Configuration de TACACS+ pour un réseau sans fil unifié Cisco

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Mise en oeuvre de TACACS+ dans le contrôleur
Authentification
Autorisation
Gestion de comptes
Configuration TACACS+ dans le WLC
Ajouter un serveur d'authentification TACACS+
Ajouter un serveur d'autorisation TACACS+
Ajouter un serveur de comptabilité TACACS+
Configurer l'ordre d'authentification
Vérifier la configuration
Configurer le serveur Cisco Secure ACS
Configuration du réseau
Configuration de l'interface
Configuration utilisateur/groupe
Enregistrements comptables dans Cisco Secure ACS
Configuration TACACS+ dans WCS
WCS à l'aide de domaines virtuels
Configurer Cisco Secure ACS pour utiliser WCS
Configuration du réseau
Configuration de l'interface
Configuration utilisateur/groupe
Déboguages
Débogues à partir du WLC pour role1=ALL
Débogues de WLC pour plusieurs rôles
Débogues à partir d'un WLC en cas d'échec d'autorisation
Informations connexes

Introduction

Ce document fournit un exemple de configuration du Terminal Access Controller Access Control System Plus (TACACS+) dans un contrôleur LAN sans fil Cisco (WLC) et un système de contrôle

sans fil Cisco (WCS) pour un réseau sans fil unifié Cisco. Ce document fournit également quelques conseils de dépannage de base.

TACACS+ est un protocole client/serveur qui fournit une sécurité centralisée aux utilisateurs qui tentent d'obtenir un accès de gestion à un routeur ou à un serveur d'accès au réseau. TACACS+ fournit les services AAA suivants :

- Authentification des utilisateurs qui tentent de se connecter à l'équipement réseau
- Autorisation permettant de déterminer le niveau d'accès que les utilisateurs doivent avoir
- Comptabilité permettant de suivre toutes les modifications apportées par l'utilisateur

Référez-vous à Configuration de TACACS+ pour plus d'informations sur les services AAA et la fonctionnalité TACACS+.

Référez-vous à Comparaison TACACS+ et RADIUS pour une comparaison de TACACS+ et RADIUS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la configuration des WLC et des points d'accès légers (LAP) pour le fonctionnement de base
- Connaissance du protocole LWAPP (Lightweight Access Point Protocol) et des méthodes de sécurité sans fil
- Connaissances de base RADIUS et TACACS+
- Connaissance de base de la configuration Cisco ACS

Components Used

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

- Cisco Secure ACS pour Windows version 4.0
- Contrôleur LAN sans fil Cisco qui exécute la version 4.1.171.0. La fonctionnalité TACACS+ sur les WLC est prise en charge sur le logiciel version 4.1.171.0 ou ultérieure.
- Cisco Wireless Control System qui exécute la version 4.1.83.0. La fonctionnalité TACACS+ sur WCS est prise en charge sur le logiciel version 4.1.83.0 ou ultérieure.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Mise en oeuvre de TACACS+ dans le contrôleur

Authentification

L'authentification peut être effectuée à l'aide d'une base de données locale, d'un serveur RADIUS ou TACACS+ qui utilise un nom d'utilisateur et un mot de passe. La mise en oeuvre n'est pas entièrement modulaire. Les services d'authentification et d'autorisation sont liés les uns aux autres. Par exemple, si l'authentification est effectuée à l'aide de la base de données RADIUS/locale, l'autorisation n'est pas effectuée avec TACACS+. Il utiliserait les autorisations associées à l'utilisateur dans la base de données locale ou RADIUS, telles que lecture seule ou lecture-écriture, alors que lorsque l'authentification est effectuée avec TACACS+, l'autorisation est liée à TACACS+.

Dans les cas où plusieurs bases de données sont configurées, une interface de ligne de commande est fournie pour déterminer la séquence dans laquelle la base de données principale doit être référencée.

Autorisation

L'autorisation est basée sur des tâches plutôt que sur une autorisation réelle par commande. Les tâches sont mappées à différents onglets correspondant aux sept éléments de la barre de menus actuellement sur l'interface utilisateur graphique Web. Il s'agit des éléments de la barre de menus :

- MONITOR
- WLAN
- CONTRÔLEUR
- SOLUTIONS SANS FIL
- SÉCURITÉ
- GESTION
- COMMANDE

La raison de ce mappage est basée sur le fait que la plupart des clients utilisent l'interface Web pour configurer le contrôleur au lieu de l'interface de ligne de commande.

Un rôle supplémentaire pour la gestion de l'administration du hall (LOBBY) est disponible pour les utilisateurs qui ont besoin de privilèges d'administration du hall uniquement.

La tâche à laquelle un utilisateur a droit est configurée dans le serveur TACACS+ (ACS) à l'aide des paires attribut-valeur (AV) personnalisées. L'utilisateur peut être autorisé pour une ou plusieurs tâches. L'autorisation minimale est MONITOR uniquement et la valeur maximale est ALL (autorisé à exécuter les sept onglets). Si un utilisateur n'a pas droit à une tâche particulière, il est toujours autorisé à accéder à cette tâche en lecture seule. Si l'authentification est activée et que le serveur d'authentification devient inaccessible ou impossible à autoriser, l'utilisateur ne peut pas se connecter au contrôleur.

Remarque : Pour que l'authentification de gestion de base via TACACS+ réussisse, vous devez configurer les serveurs d'authentification et d'autorisation sur le WLC. La configuration de la comptabilité est facultative.

Gestion de comptes

La comptabilité se produit chaque fois qu'une action initiée par l'utilisateur est exécutée avec succès. Les attributs modifiés sont consignés dans le serveur de comptabilité TACACS+ avec les éléments suivants :

- ID utilisateur de la personne qui a effectué la modification
- Hôte distant à partir duquel l'utilisateur est connecté
- Date et heure auxquelles la commande a été exécutée
- Niveau d'autorisation de l'utilisateur
- Chaîne fournissant des informations sur l'action exécutée et les valeurs fournies

Si le serveur de comptabilité devient inaccessible, l'utilisateur peut continuer la session.

Remarque : Les enregistrements comptables ne sont pas générés à partir de WCS dans la version 4.1 ou antérieure du logiciel.

Configuration TACACS+ dans le WLC

Le logiciel WLC version 4.1.171.0 et ultérieure introduit de nouvelles CLI et des modifications de l'interface utilisateur graphique Web afin d'activer la fonctionnalité TACACS+ sur le WLC. Les CLI présentées sont répertoriées dans cette section à titre de référence. Les modifications correspondantes pour l'interface utilisateur graphique Web sont ajoutées sous l'onglet Sécurité.

Ce document suppose que la configuration de base du WLC est déjà terminée.

Afin de configurer TACACS+ dans le contrôleur WLC, vous devez effectuer les étapes suivantes :

1. Ajouter un serveur d'authentification TACACS+
2. Ajouter un serveur d'autorisation TACACS+
3. Ajouter un serveur de comptabilité TACACS+
4. Configurer l'ordre d'authentification

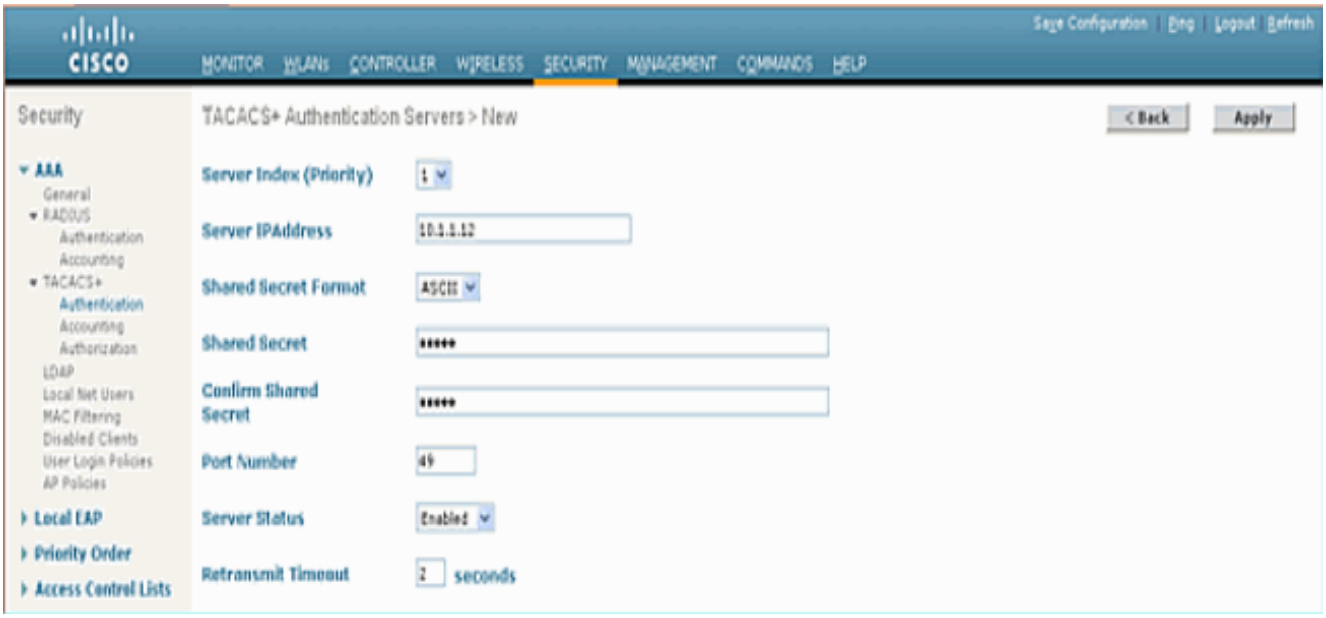
Ajouter un serveur d'authentification TACACS+

Complétez ces étapes afin d'ajouter un serveur d'authentification TACACS+ :

1. Utilisez l'interface utilisateur graphique et accédez à **Security > TACACS+ > Authentication**.



2. Ajoutez l'adresse IP du serveur TACACS+ et saisissez la clé secrète partagée. Si nécessaire, modifiez le port par défaut de TCP/49.



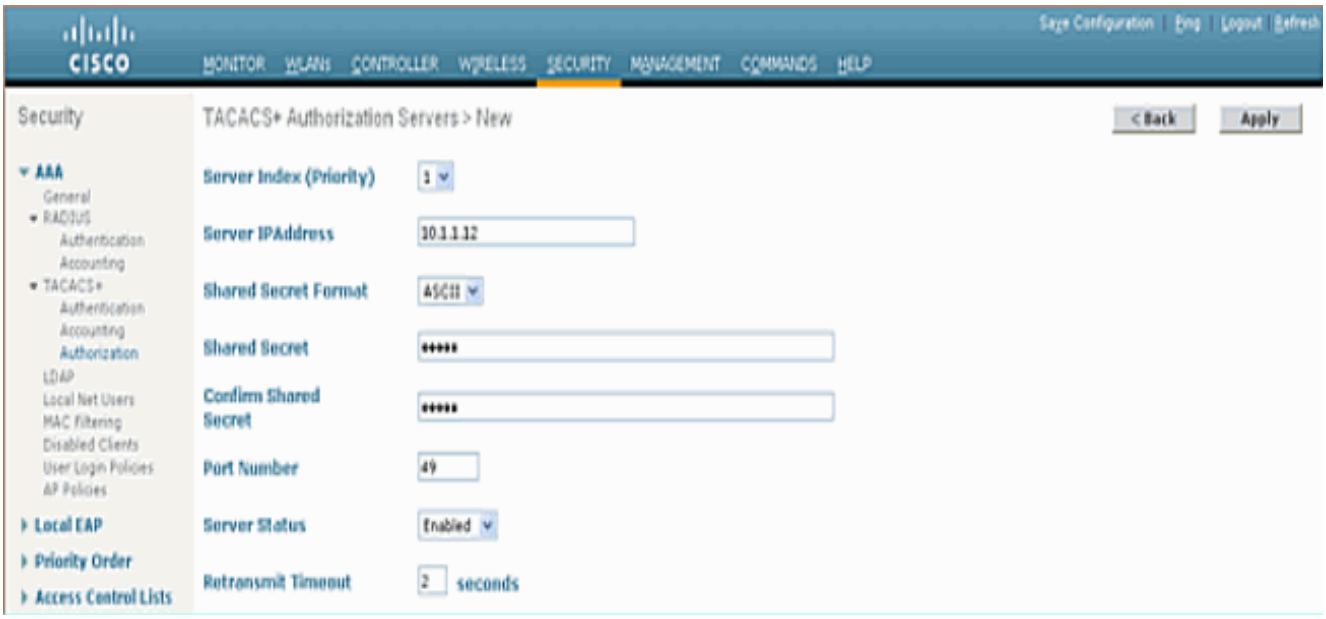
3. Cliquez sur Apply.Vous pouvez accomplir cela à partir de l'interface de ligne de commande à l'aide de la commande **config tacacs auth add** *<Index du serveur> <adresse IP> <port> [ascii/hex]* **<secret>** :

```
(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123
```

Ajouter un serveur d'autorisation TACACS+

Complétez ces étapes afin d'ajouter un serveur d'autorisation TACACS+ :

1. Àpartir de l'interface utilisateur graphique, accédez à **Security > TACACS+ > Authorization**.
2. Ajoutez l'adresse IP du serveur TACACS+ et saisissez la clé secrète partagée. Si nécessaire, modifiez le port par défaut de TCP/49.



3. Cliquez sur Apply.Vous pouvez accomplir cela à partir de l'interface de ligne de commande à l'aide de la commande **config tacacs athr add** *<Server Index> <IP addr> <port> [ascii/hex]* **<secret>** :

```
(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123
```

Ajouter un serveur de comptabilité TACACS+

Complétez ces étapes afin d'ajouter un serveur de comptabilité TACACS+ :

1. Utilisez l'interface utilisateur graphique et accédez à **Security > TACACS+ > Accounting**.
2. Ajoutez l'adresse IP du serveur et saisissez la clé secrète partagée. Si nécessaire, modifiez le port par défaut de
   TCP/49.



3. Cliquez sur Apply.Vous pouvez effectuer cette opération à partir de l'interface de ligne de commande à l'aide de la commande **config tacacs acct add** *<Server Index> <IP addr> <port> [ascii/hex]* **<secret>** :

```
(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123
```

Configurer l'ordre d'authentification

Cette étape explique comment configurer l'ordre d'authentification AAA lorsqu'il y a plusieurs bases de données configurées. L'ordre d'authentification peut être **local et RADIUS**, ou **local et TACACS**. La configuration par défaut du contrôleur pour l'ordre d'authentification est *local et RADIUS*.

Complétez ces étapes afin de configurer l'ordre d'authentification :

1. Àpartir de l'interface utilisateur graphique, accédez à **Sécurité > Ordre de priorité > Utilisateur de gestion**.
2. Sélectionnez Authentication Priority (Priorité d'authentification).Dans cet exemple, TACACS+ a été sélectionné.
3. Cliquez sur **Apply** afin que la sélection ait
   lieu.



Vous pouvez accomplir cela à partir de l'interface de ligne de commande à l'aide de la commande **config aaa auth mgmt** *<server1> <server2>* :

```
(Cisco Controller) >config aaa auth mgmt tacacs local
```

Vérifier la configuration

Cette section décrit les commandes utilisées pour vérifier la configuration TACACS+ sur le WLC. Voici quelques commandes **show** utiles qui permettent de déterminer si la configuration est correcte :

- **show aaa auth** - Fournit des informations sur l'ordre de l'authentification.

```
(Cisco Controller) >show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... Tacacs
```

- **show tacacs summary** : affiche un résumé des services et statistiques TACACS+.

```
(Cisco Controller) >show tacacs summary
Authentication Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Authorization Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2
```

- **show tacacs auth stats** : affiche les statistiques du serveur d'authentification TACACS+.

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:

Server Index..................................... 1
Server Address..................................... 10.1.1.12
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 7
Retry Requests................................... 3
Accept Responses................................. 3
```

```
Reject Responses.............................. 0
Error Responses............................... 0
Restart Responses............................. 0
Follow Responses.............................. 0
GetData Responses............................. 0
Encrypt no secret Responses................... 0
Challenge Responses........................... 0
Malformed Msgs................................ 0
Bad Authenticator Msgs........................ 0
Timeout Requests.............................. 12
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

- **show tacacs athr stats** : affiche les statistiques du serveur d'autorisation TACACS+.

```
(Cisco Controller) >show tacacs athr statistics
Authorization Servers:

Server Index.................................. 1
Server Address................................ 10.1.1.12
Msg Round Trip Time........................... 0 (1/100 second)
First Requests................................ 3
Retry Requests................................ 3
Received Responses............................ 3
Authorization Success......................... 3
Authorization Failure......................... 0
Challenge Responses........................... 0
Malformed Msgs................................ 0
Bad Athrenticator Msgs........................ 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

- **show tacacs acct stats** : affiche les statistiques du serveur de comptabilité TACACS+.

```
(Cisco Controller) >show tacacs acct statistics
Accounting Servers:

Server Index.................................. 1
Server Address................................ 10.1.1.12
Msg Round Trip Time........................... 0 (1/100 second)
First Requests................................ 133
Retry Requests................................ 0
Accounting Response........................... 0
Accounting Request Success.................... 0
Accounting Request Failure.................... 0
Malformed Msgs................................ 0
Bad Authenticator Msgs........................ 0
Timeout Requests.............................. 399
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

Configurer le serveur Cisco Secure ACS

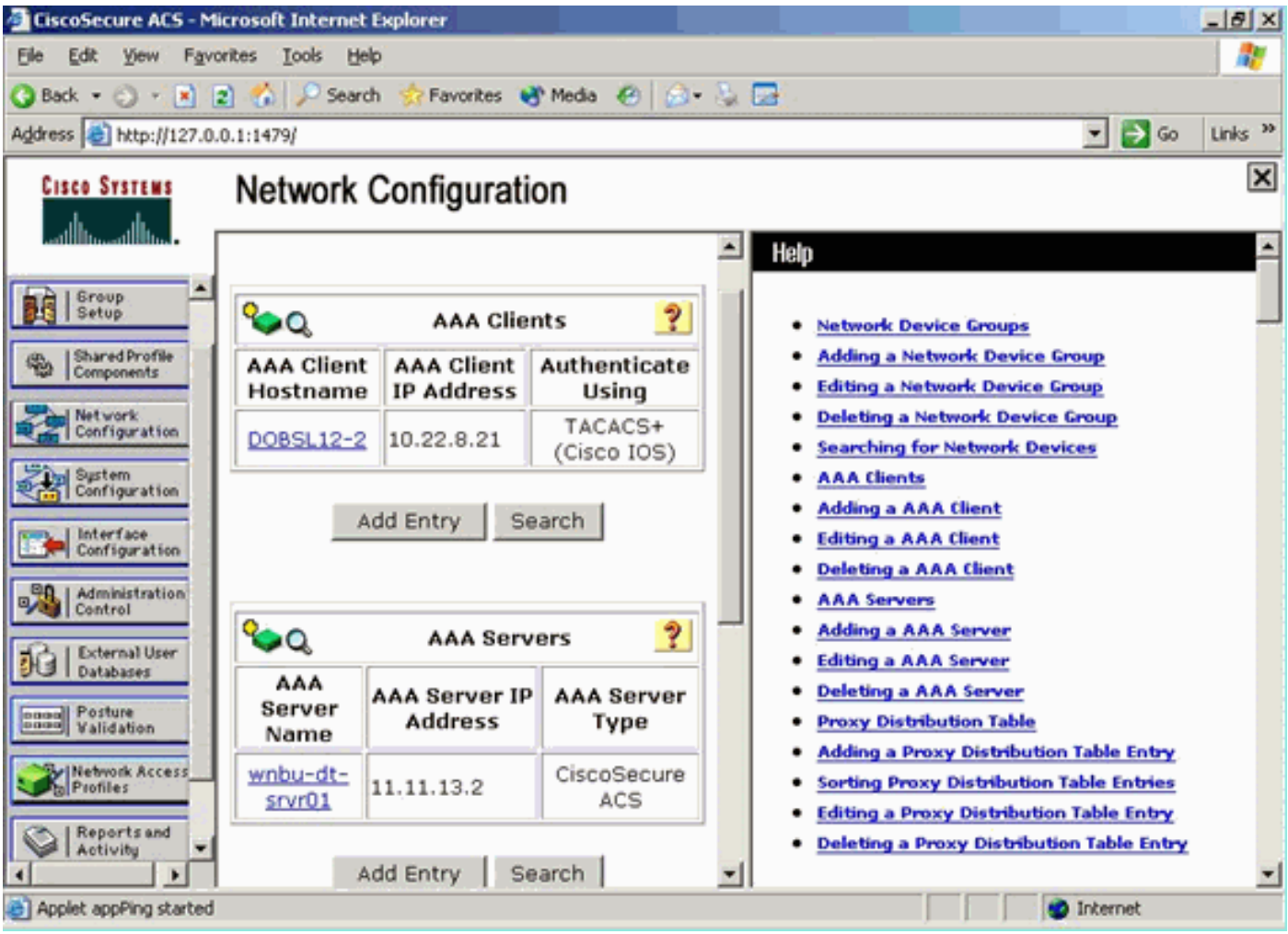
Cette section décrit les étapes à suivre dans le serveur TACACS+ ACS pour créer des services et des attributs personnalisés, et pour attribuer les rôles aux utilisateurs ou aux groupes.

La création d'utilisateurs et de groupes n'est pas expliquée dans cette section. On suppose que les utilisateurs et les groupes sont créés en fonction des besoins. Reportez-vous au Guide de l'utilisateur de Cisco Secure ACS pour Windows Server 4.0 pour plus d'informations sur la création d'utilisateurs et de groupes d'utilisateurs.

Configuration du réseau

Complétez cette étape :

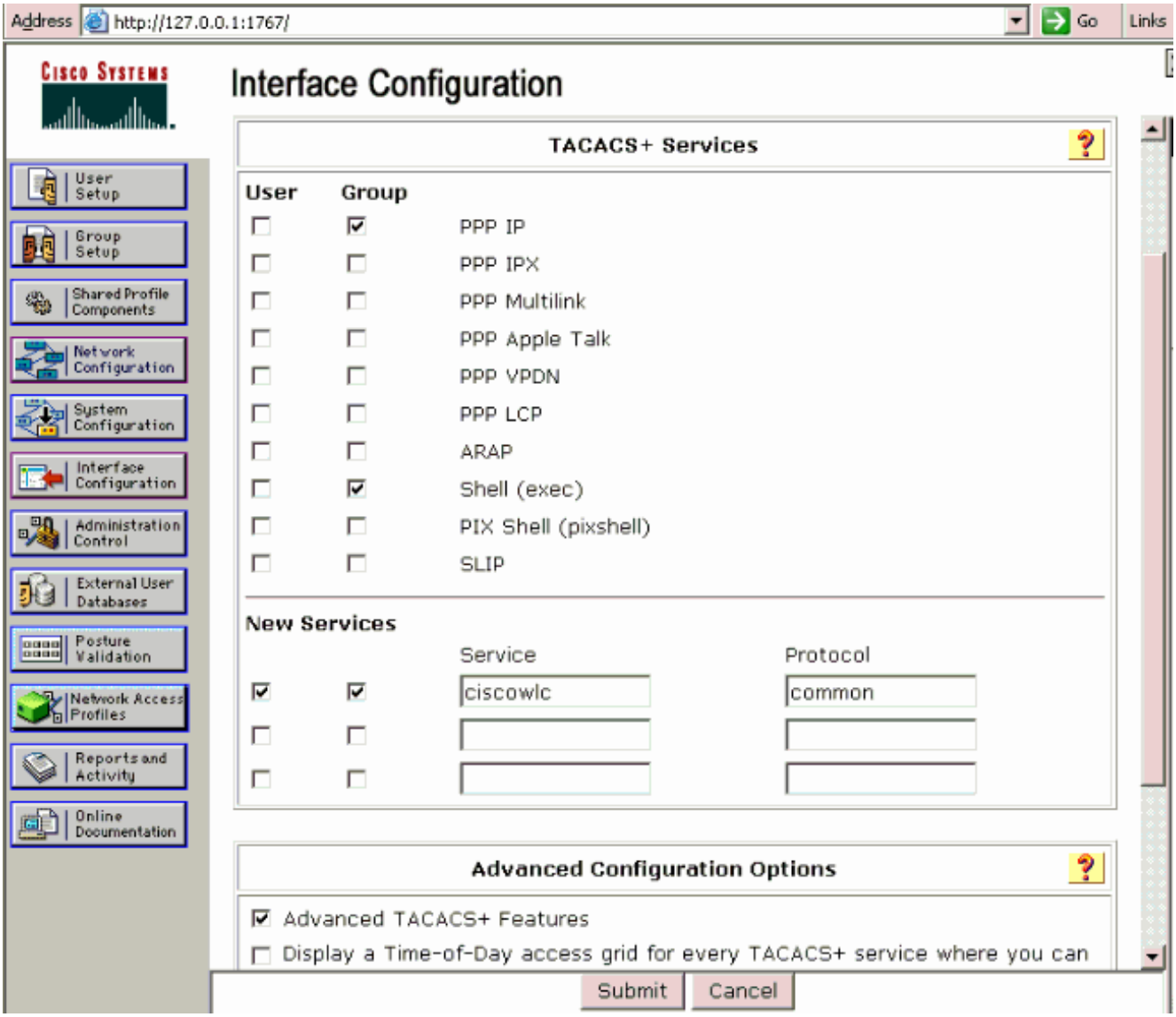
Ajoutez l'adresse IP de gestion du contrôleur en tant que client AAA avec le mécanisme d'authentification TACACS+ (Cisco IOS).



Configuration de l'interface

Procédez comme suit :

1. Dans le menu Interface Configuration, sélectionnez le lien **TACACS+** (Cisco IOS).
2. Activez les **nouveaux services**.
3. Cochez les cases **Utilisateur** et **Groupe**.
4. Entrez **ciscowlc** pour Service et **common** pour Protocol.
5. Activez les **fonctionnalités TACACS+ avancées**.

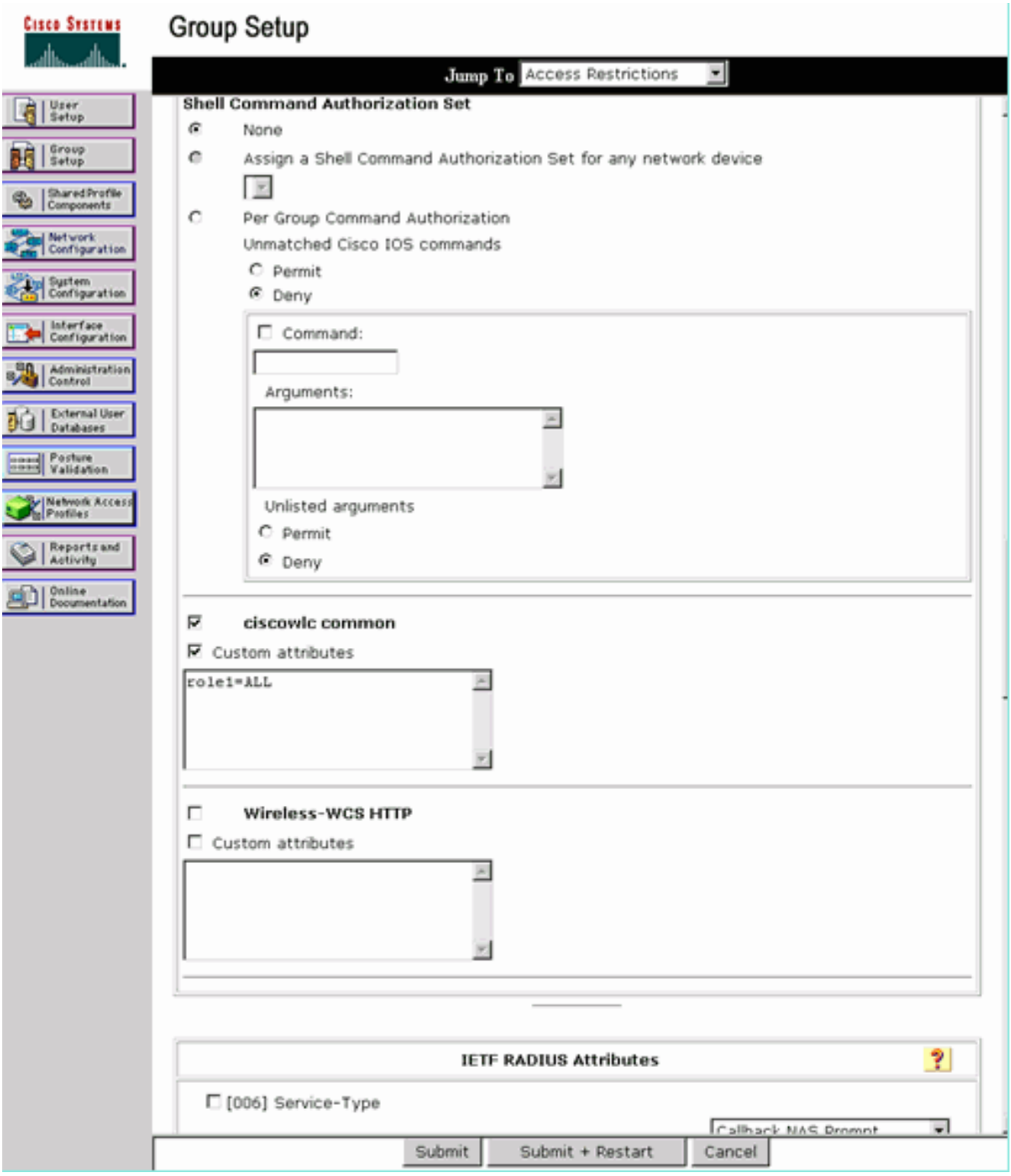


6. Cliquez sur **Soumettre** afin d'appliquer les modifications.

Configuration utilisateur/groupe

Procédez comme suit :

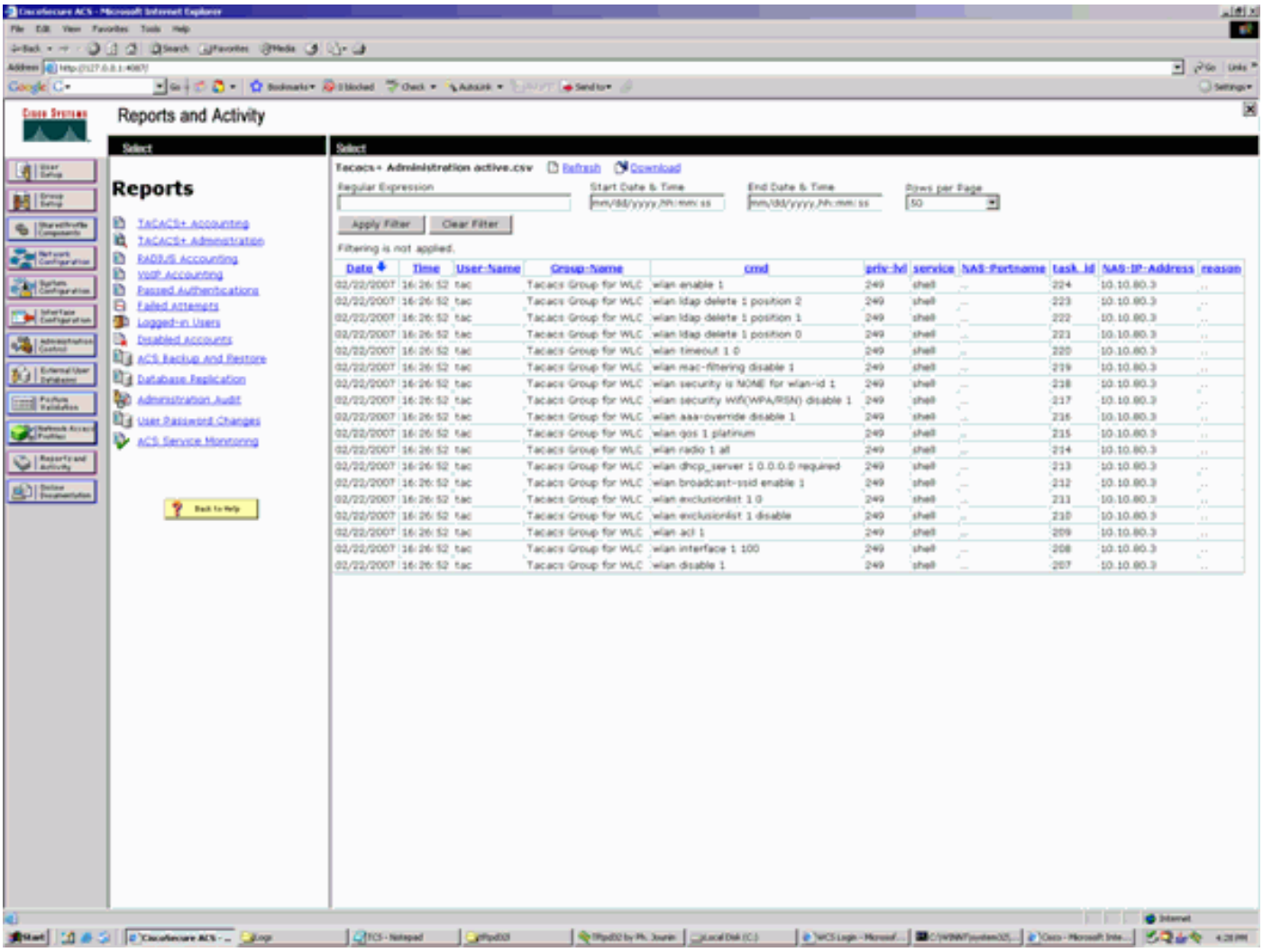
1. Sélectionnez un utilisateur/groupe précédemment créé.
2. Accédez à **Paramètres TACACS+**.
3. Cochez la case qui correspond au service *ciscowlc* créé dans la section Configuration de l'interface.
4. Cochez la case **Attributs personnalisés**.



5. Dans la zone de texte sous Attributs personnalisés, saisissez ce texte si l'utilisateur créé a besoin d'un accès uniquement au WLAN, à la SÉCURITÉ et au CONTRÔLEUR : **role1=Rôle WLAN2=Rôle SECURITY3=CONTRÔLEUR**.Si l'utilisateur doit accéder uniquement à l'onglet SECURITY (SÉCURITÉ), saisissez le texte suivant : **role1=SÉCURITÉ**.Le rôle correspond aux sept éléments de la barre de menus de l'interface utilisateur graphique Web du contrôleur. Les éléments de la barre de menus sont MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT and COMMAND.
6. Saisissez le rôle dont un utilisateur a besoin pour role1, role2, etc. Si un utilisateur a besoin de tous les rôles, le mot clé **ALL** doit être utilisé. Pour le rôle admin du hall, le mot clé **LOBBY** doit être utilisé.

Enregistrements comptables dans Cisco Secure ACS

Les enregistrements comptables TACACS+ du WLC sont disponibles dans Cisco Secure ACS dans TACACS+ Administration des rapports et de l'activité :



Configuration TACACS+ dans WCS

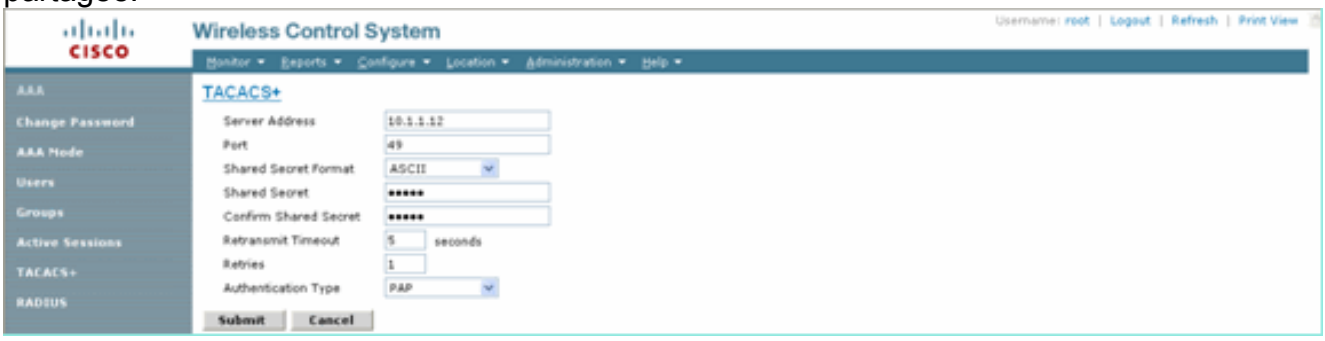
Procédez comme suit :

1. Àpartir de l'interface utilisateur graphique, connectez-vous au WCS avec le compte racine.
2. Ajoutez le serveur TACACS+. Accédez à **Administration > AAA > TACACS+ > Ajouter un serveur TACACS+**.



3. Ajoutez les détails du serveur TACACS+, tels que l'adresse IP, le numéro de port (49 par

défaut) et la clé secrète partagée.



4. Activez l'authentification TACACS+ pour l'administration dans WCS. Accédez à **Administration > AAA > Mode AAA > Sélectionnez TACACS+**.



WCS à l'aide de domaines virtuels

Virtual Domain est une nouvelle fonctionnalité introduite avec WCS version 5.1. Un domaine virtuel WCS se compose d'un ensemble de périphériques et de mappages et limite la vue d'un utilisateur aux informations relatives à ces périphériques et mappages. Par le biais d'un domaine virtuel, un administrateur peut s'assurer que les utilisateurs ne peuvent afficher que les périphériques et les cartes dont ils sont responsables. En outre, en raison des filtres du domaine virtuel, les utilisateurs peuvent configurer, afficher les alarmes et générer des rapports uniquement pour la partie du réseau qui leur est attribuée. L'administrateur spécifie un ensemble de domaines virtuels autorisés pour chaque utilisateur. Seul l'un d'eux peut être actif pour cet utilisateur à la connexion. L'utilisateur peut modifier le domaine virtuel actuel en sélectionnant un autre domaine virtuel autorisé dans le menu déroulant Domaine virtuel en haut de l'écran. Tous les rapports, alarmes et autres fonctionnalités sont désormais filtrés par ce domaine virtuel.

Si un seul domaine virtuel (racine) est défini dans le système et que l'utilisateur ne possède aucun domaine virtuel dans les champs d'attributs personnalisés du serveur TACACS+/RADIUS, le domaine virtuel racine est attribué par défaut à l'utilisateur.

S'il existe plusieurs domaines virtuels et que l'utilisateur n'a aucun attribut spécifié, l'utilisateur est bloqué pour se connecter. Pour permettre à l'utilisateur de se connecter, les attributs personnalisés du domaine virtuel doivent être exportés vers le serveur Radius/TACACS+.

La fenêtre Attributs personnalisés du domaine virtuel vous permet d'indiquer les données spécifiques au protocole appropriées pour chaque domaine virtuel. Le bouton Exporter de la barre latérale Hiérarchie de domaine virtuel préformate les attributs RADIUS et TACACS+ du domaine virtuel. Vous pouvez copier et coller ces attributs dans le serveur ACS. Cela vous permet de copier uniquement les domaines virtuels applicables sur l'écran du serveur ACS et garantit que les utilisateurs n'ont accès qu'à ces domaines virtuels.

Afin d'appliquer les attributs RADIUS et TACACS+ préformatés au serveur ACS, complétez les étapes décrites dans la section Attributs RADIUS et TACACS+ du domaine virtuel.

Configurer Cisco Secure ACS pour utiliser WCS

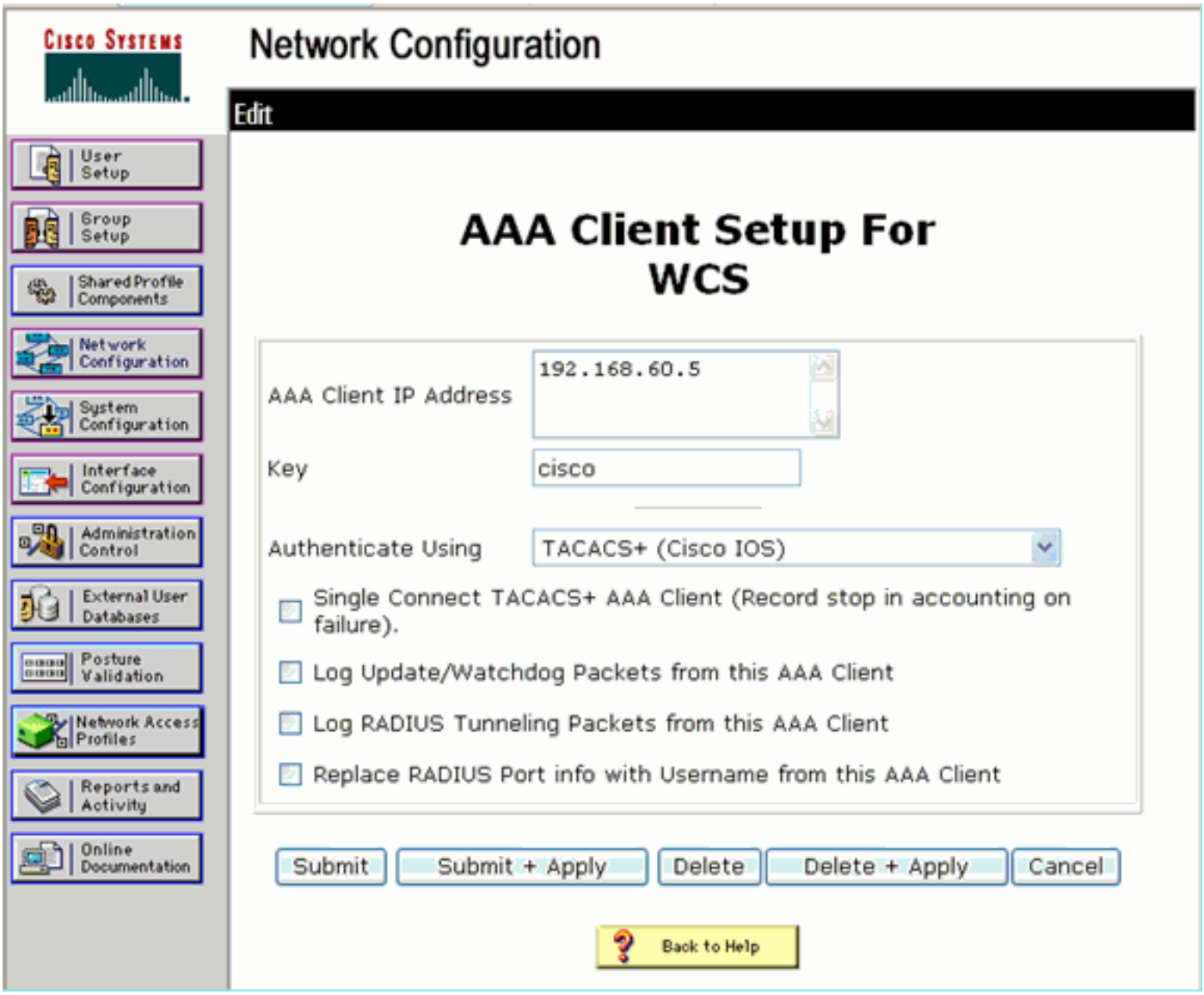
La section décrit les étapes à suivre dans le serveur TACACS+ ACS pour créer des services et des attributs personnalisés, et pour attribuer les rôles aux utilisateurs ou aux groupes.

La création d'utilisateurs et de groupes n'est pas expliquée dans cette section. On suppose que les utilisateurs et les groupes sont créés en fonction des besoins.

Configuration du réseau

Complétez cette étape :

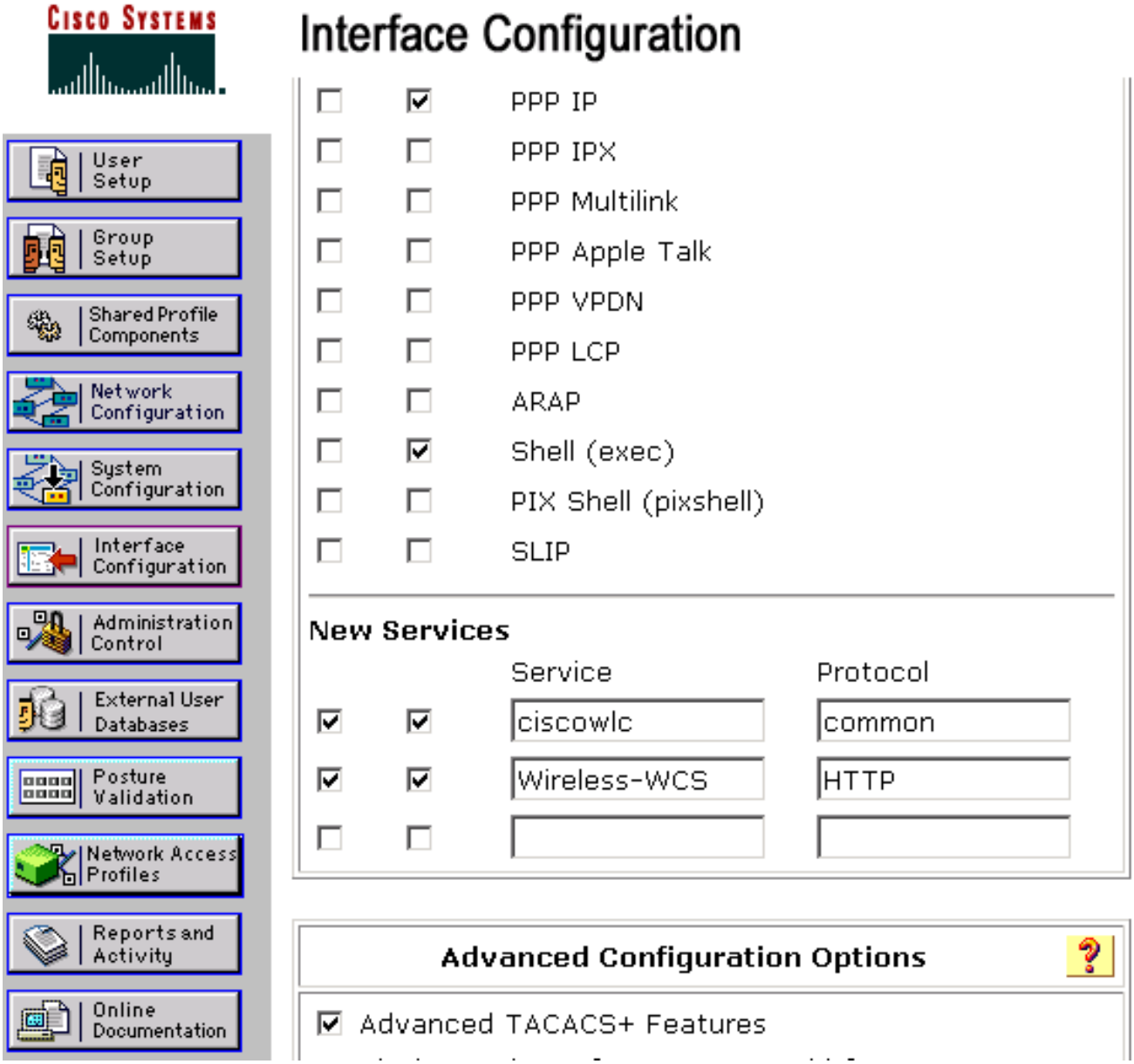
Ajoutez l'adresse IP WCS en tant que client AAA avec le mécanisme d'authentification TACACS+ (Cisco IOS).



Configuration de l'interface

Procédez comme suit :

1. Dans le menu Interface Configuration, sélectionnez le lien **TACACS+** (Cisco IOS).
2. Activez les **nouveaux services**.
3. Cochez les cases **Utilisateur** et **Groupe**.
4. Entrez **Wireless-WCS** for Service et **HTTP** for Protocol.**Remarque :** HTTP doit être dans CAPS.
5. Activez les **fonctionnalités TACACS+ avancées**.

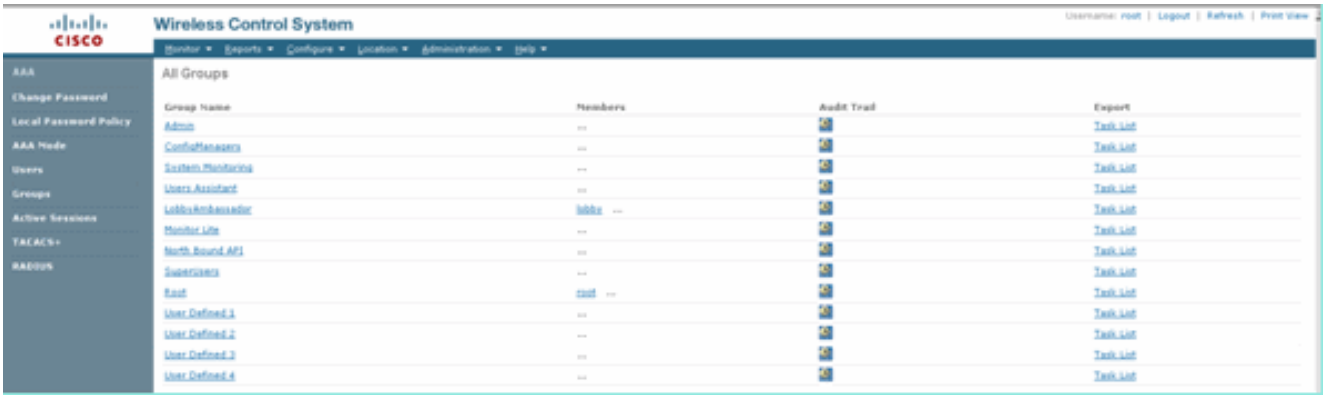


6. Cliquez sur **Soumettre** afin d'appliquer les modifications.

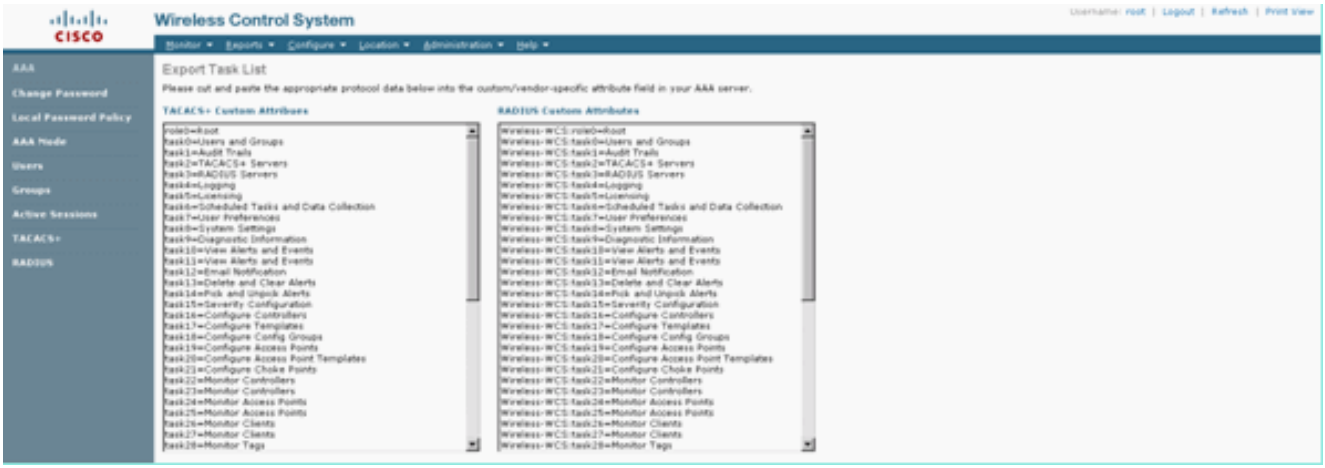
Configuration utilisateur/groupe

Procédez comme suit :

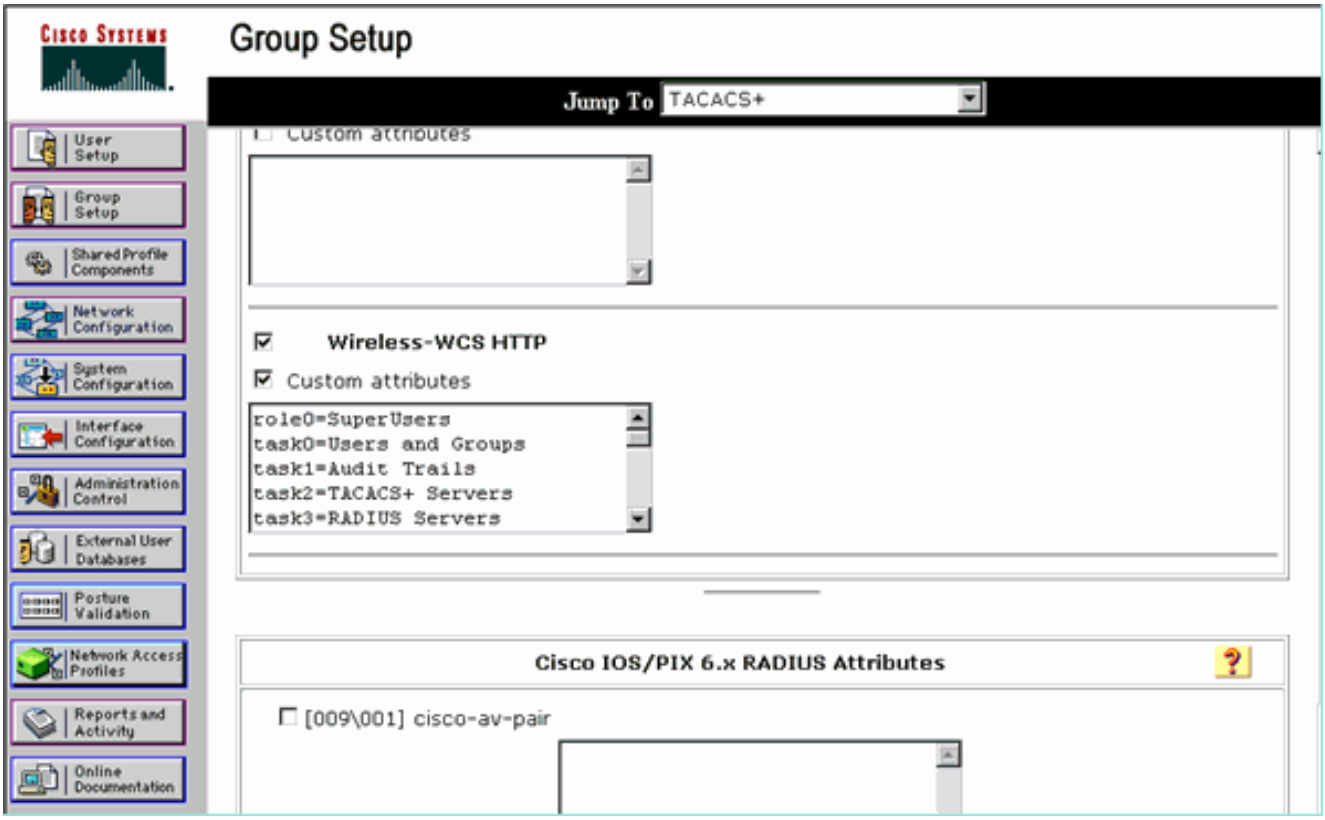
1. Dans l'interface utilisateur graphique WCS, accédez à **Administration > AAA > Groups** pour sélectionner l'un des groupes d'utilisateurs préconfigurés, tels que SuperUsers dans WCS.



2. Sélectionnez la liste des tâches pour les groupes d'utilisateurs préconfigurés et copiez le collage dans
ACS.



3. Sélectionnez un utilisateur/groupe précédemment créé et accédez à **Paramètres TACACS+**.
4. Dans l'interface utilisateur graphique ACS, activez la case à cocher correspondant au service Wireless-WCS créé précédemment.
5. Dans l'interface utilisateur graphique ACS, cochez la case **Attributs personnalisés**.
6. Dans la zone de texte située sous Attributs personnalisés, entrez ce rôle et les informations de tâche copiées à partir de WCS. Par exemple, entrez la liste des tâches autorisées par les SuperUtilisateurs.



7. Ensuite, connectez-vous au WCS avec le nom d'utilisateur/mot de passe nouvellement créé dans l'ACS.

Déboguages

Débogues à partir du WLC pour role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable

(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
```

Débogues de WLC pour plusieurs rôles

```
(Cisco Controller) >debug aaa tacacs enable

Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
```

```
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

Débogues à partir d'un WLC en cas d'échec d'autorisation

```
(Cisco Controller) >debug aaa tacacs enable

Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007:User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

Informations connexes

- Exemple de configuration de Cisco Wireless LAN Controller (WLC) et Cisco ACS 5.x (TACACS+) pour l'authentification Web
- Configuration de TACACS+
- Configuration de l'authentification et de l'autorisation TACACS pour les utilisateurs Admin et non Admin dans ACS 5.1
- Comparaison entre TACACS+ et RADIUS
- Support et documentation techniques - Cisco Systems