骤1.导航至**Platform Settings > AAA。**

步骤2.单击TACACS**选项**卡。

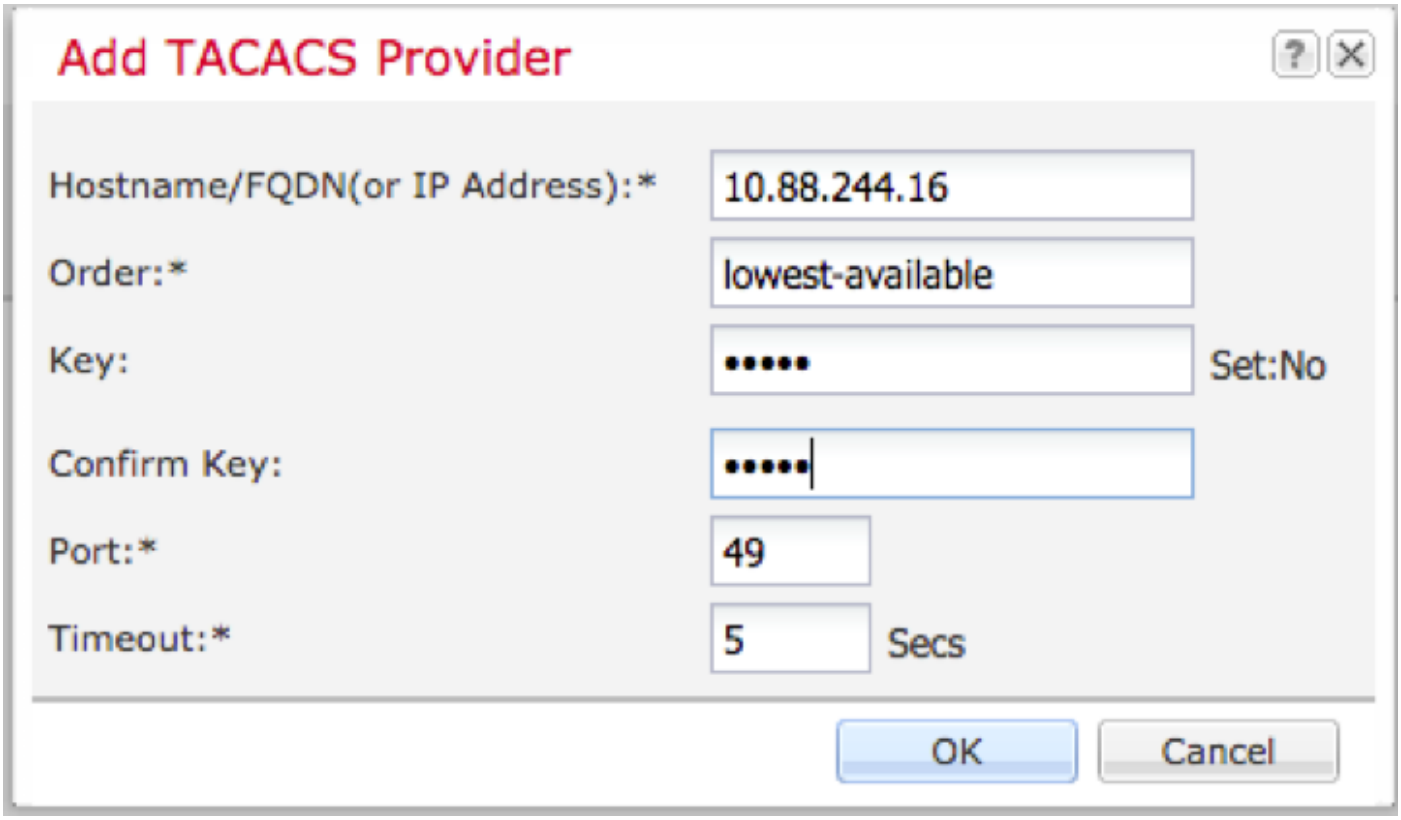


步骤3.对于要添加的每个TACACS+提供程序（最多16个提供程序）。

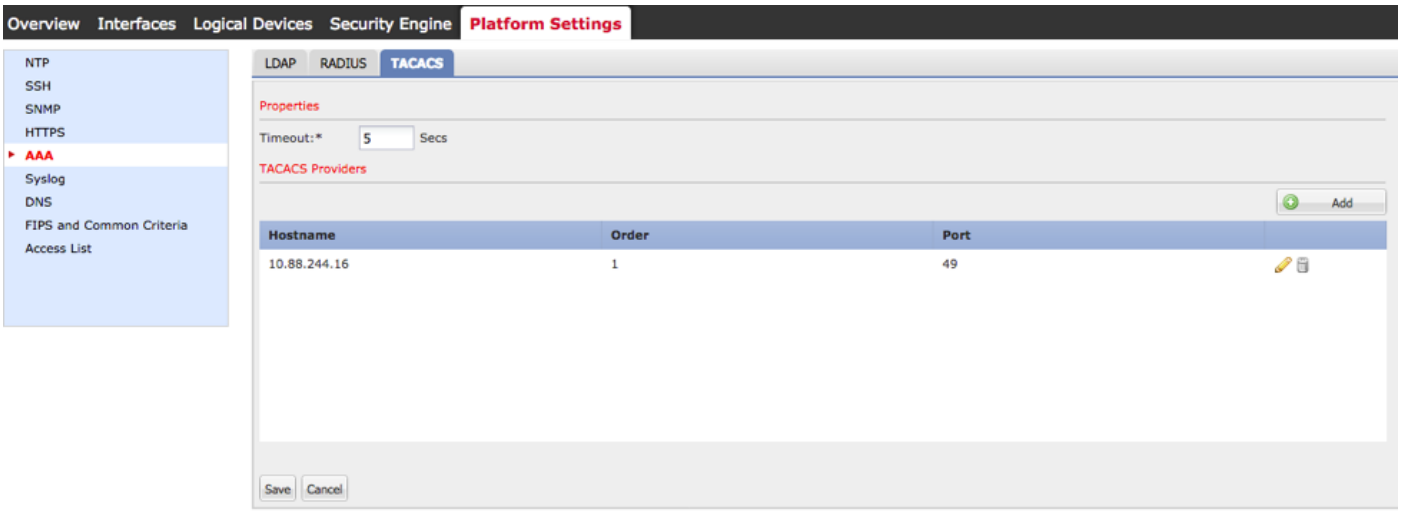
3.1.在TACACS提供程序区域中，单击**添加。**

3.2.在“添加TACACS提供程序”对话框中，输入所需的值。

3.3.单击“**确定**”关闭“添加TACACS提供程序”对话框。

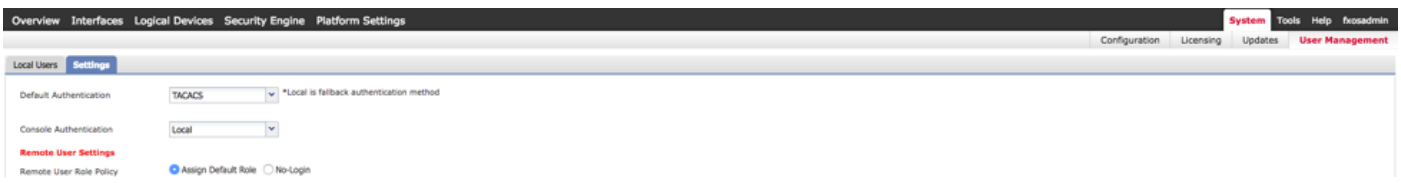


步骤4.单击“保**存**”。



步骤5.导航至**System > User Management > Settings**。

步骤6.在Default Authentication下，选择**TACACS**。



使用CLI创建TACACS+提供程序

步骤1.要启用TACACS身份验证，请运行以下命令。

fpr4120-TAC-A#范围**安全**

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

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

步骤2.使用**show detail**命令显示结果。

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

默认身份验证：

管理领域：**塔卡奇**

运营领域：**塔卡奇**

Web会话刷新期（秒）：600

Web、ssh、telnet会话的会话超时（秒）：600

Web、ssh、telnet会话的绝对会话超时（秒）：3600

串行控制台会话超时（秒）：600

串行控制台绝对会话超时（秒）：3600

管理员身份验证服务器组：

操作身份验证服务器组：

第2因素的使用：无

步骤3.要配置TACACS服务器参数，请运行以下命令。

fpr4120-TAC-A#范围**安全**

fpr4120-TAC-A /security # **scope tacacs**

fpr4120-TAC-A /security/tacacs #**输入server 10.88.244.50**

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

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

输入密钥：******

确认密钥：******

步骤4.使用**show detail**命令显示结果。

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

TACACS+ 服务器:

主机名、FQDN或IP地址：10.88.244.50

描述：

订单：1

端口：49

密钥:****

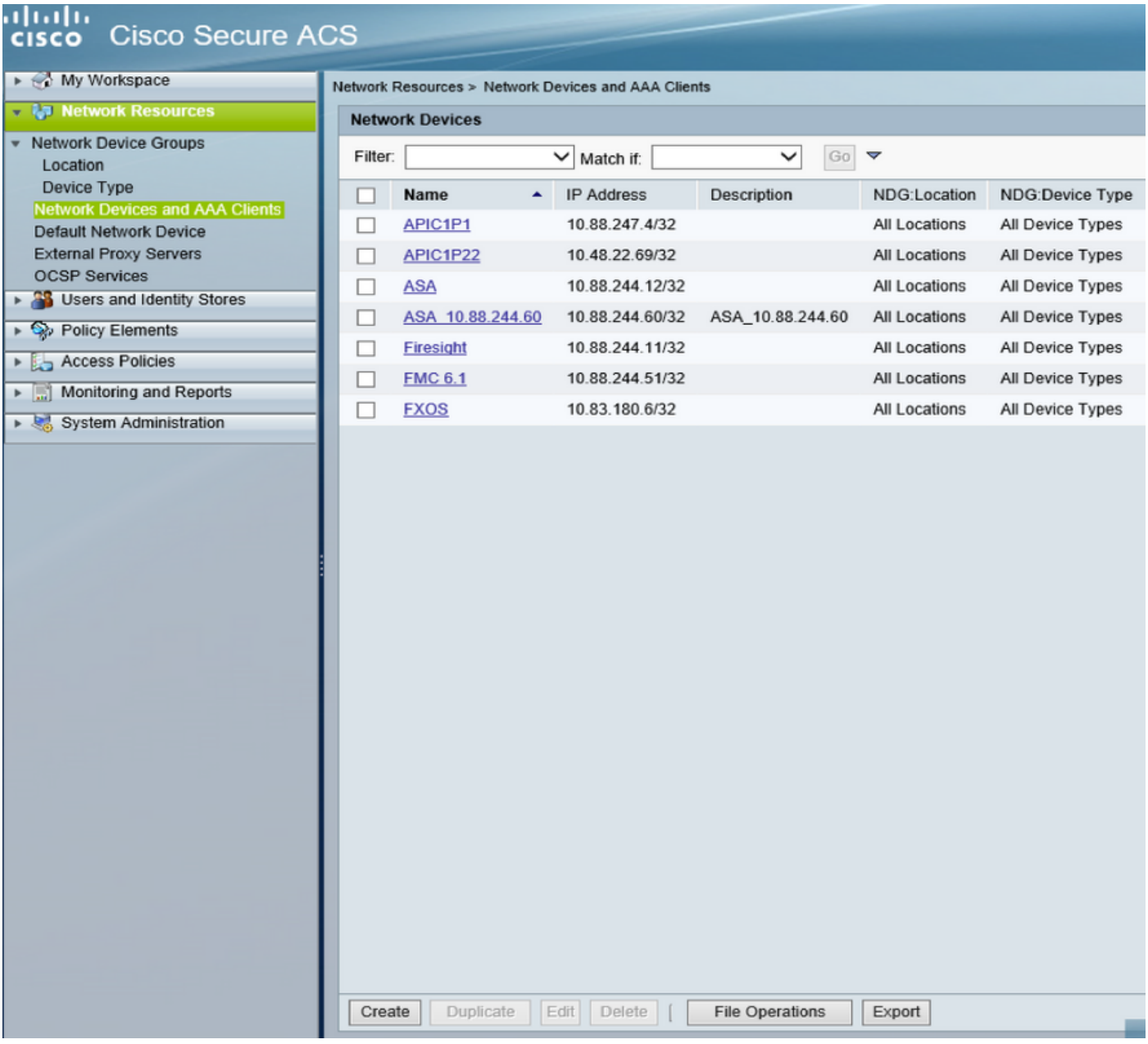
超时：5

配置ACS服务器

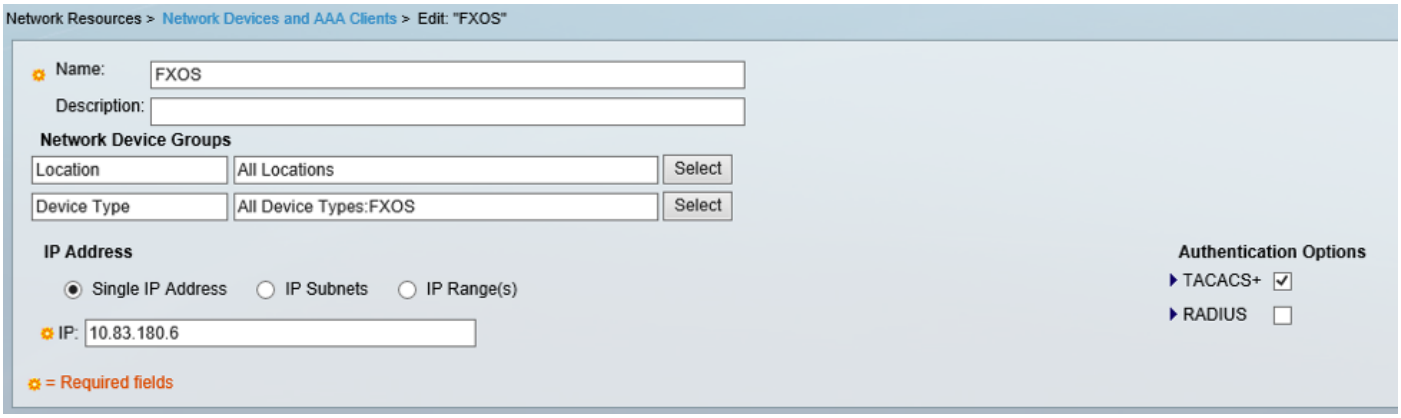
将FXOS添加为网络资源

步骤1.导航至**Network Resources > Network Devices and AAA Clients**。

步骤2.单击“创**建”。**



步骤3.输入所需的值（Name、IP Address、Device Type和Enable TACACS+并添加KEY）。


Network Resources > Network Devices and AAA Clients > Edit: "FXOS"
Name: FXOS
Description:
Network Device Groups
Location
All Locations
Select
Device Type
All Device Types:FXOS
Select
IP Address
Single IP Address
IP Subnets
IP Range(s)
IP: 10.83.180.6
= Required fields
Authentication Options
TACACS+
RADIUS

步骤4.单击“提交”。