

Intégration de version 5.x ACS avec l'exemple de configuration WAAS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Configurez ACS](#)

[Configuration sur le WAAS](#)

[Vérifiez](#)

[Dépannez](#)

Introduction

Ce document décrit comment configurer l'intégration du Cisco Wide Area Application Services (WAAS) avec la version 5.x du serveur de contrôle d'accès de Cisco (ACS). Une fois configurés par étapes dans ce document, les utilisateurs peuvent authentifier à WAAS avec des qualifications TACACS+ par l'intermédiaire d'ACS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Version 5.x de Cisco Secure ACS
- Cisco WAAS

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

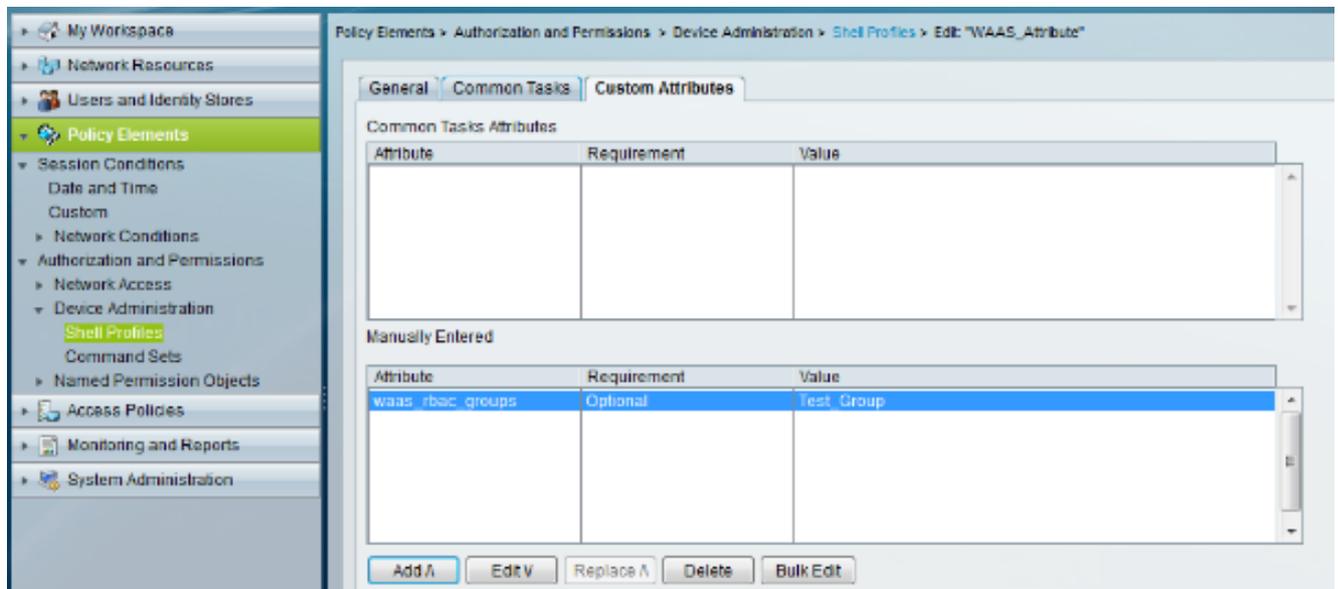
Configurez ACS

1. Afin de définir un client d'AAA sur la version 5.x ACS, naviguez vers des **ressources de réseau > des périphériques de réseau et des clients d'AAA**. Configurez le client d'AAA avec un nom descriptif, une adresse IP simple, et une clé secrète partagée pour TACACS+.

The screenshot shows the 'Create' configuration page for a new AAA client in the Cisco ACS 5.x web interface. The left sidebar contains a navigation tree with 'Network Resources' expanded to 'Network Devices and AAA Clients'. The main content area is titled 'Network Resources > Network Devices and AAA Clients > Create'. The form includes the following fields and options:

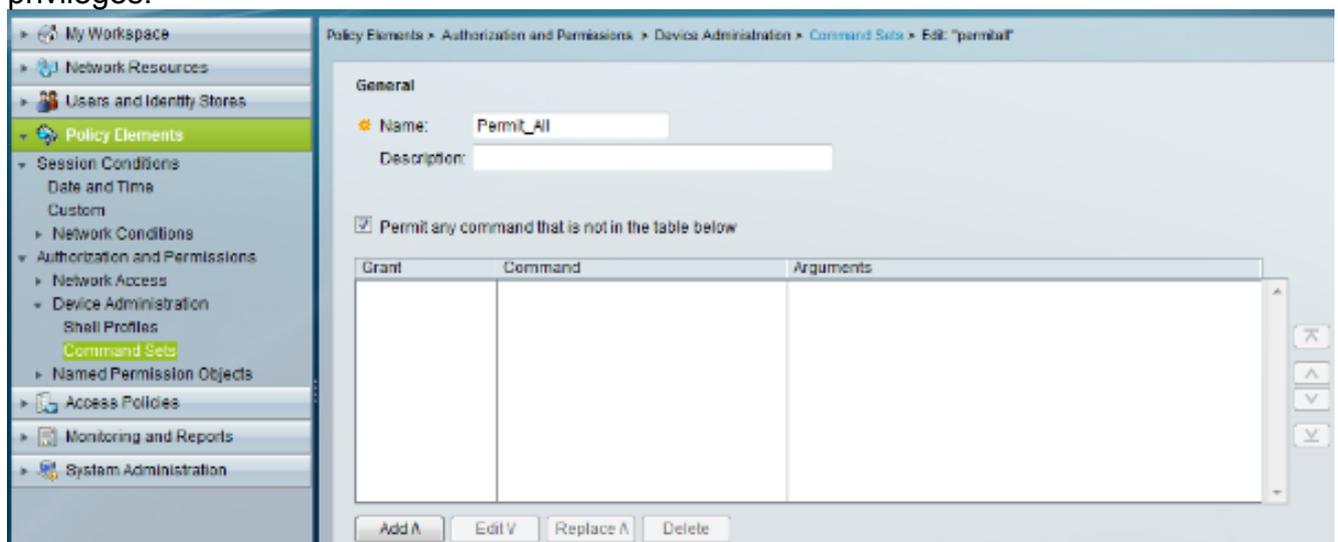
- Name:** WAAS
- Description:** test AAA client
- Network Device Groups:**
 - Location: All Locations (with a 'Select' button)
 - Device Type: All Device Types (with a 'Select' button)
- IP Address:**
 - Radio buttons for 'Single IP Address' (selected), 'IP Subnets', and 'IP Range(s)'.
 - IP: 1.1.1.1
- Authentication Options:**
 - TACACS+ (checked):
 - Shared Secret: disco (with a 'Hide' button)
 - Single Connect Device (unchecked)
 - Legacy TACACS+ Single Connect Support (checked)
 - TACACS+ Draft Compliant Single Connect Support (unchecked)
 - RADIUS (unchecked):
 - Shared Secret (with a 'Show' button)
 - CoA port: 1700
 - Enable KeyWrap (unchecked)
 - Key Encryption Key: (empty field)
 - Message Authenticator Code Key: (empty field)
 - Key Input Format: ASCII (unchecked), HEXADECIMAL (checked)

2. Afin de définir un profil de shell, naviguez des **profils vers des éléments de stratégie > l'autorisation et des autorisations > de périphérique gestion > shell**. Dans cet exemple, un nouveau profil de shell appelé **WAAS_Attribute** est configuré. Cet attribut personnalisé est envoyé au WAAS, qui lui permet pour impliquer quel groupe d'utilisateurs est le groupe d'administrateur. Configurez ces attributs personnalisés :
L'attribut est des waas_rbac_groups. La condition requise est facultative de sorte qu'elle ne touche à aucun autre périphérique. **La valeur est le nom du groupe qui doit être assigné l'accès administratif (groupe de test).**



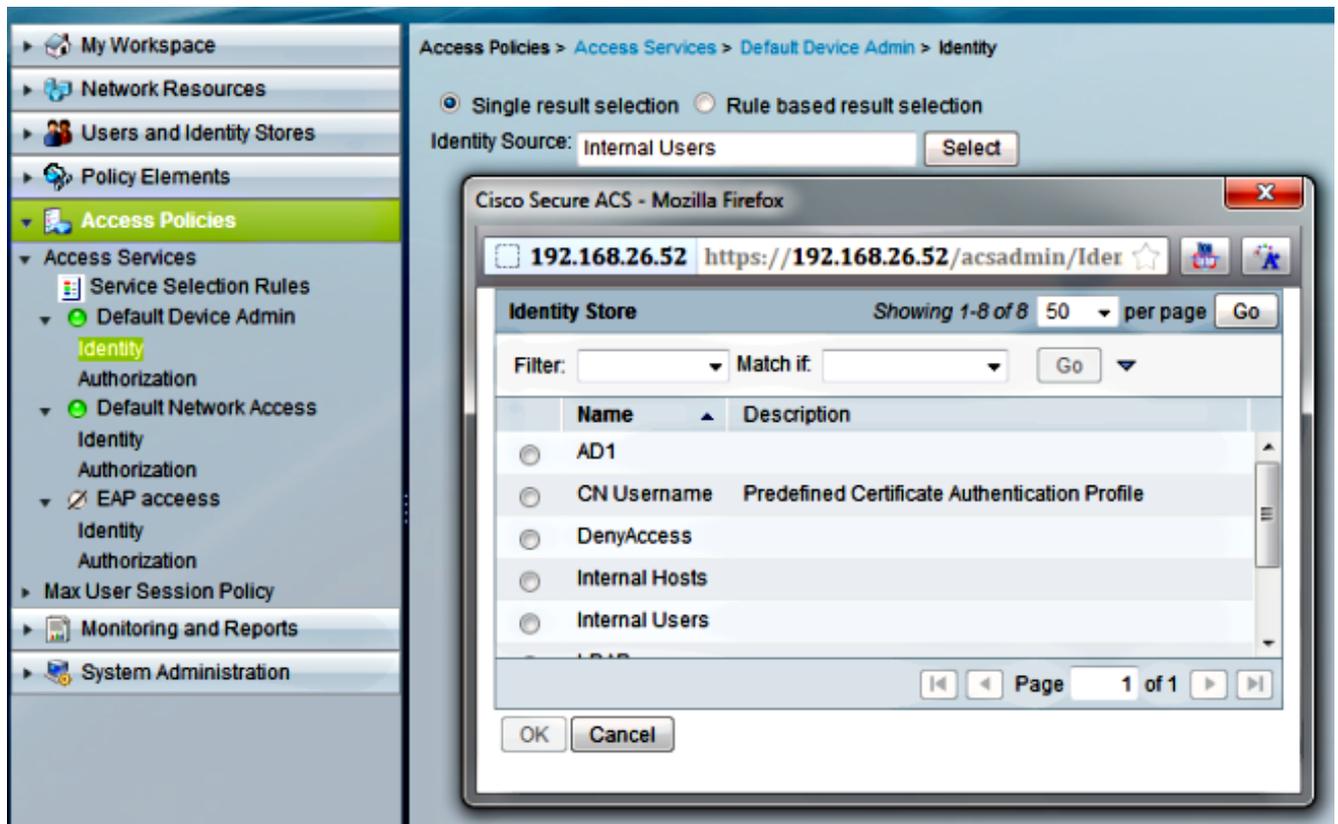
3. Afin de définir un positionnement de commande pour permettre toutes les commandes, naviguez vers des **éléments de stratégie > l'autorisation et les autorisations > la gestion > la commande de périphérique place**.

Éditez le positionnement de commande de **Permit_All**. Si vous cochez l'autorisation n'importe quelle commande qui n'est pas dans la table au-dessous de case, on accorde l'utilisateur de pleins privilèges.

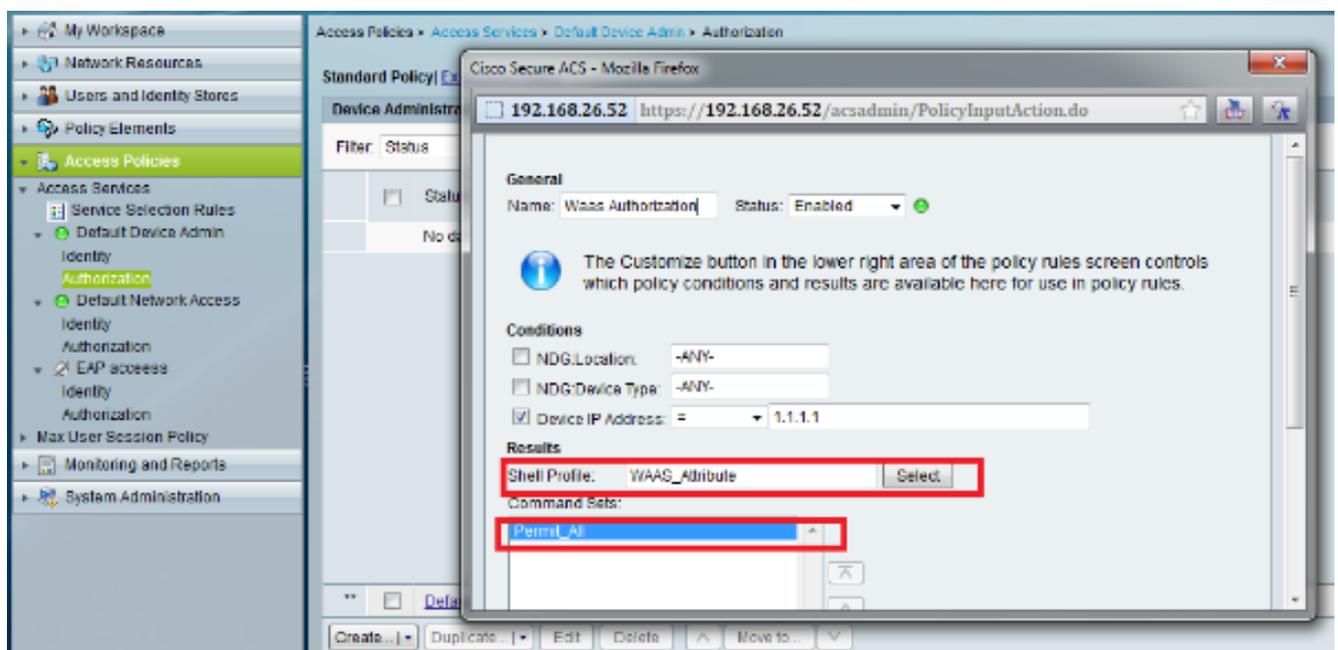


Remarque: Puisque cet exemple utilise TACACS, le service par défaut sélectionné est **admin par défaut de périphérique**.

4. Afin d'indiquer l'identité la source correcte d'identité, naviguez pour accéder à des stratégies > des services d'accès > l'admin > l'identité de périphérique de par défaut. Si l'utilisateur existe dans la base de données des gens du pays ACS, les **utilisateurs internes** choisis. Si l'utilisateur existe dans le Répertoire actif, sélectionnez la mémoire configurée d'identité (**AD1** dans cet exemple).



5. Afin de créer une règle d'autorisation, naviguez pour accéder à des services de >Access de stratégies > l'admin > l'autorisation de périphérique de par défaut. Créez une nouvelle stratégie d'autorisation appelée l'autorisation WAAS. Ceci vérifie des demandes de WAAS. Dans cet exemple, l'IP de périphérique est utilisé comme condition. Cependant, ceci peut être changé a basé sur les conditions requises de déploiement. Appliquez le profil de shell et commandez les positionnements configurés dans les étapes 2 et 3 en cela section.



Configuration sur le WAAS

1. Afin de définir un serveur TACACS+, naviguez vers des périphériques > système <Central Name> de gestionnaire > configurent > Sécurité > AAA > TACACS+. Configurez l'adresse IP de serveur ACS et la clé pré-partagée.

Devices > pi-wavecm01 > Configure > Security > AAA > TACACS+

TACACS+ Server Settings for Central Manager, [redacted] Print Apply Defaults Remove Settings

TACACS+ Server Settings

Use ASCII Password Authentication:

Time to Wait: (seconds) (1-20)

Number of Retransmits: (1-3)

Security Word:

Primary Server: Primary Server Port:

Secondary Server: Secondary Server Port:

Tertiary Server: Tertiary Server Port:

* To use TACACS+ for Login or Configuration Authentication, please go to the Authentication Methods page.

2. Afin de modifier l'authentification et les autorizations method, naviguez vers des **périphériques > système <Central Name> de gestionnaire > configurer > Sécurité > AAA > méthodes d'authentification**. Dans ce tir d'écran, la méthode de procédure de connexion primaire est configurée pour des **gens du pays** avec le secondaire configuré pour **TACACS+**.

Devices > pi-wavecm01 > Configure > Security > AAA > Authentication Methods

Authentication and Authorization Methods for Central Manager, pi-wave... Print Apply Defaults Remove Settings

Authentication and Authorization Methods

Fallover to next available authentication method:

Authentication Login Methods: It is highly recommended to set the auther

Primary Login Method:

Secondary Login Method:

Tertiary Login Method:

Quaternary Login Method:

Authorization Methods:

Primary Configuration Method:

Secondary Configuration Method:

Tertiary Configuration Method:

Quaternary Configuration Method:

3. Naviguez pour **autoguidé > admin > AAA > groupes d'utilisateurs** afin d'ajouter le nom de groupe qui apparie la **valeur d'attribut personnalisé** (voir l'étape 2 dans la section du **configurer ACS**) dans WAAS.

Home > Admin > AAA > User Groups

Creating New User Group 

User Group Information

Name:

Comments

Note: * - Required Field

- Attribuez les droits **niveau de l'admin** de ce groupe (Test_Group) sur la **maison > l'admin > l'AAA > l'onglet de Gestion de rôle de groupes d'utilisateurs**. Le rôle d'admin sur le gestionnaire central est préconfiguré.

Home > Admin > AAA > User Groups

External User Group Management **Role Management** Domain Management

 Refresh Table  Assign all Roles  Remove all Roles

Roles

Filter: Name Match if: like

Role	Admin role
  admin	Admin role

Vérifiez

Tentative d'ouvrir une session à WAAS avec des qualifications TACACS+. Si tout est configuré correctement, on t'accorde l'accès.

Dépannez

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