WAAS を使った ACS バージョン 5.x 統合の設定例

目次

概要

このドキュメントでは、Cisco Wide Area Application Services（WAAS）と Cisco Access Control Server（ACS）バージョン 5.x の統合の設定方法について説明します。 このドキュメントの手順に従って設定する場合、ユーザは ACS を介して TACACS+ クレデンシャルを使用して WAAS に認証できます。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

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。

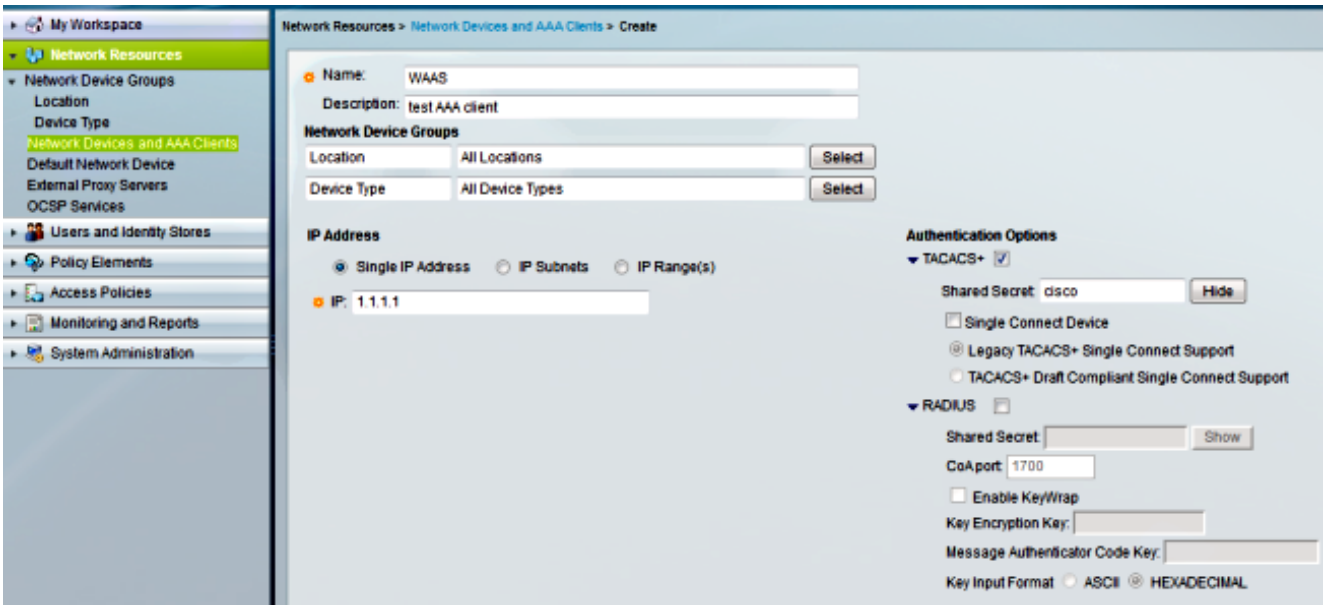
- Cisco Secure ACS バージョン 5.x
- Cisco WAAS

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。

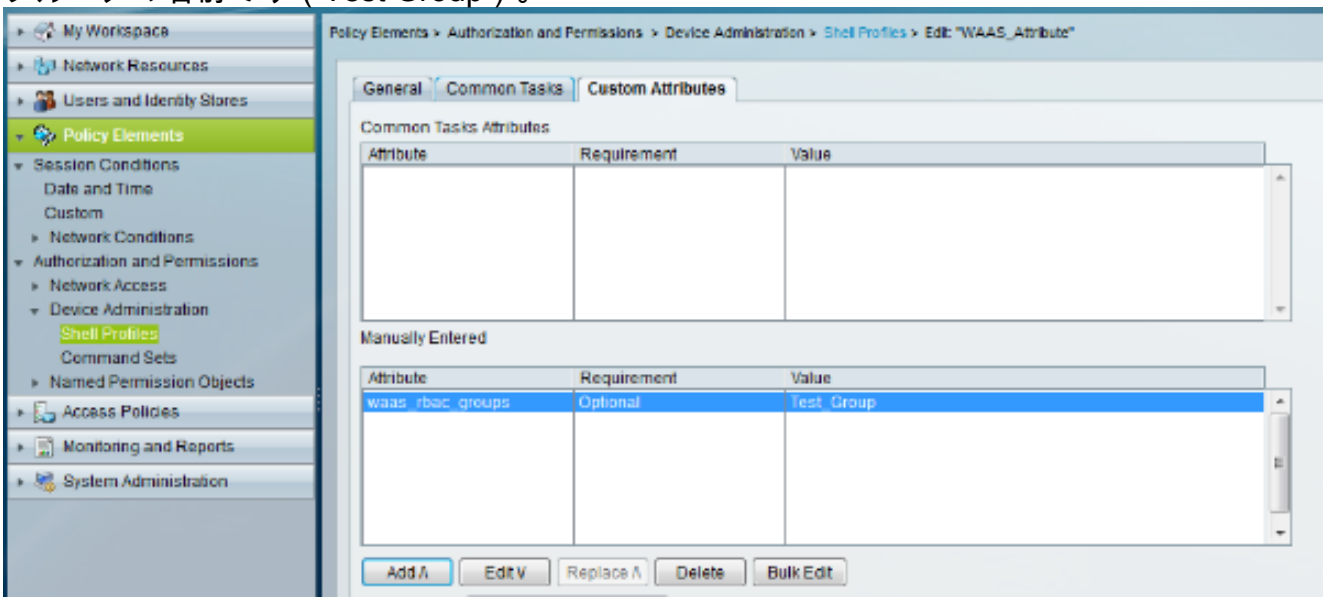
設定

ACS の設定

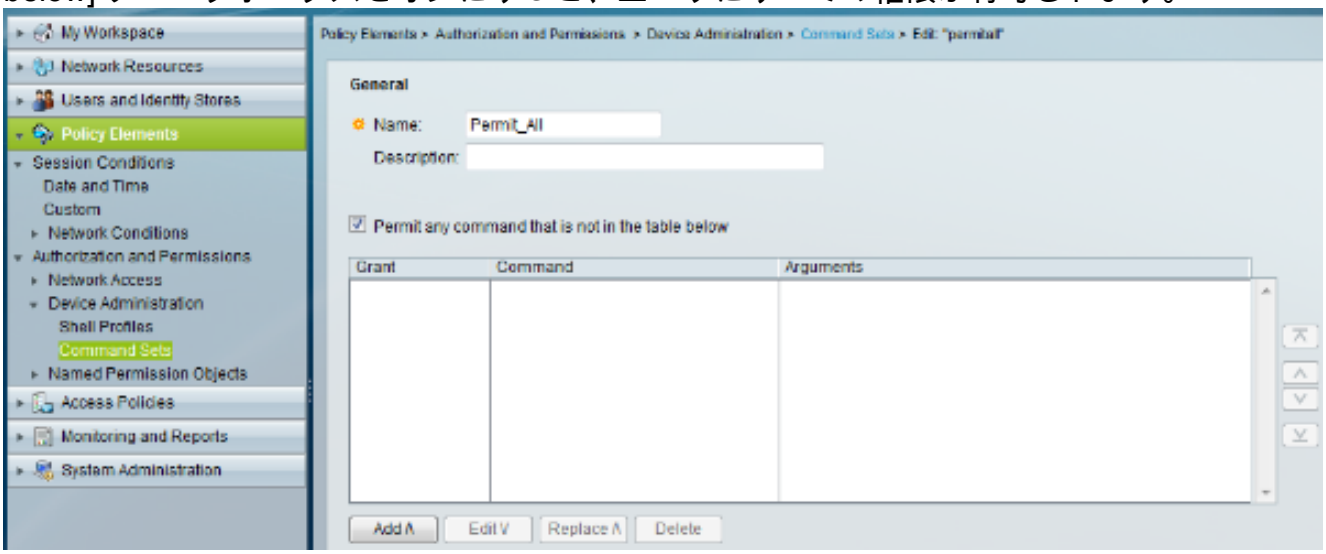
1. ACS バージョン 5.x で AAA クライアントを定義するため、[Network Resources] > [Network Devices and AAA Clients] に移動します。 AAA クライアントに、わかりやすい名前、1 つの IP アドレス、TACACS+ の共有秘密キーを設定します。



2. シェル プロファイルを定義するため、[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] に移動します。 この例では、**WAAS_Attribute** という新しいシェル プロファイルが設定されます。 このカスタム属性は WAAS に送信されます。これにより、WAAS はどのユーザ グループが管理者グループであるかを推測できます。次のカスタム属性を設定します。
[Attribute] は [waas_rbac_groups] です。[Requirement] は [Optional] です。これによりその他のデバイスが影響を受けません。[Value] は、管理アクセス権限を割り当てる必要があるグループの名前です（ Test Group ）。

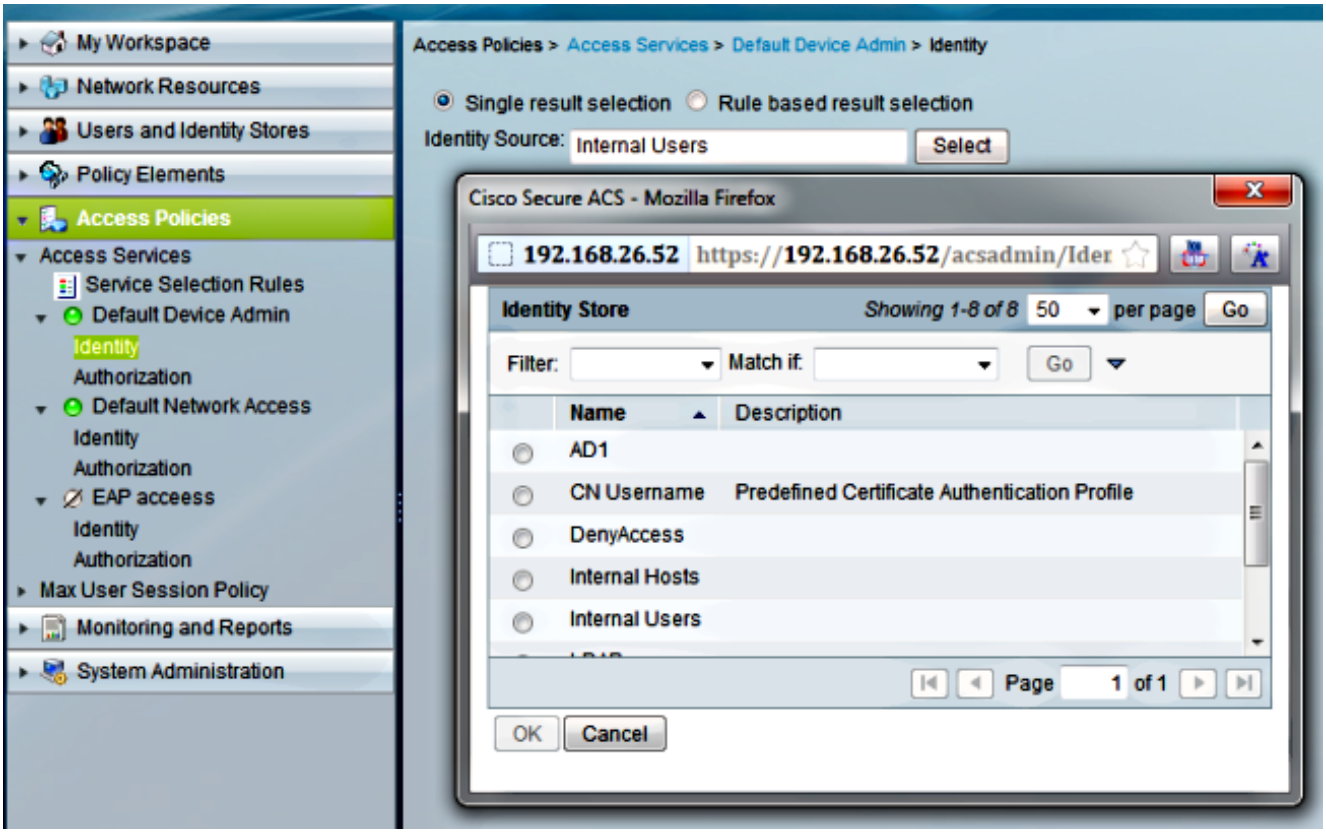


3. すべてのコマンドを許可するようにコマンド セットを定義するため、[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Command Sets] に移動します。
[Permit_All] コマンド セットを編集します。[Permit any command that is not in the table below] チェックボックスをオンにすると、ユーザにすべての権限が付与されます。



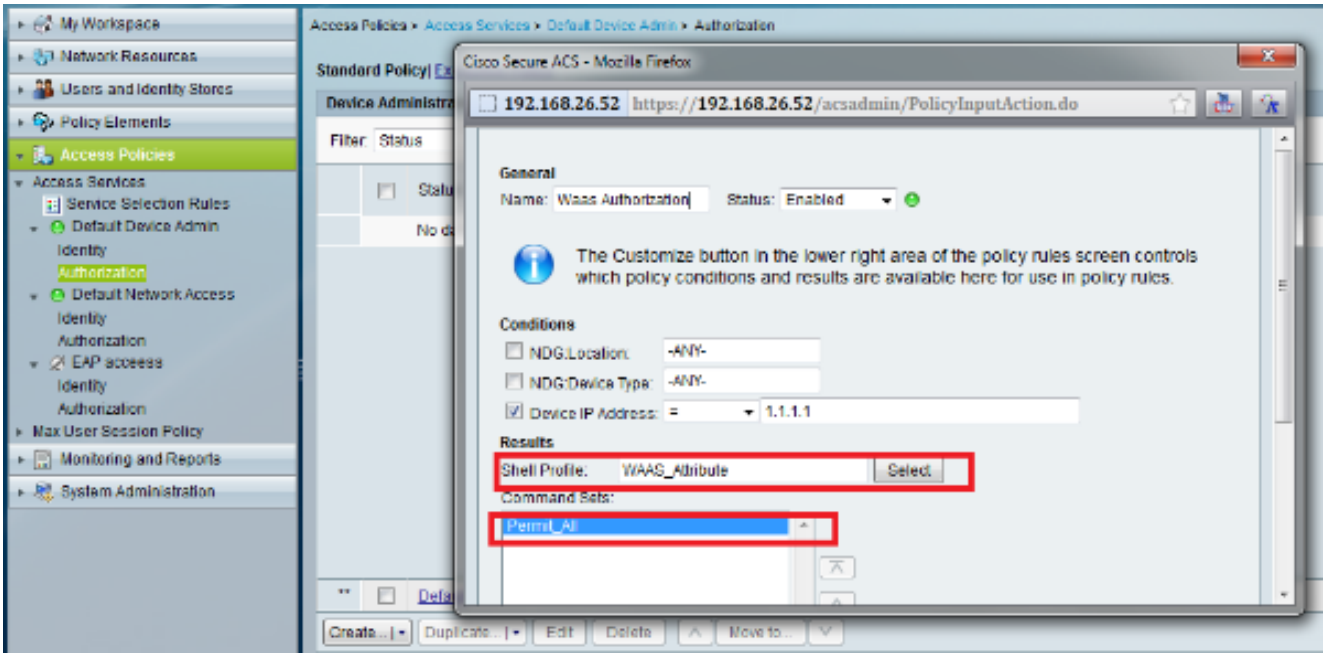
注: この例では TACACS を使用するため、選択されるデフォルトのサービスは **default device admin** です。

4. ID が正しい ID ソースを指すようにするため、[Access Policies] > [Access Services] > [Default Device Admin] > [Identity] に移動します。 ユーザがローカル ACS データベースに存在している場合は [Internal Users] を選択します。 ユーザが Active Directory に存在している場合は、設定されている ID ストア（この例では **AD1**）を選択します。



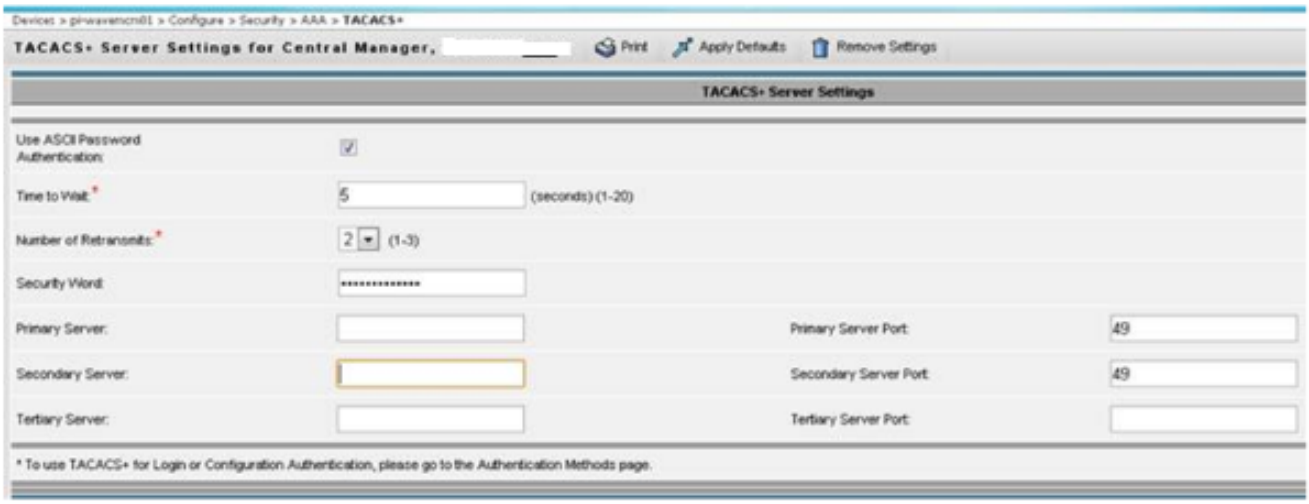
5. 認可ルールを作成するため、[Access Policies] > [Access Services] > [Default Device Admin] > [Authorization] の順に移動します。 **WAAS Authorization** という名前の認可ポリシーを作成

します。 これは WAAS からの要求をチェックします。 この例では、デバイス IP が条件として使用されます。 ただし、導入要件に応じてこれは変更されることがあります。 この項のステップ 2 と 3 で設定したシェル プロファイルとコマンド セットを適用します。

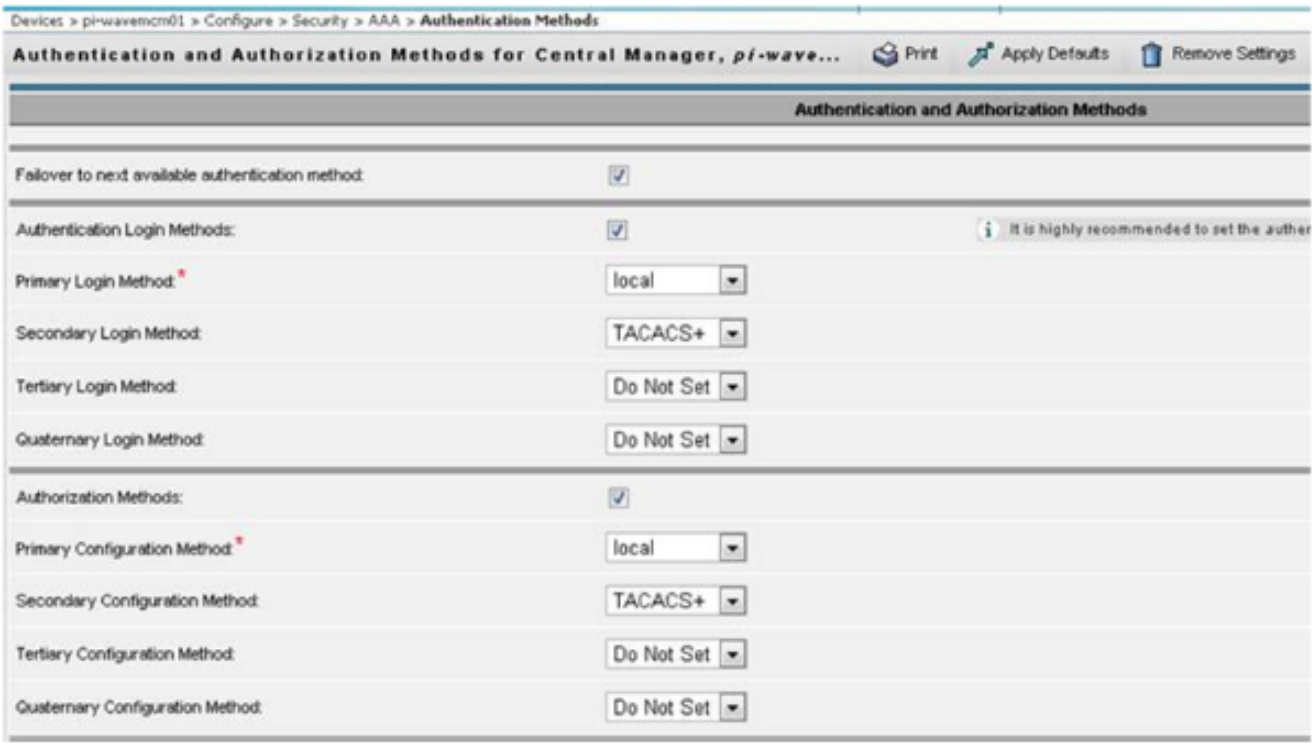


WAAS での設定

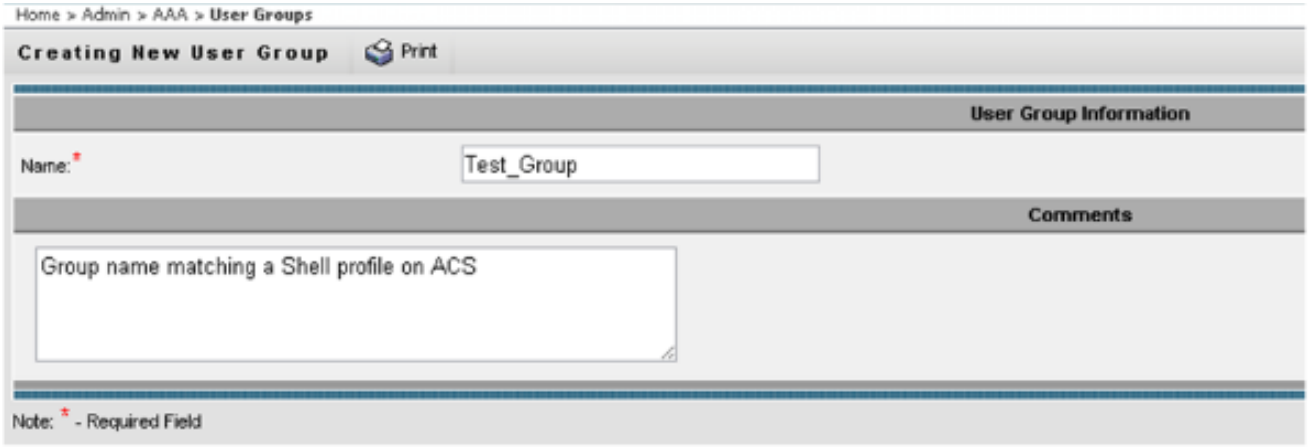
1. TACACS+ サーバを定義するため、[Devices] > [*<Central Manager System Name>*] > [Configure] > [Security] > [AAA] > [TACACS+] の順に移動します。 ACS サーバの IP アドレスと事前共有キーを設定します。



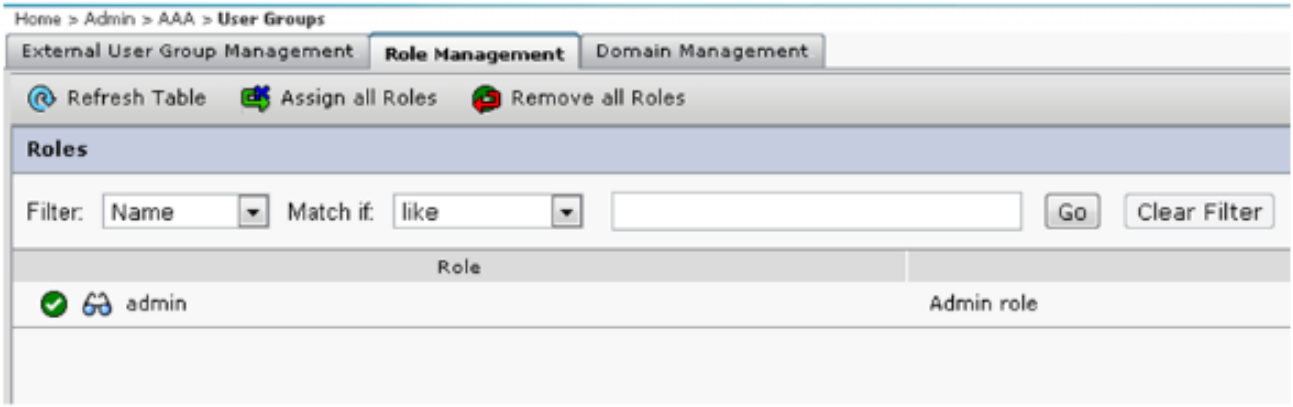
2. 認証方式と認可方式を変更するため、[Devices] > [*<Central Manager System Name>*] > [Configure] > [Security] > [AAA] > [Authentication Methods] の順に移動します。 このスクリーンショットでは、プライマリ ログイン方式が [local]、セカンダリ ログイン方式が [TACACS+] として設定されています。



3. WAAS でカスタム属性 [Value] と一致するグループ名を追加するため、[Home] > [Admin] > [AAA] > [User Groups] に移動します（「**ACS の設定**」のステップ 2 を参照）。



4. [Home] > [Admin] > [AAA] > [User Groups Role Management] タブで、このグループ（Test_Group）に **admin** レベルの権限を付与します。 Central Manager の **admin** ロールは事前に設定されています。



確認

TACACS+ クレデンシャルを使用して WAAS への ログインを試行します。 すべてが正しく設定されていれば、アクセス権が付与されます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。