Exemple de configuration de l'intégration ACS version 5.x avec WAAS

Table des matières

Introduction

Ce document décrit comment configurer l'intégration de Cisco Wide Area Application Services (WAAS) avec Cisco Access Control Server (ACS) Version 5.x . Lorsqu'ils sont configurés conformément aux étapes de ce document, les utilisateurs peuvent s'authentifier auprès de WAAS avec des informations d'identification TACACS+ via ACS.

Conditions préalables

Exigences

There are no specific requirements for this document.

Composants utilisés

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

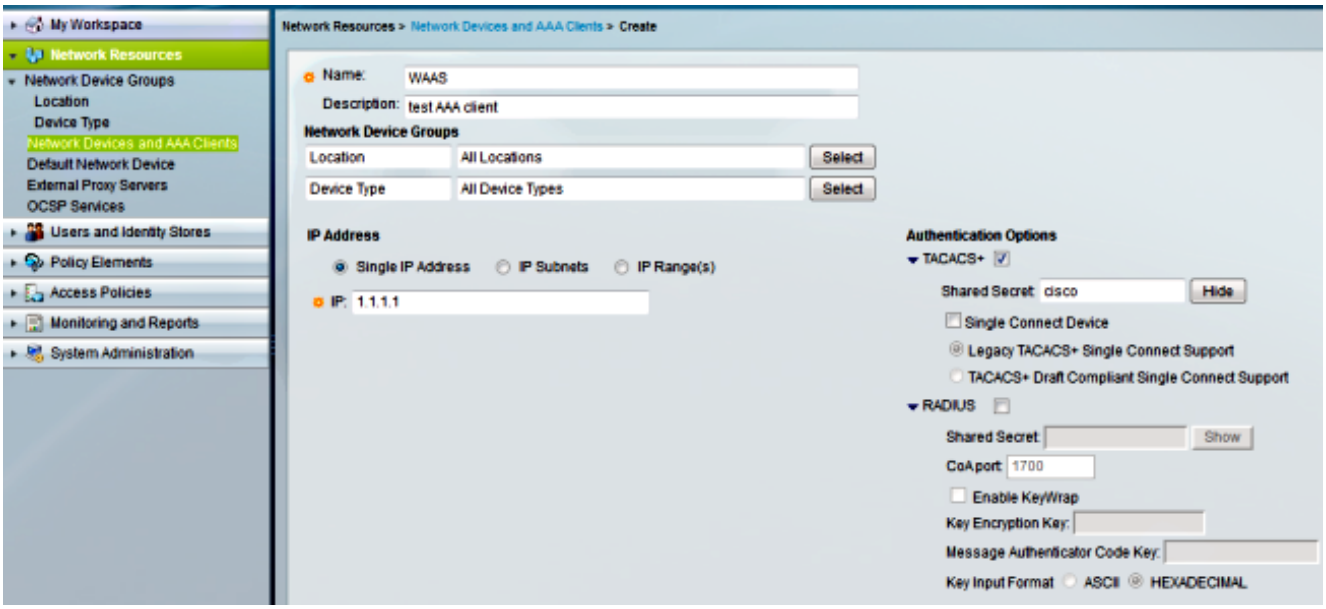
- Cisco Secure ACS version 5.x
- Cisco WAAS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

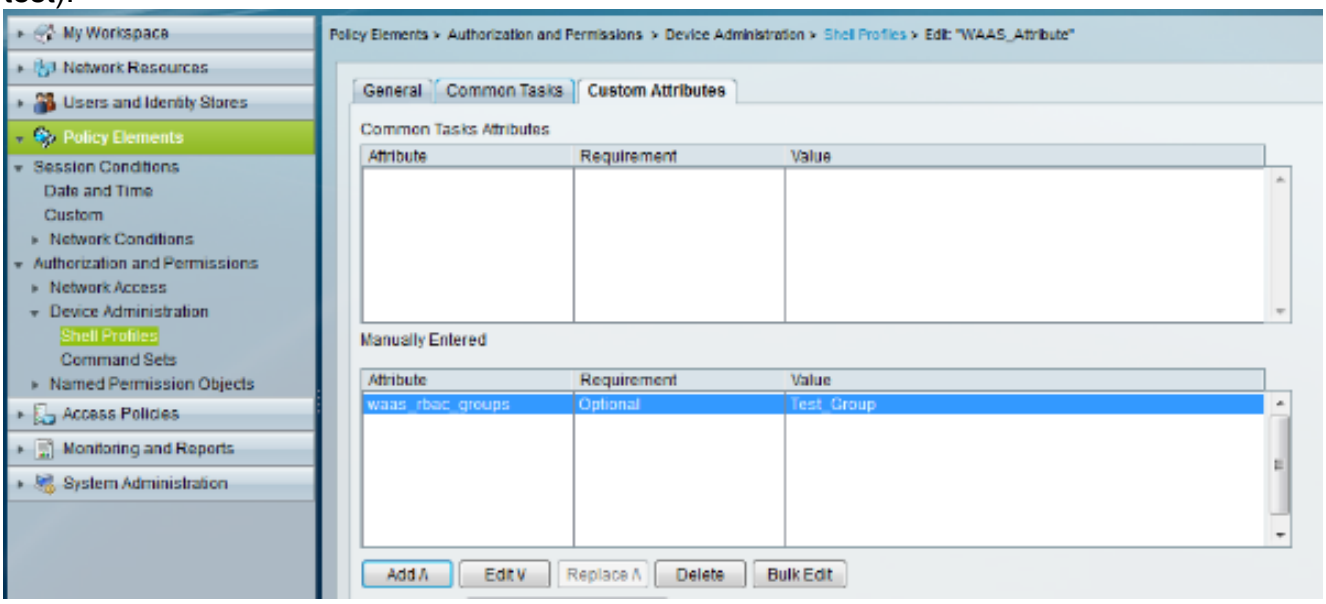
Configurer

Configurer ACS

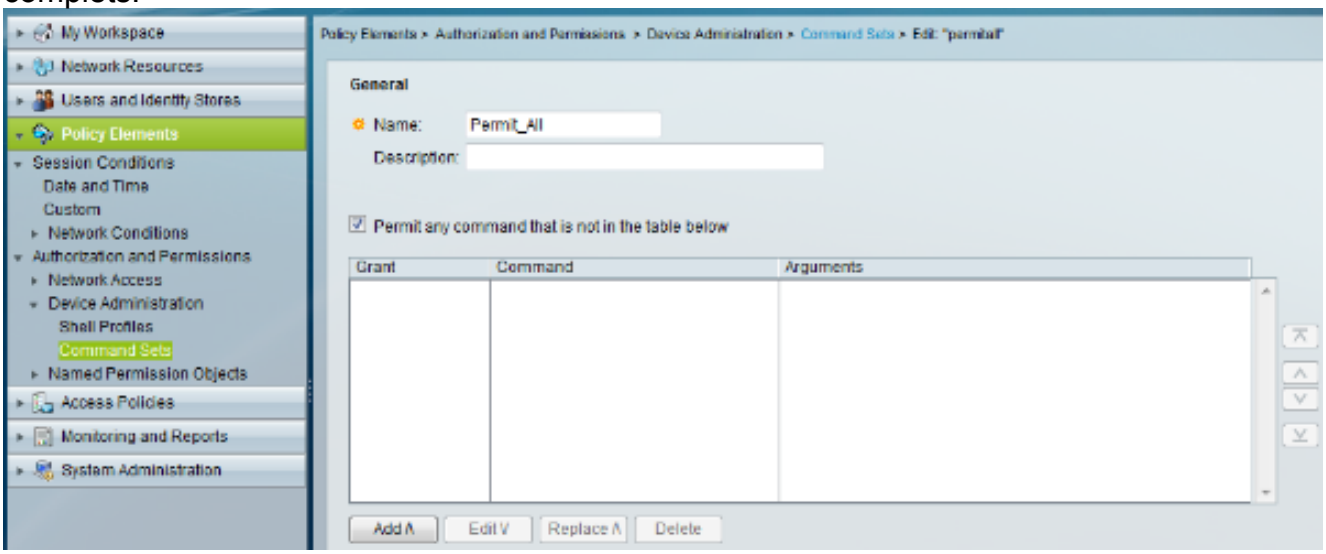
1. Afin de définir un client AAA sur ACS Version 5.x, naviguez à **Ressources réseau > Périphériques réseau et clients AAA.** Configurez le client AAA avec un nom descriptif, une adresse IP unique et une clé secrète partagée pour TACACS+.



2. Afin de définir un profil Shell, naviguez vers **Éléments de stratégie > Autorisations et autorisations > Administration de périphérique > Profils Shell**. Dans cet exemple, un nouveau profil shell appelé **WAAS_Attribute** est configuré. Cet attribut personnalisé est envoyé au WAAS, ce qui lui permet de déduire quel groupe d'utilisateurs est le groupe d'administrateurs. Configurez ces attributs personnalisés :
L'**attribut** est **waas_rbac_groups**.La **configuration requise** est **facultative** afin qu'elle ne perturbe aucun autre périphérique.La **valeur** est le nom du groupe auquel un accès administratif doit être attribué (Groupe de test).

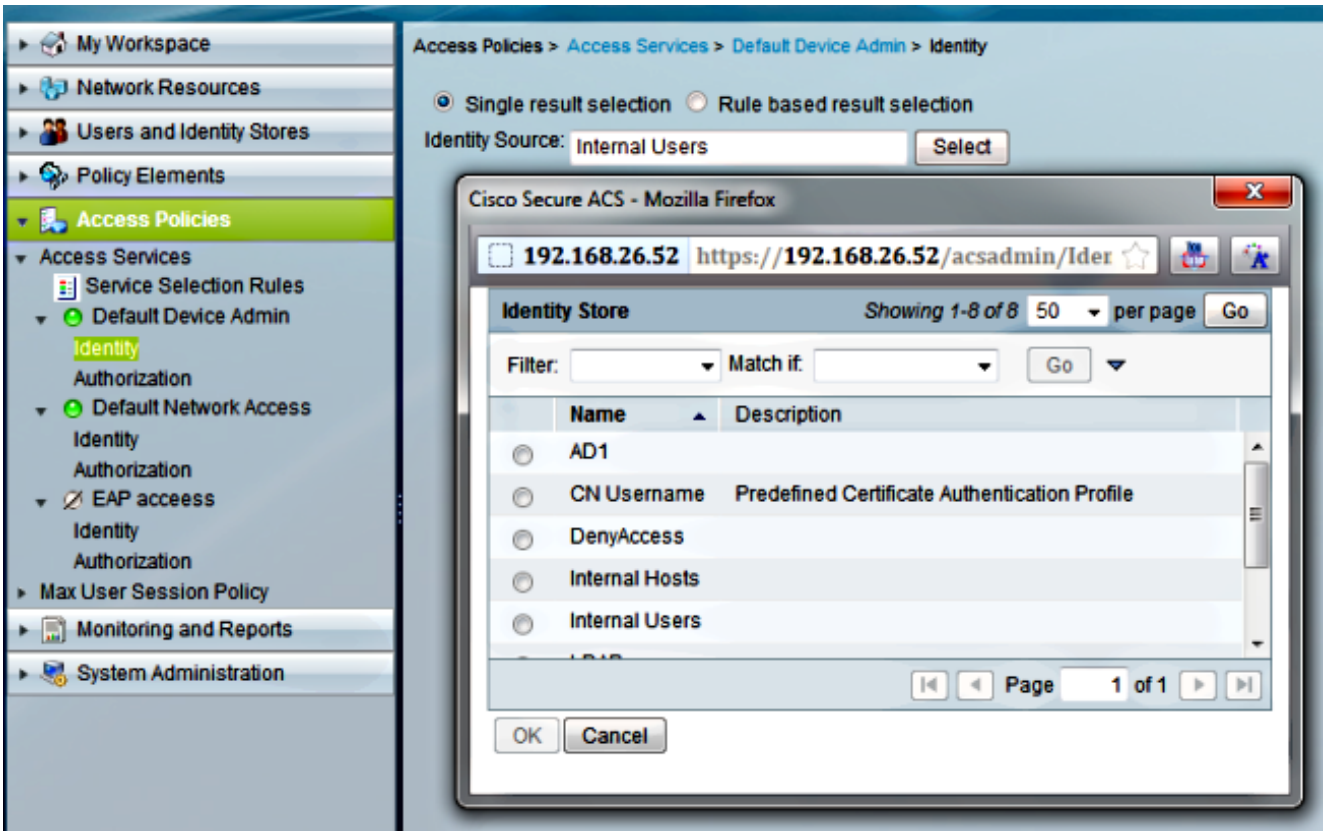


3. Afin de définir un jeu de commandes pour autoriser toutes les commandes, naviguez vers **Policy Elements > Authorization and Permissions > Device Administration > Command Sets**. Modifiez le jeu de commandes **Permit_All**.Si vous cochez la case **Autoriser une commande qui ne figure pas dans le tableau ci-dessous**, l'utilisateur bénéficie de privilèges complets.



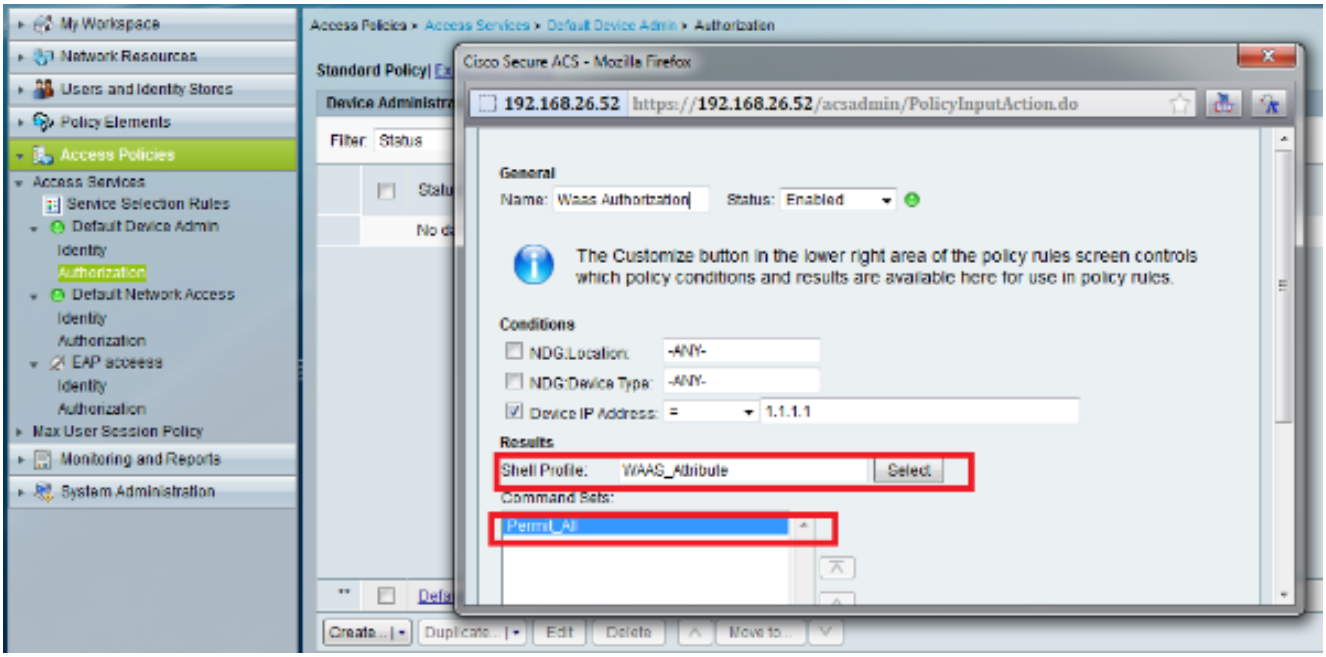
Remarque : comme cet exemple utilise TACACS, le service par défaut sélectionné est **default device admin**.

4. Afin de pointer l'identité vers la source d'identité correcte, naviguez vers **Access Policies > Access Services > Default Device Admin > Identity. Si l'utilisateur existe dans la base de données ACS locale, sélectionnez Internal Users**. Si l'utilisateur existe dans Active Directory, sélectionnez le magasin d'identités configuré (**AD1** dans cet exemple).



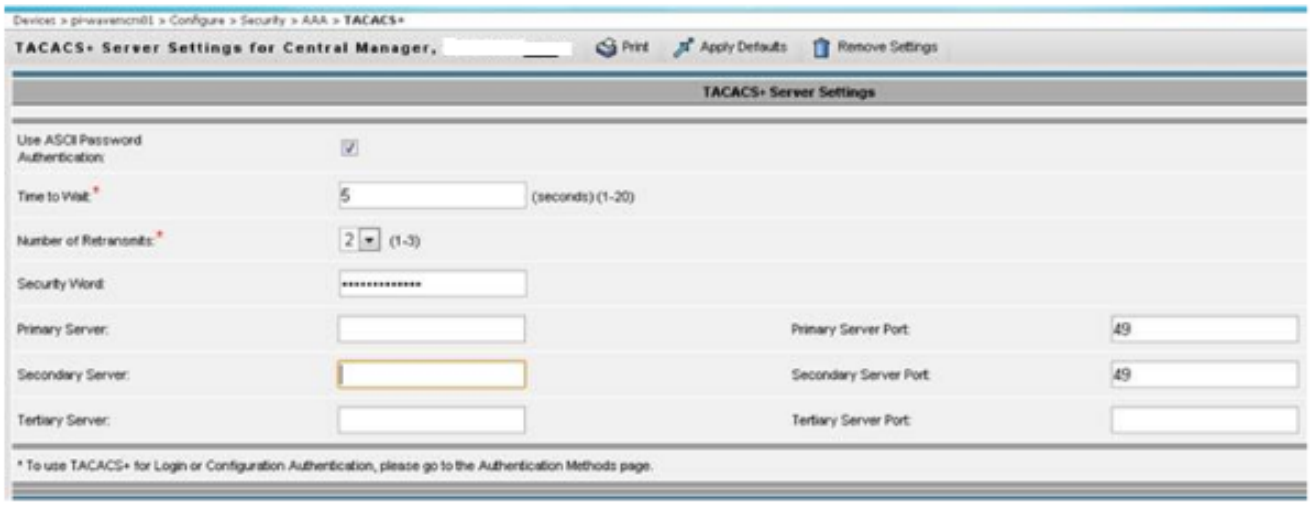
5. Afin de créer une règle d'autorisation, naviguez vers **Access Policies > Access Services >**

Default Device Admin > Authorization. Créez une nouvelle stratégie d'autorisation appelée **Autorisation WAAS**. Cette commande recherche les requêtes de WAAS. Dans cet exemple, l'adresse IP du périphérique est utilisée comme condition. Toutefois, cette configuration peut être modifiée en fonction des exigences de déploiement. Appliquez le profil de shell et les jeux de commandes configurés aux étapes 2 et 3 de cette section.

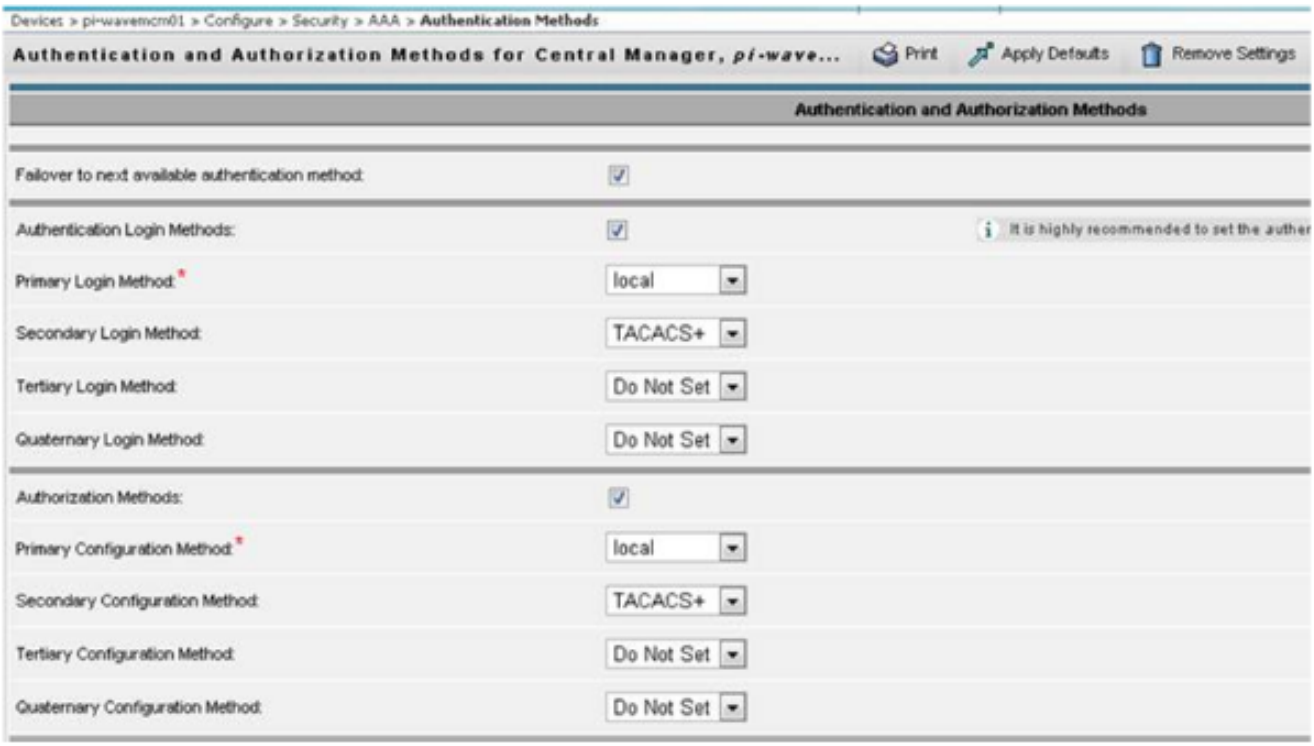


Configuration sur le WAAS

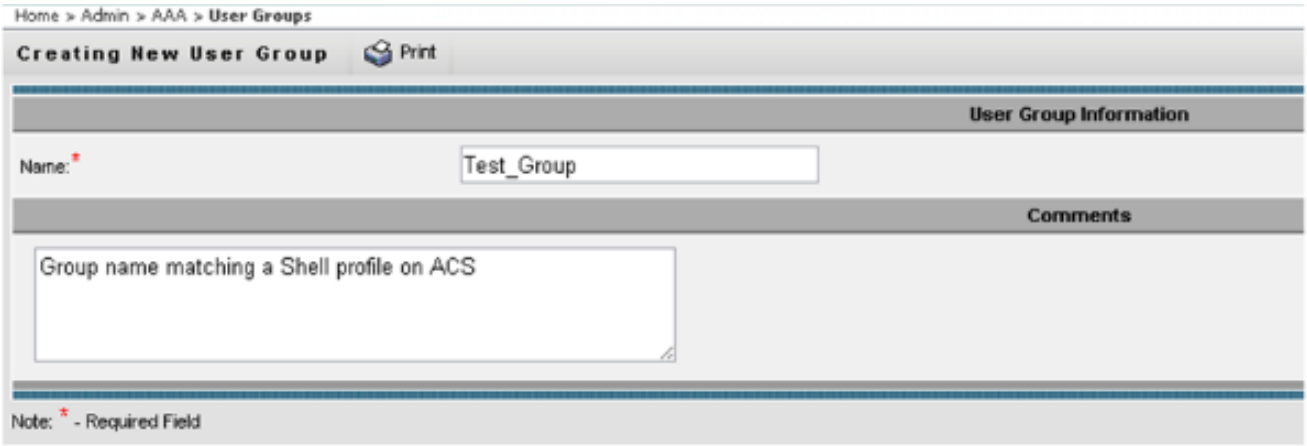
1. Afin de définir un serveur TACACS+, naviguez vers **Devices > *<Central Manager System Name>* > Configure > Security > AAA > TACACS+**. Configurez l'adresse IP du serveur ACS et la clé pré-partagée.



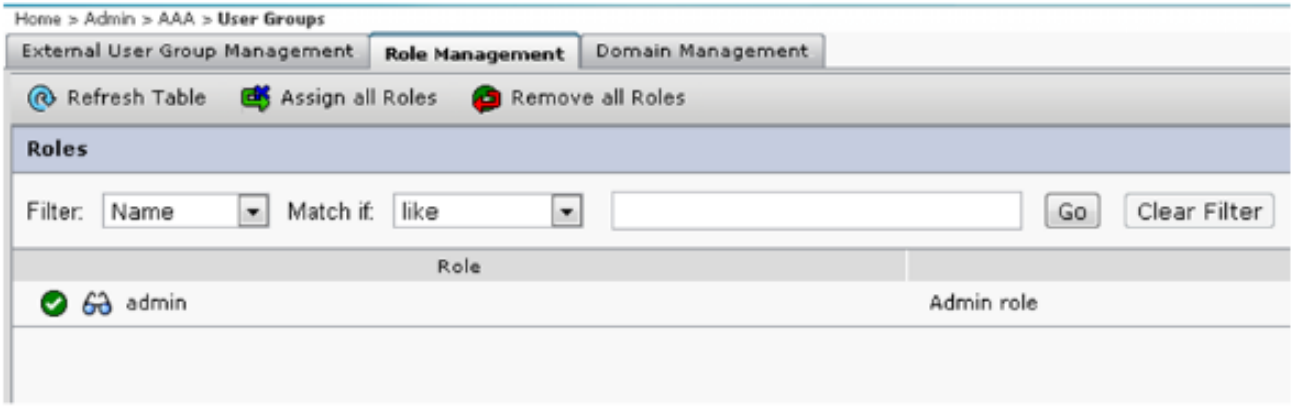
2. Afin de modifier les méthodes d'authentification et d'autorisation, accédez à **Devices > *<Central Manager System Name>* > Configure > Security > AAA > Authentication Methods**. Dans cette capture d'écran, la méthode de connexion principale est configurée pour **local** et la méthode secondaire est configurée pour **TACACS+**.



3. Accédez à **Home > Admin > AAA > User Groups** afin d'ajouter le nom de groupe qui correspond à l'attribut personnalisé **Value** (voir l'étape 2 dans la section **Configure ACS**) dans WAAS.



4. Attribuez ce groupe (Test_Group) **aux** droits de **niveau admin** dans l'onglet **Accueil > Admin > AAA > Gestion des rôles des groupes d'utilisateurs**. Le rôle **admin** sur le Gestionnaire central est préconfiguré.



Vérifier

Tentative de connexion à WAAS avec les informations d'identification TACACS+. Si tout est configuré correctement, vous disposez d'un droit d'accès.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.