Exemple de configuration des jeux d'autorisation du shell ACS sur IOS et ASA/PIX/FWSM

Contenu

Introduction

Ce document décrit comment configurer les jeux d'autorisations de shell dans Cisco Secure Access Control Server (ACS) pour les clients AAA, tels que les routeurs ou commutateurs Cisco IOS® et les appareils de sécurité Cisco (ASA/PIX/FWSM) avec TACACS+ comme protocole d'autorisation.

Remarque : ACS Express ne prend pas en charge l'autorisation de commande.

Conditions préalables

Conditions requises

Ce document suppose que les configurations de base sont définies dans les clients AAA et ACS.

Dans ACS, choisissez **Interface Configuration > Advanced Options**, et assurez-vous que la case **Per-user TACACS+/RADIUS Attributes** est cochée.

Components Used

Les informations contenues dans ce document sont basées sur le serveur Cisco Secure Access Control Server (ACS) qui exécute le logiciel version 3.3 et 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.

Jeux d'autorisations de commande

Les jeux d'autorisations de commande fournissent un mécanisme central pour contrôler l'autorisation de chaque commande émise sur un périphérique réseau donné. Cette fonctionnalité améliore considérablement l'évolutivité et la facilité de gestion requises pour définir les restrictions d'autorisation.

Dans ACS, les jeux d'autorisation de commande par défaut incluent les jeux d'autorisation de commande Shell et les jeux d'autorisation de commande PIX. Les applications de gestion des périphériques Cisco, telles que CiscoWorks Management Center for Firewalls, peuvent demander à ACS de prendre en charge des types de jeux d'autorisations de commande supplémentaires.

Remarque : les ensembles d'autorisations de commande PIX nécessitent que la demande d'autorisation de commande TACACS+ identifie le service comme *pixshell*. Vérifiez que ce service a été implémenté dans la version du système d'exploitation PIX que vos pare-feu utilisent ; sinon, utilisez les ensembles d'autorisation de commande Shell pour effectuer l'autorisation de commande pour les périphériques PIX. Référez-vous à Configuration d'un jeu d'autorisations de commande Shell pour un groupe d'utilisateurs pour plus d'informations.

Remarque : depuis la version 6.3 du système d'exploitation PIX, le service pixshell n'a pas été implémenté.

Remarque : les appareils de sécurité Cisco (ASA/PIX) ne permettent pas actuellement à l'utilisateur d'être placé directement en mode enable pendant la connexion. L'utilisateur doit passer manuellement en mode enable.

Afin d'offrir un meilleur contrôle des sessions Telnet administratives hébergées par les périphériques, un périphérique réseau qui utilise TACACS+ peut demander une autorisation pour chaque ligne de commande avant de l'exécuter. Vous pouvez définir un ensemble de commandes dont l'exécution est autorisée ou refusée par un utilisateur particulier sur un périphérique donné. ACS a encore amélioré cette fonctionnalité avec ces fonctionnalités :

- **Jeux d'autorisations de commandes nommées réutilisables** : sans citer directement un utilisateur ou un groupe d'utilisateurs, vous pouvez créer un jeu d'autorisations de

commandes nommé. Vous pouvez définir plusieurs jeux d'autorisations de commande qui délimitent différents profils d'accès. Exemple :Un jeu d'autorisations de commande du *centre d'assistance* peut autoriser l'accès à des commandes de navigation de haut niveau, telles que **show run**, et refuser toute commande de configuration.Un jeu d'autorisations de commande *Tous les ingénieurs réseau* peut contenir une liste limitée de commandes autorisées pour tout ingénieur réseau de l'entreprise.Un jeu d'autorisations de commande *Local network ingénieurs* peut autoriser toutes les commandes (et inclure des commandes de configuration d'adresse IP).

- **Précision de la granularité de la configuration** : vous pouvez créer des associations entre des jeux d'autorisations de commande nommés et des groupes de périphériques réseau (NDG). Ainsi, vous pouvez définir différents profils d'accès pour les utilisateurs en fonction des périphériques réseau auxquels ils accèdent. Vous pouvez associer le même jeu d'autorisations de commande nommé à plusieurs NDG et l'utiliser pour plusieurs groupes d'utilisateurs. ACS garantit l'intégrité des données. Les jeux d'autorisations de commande nommés sont conservés dans la base de données interne ACS. Vous pouvez utiliser les fonctions de sauvegarde et de restauration ACS pour les sauvegarder et les restaurer. Vous pouvez également répliquer des jeux d'autorisations de commande sur des ACS secondaires avec d'autres données de configuration.

Pour les types de jeux d'autorisations de commande qui prennent en charge les applications de gestion des périphériques Cisco, les avantages sont similaires lorsque vous utilisez des jeux d'autorisations de commande. Vous pouvez appliquer des jeux d'autorisations de commande à des groupes ACS qui contiennent des utilisateurs de l'application de gestion des périphériques afin d'appliquer l'autorisation de divers privilèges dans une application de gestion des périphériques. Les groupes ACS peuvent correspondre à différents rôles au sein de l'application de gestion des périphériques et vous pouvez appliquer différents jeux d'autorisations de commande à chaque groupe, le cas échéant.

ACS comporte trois étapes séquentielles de filtrage d'autorisation de commande. Chaque demande d'autorisation de commande est évaluée dans l'ordre indiqué :

1. **Command Match** : ACS détermine si la commande traitée correspond à une commande répertoriée dans le jeu d'autorisations de commande. Si la commande ne correspond pas, l'autorisation de la commande est déterminée par le paramètre Commandes sans correspondance : *autoriser* ou *refuser*. Sinon, si la commande correspond, l'évaluation continue.
2. **Argument Match** : ACS détermine si les arguments de commande présentés correspondent aux arguments de commande répertoriés dans le jeu d'autorisations de commande.Si aucun argument ne correspond, l'autorisation de la commande est déterminée par l'activation ou non de l'option Autoriser les arguments sans correspondance. Si des arguments sans correspondance sont autorisés, la commande est autorisée et l'évaluation se termine ; sinon, la commande n'est pas autorisée et l'évaluation se termine.Si tous les arguments correspondent, l'évaluation continue.
3. **Argument Policy** : une fois qu'ACS détermine que les arguments de la commande correspondent aux arguments du jeu d'autorisations de commande, ACS détermine si chaque argument de commande est explicitement autorisé. Si tous les arguments sont explicitement autorisés, ACS accorde l'autorisation de commande. Si aucun argument n'est autorisé, ACS refuse l'autorisation de la commande.

Ajouter un jeu d'autorisations de commande Shell

Cette section comprend les scénarios suivants qui décrivent comment ajouter un jeu d'autorisations de commande :

- Scénario 1 : Privilège d'accès en lecture-écriture ou d'accès complet
- Scénario 2 : Privilège d'accès en lecture seule
- Scénario 3 : Privilège d'accès restreint

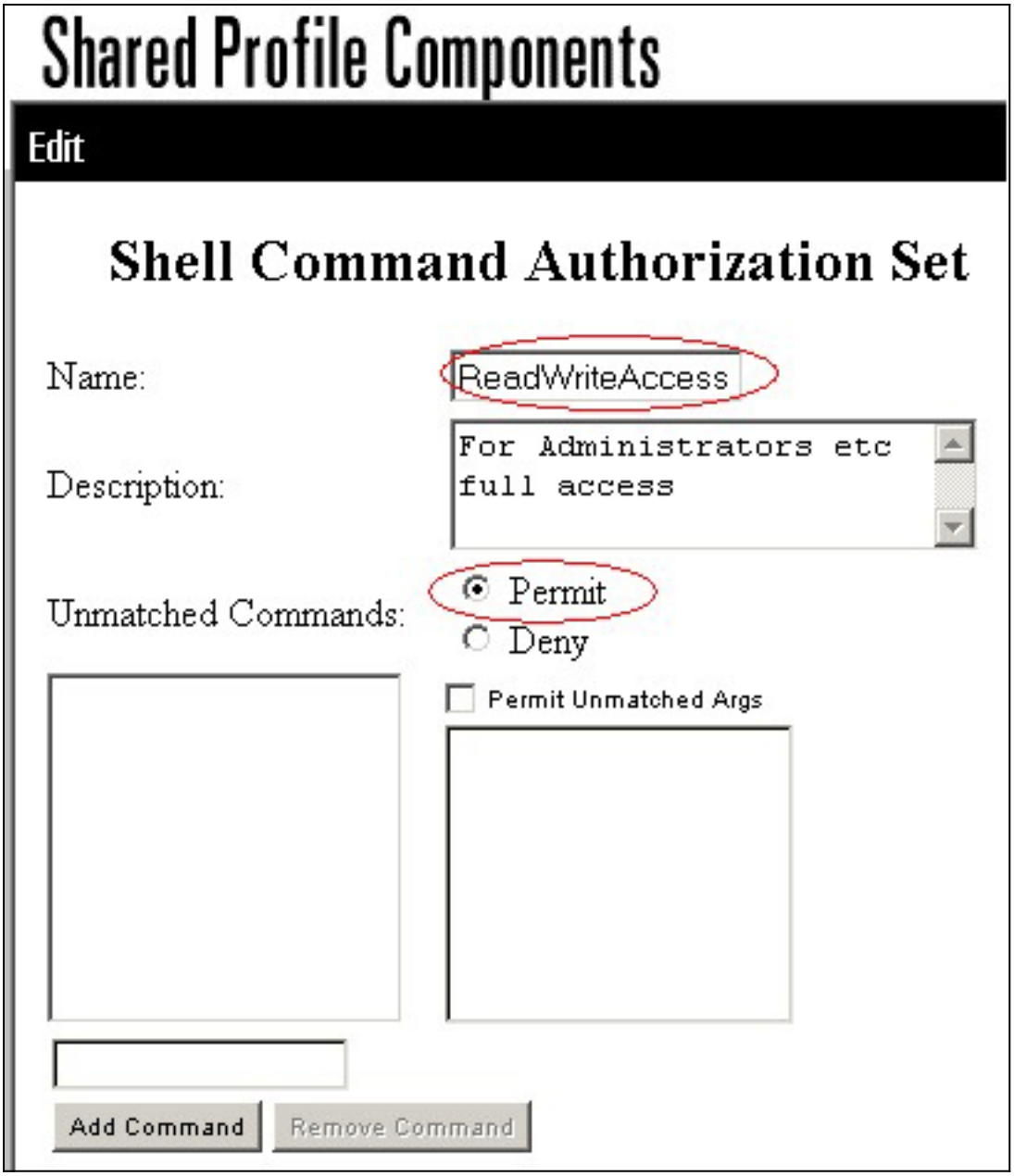
Remarque : reportez-vous à la section Ajout d'un jeu d'autorisations de commande du Guide de l'utilisateur de Cisco Secure Access Control Server 4.1 pour plus d'informations sur la création de jeux d'autorisations de commande. Référez-vous à Modification d'un jeu d'autorisations de commande et Suppression d'un jeu d'autorisations de commande pour plus d'informations sur la façon de modifier et supprimer des jeux d'autorisations de commande.

Scénario 1 : Privilège d'accès en lecture-écriture ou d'accès complet

Dans ce scénario, les utilisateurs disposent d'un accès en lecture/écriture (ou d'un accès complet).

Dans la zone Jeu d'autorisations de commande Shell de la fenêtre Composants du profil partagé, configurez les paramètres suivants :

1. Dans le champ Nom, entrez **ReadWriteAccess** comme nom du jeu d'autorisations de commande.
2. Dans le champ Description, saisissez une description pour le jeu d'autorisations de la commande.
3. Cliquez sur la case d'option **Autoriser**, puis sur **Envoyer**.

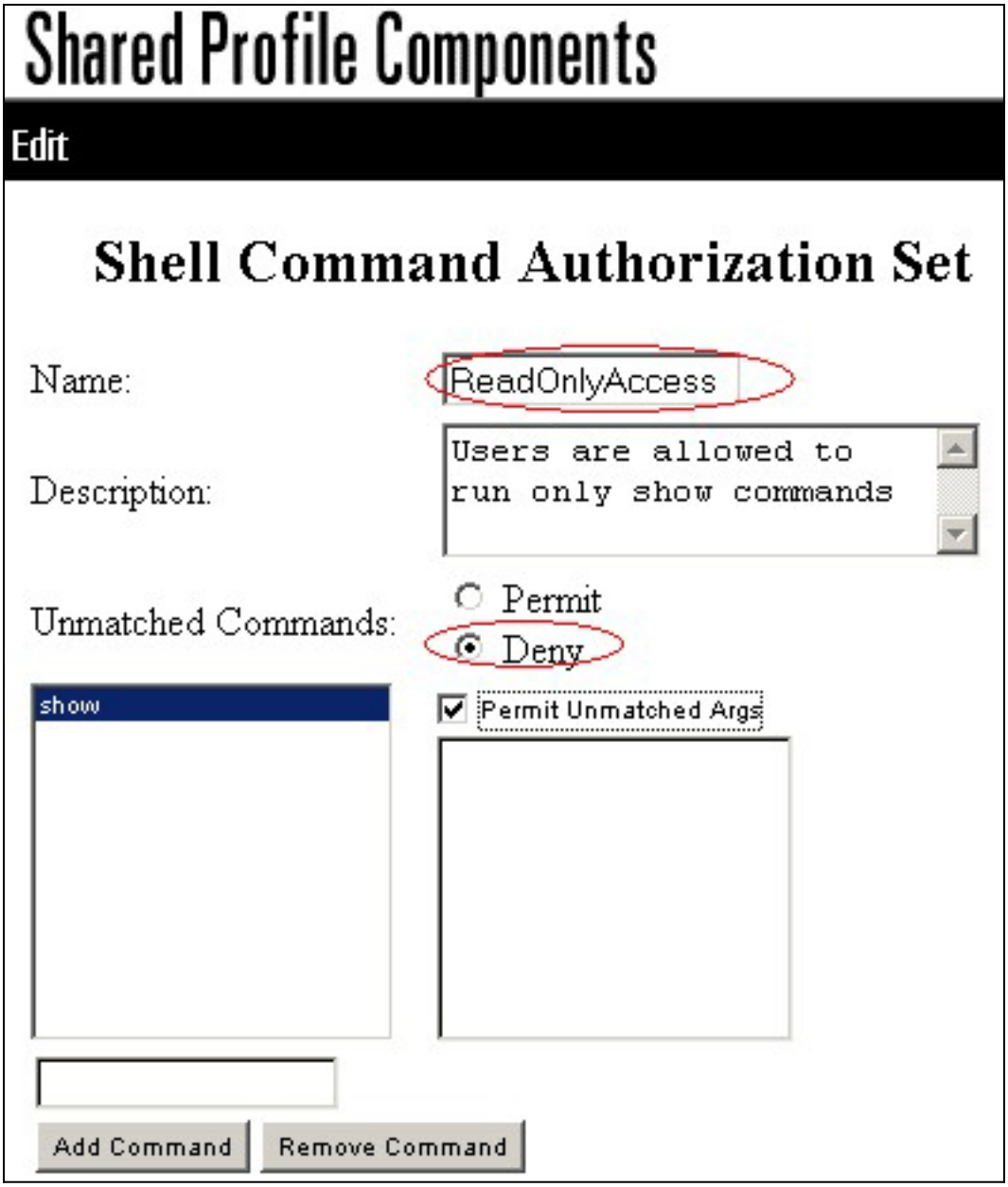


Scénario 2 : Privilège d'accès en lecture seule

Dans ces scénarios, les utilisateurs ne peuvent utiliser que des commandes **show**.

Dans la zone Jeu d'autorisations de commande Shell de la fenêtre Composants du profil partagé, configurez les paramètres suivants :

1. Dans le champ Nom, entrez **ReadOnlyAccess** comme nom du jeu d'autorisations de commande.
2. Dans le champ Description, saisissez une description pour le jeu d'autorisations de la commande.
3. Cliquez sur la case d'option **Deny**.
4. Entrez la commande **show** dans le champ au-dessus du bouton Ajouter une commande, puis cliquez sur **Ajouter une commande**.
5. Cochez la case **Autoriser les arguments sans correspondance**, puis cliquez sur **Envoyer**

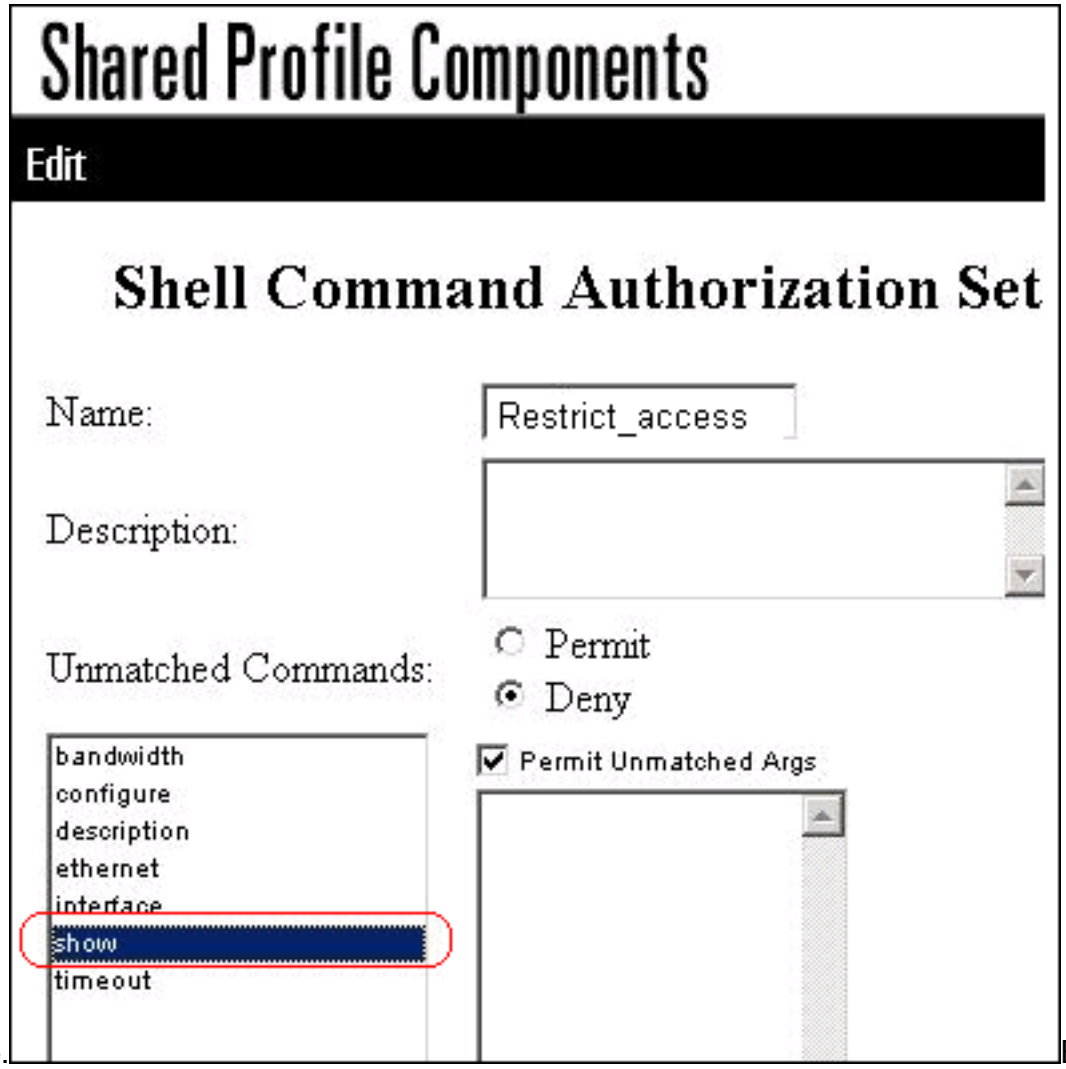


Scénario 3 : Privilège d'accès restreint

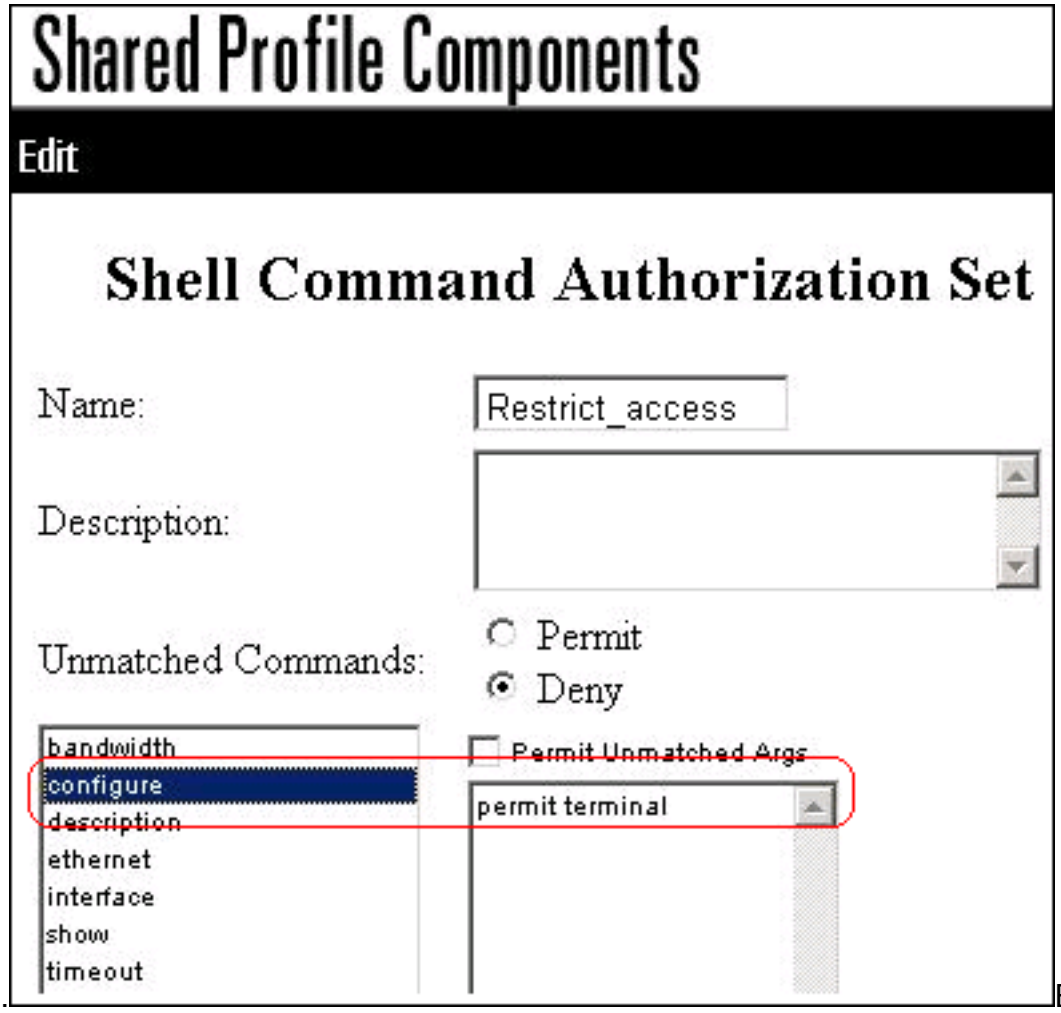
Dans ce scénario, les utilisateurs peuvent utiliser des commandes sélectives.

Dans la zone Jeu d'autorisations de commande Shell de la fenêtre Composants du profil partagé, configurez les paramètres suivants :

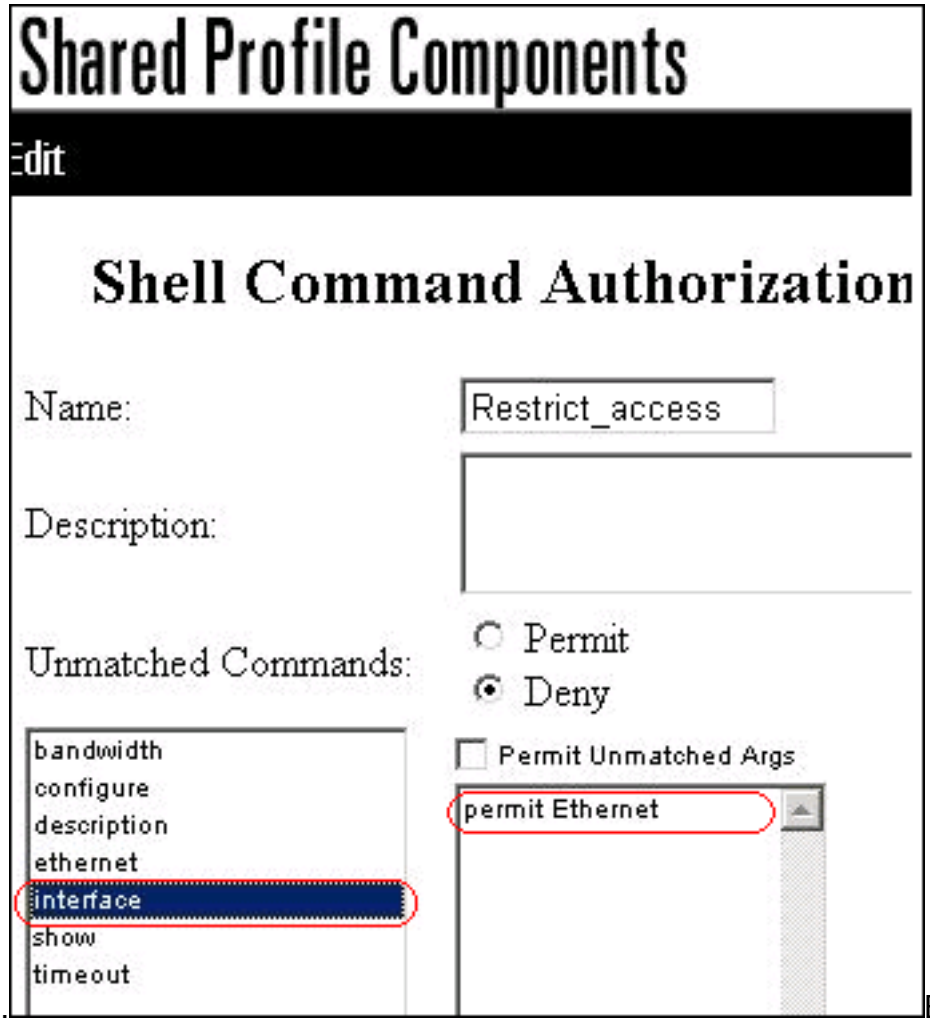
1. Dans le champ du nom, entrez **Restrict_access** comme nom du jeu d'autorisations de commande.
2. Cliquez sur la case d'option **Deny**.
3. Entrez les commandes que vous souhaitez autoriser sur les clients AAA.Dans le champ situé au-dessus du bouton Ajouter une commande, entrez la commande **show** et cliquez sur **Ajouter une**



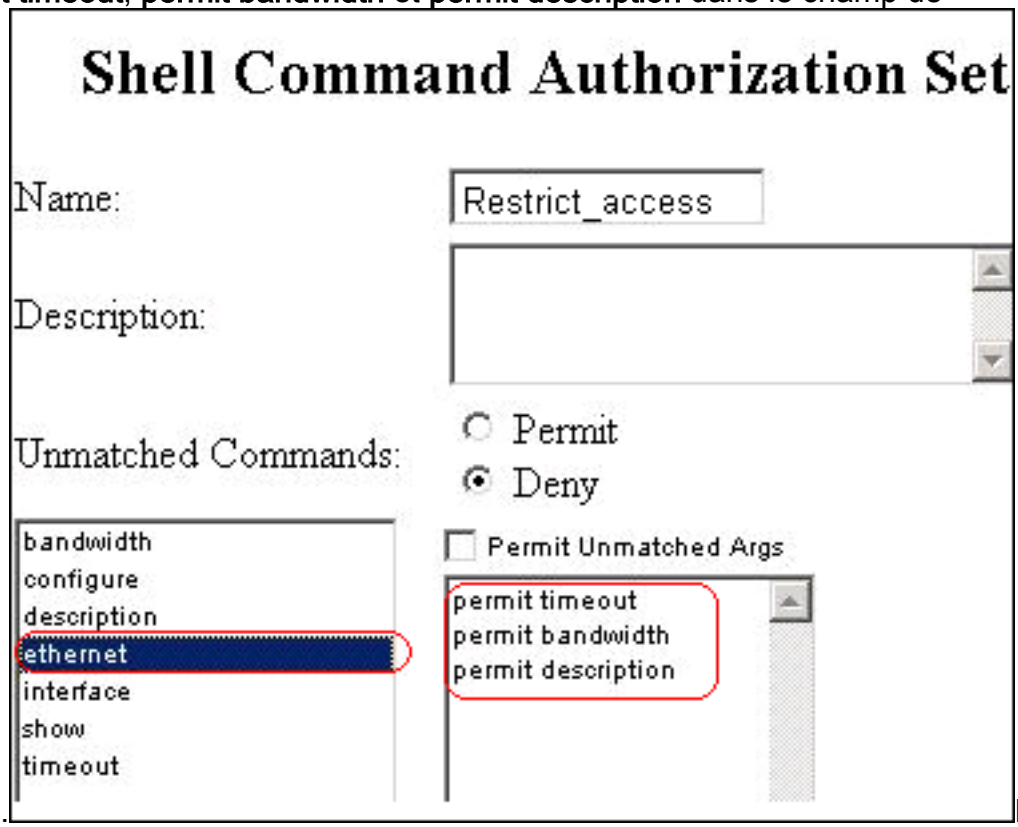
commande.Entrez la commande **configure**, puis cliquez sur **Add Command**.Sélectionnez la commande **configure**, et entrez **permit terminal** dans le champ à



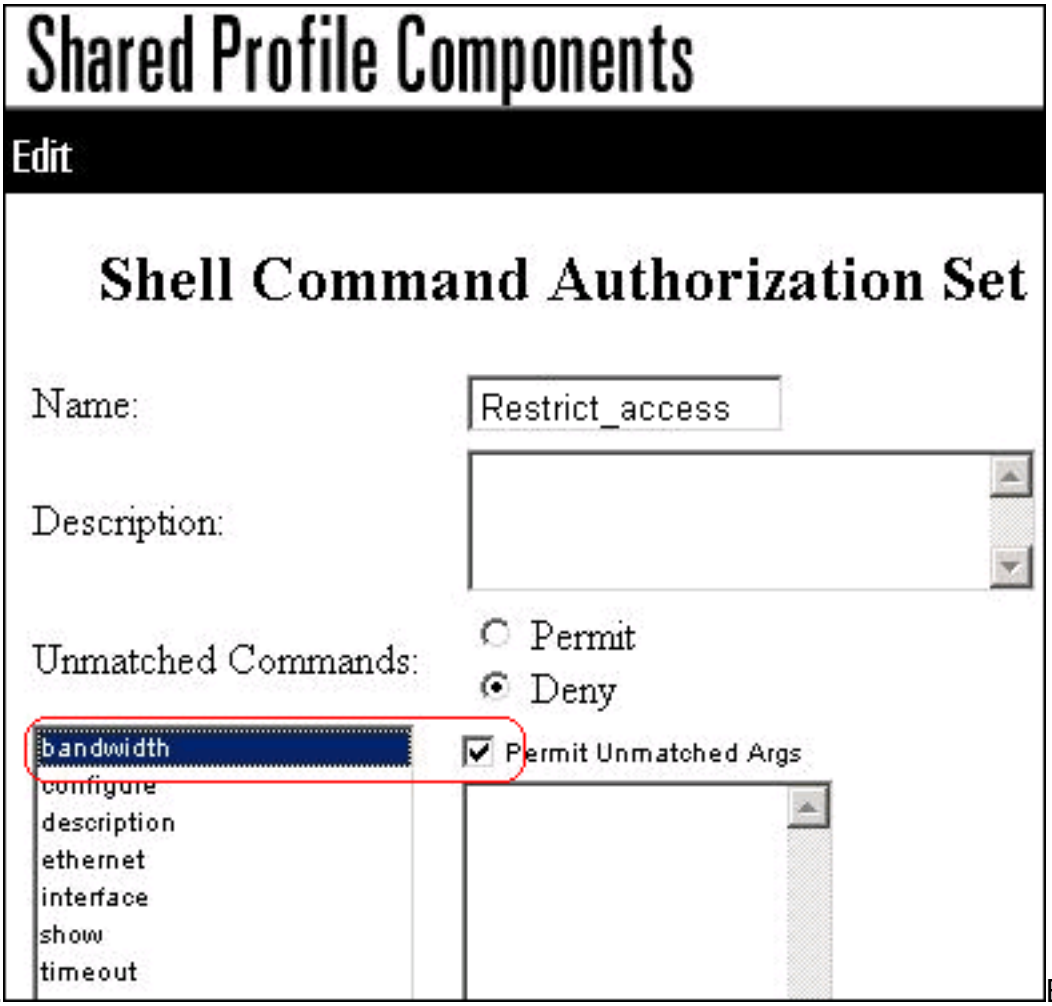
droite.Entrez la commande **interface**, puis cliquez sur **Add Command**.Sélectionnez la commande **interface**, et entrez **permit Ethernet** dans le champ à



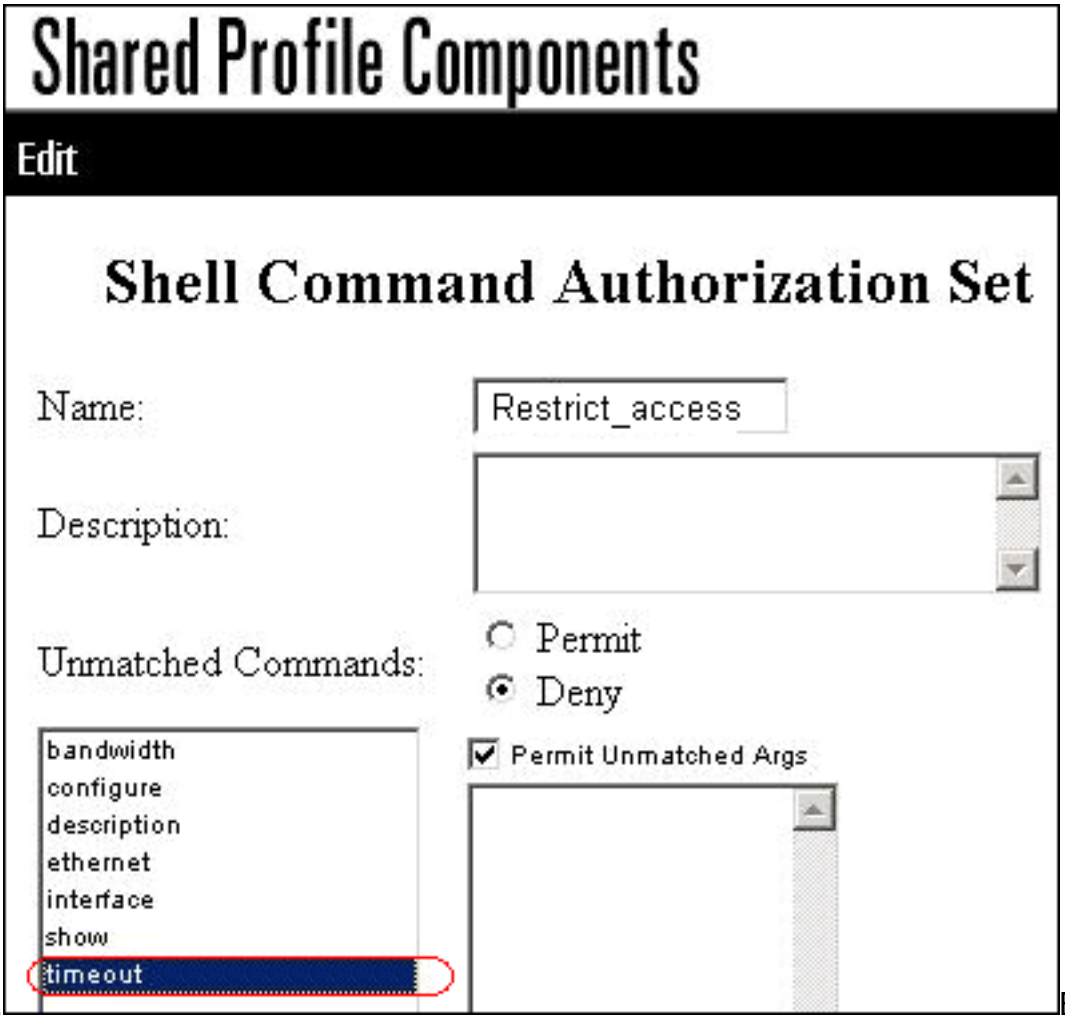
droite.Entrez la commande **ethernet**, puis cliquez sur **Add Command**.Sélectionnez la commande **interface**, et entrez **permit timeout**, **permit bandwidth** et **permit description** dans le champ de



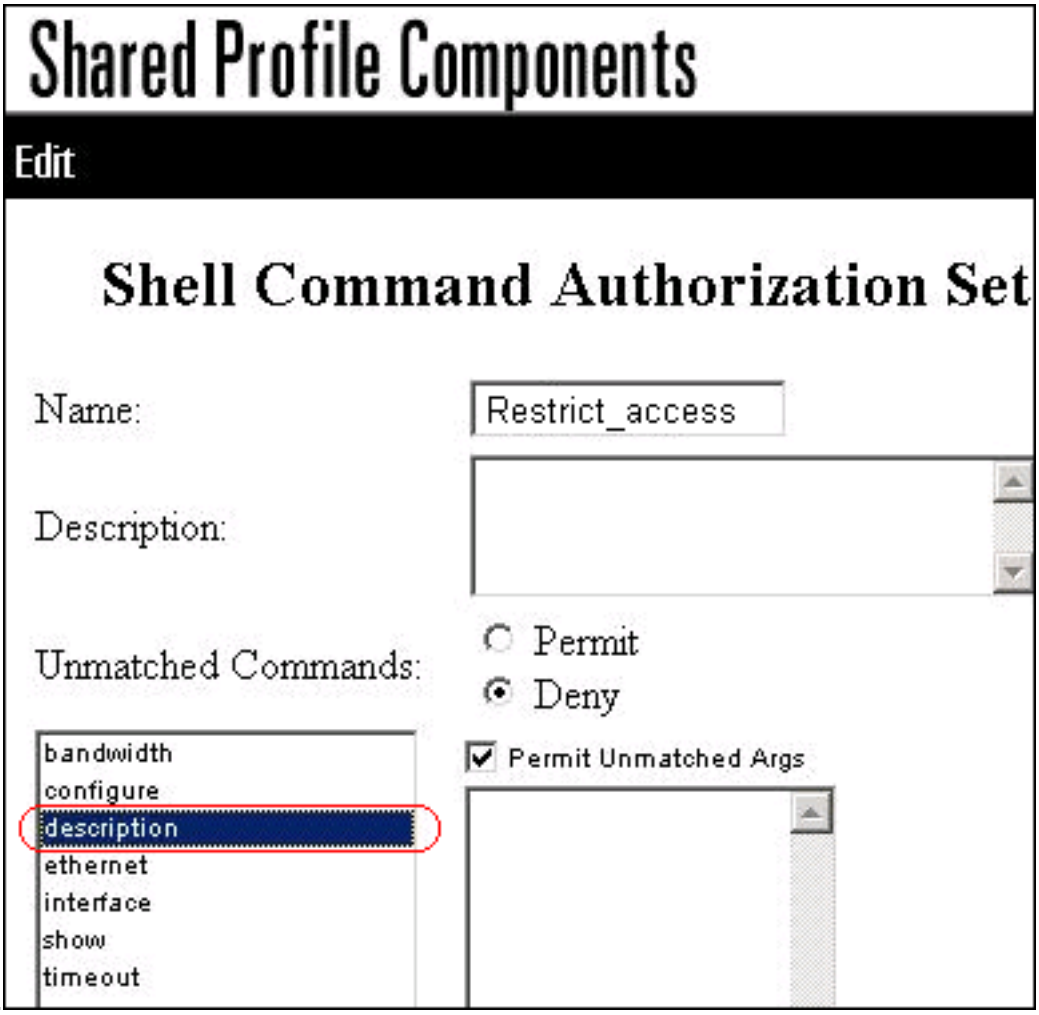
droite.Entrez la commande **bandwidth**, puis cliquez sur **Add**



Command.Entrez la commande **timeout**, puis cliquez sur **Add**



Command. Entrez la commande **description**, puis cliquez sur **Add**



Command.

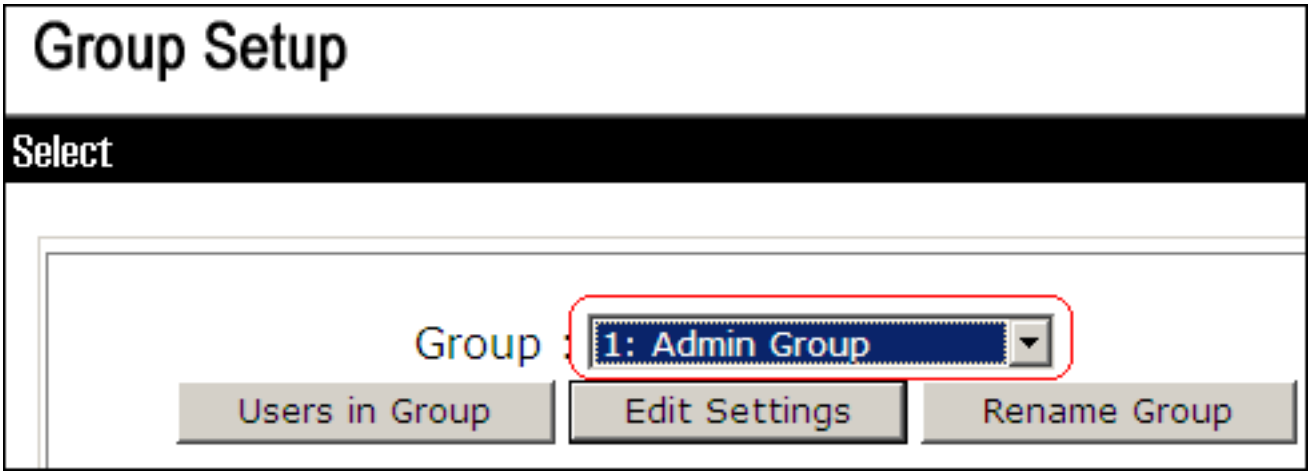
4. Cliquez sur Submit.

Associer le jeu d'autorisations de commande Shell au groupe d'utilisateurs

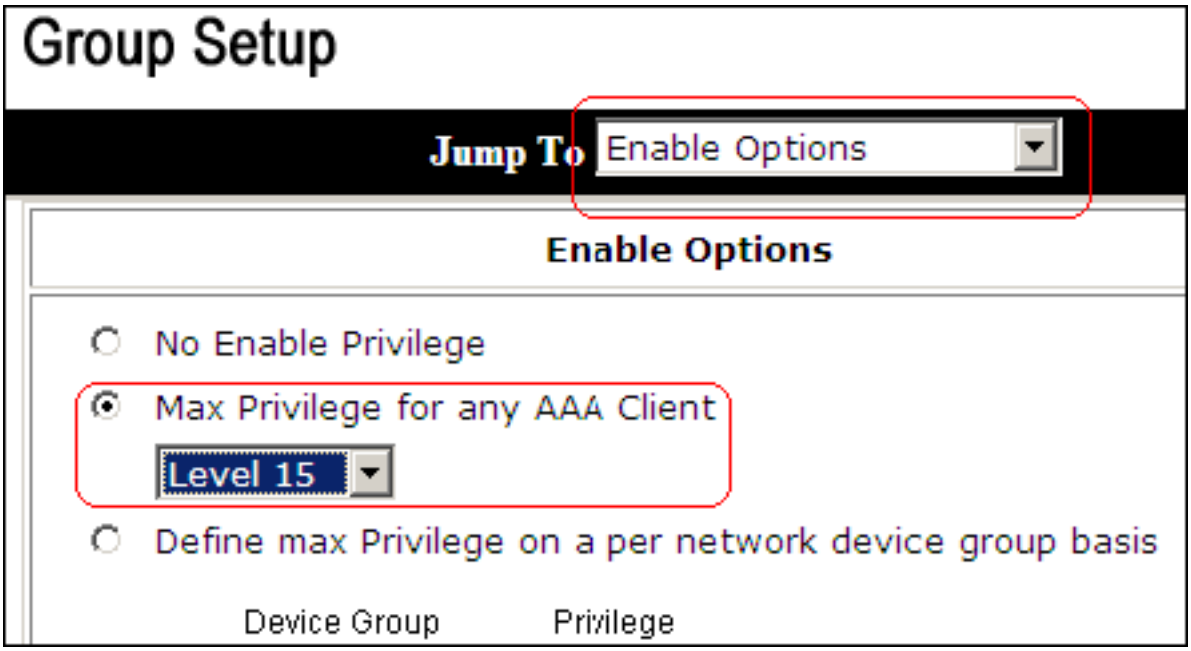
Référez-vous à la section Configuration d'un jeu d'autorisations de commande shell pour un groupe d'utilisateurs du Guide de l'utilisateur de Cisco Secure Access Control Server 4.1 pour plus d'informations sur la façon de configurer le jeu d'autorisations de commande shell pour des groupes d'utilisateurs.

Associez le jeu d'autorisations de commande Shell (accès ReadWrite) au groupe d'utilisateurs (groupe d'administrateurs)

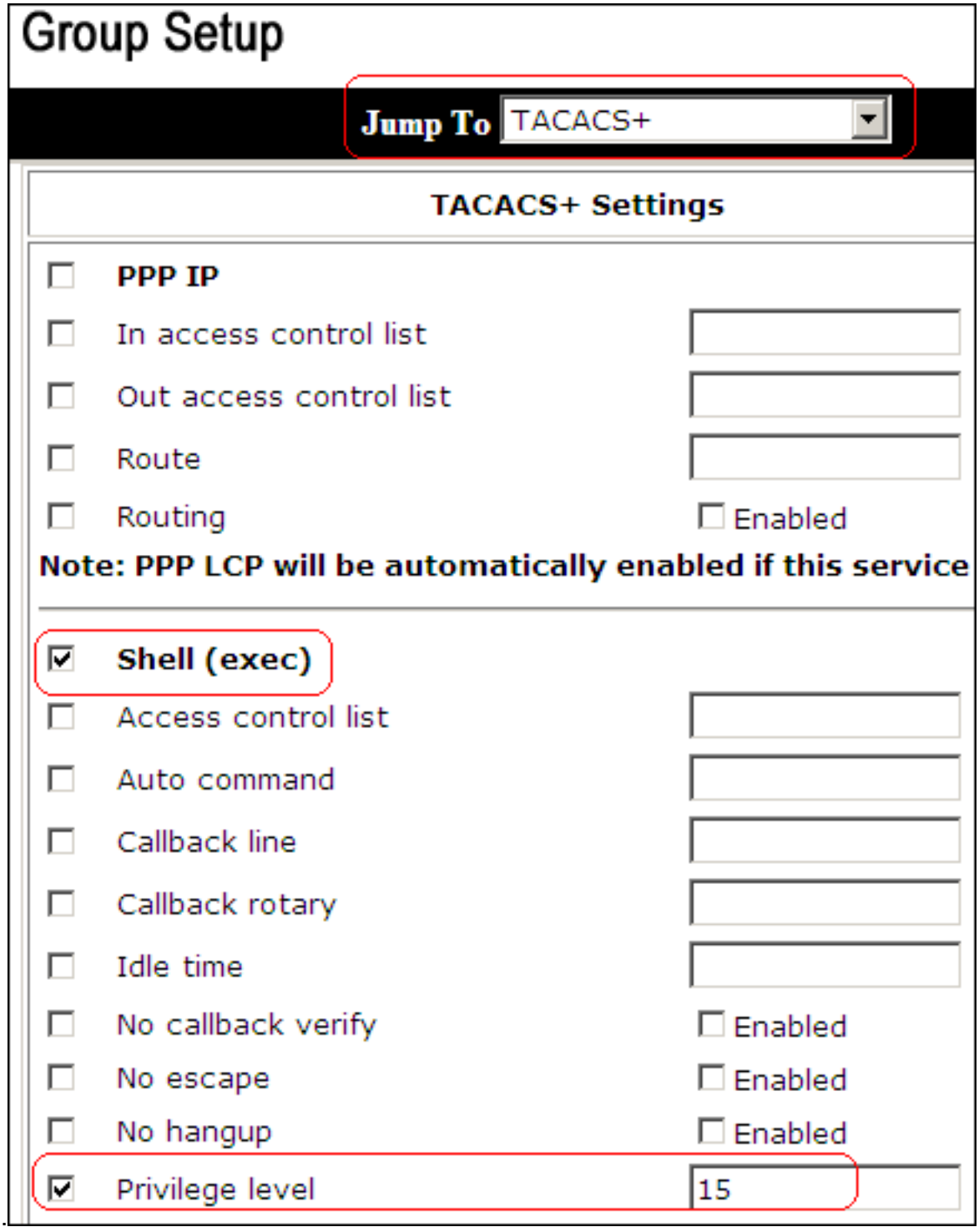
1. Dans la fenêtre ACS, cliquez sur **Group Setup**, et choisissez **Admin Group** dans la liste déroulante
Group.



2. Cliquez sur **Edit Settings**.
3. Dans la liste déroulante Aller à, sélectionnez **Activer les options**.
4. Dans la zone Enable Options, cliquez sur la case d'option **Max Privilege for any AAA client** et choisissez **Level 15** dans la liste déroulante.

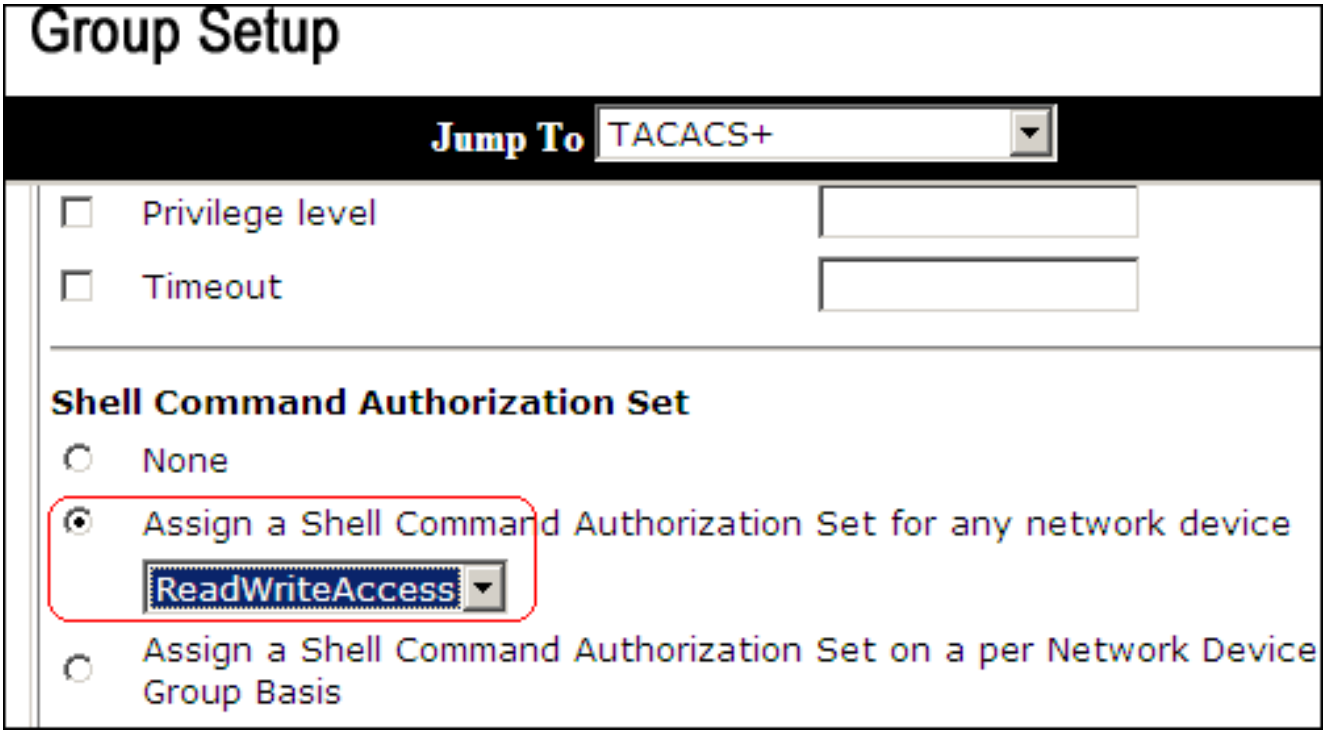


5. Dans la liste déroulante Aller à, sélectionnez **TACACS+**.
6. Dans la zone Paramètres TACACS+, cochez la case **Shell (exec)**, cochez la case **Niveau de privilège** et entrez **15** dans le champ Niveau de



privilège.

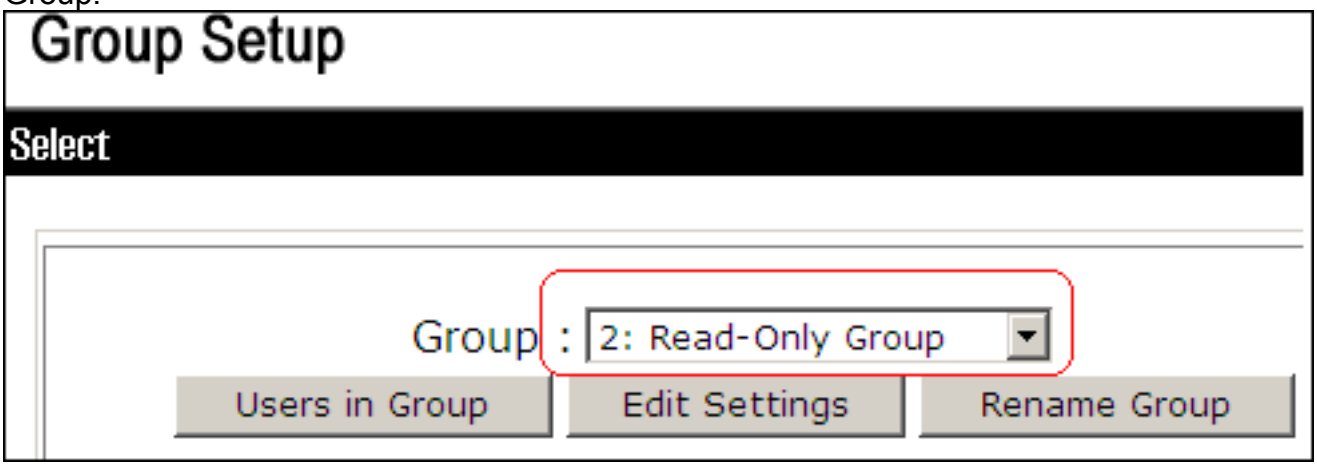
7. Dans la zone Jeu d'autorisations de commandes Shell, cliquez sur la case d'option **Affecter un jeu d'autorisations de commandes Shell pour n'importe quel périphérique réseau**, et choisissez **ReadWriteAccess** dans la liste déroulante.



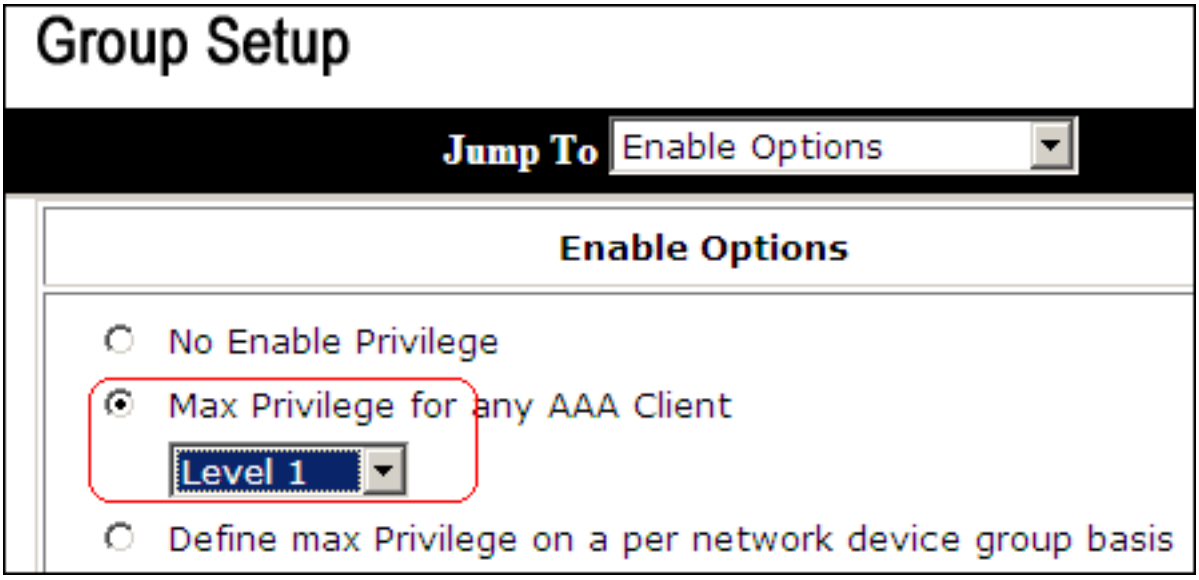
8. Cliquez sur Submit

Associer le jeu d'autorisations de commande Shell (accès en lecture seule) au groupe d'utilisateurs (groupe en lecture seule)

1. Dans la fenêtre ACS, cliquez sur **Group Setup**, et choisissez **Read-Only Group** dans la liste déroulante
   Group.

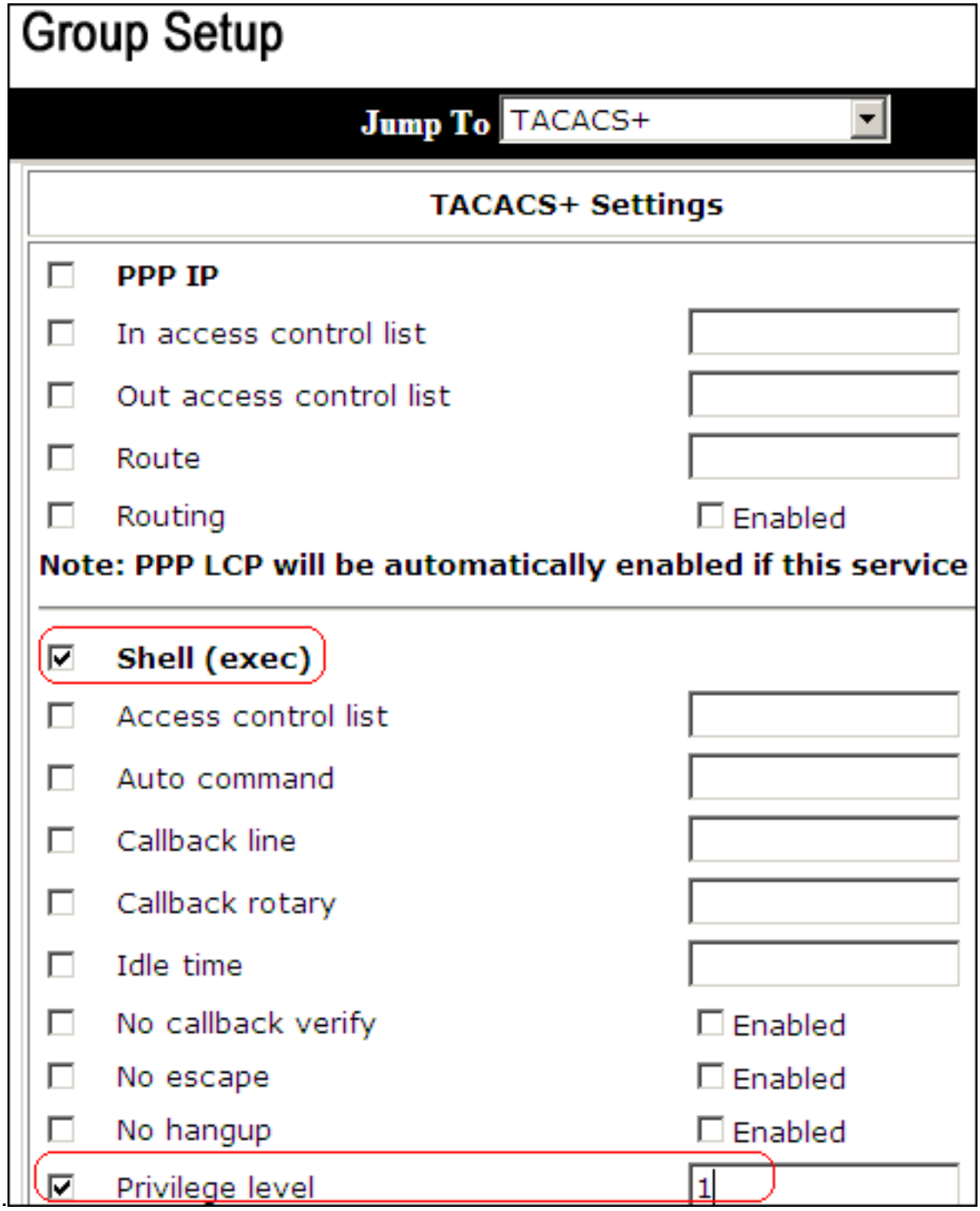


2. Cliquez sur **Edit Settings**.
3. Dans la liste déroulante Aller à, sélectionnez **Activer les options**.
4. Dans la zone Enable Options, cliquez sur la case d'option **Max Privilege for any AAA client** et choisissez **Level 1** dans la liste
   déroulante.



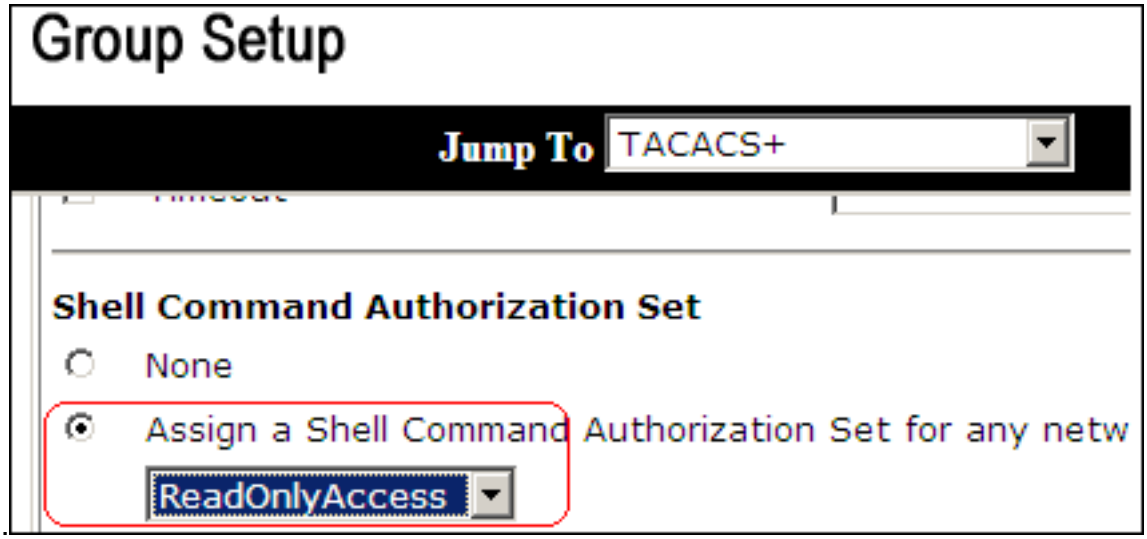
5. Dans la zone Paramètres TACACS+, cochez la case **Shell (exec)**, cochez la case **Niveau de privilège** et entrez **1** dans le champ Niveau de

privilège.



6. Dans la zone Jeu d'autorisations de commandes Shell, cliquez sur la case d'option **Affecter un jeu d'autorisations de commandes Shell pour n'importe quel périphérique réseau**, et choisissez **ReadOnlyAccess** dans la liste

déroulante.



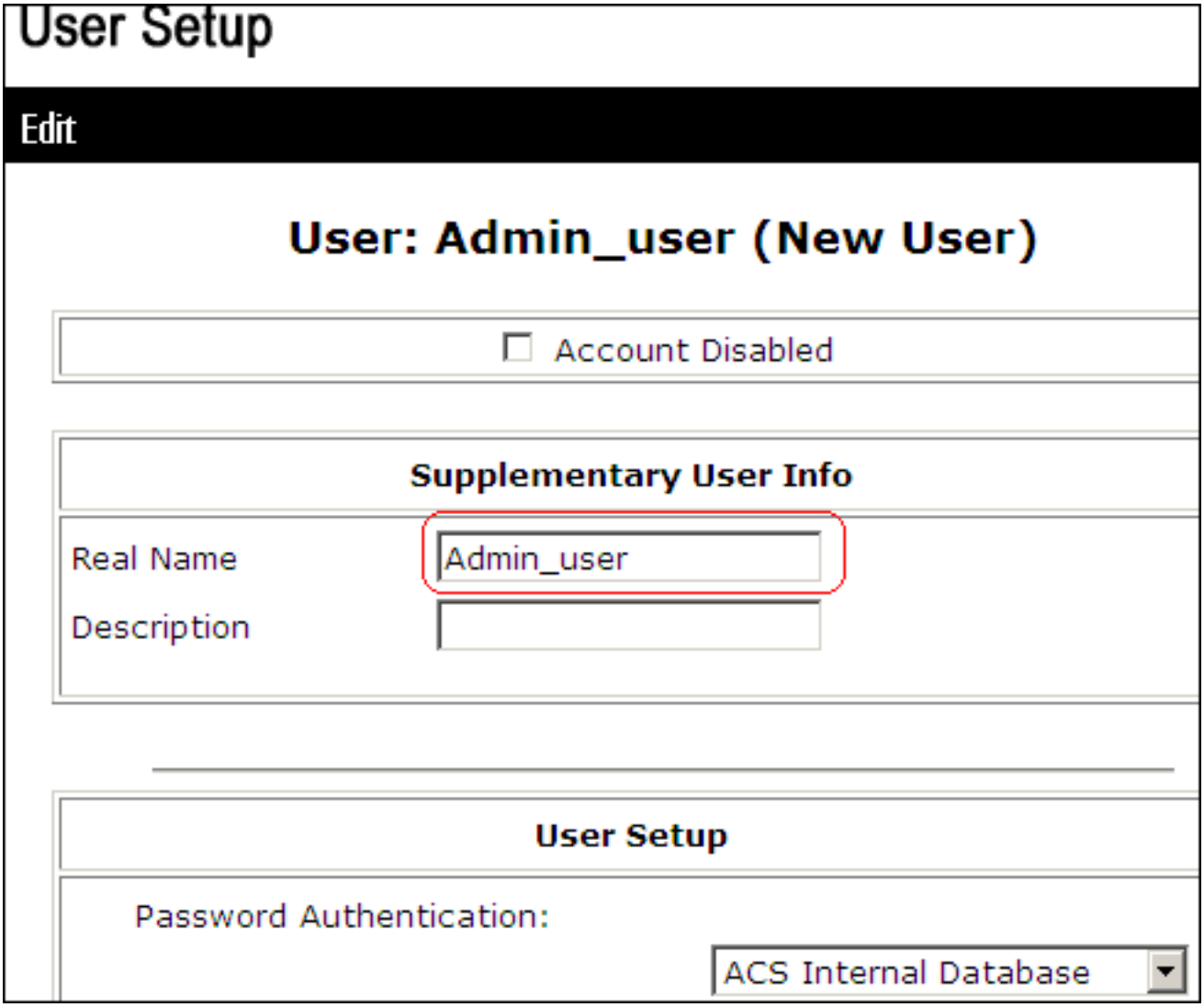
7. Cliquez sur Submit

Associez le jeu d'autorisations de commande Shell (Restrict_access) à User

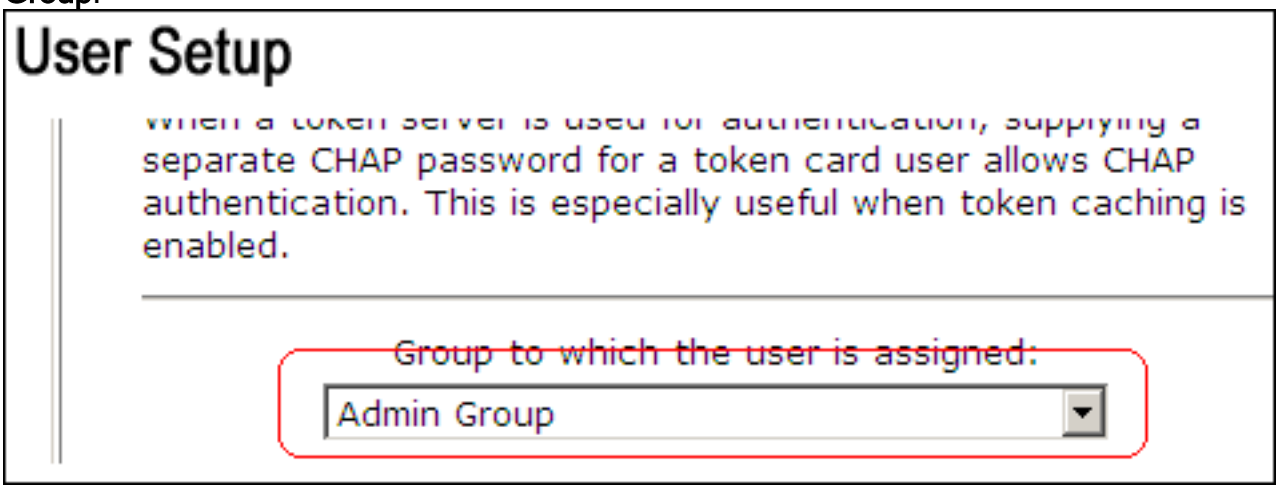
Référez-vous à la section Configuration d'un jeu d'autorisations de commande shell pour un utilisateur du Guide de l'utilisateur pour Cisco Secure Access Control Server 4.1 pour plus d'informations sur la façon de configurer le jeu d'autorisations de commande shell pour les utilisateurs.

Remarque : les paramètres de niveau utilisateur remplacent les paramètres de niveau groupe dans ACS, ce qui signifie que si l'utilisateur dispose d'une autorisation de commande shell définie dans les paramètres de niveau utilisateur, alors il remplace les paramètres de niveau groupe.

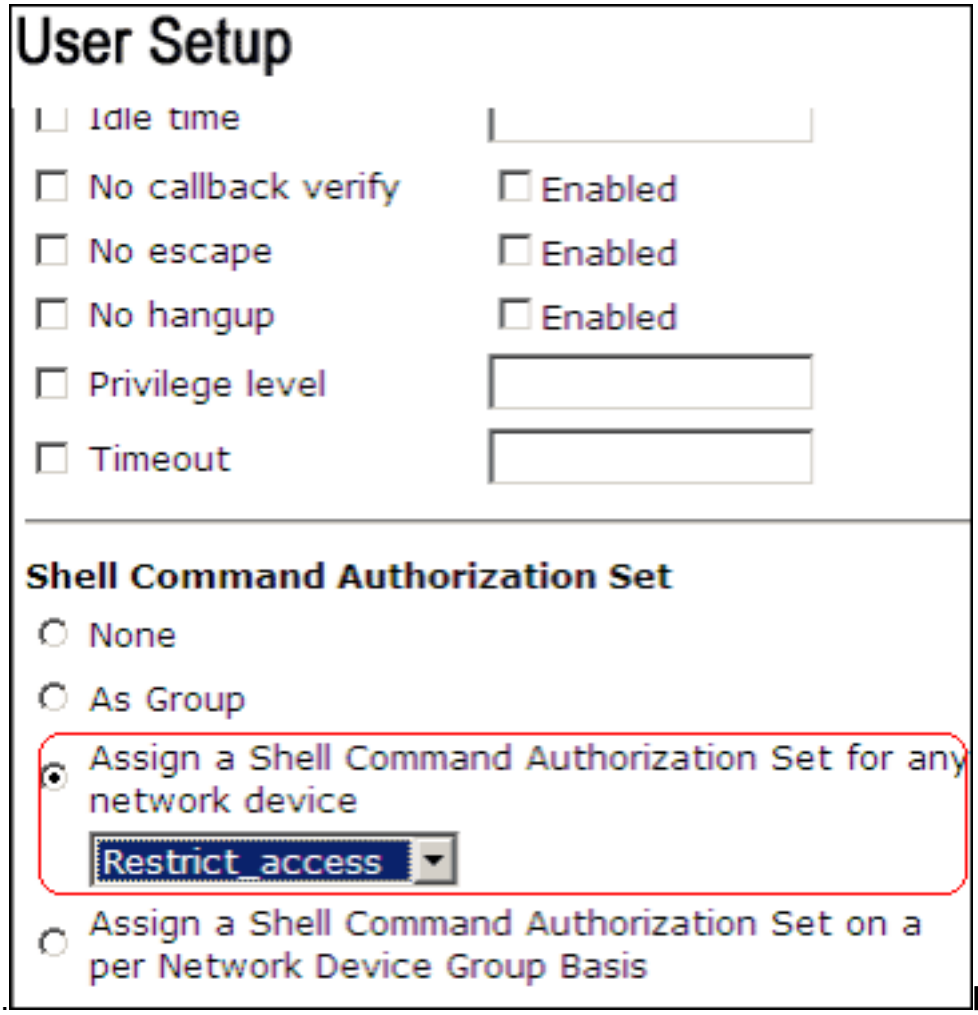
1. Cliquez sur **User Setup > Add/Edit** afin de créer un nouvel utilisateur nommé *Admin_user* pour faire partie du groupe
   Admin.



2. Dans la liste déroulante du groupe auquel l'utilisateur est affecté, sélectionnez **Admin Group**.



3. Dans la zone Jeu d'autorisations de commandes Shell, cliquez sur la case d'option **Affecter un jeu d'autorisations de commandes Shell pour n'importe quel périphérique réseau**, et choisissez **Restrict_access** dans la liste déroulante.**Remarque :** dans ce scénario, cet utilisateur fait partie du groupe Admin. Le jeu d'autorisations du shell *Restrict_access* est applicable ; le jeu d'autorisations du shell *ReadWrite Access* n'est pas



applicable. **Remarque :** dans la section TACACS+ (Cisco) de la zone Interface Configuration, assurez-vous que l'option **Shell (exec)** est sélectionnée dans la colonne User.

Configuration du routeur IOS

Outre votre configuration prédéfinie, ces commandes sont requises sur un routeur ou un commutateur IOS afin de mettre en oeuvre l'autorisation de commande via un serveur ACS :

```
aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ local
aaa authorization commands 1 default  group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123
```

Configuration ASA/PIX/FWSM

Outre votre configuration prédéfinie, ces commandes sont requises sur ASA/PIX/FWSM afin de mettre en oeuvre l'autorisation de commande via un serveur ACS :

```
aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver
```

Remarque : il n'est pas possible d'utiliser le protocole RADIUS afin de restreindre l'accès

utilisateur à ASDM à des fins de lecture seule. Puisque les paquets RADIUS contiennent simultanément l'authentification et l'autorisation, tous les utilisateurs qui sont authentifiés dans le serveur RADIUS ont un niveau de privilège de 15. Vous pouvez y parvenir via TACACS avec l'implémentation de jeux d'autorisations de commande.

Remarque : ASA/PIX/FWSM met beaucoup de temps à exécuter chaque commande saisie, même si ACS n'est pas disponible pour effectuer l'autorisation de commande. Si ACS n'est pas disponible et que l'autorisation de commande est configurée sur ASA, ASA demande toujours l'autorisation de commande pour chaque commande.

Dépannage

Erreur : échec d'autorisation de commande

Problème

Une fois que vous êtes connecté au pare-feu via la journalisation TACACS, les commandes ne fonctionnent pas. Lorsque vous entrez une commande, cette erreur est reçue : `l'autorisation de commande a échoué.`

Solution

Procédez comme suit pour résoudre ce problème :

1. Vérifiez que le nom d'utilisateur correct est utilisé et que tous les privilèges requis sont attribués à l'utilisateur.
2. Si le nom d'utilisateur et les privilèges sont corrects, vérifiez que l'ASA est connecté à l'ACS et que l'ACS est actif.

Remarque : cette erreur peut également se produire si l'administrateur a configuré par erreur l'autorisation de commande pour les utilisateurs locaux et TACACS. Dans ce cas, effectuez une récupération de mot de passe afin de résoudre le problème.

Informations connexes

- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Page d'assistance de Cisco Secure Control Access Control Server
- Support et documentation techniques - Cisco Systems

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.