Configuration de TACACS+ pour un réseau sans fil unifié Cisco

Contenu

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 de client/serveur qui fournit la Sécurité centralisée pour les utilisateurs qui tentent de gagner l'accès de Gestion à un routeur ou à un serveur d'accès à distance. TACACS+ fournit ces services d'AAA :

- Authentification des utilisateurs tentant d'ouvrir une session à l'équipement réseau
- Autorisation de déterminer ce que les utilisateurs de niveau d'accès devraient avoir
- La comptabilité pour maintenir toutes les modifications l'utilisateur fait

Référez-vous à configurer TACACS+ pour plus d'informations sur des services d'AAA et la fonctionnalité TACACS+.

Référez-vous à la comparaison TACACS+ et de RAYON pour une comparaison de TACACS+ et de RAYON.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la façon configurer WLCs et Point d'accès léger (recouvrements) pour le fonctionnement de base
- La connaissance du point d'accès léger Protocol (LWAPP) et des méthodes de sécurité sans fil
- RAYON de connaissance de base et TACACS+
- Connaissance de base de configuration de Cisco ACS

Composants utilisés

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

- Cisco Secure ACS pour la version 4.0 de Windows
- Contrôleur LAN Sans fil de Cisco qui exécute la version 4.1.171.0. La fonctionnalité TACACS+ sur WLCs est prise en charge sur version de logiciel 4.1.171.0 ou plus tard.
- Système de contrôle sans fil Cisco qui exécute la version 4.1.83.0. La fonctionnalité TACACS+ sur WCS est prise en charge sur version de logiciel 4.1.83.0 ou plus tard.

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.

Conventions

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

Implémentation TACACS+ dans le contrôleur

Authentification

L'authentification peut être exécutée utilisant une base de données locale, un serveur de RAYON, ou TACACS+ qui utilise un nom d'utilisateur et un mot de passe. L'implémentation n'est pas entièrement modulaire. Des services d'authentification et d'autorisation sont attachés entre eux. Par exemple, si l'authentification est exécutée utilisant la base de données RADIUS/local, puis l'autorisation n'est pas exécutée avec TACACS+. Il utiliserait les autorisations associées pour l'utilisateur dans les gens du pays ou base de données de RAYON, telle qu'en lecture seule ou lecture/écriture, tandis que quand l'authentification est exécutée avec TACACS+, l'autorisation est attachée à TACACS+.

Dans les cas où de plusieurs bases de données sont configurées, un CLI est fourni pour dicter l'ordre dans lequel la base de données principale devrait être référée.

Autorisation

L'autorisation est tâche basée plutôt qu'une autorisation basée parcommande réelle. Les tâches sont tracées aux divers onglets qui correspondent aux sept éléments de barre de menus qui sont actuellement sur le GUI de Web. Ce sont les éléments de barre de menus :

- MONITEUR
- WLANS
- CONTRÔLEUR
- RADIO
- SÉCURITÉ
- GESTION
- COMMANDE

La raison pour ce mappage est basée sur le fait que la plupart des clients emploient l'interface web pour configurer le contrôleur au lieu du CLI.

Un rôle supplémentaire pour la Gestion d'admin de lobby (LOBBY) est disponible pour les utilisateurs qui doivent avoir des privilèges d'admin de lobby seulement.

La tâche qu'un utilisateur est autorisé est configurée dans le serveur TACACS+ (ACS) utilisant les paires faites sur commande de l'Attribut-valeur (poids du commerce). L'utilisateur peut être autorisé pour un ou des tâches de multiple. L'autorisation minimum est MONITEUR seulement et le maximum est TOUT (autorisé à exécuter chacun des sept onglets). Si un utilisateur n'est pas autorisé pour une tâche particulière, on permet encore à l'l'utilisateur pour accéder à cette tâche en mode en lecture seule. Si l'authentification est activée et le serveur d'authentification devient inaccessible ou incapable d'autoriser, l'utilisateur ne peut pas ouvrir une session au contrôleur.

Remarque: Afin de l'authentification de Gestion de base par l'intermédiaire de TACACS+ à réussir, vous devez configurer des serveurs d'authentification et d'autorisation sur le WLC. La configuration de comptabilité est facultative.

Comptabilité

La comptabilité se produit toutes les fois qu'une action utilisateur-initiée par détail est exécutée

avec succès. Les attributs changés sont ouverts une session le serveur de comptabilité TACACS+ avec ces derniers :

- L'user-id de la personne qui a apporté la modification
- Le serveur distant d'où l'utilisateur est ouvert une session
- La date et le moment où la commande a été exécutée
- Niveau d'autorisation de l'utilisateur
- Une chaîne qui fournit des informations quant à quelle action a été exécutée et les valeurs fournies

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

Remarque: Des enregistrements des comptes ne sont pas générés de WCS dans la version de logiciel 4.1 ou plus tôt.

Configuration TACACS+ dans le WLC

La version logicielle 4.1.171.0 WLC et introduit plus tard nouveau CLIs et le GUI de Web change afin d'activer la fonctionnalité TACACS+ sur le WLC. Le CLIs introduit sont répertoriés dans cette section pour la référence. Les modifications correspondantes pour le GUI de 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 se terminer ces étapes :

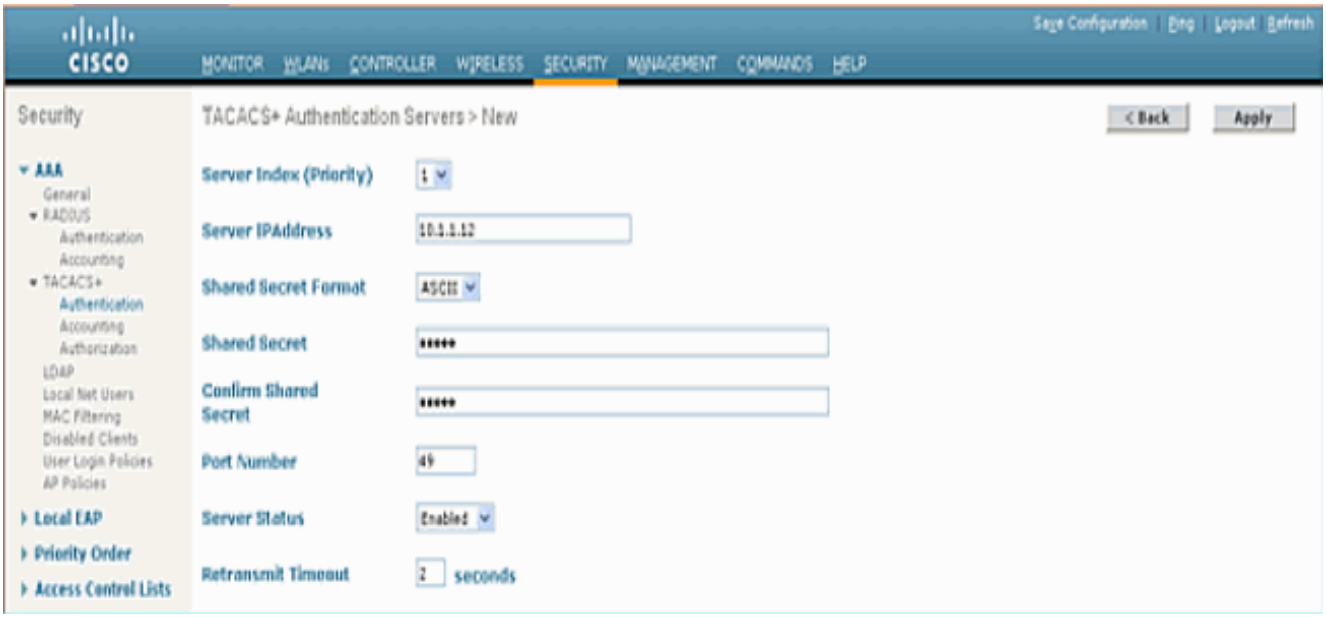
1. Ajoutez un serveur d'authentification TACACS+
2. Ajoutez un serveur d'autorisation TACACS+
3. Ajoutez un serveur de comptabilité TACACS+
4. Configurez la commande de l'authentification

Ajoutez un serveur d'authentification TACACS+

Terminez-vous ces étapes afin d'ajouter un serveur d'authentification TACACS+ :

1. Utilisez le GUI, et allez à la **Sécurité > au TACACS+ > à l'authentification**.

2. Ajoutez l'adresse IP du serveur TACACS+ et introduisez la clé secrète partagée. S'il y a lieu, changez le port par défaut de TCP/49.

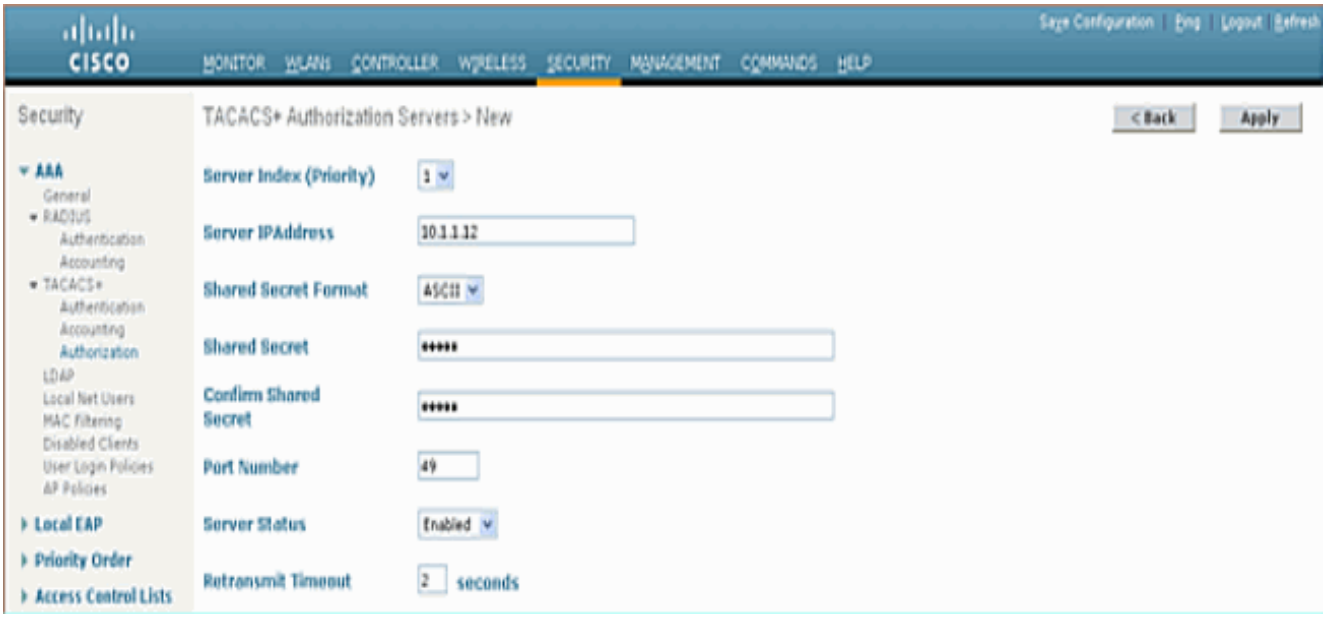


3. Cliquez sur **Apply**.Vous pouvez accomplir ceci du CLI utilisant le **config tacacs auth ajoutez la** commande de **<secret> de** *<port> d'addr> d'Index> <IP de <Server [ASCII/hexa]* :`(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123`

Ajoutez un serveur d'autorisation TACACS+

Terminez-vous ces étapes afin d'ajouter un serveur d'autorisation TACACS+ :

1. Du GUI, allez à la **Sécurité > au TACACS+ > à l'autorisation**.
2. Ajoutez l'adresse IP du serveur TACACS+ et introduisez la clé secrète partagée. S'il y a lieu, changez le port par défaut de
TCP/49.



3. Cliquez sur **Apply**.Vous pouvez accomplir ceci du CLI utilisant le **config tacacs athr ajoutez la** commande de **<secret> de** *<port> d'addr> d'Index> <IP de <Server [ASCII/hexa]* :`(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123`

Ajoutez un serveur de comptabilité TACACS+

Terminez-vous ces étapes afin d'ajouter un serveur de comptabilité TACACS+ :

1. Utilisez le GUI, et allez à la **Sécurité > au TACACS+ > à la comptabilité**.
2. Ajoutez l'adresse IP du serveur et introduisez la clé secrète partagée. S'il y a lieu, changez le port par défaut de
   TCP/49.

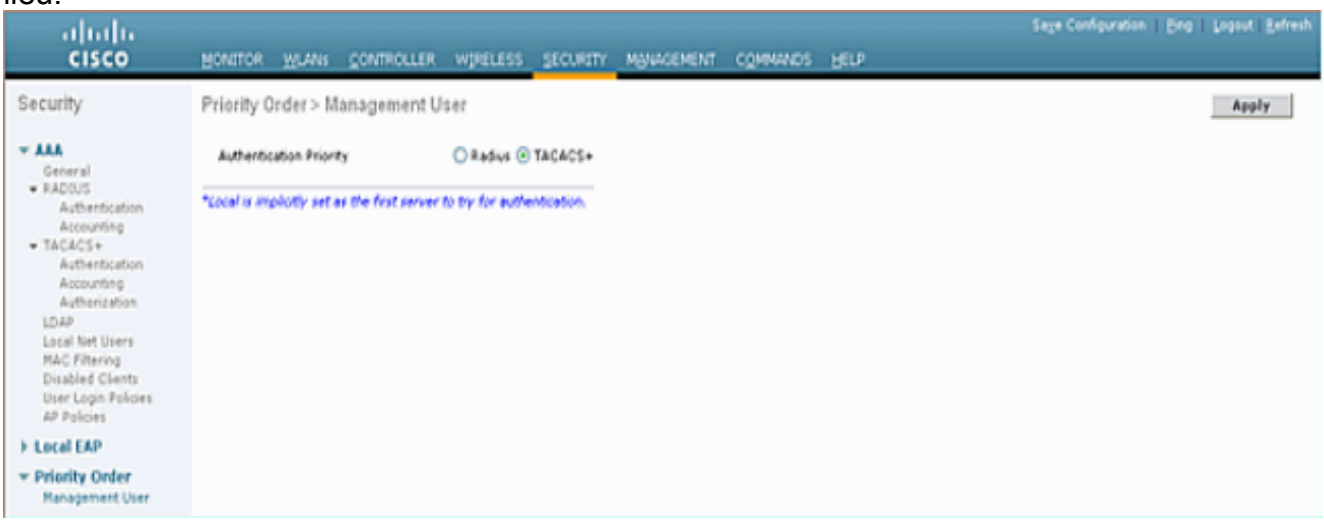
3. Cliquez sur **Apply**.Vous pouvez accomplir ceci du CLI utilisant le **config tacacs acct ajoutez la** commande de **<secret> de** *<port> d'addr> d'Index> <IP de <Server [ASCII/hexa]* :`(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123`

Configurez la commande de l'authentification

Cette étape explique comment configurer la commande d'AAA de l'authentification quand il y a de plusieurs bases de données configurées. La commande de l'authentification peut être **locale et RAYON**, ou **gens du pays et TACACS**. La configuration par défaut de contrôleur pour la commande de l'authentification est *locale et RAYON*.

Terminez-vous ces étapes afin de configurer la commande de l'authentification :

1. Du GUI, allez à l'**utilisateur de Sécurité > de commande > de Gestion prioritaire**.
2. Sélectionnez l'authentication priority.Dans cet exemple, TACACS+ a été sélectionné.
3. Cliquez sur Apply pour que la sélection ait
   lieu.



   Vous pouvez accomplir ceci du CLI utilisant la commande du **config aaa auth mgmt**

<server1> <server2> :`(Cisco Controller) >config aaa auth mgmt tacacs local`

Vérifiez la configuration

Cette section décrit les commandes utilisées pour vérifier la configuration TACACS+ sur le WLC. Ce sont quelques **commandes show** utiles qui aident à 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 des 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`
- **stats authentiques de show tacacs** — Statistiques de serveur d'authentification des affichages 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`
- **stats d'athr de show tacacs** — Statistiques de serveur d'autorisation des affichages 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`
- **stats d'acct de show tacacs** — Statistiques de serveur de comptabilité des affichages 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
```

Configurez le serveur de Cisco Secure ACS

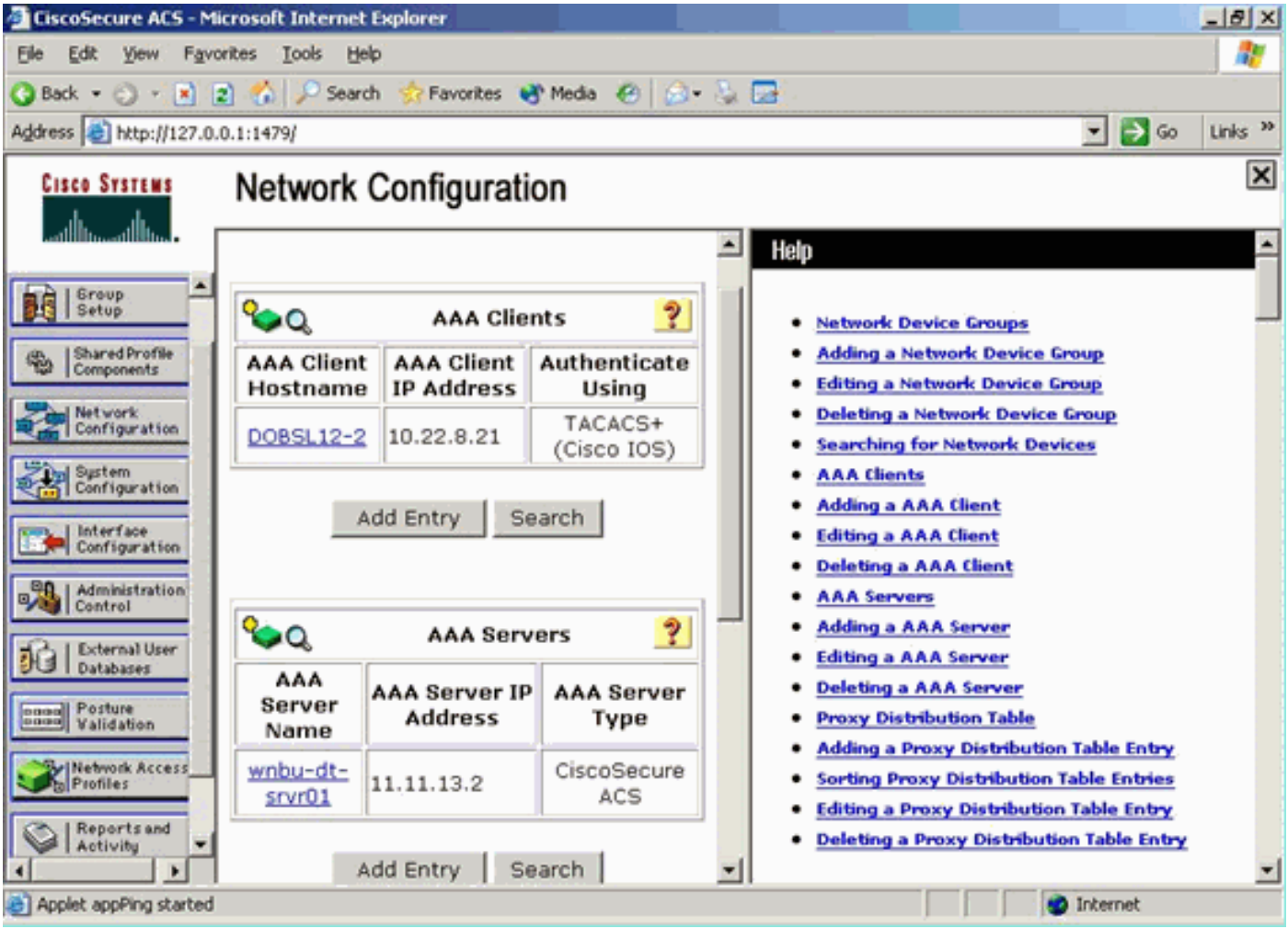
Cette section fournit les étapes impliquées dans le serveur ACS TACACS+ pour créer des services et des attributs personnalisés, et assigne les rôles aux utilisateurs ou aux groupes.

La création des utilisateurs et du groupe n'est pas expliquée dans cette section. On le suppose que les utilisateurs et les groupes sont créés comme nécessaires. Référez-vous au guide utilisateur pour le Cisco Secure ACS pour les Windows Server 4.0 pour les informations sur la façon dont créer des utilisateurs et des groupes d'utilisateurs.

Configuration du réseau

Complétez cette étape :

Ajoutez l'adresse IP de Gestion de contrôleur comme client d'AAA avec le mécanisme d'authentification comme TACACS+ (Cisco IOS).

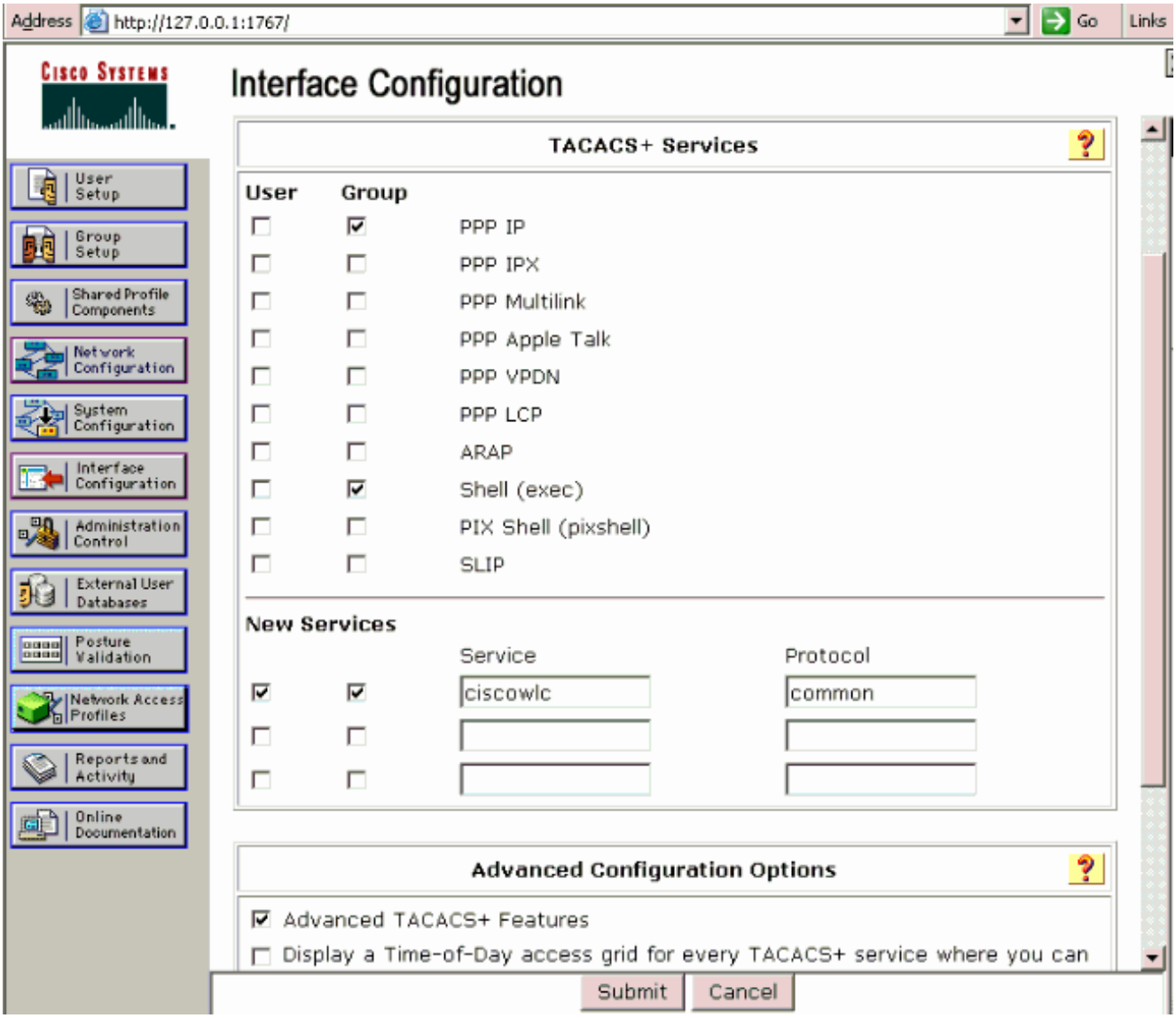


Configuration d'interface

Procédez comme suit :

1. Dans le menu de configuration d'interface, sélectionnez le lien **TACACS+** (Cisco IOS).

2. Activez les **nouveaux services**.
3. Vérifiez les cases d'**utilisateur** et de **groupe**.
4. Écrivez le **ciscowlc** pour le service et le **terrain communal** pour Protocol.
5. Activez les **caractéristiques avancées TACACS+**.

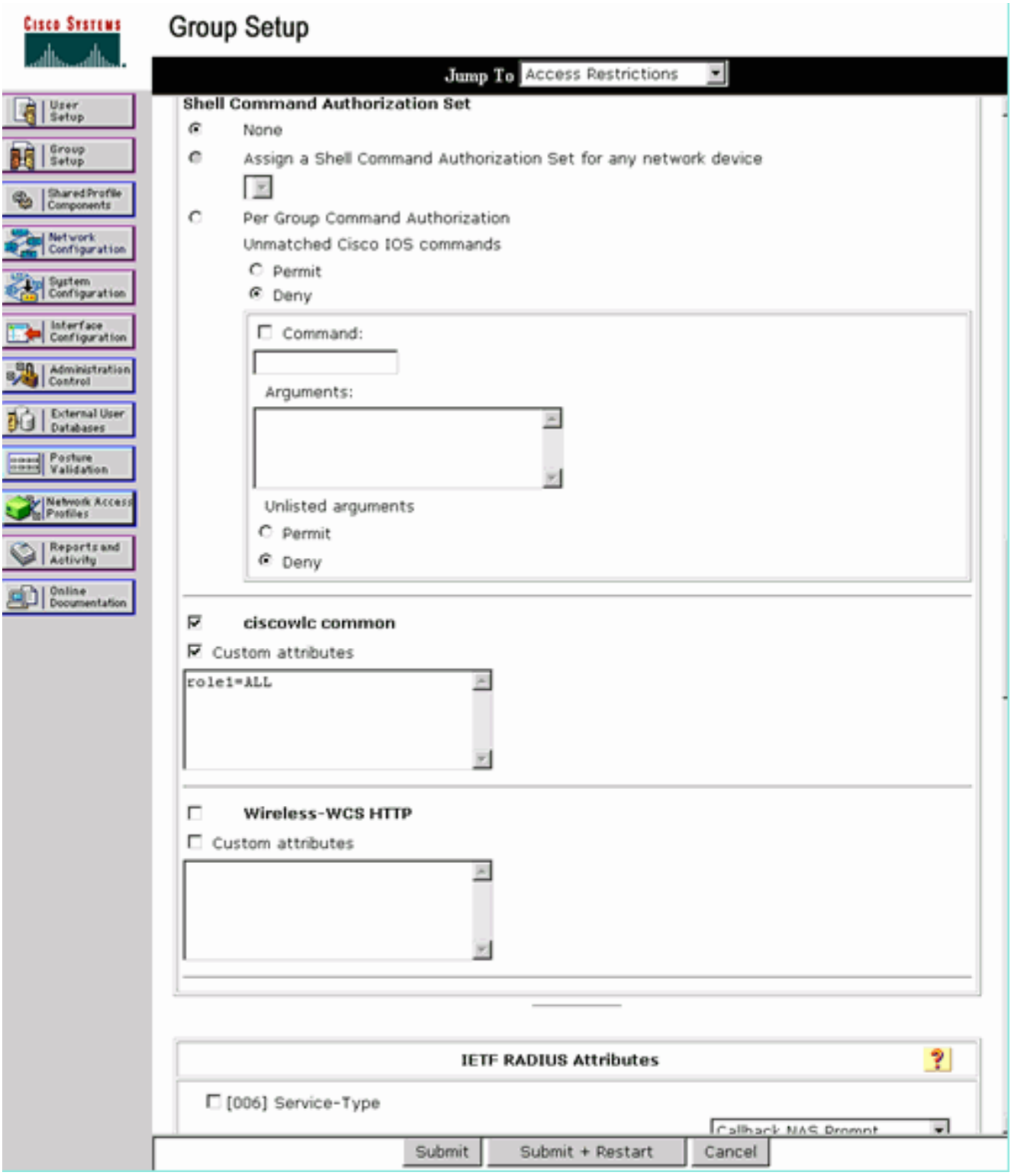


6. Cliquez sur Submit afin d'appliquer les modifications.

Utilisateur/Group Setup

Procédez comme suit :

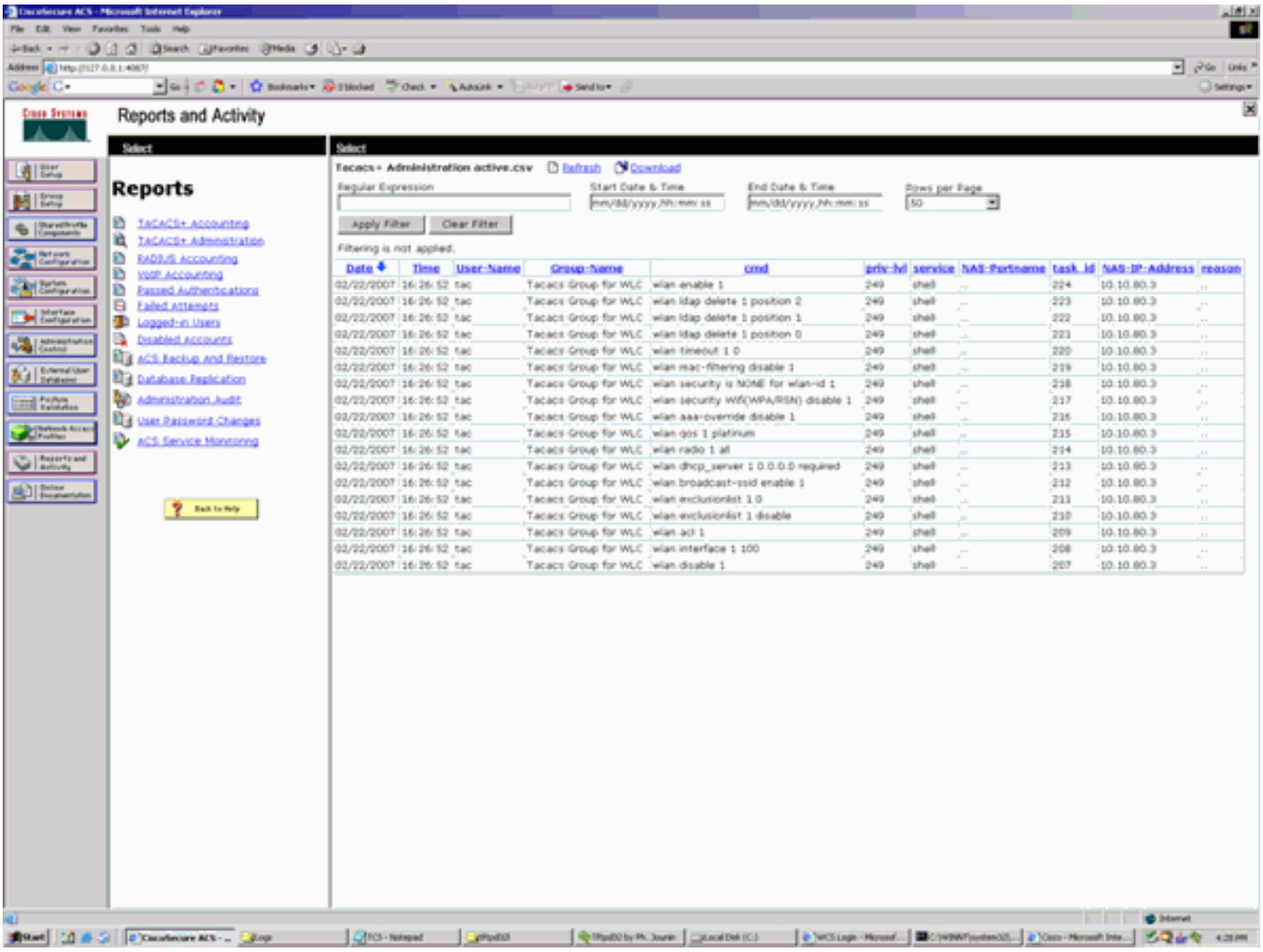
1. Sélectionnez un utilisateur/groupe précédemment créés.
2. Allez aux **configurations TACACS+**.
3. Cochez la case qui correspond au service de *ciscowlc* qui a été créé dans la section de configuration d'interface.
4. Cochez la case d'**attributs personnalisés**.



5. Dans la zone de texte au-dessous des attributs personnalisés, entrez dans ce texte si les besoins créés par l'utilisateur accèdent à seulement au WLAN, à la SÉCURITÉ et au CONTRÔLEUR : **role1=WLAN role2=SECURITY role3=CONTROLLER**.Si les besoins de l'utilisateur accèdent à seulement à l'onglet Sécurité, entrez dans ce texte : **role1=SECURITY**.Le rôle correspond aux sept éléments de barre de menus dans le GUI de Web de contrôleur. Les éléments de barre de menus sont MONITEUR, WLAN, CONTRÔLEUR, RADIO, SÉCURITÉ, GESTION et COMMANDE.
6. Écrivez le rôle qui les besoins de l'utilisateur pour role1, role2 et ainsi de suite. Si les besoins de l'utilisateur tous les rôles, alors **TOUT le** mot clé sont utilisés. Pour le rôle d'admin de lobby, le **LOBBY de** mot clé devrait être utilisé.

Enregistrements des comptes dans le Cisco Secure ACS

Les enregistrements des comptes TACACS+ du WLC sont disponibles dans le Cisco Secure ACS dans la gestion TACACS+ des états et de l'activité :



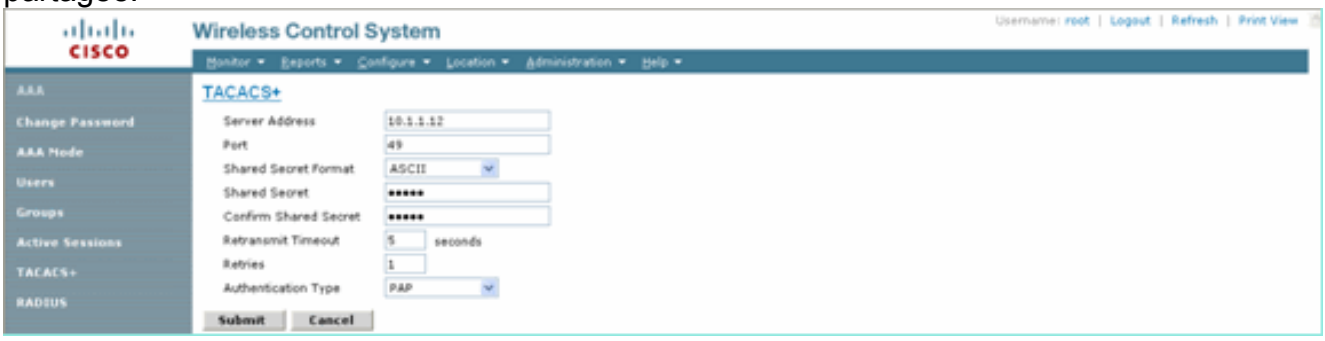
Configuration TACACS+ dans le WCS

Procédez comme suit :

1. Du GUI, procédure de connexion au WCS avec le compte de racine.
2. Ajoutez le serveur TACACS+. Allez à la **gestion > à l'AAA > au TACACS+ > ajoutent le serveur TACACS+**.

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

est par défaut), et la clé secrète partagée.



4. Activez l'authentification TACACS+ pour la gestion dans le WCS. Allez à la **gestion > au mode d'AAA > d'AAA > TACACS+ choisi**.

WCS utilisant les domaines virtuels

Le domaine virtuel est une nouvelle fonctionnalité introduite avec la version 5.1 WCS. Un domaine virtuel WCS se compose d'un ensemble de périphériques et de cartes et limite une vue standard aux informations concernant ces périphériques et cartes. Par un domaine virtuel, un administrateur peut s'assurer que les utilisateurs peuvent seulement visualiser les périphériques et les cartes dont ils sont responsables. En outre, en raison des filtres du domaine virtuel, les utilisateurs peuvent configurer, visualiser des alarmes, et générer des états pour seulement leur partie assignée du réseau. L'administrateur spécifie un ensemble de domaines virtuels permis pour chaque utilisateur. Seulement un de ces derniers peut être en activité pour cet utilisateur à la procédure de connexion. L'utilisateur peut changer le domaine virtuel en cours en sélectionnant un domaine virtuel permis différent du menu déroulant virtuel de domaine en haut de l'écran. Tout signale, des alarmes, et l'autre fonctionnalité sont maintenant filtrées par ce domaine virtuel.

S'il y a seulement un domaine virtuel défini (racine) dans le système et l'utilisateur n'a aucun domaine virtuel dans les attributs personnalisés met en place dans le serveur TACACS+/RADIUS, l'utilisateur est assigné le domaine virtuel de racine par défaut.

S'il y a plus d'un domaine virtuel, et l'utilisateur n'a aucun attribut spécifié, alors l'utilisateur est bloqué d'ouvrir une session. Afin de permettre à l'utilisateur pour ouvrir une session, les attributs personnalisés virtuels de domaine doivent être exportés au serveur Radius/TACACS+.

La fenêtre virtuelle d'attributs personnalisés de domaine te permet pour indiquer les données appropriées de Protocol-particularité pour chaque domaine virtuel. Le bouton d'exportation sur la barre latérale virtuelle de hiérarchie de domaine préformate les attributs du RAYON et TACACS+ du domaine virtuel. Vous pouvez copier et coller ces attributs dans le serveur ACS. Ceci te permet pour copier seulement les domaines virtuels applicables sur l'écran de serveur ACS et s'assure que les utilisateurs ont seulement accès à ces domaines virtuels.

Afin d'appliquer les attributs préformatés de RAYON et TACACS+ au serveur ACS, terminez-vous les étapes expliquées section dans de domaine de RAYON et TACACS+ attributs virtuels.

Configurez le Cisco Secure ACS pour utiliser WCS

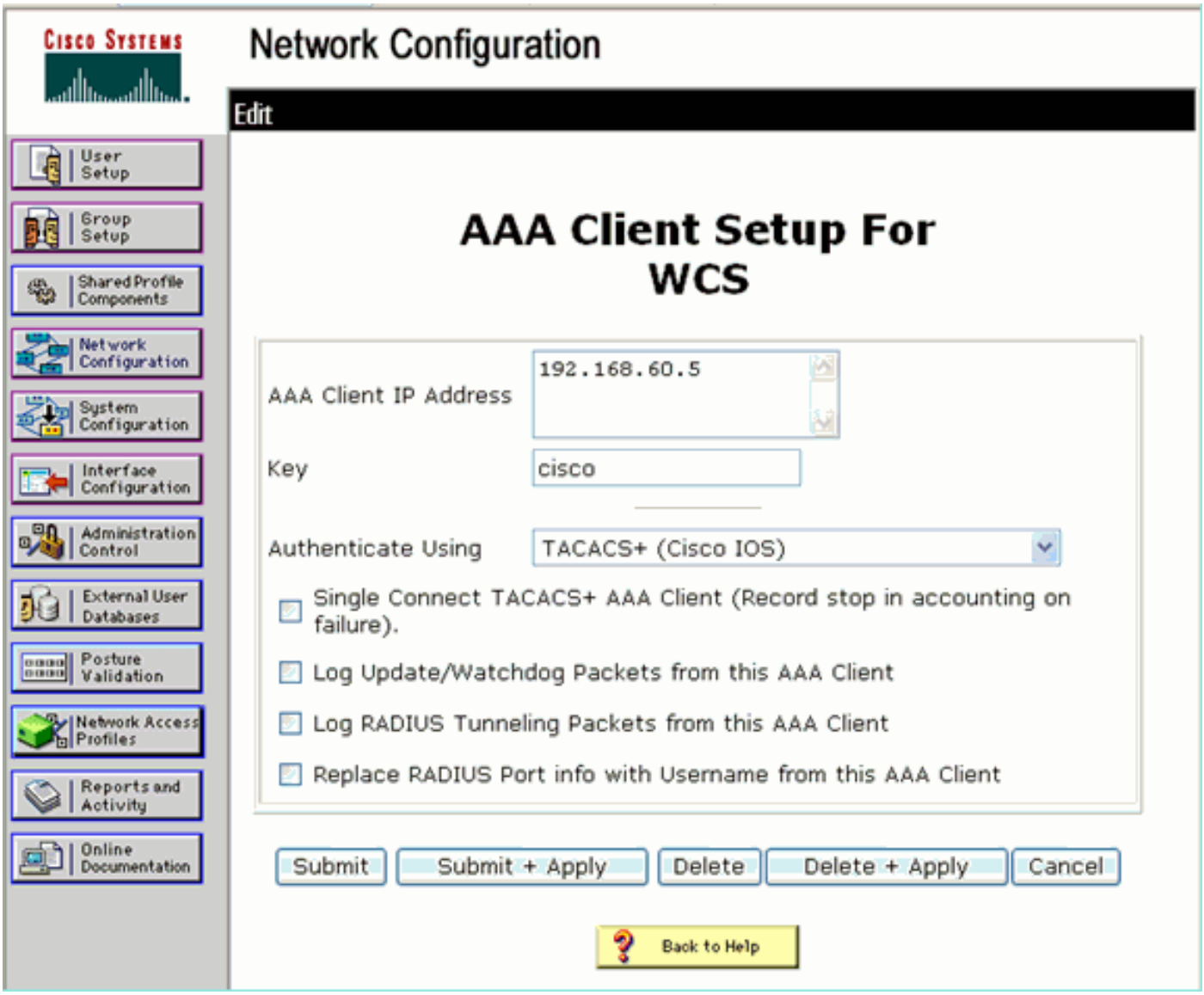
La section fournit les étapes impliquées dans le serveur ACS TACACS+ pour créer des services et des attributs personnalisés, et assigne les rôles aux utilisateurs ou aux groupes.

La création des utilisateurs et du groupe n'est pas expliquée dans cette section. On le suppose que les utilisateurs et les groupes sont créés comme nécessaires.

Configuration du réseau

Complétez cette étape :

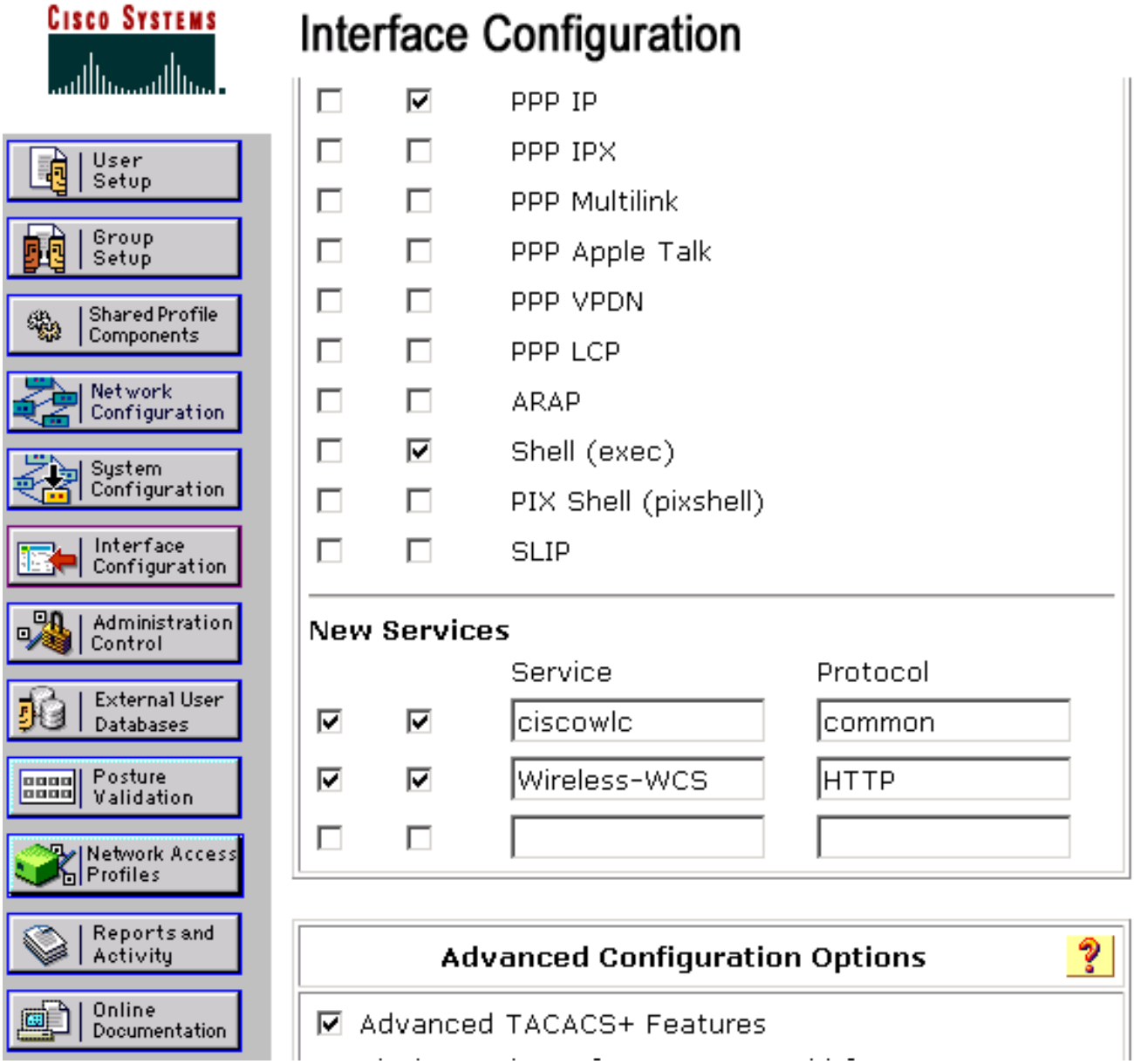
Ajoutez l'adresse IP WCS comme client d'AAA avec le mécanisme d'authentification comme TACACS+ (Cisco IOS).



Configuration d'interface

Procédez comme suit :

1. Dans le menu de configuration d'interface, sélectionnez le lien **TACACS+** (Cisco IOS).
2. Activez les **nouveaux services**.
3. Vérifiez les cases d'**utilisateur** et de **groupe**.
4. Entrez dans la **radio-WCS** pour le service et le **HTTP** pour Protocol.**Remarque:** Le HTTP doit être dans des CAPS.
5. Activez les **caractéristiques avancées TACACS+**.

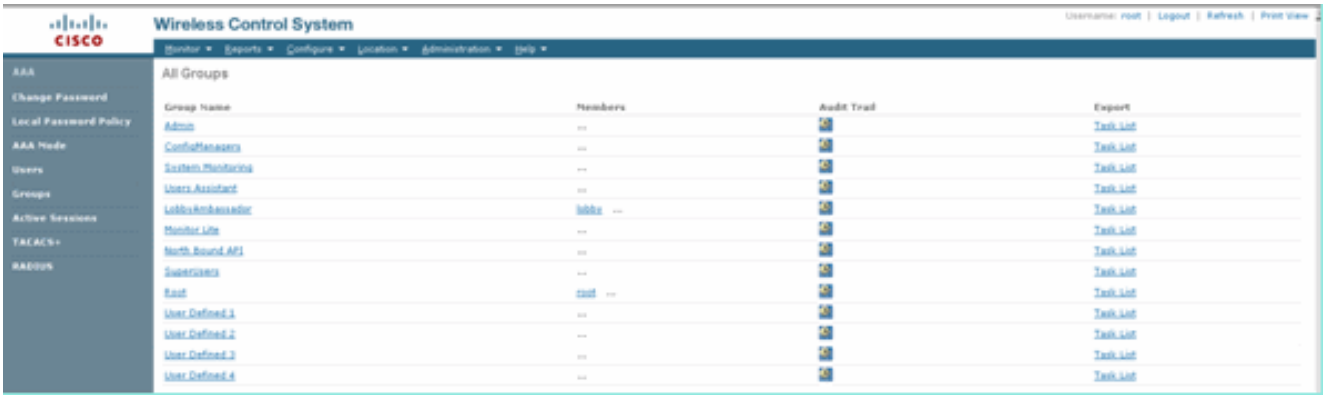


6. Cliquez sur Submit afin d'appliquer les modifications.

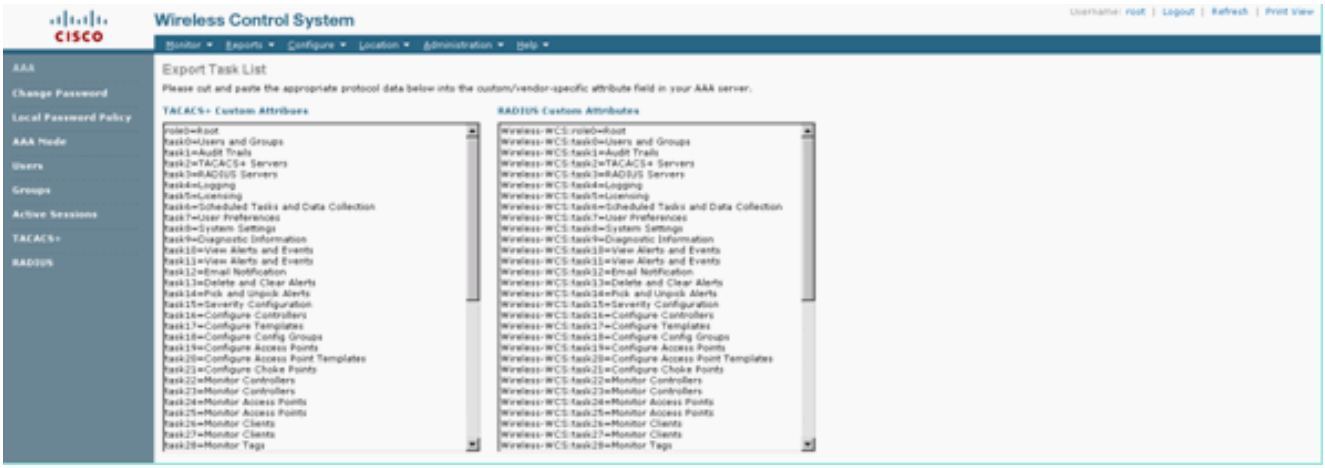
Utilisateur/Group Setup

Procédez comme suit :

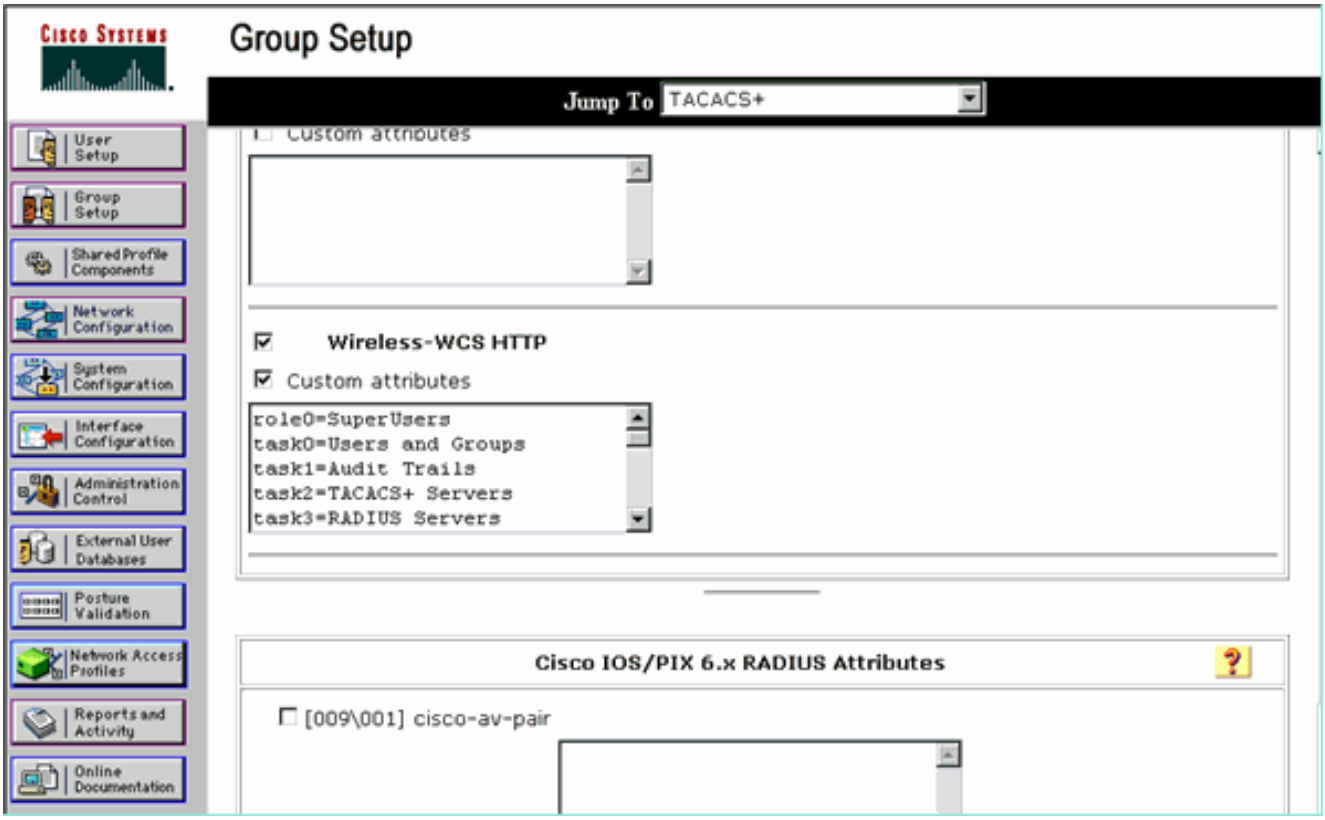
1. Dans le GUI WCS, naviguez vers la **gestion > l'AAA > les groupes** pour sélectionner les groupes d'utilisateurs préconfigurés l'uns des, tels que des super utilisateurs dans le WCS.



2. Sélectionnez la liste des tâches pour les groupes d'utilisateurs et la pâte préconfigurés de copie à
l'ACS.



3. Sélectionnez un utilisateur/groupe précédemment créés et allez aux **configurations TACACS+**.
4. Dans le GUI ACS, sélectionnez la case qui correspond au service de radio-WCS qui a été créé plus tôt.
5. Dans le GUI ACS, cochez la case d'**attributs personnalisés**.
6. Dans la zone de texte au-dessous des attributs personnalisés, écrivez ce rôle et chargez les informations copiées du WCS. Par exemple, écrivez la liste de tâches permises des super utilisateurs.



7. Puis, procédure de connexion au WCS avec le nom d'utilisateur/mot de passe de création récente dans l'ACS.

Debugs

Debugs de 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
```

Debugs de WLC pour de 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
```

Debugs d'un WLC pour la panne 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 Sans fil du contrôleur LAN de Cisco (WLC) et de la configuration de Cisco ACS 5.x (TACACS+) pour l'authentification Web
- Configurer TACACS+
- Comment configurer l'authentification et l'autorisation TACACS pour des utilisateurs d'admin et de non-admin dans ACS 5.1
- Comparaison entre TACACS+ et RADIUS
- Support et documentation techniques - Cisco Systems