Firepower eXtensible Operating System(FXOS)2.2:TACACS+を使用したACSによるリモート管理のためのシャーシ認証と許可

内容

概要

このドキュメントでは、アクセスコントロールサーバ(ACS)を介してFirepower eXtensible Operating System(FXOS)シャーシのTACACS+認証および認可を設定する方法について説明します。

FXOSシャーシには、次のユーザロールが含まれます。

- 管理者：システム全体への読み取り/書き込みアクセスを完了します。デフォルトの管理者アカウントにはデフォルトでこのロールが割り当てられ、変更できません。
- 読み取り専用：システムの状態を変更する権限のない、システム設定への読み取り専用アクセス。
- 操作：NTP設定、スマートライセンス用のSmart Call Home設定、システムログ（syslogサーバと障害を含む）への読み取りと書き込みのアクセス。システムの残りの部分への読み取りアクセス。
- AAA：ユーザ、ロール、およびAAA設定への読み取りおよび書き込みアクセス。システムの残りの部分への読み取りアクセス。

CLIでは、次のように表示できます。

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

ロール：

ロール名の特権

— —

aaa

admin admin

運用業務

読み取り専用

著者：Cisco TACエンジニア、Tony Remirez、Jose Soto

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower eXtensible Operating System(FXOS)に関する知識
- ACS設定に関する知識

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いています。

- Cisco Firepower 4120セキュリティアプライアンスバージョン2.2
- 仮想Cisco Access Control Serverバージョン5.8.0.32

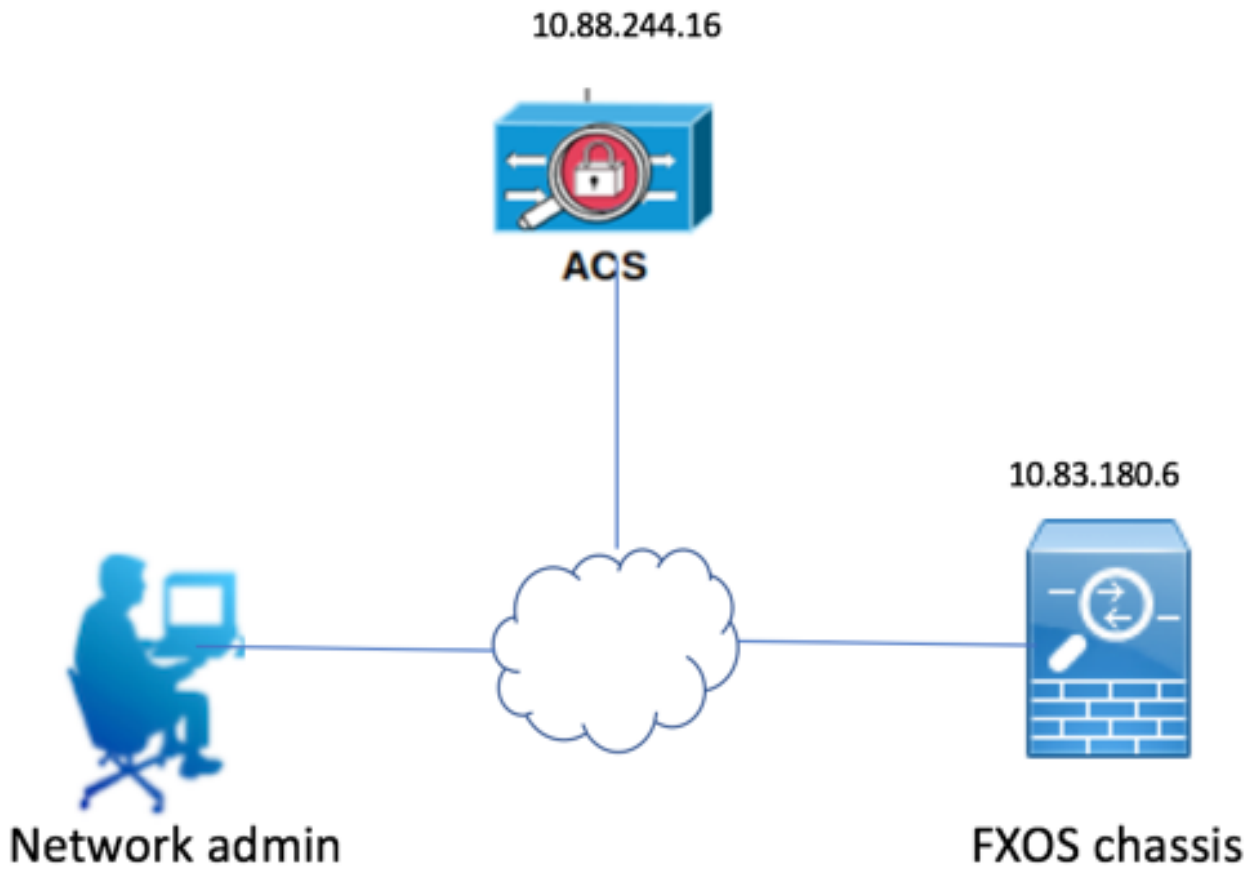
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

設定の目的は次のとおりです。

- ACSを使用して、FXOSのWebベースGUIおよびSSHにログインするユーザを認証します。
- ACSを使用して、FXOSのWebベースGUIおよびSSHにログインするユーザを、それぞれのユーザロールに従って許可します。
- ACSを使用して、FXOSでの認証と許可の適切な動作を確認します。

ネットワーク図



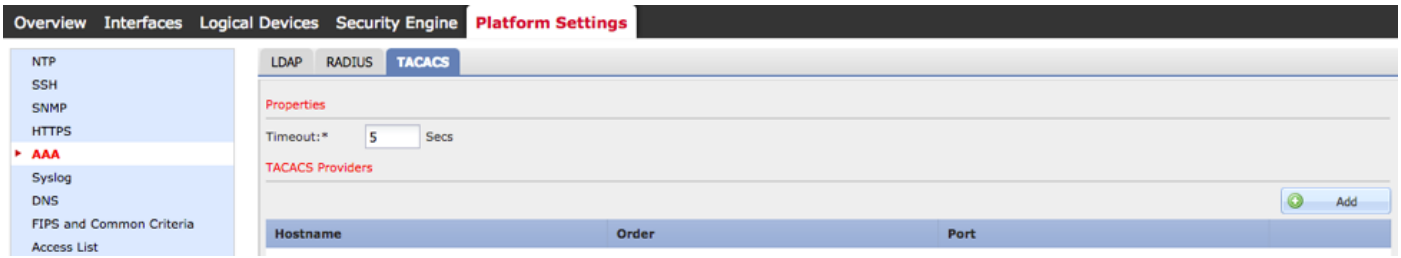
設定

FXOSシャーシの設定

シャーシマネージャを使用したTACACSプロバイダーの作成

ステップ1:[Platform Settings] > [AAA]に移動します。

ステップ2:[TACACS]タブをクリックします。

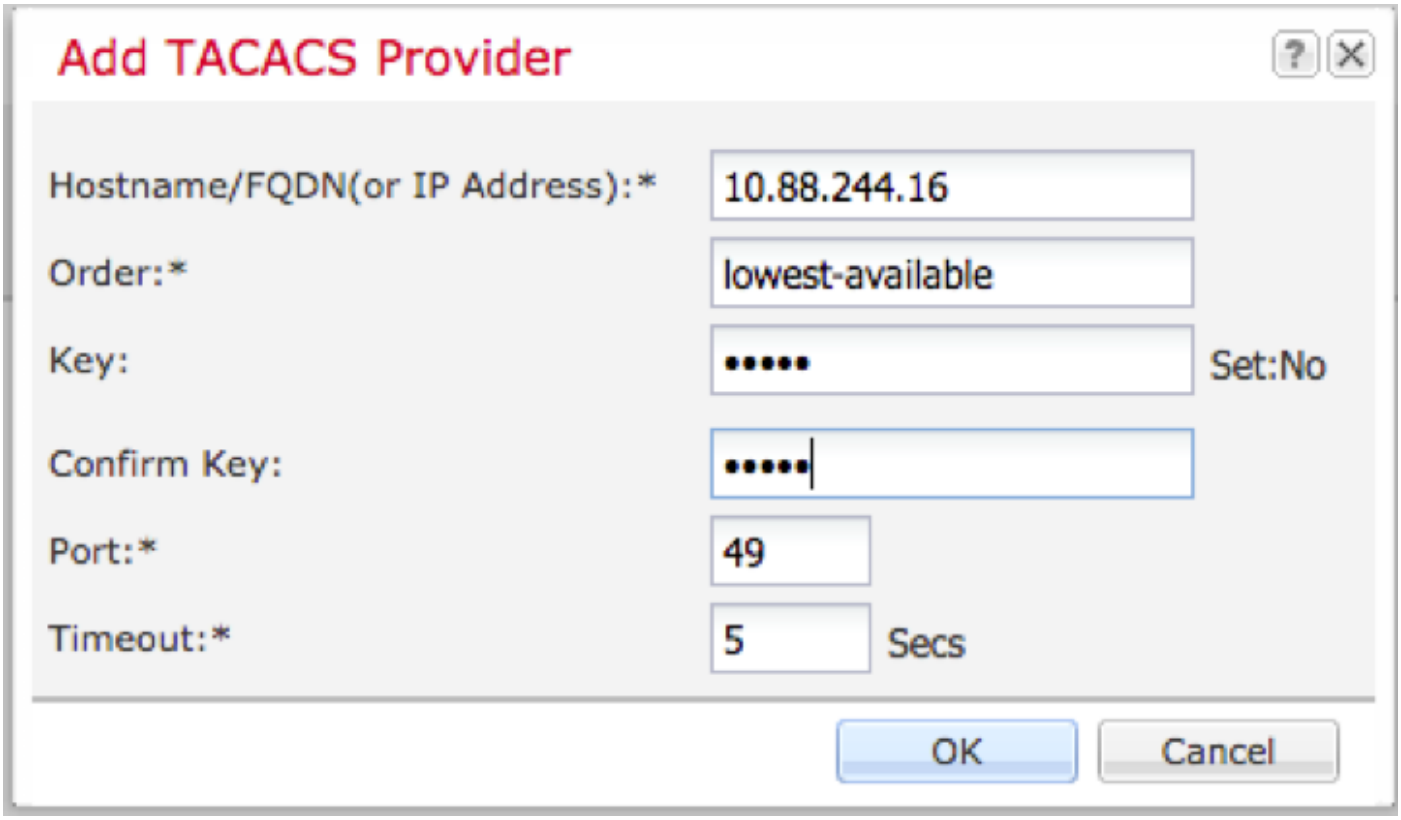


ステップ3：追加する各TACACS+プロバイダー（最大16プロバイダー）について。

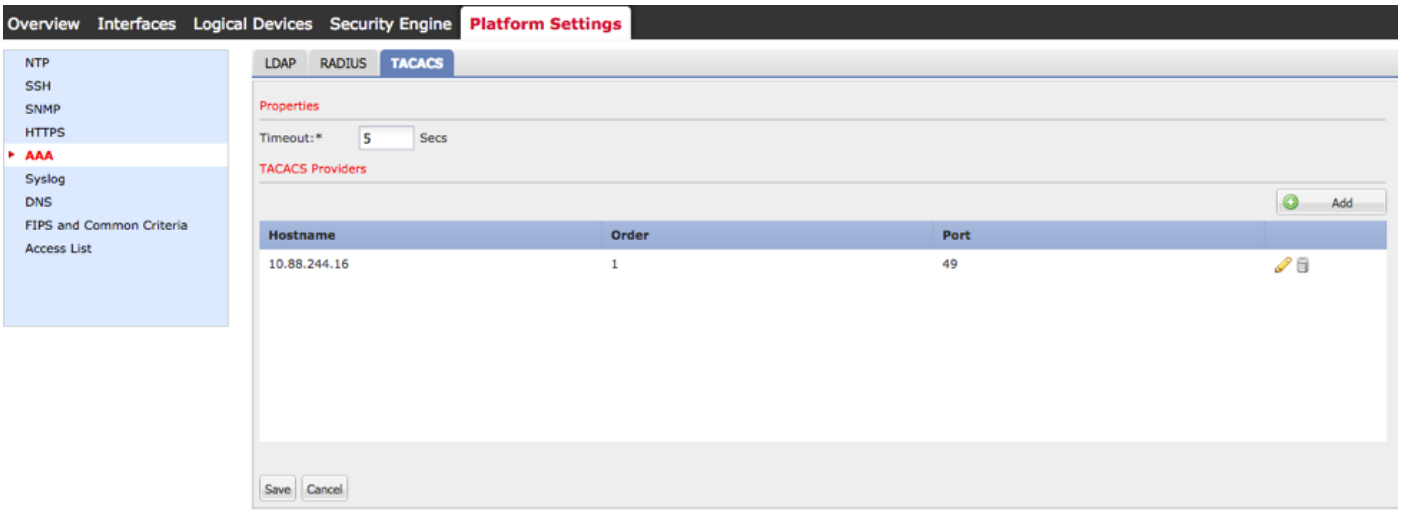
3.1. [TACACS Providers]領域で、[Add]をクリックします。

3.2. [Add TACACS Provider]ダイアログボックスで、必要な値を入力します。

3.3. 「OK」をクリックし、「TACACSプロバイダーの追加」ダイアログ・ボックスを閉じます。

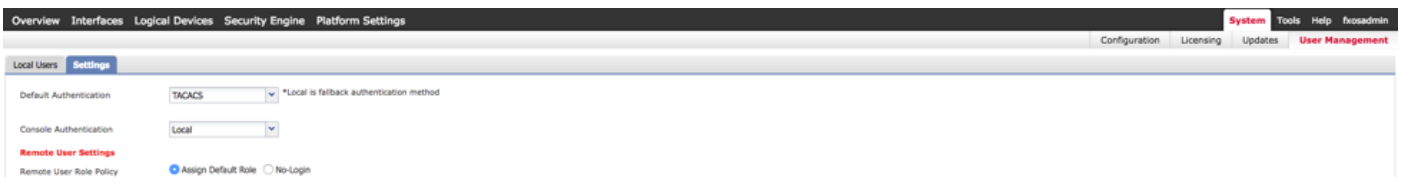


ステップ4:[Save]をクリックします。



ステップ5:[System] > [User Management] > [Settings]に移動します。

ステップ6:[Default Authentication]で[TACACS]を選択します。



CLIを使用したTACACS+プロバイダーの作成

ステップ1:TACACS認証を有効にするには、次のコマンドを実行します。

fpr4120-TAC-A#スコープセキュリティ

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

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

ステップ2:**show detailコマンド**を使用して結果を表示します。

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

デフォルト認証：

管理レルム：**TACACS**

動作領域：**TACACS**

Webセッションの更新間隔（秒）:600

Web、ssh、telnetセッションのセッションタイムアウト（秒）:600

Web、ssh、telnetセッションの絶対セッションタイムアウト（秒）:3600

シリアルコンソールセッションのタイムアウト（秒）:600

シリアルコンソールの絶対セッションタイムアウト（秒）:3600

管理認証サーバグループ：

動作認証サーバグループ：

2次係数の使用：No

ステップ3:TACACSサーバパラメータを設定するには、次のコマンドを実行します。

fpr4120-TAC-A#スコープセキュリティ

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

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

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

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

キーを入力します。******

キーを確認します。******

ステップ4:**show detailコマンド**を使用して結果を表示します。

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

TACACS+サーバ：

ホスト名、FQDN、またはIPアドレス：10.88.244.50

descr　　：

発注：1

[Port]：49

ポイント：****

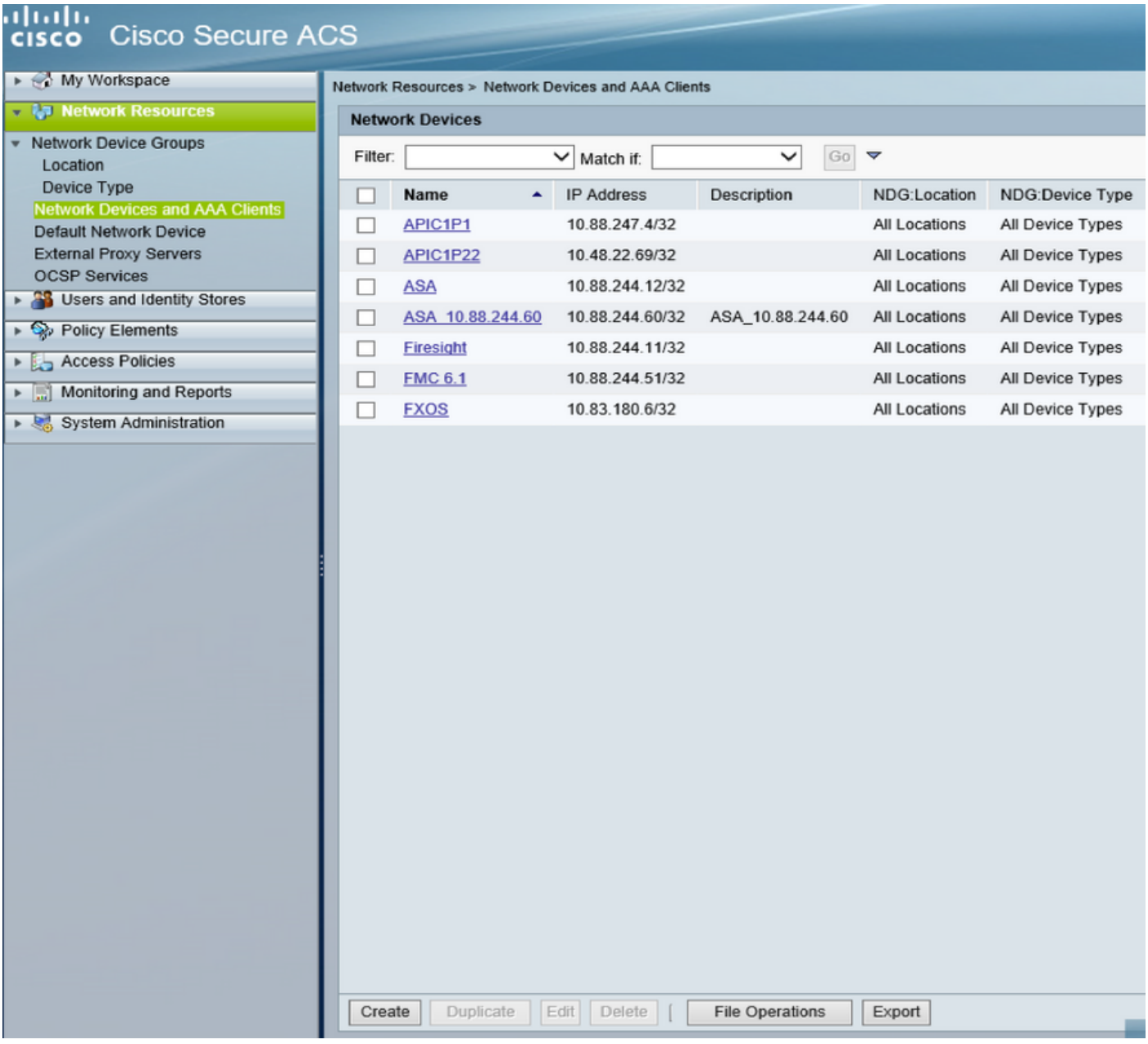
タイムアウト：5

ACSサーバの設定

ネットワークリソースとしてのFXOSの追加

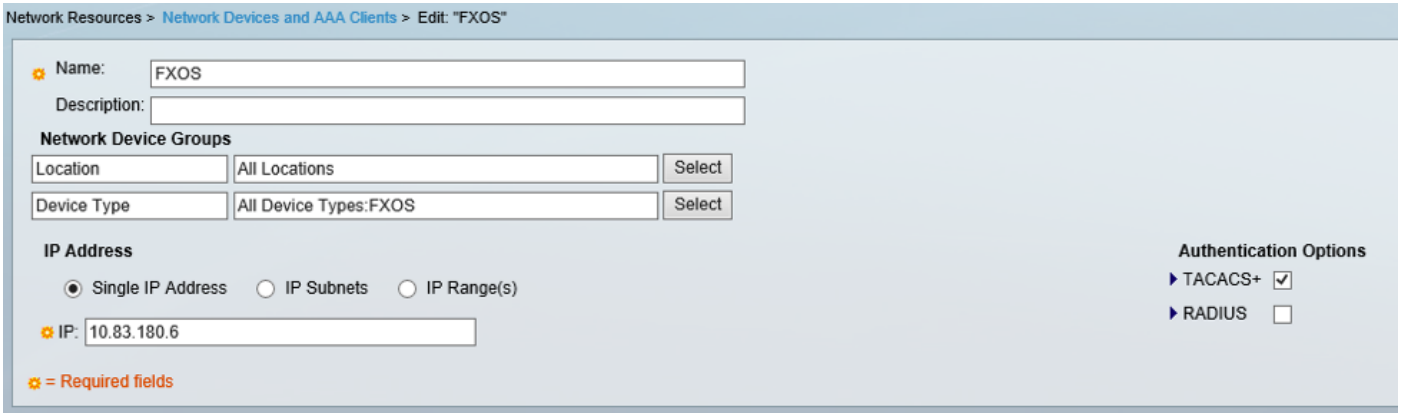
ステップ1:[Network Resources] > [**Network Devices and AAA Clients]に移動します。**

ステップ2:[Create]をクリック**します。**



ステップ3：必要な値（[Name]、[IP Address]、[Device Type]、および[Enable TACACS+]）を入

カし、KEYを追加します。



ステップ 4：[Submit] をクリックします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。