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

Contenu

Introduction

Ce document décrit comment configurer les positionnements d'autorisation de shell dans le Cisco Secure Access Control Server (ACS) pour des clients d'AAA, tels que des Routeurs de Cisco IOS® ou des Commutateurs et des appliances de sécurité Cisco (ASA/PIX/FWSM) avec TACACS+ comme protocole d'autorisation.

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

Conditions préalables

Conditions requises

Ce document suppose que les configurations de base sont placées dans des clients d'AAA et

ACS.

Dans ACS, choisissez la **configuration d'interface > a avancé des options**, et s'assure que la case d'**attributs du Par-utilisateur TACACS+/RADIUS** est cochée.

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Secure Access Control Server (ACS) ces passages la version de logiciel 3.3 et 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.

Positionnements d'autorisation de commande

Les positionnements d'autorisation de commande fournissent un mécanisme central pour contrôler l'autorisation de chaque commande qui est émise sur n'importe quel périphérique donné de réseau. Cette caractéristique améliore considérablement l'évolutivité et la gestionnabilité exigées pour placer des restrictions d'autorisation.

Dans ACS, les positionnements par défaut d'autorisation de commande incluent des positionnements d'autorisation de commande shell et l'autorisation de commande PIX place. Les applications de gestion de périphériques de Cisco, telles que le CiscoWorks Management Center pour pare-feux, peuvent demander à ACS pour prendre en charge les sets types supplémentaires d'autorisation de commande.

Remarque: Les positionnements d'autorisation de commande PIX exigent que la demande d'autorisation de commande TACACS+ identifient le service comme *pixshell*. Vérifiez que ce service a été mis en application dans le SYSTÈME D'EXPLOITATION de version de PIX que vos Pare-feu utilisent ; sinon, l'autorisation de commande shell d'utilisation place pour exécuter l'autorisation de commande pour des périphériques PIX. Référez-vous à configurer une autorisation de commande shell réglée pour un pour en savoir plus de groupe d'utilisateurs.

Remarque: En date de la version 6.3 OS PIX, le service de pixshell n'a pas été mis en application.

Remarque: Les appliances de sécurité Cisco (ASA/PIX) ne permet pas actuellement l'utilisateur à placer directement dans le mode enable pendant la procédure de connexion. L'utilisateur doit manuellement entamer le mode enable.

Afin d'offrir plus de contrôle des sessions de telnet administratives périphérique-hébergées, un périphérique de réseau qui utilise TACACS+ peut demander l'autorisation pour chaque ligne de commande avant qu'il exécute. Vous pouvez définir un ensemble de commandes qui sont permises ou refusées pour l'exécution par un utilisateur particulier sur un périphérique donné. ACS a plus loin amélioré cette capacité avec ces configurations :

- **Positionnements Désignés réutilisables de Command Authorization** — Sans citer directement n'importe quel utilisateur ou groupe d'utilisateurs, vous pouvez créer un ensemble Désigné d'autorisations de commande. Vous pouvez définir plusieurs les positionnements d'autorisation de commande qui tracent différents profils d'accès. Exemple :Un positionnement d'autorisation de commande de *centre d'assistance* a pu permettre l'accès aux commandes de haut niveau de furetage, telles que le **passage d'exposition**, et refuse toutes les commandes de configuration.*Un tout le* positionnement d'autorisation d'ordre d'*ingénieurs réseau* a pu contenir une liste limitée de commandes permises pour n'importe quel ingénieur réseau à l'entreprise.*Un réseau local machine le* positionnement d'autorisation de commande pourrait permettre toutes les commandes (et inclure des commandes de configuration des adresses IP).
- **Finesse correcte de configuration** — Vous pouvez créer des associations entre les positionnements Désignés d'autorisation de commande et les groupes de périphériques réseau (NDGs). Ainsi, vous pouvez définir différents profils d'accès pour les utilisateurs selon lesquels les périphériques de réseau ils accèdent à. Vous pouvez associer le même positionnement Désigné d'autorisation de commande avec plus d'un NDG et l'utiliser pour plus d'un groupe d'utilisateurs. ACS impose l'intégrité des données. Des positionnements Désignés d'autorisation de commande sont maintenus dans la base de données interne ACS. Vous pouvez employer les caractéristiques de sauvegarde ACS et de restauration pour les sauvegarder et restaurer. Vous pouvez également répliquer des positionnements d'autorisation de commande vers ACSs secondaire avec d'autres données de configuration.

Pour les sets types d'autorisation de commande qui prennent en charge des applications de gestion de périphériques de Cisco, les avantages sont semblables quand vous utilisez des positionnements d'autorisation de commande. Vous pouvez appliquer des positionnements d'autorisation de commande aux groupes ACS qui contiennent des utilisateurs de l'application de gestion de périphériques afin d'imposer l'autorisation de divers privilèges dans une application de gestion de périphériques. Les groupes ACS peuvent correspondre à différents rôles dans l'application de gestion de périphériques, et vous pouvez appliquer différents positionnements d'autorisation de commande à chaque groupe, comme applicable.

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

1. **Correspondance de commande** — ACS détermine si la commande qui est traitée apparie une commande répertoriée dans le positionnement d'autorisation de commande. Si la commande n'est pas appariée, l'autorisation de commande est déterminée par l'établissement inégalé de commandes : *laissez* ou *refusez*. Autrement, si la commande est appariée, l'évaluation continue.
2. **Correspondance d'argument** — ACS détermine si les arguments de commande ont présenté à correspondance les arguments de commande répertoriés dans le positionnement d'autorisation de commande.Si aucun argument n'est pondéré, l'autorisation de commande est déterminée par si l'option inégalée d'Args d'autorisation est activée. Si on permet des arguments inégalés, la commande est autorisée et des extrémités d'évaluation ; autrement, la commande n'est pas autorisée et des extrémités d'évaluation.Si tous les arguments sont pondérés, l'évaluation continue.
3. **Stratégie d'argument** — Une fois qu'ACS détermine que les arguments dans les arguments de correspondance de commande dans le positionnement d'autorisation de commande, ACS détermine si chaque argument de commande est explicitement permis. Si on permet explicitement tous les arguments, ACS accorde l'autorisation de commande. Si on ne permet

aucun argument, ACS refuse l'autorisation de commande.

Ajoutez un positionnement d'autorisation de commande shell

Cette section inclut ces scénarios qui décrivent comment ajouter une autorisation de commande réglée :

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

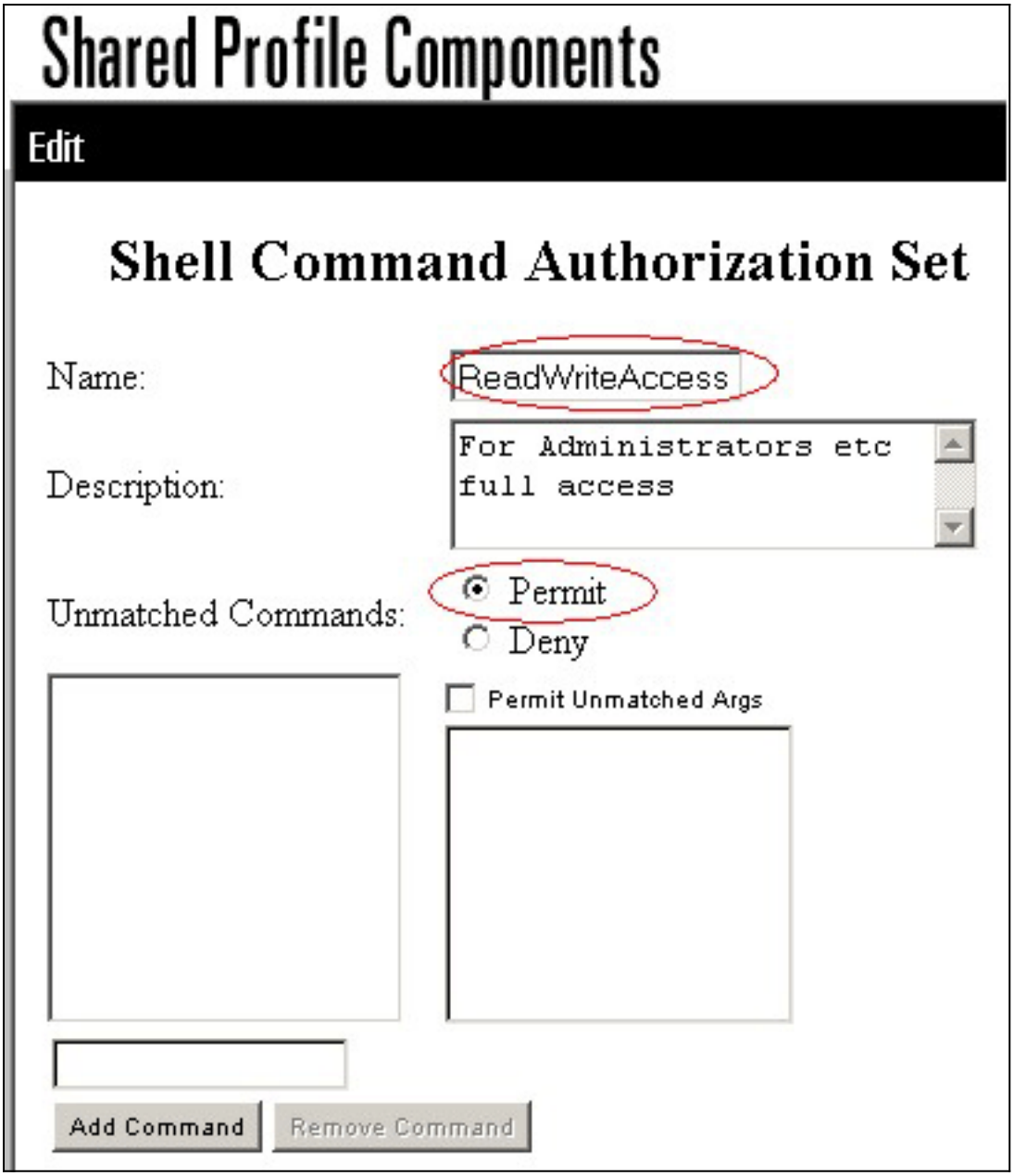
Remarque: Référez-vous à ajouter une section réglée d'autorisation de commande du guide utilisateur pour le Cisco Secure Access Control Server 4.1 pour plus d'informations sur la façon créer des positionnements d'autorisation de commande. Référez-vous à éditer une autorisation de commande réglée et à supprimer une autorisation de commande réglée pour plus d'informations sur la façon éditer et supprimer des positionnements d'autorisation de commande.

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

En cela on accorde des scénarios, des utilisateurs l'accès lecture/écriture (ou plein).

Dans la région réglée d'autorisation de commande shell de la fenêtre partagée de composants de profil, configurez ces configurations :

1. Dans la zone d'identification, entrez dans **ReadWriteAccess** comme nom réglé d'autorisation de commande.
2. Dans le champ description, écrivez une description pour le positionnement d'autorisation de commande.
3. Cliquez sur la case d'option d'**autorisation**, et puis cliquez sur Submit.

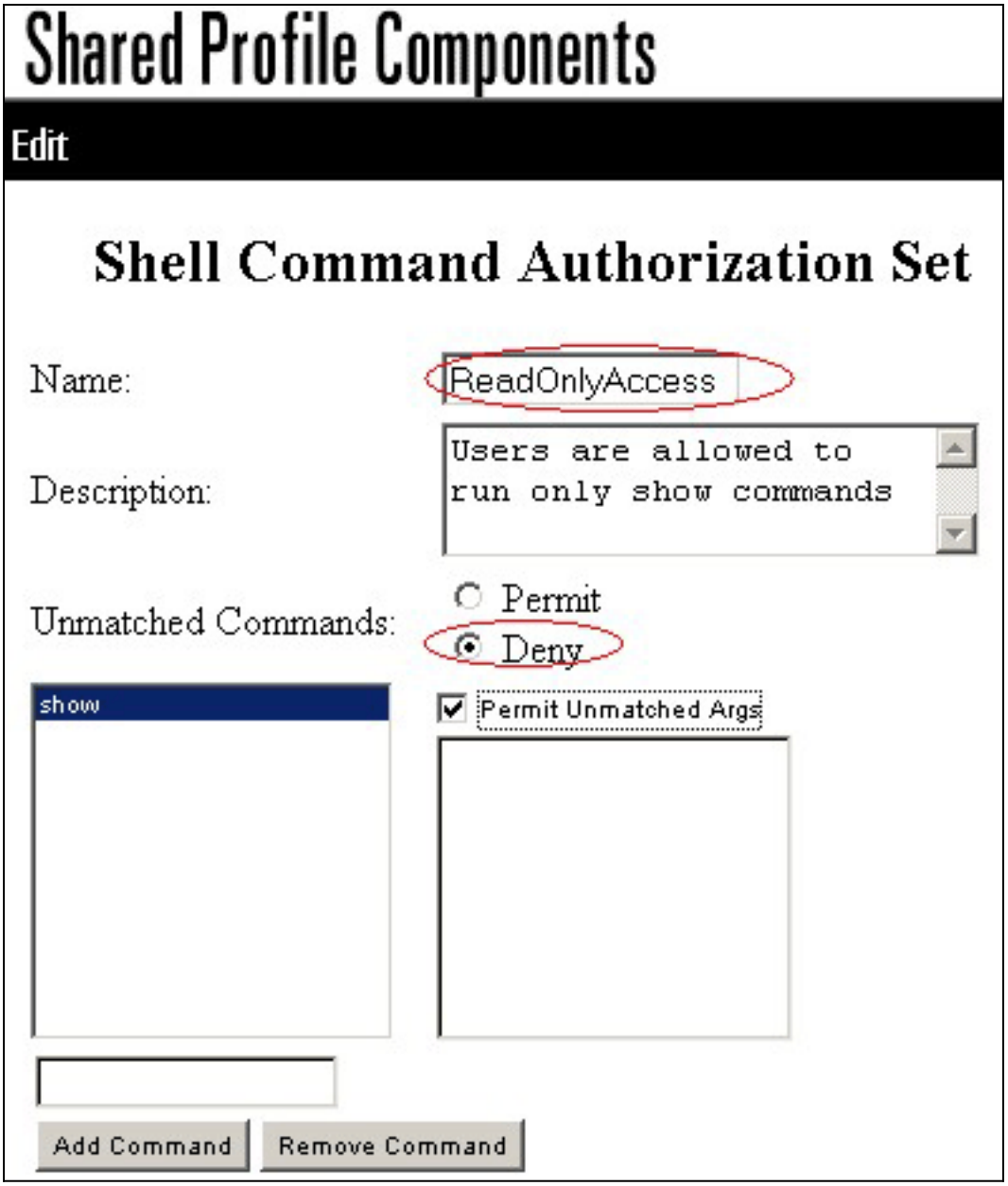


Scénario 2 : Privilège pour l'accès en lecture seule

En cela les scénarios, des utilisateurs peuvent utiliser seulement des **commandes show**.

Dans la région réglée d'autorisation de commande shell de la fenêtre partagée de composants de profil, configurez ces configurations :

1. Dans la zone d'identification, entrez dans **ReadOnlyAccess** comme le nom du positionnement d'autorisation de commande.
2. Dans le champ description, écrivez une description pour le positionnement d'autorisation de commande.
3. Cliquez sur la case d'option de **refuser**.
4. Sélectionnez la **commande show** dans le domaine au-dessus du bouton de commande d'ajouter, et puis cliquez sur Add la **commande**.
5. Cochez la case **inégalée d'Args d'autorisation**, et cliquez sur Submit

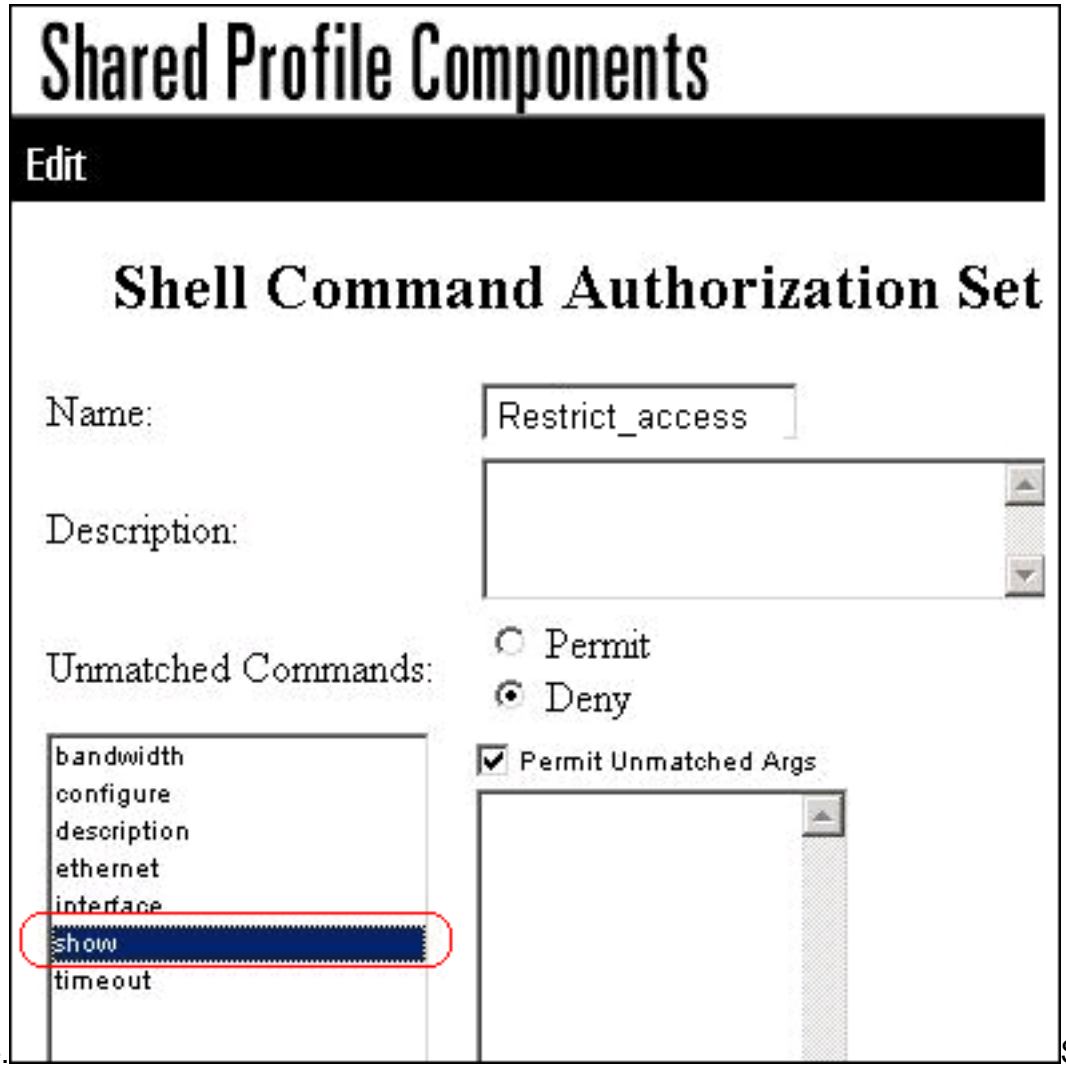


Scénario 3 : Privilège pour Access restreint

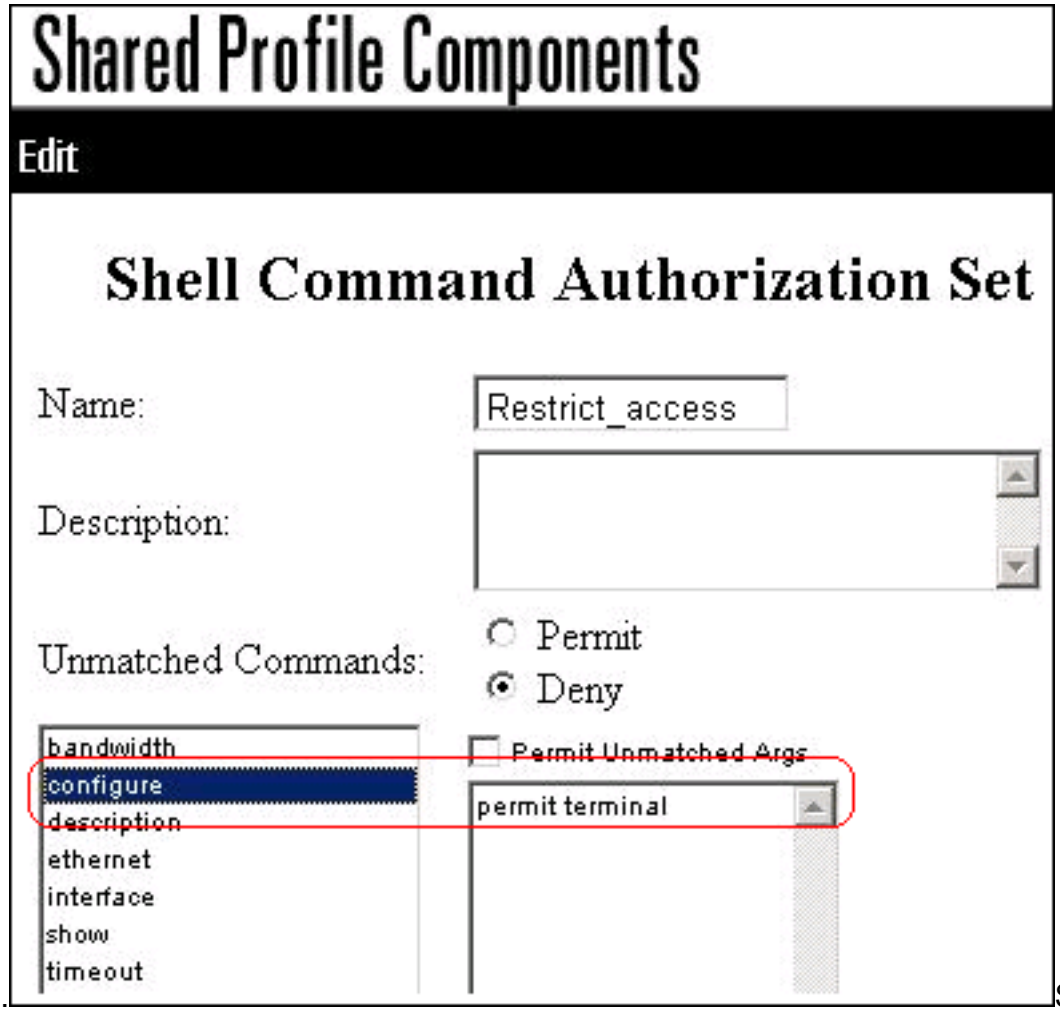
Dans ce scénario, les utilisateurs peuvent utiliser des commandes sélectives.

Dans la région réglée d'autorisation de commande shell de la fenêtre partagée de composants de profil, configurez ces configurations :

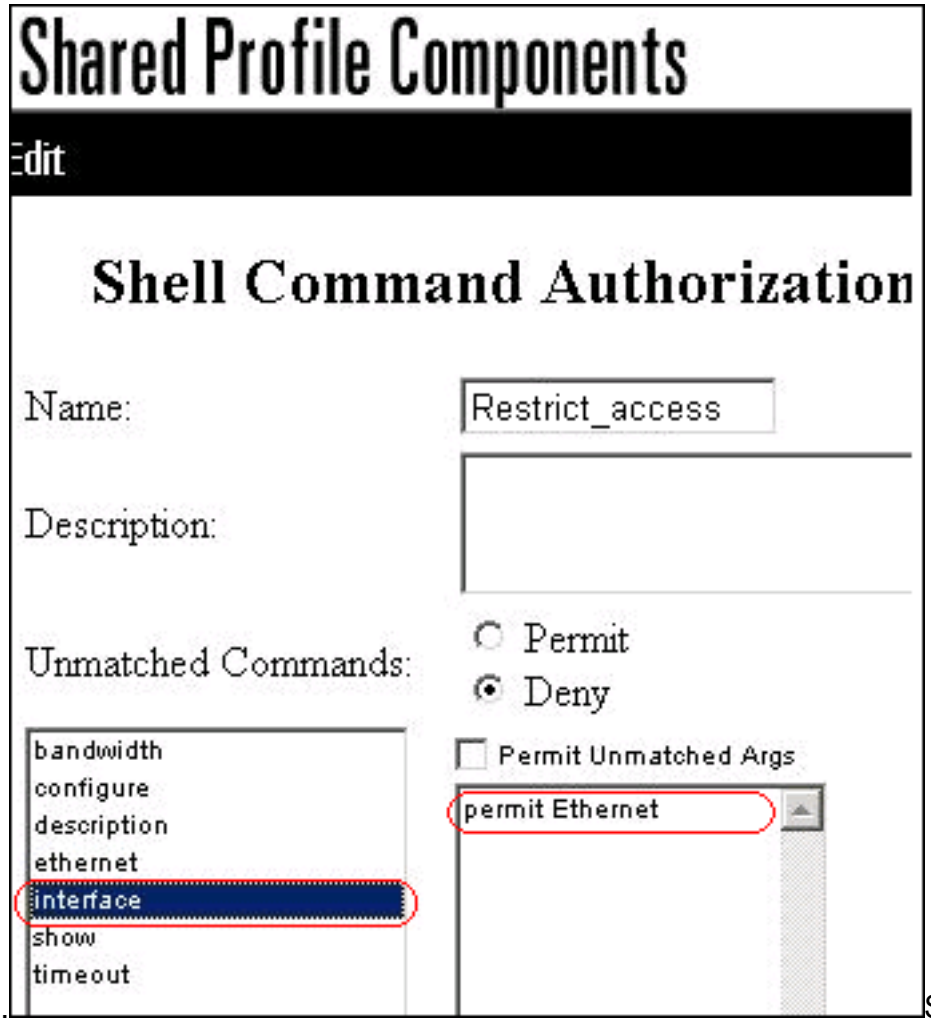
1. Dans la zone d'identification, entrez dans **Restrict_access** comme le nom du positionnement d'autorisation de commande.
2. Cliquez sur la case d'option de **refuser**.
3. Sélectionnez les commandes que vous voulez permettre sur les clients d'AAA.Dans le domaine situé au-dessus du bouton de commande d'ajouter, sélectionnez la **commande show**, et cliquez sur Add la



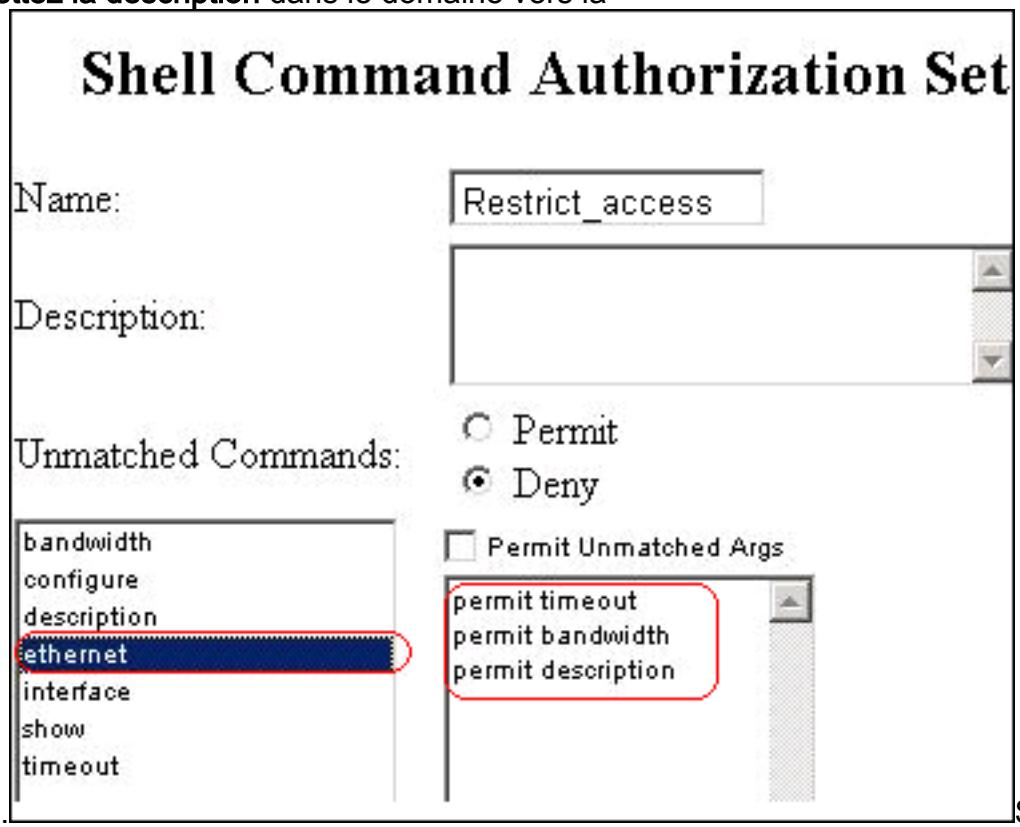
commande.Sélectionnez la commande de **configurer**, et cliquez sur Add la **commande**.Sélectionnez la commande de **configurer**, et entrez dans le **terminal d'autorisation** dans le domaine vers la



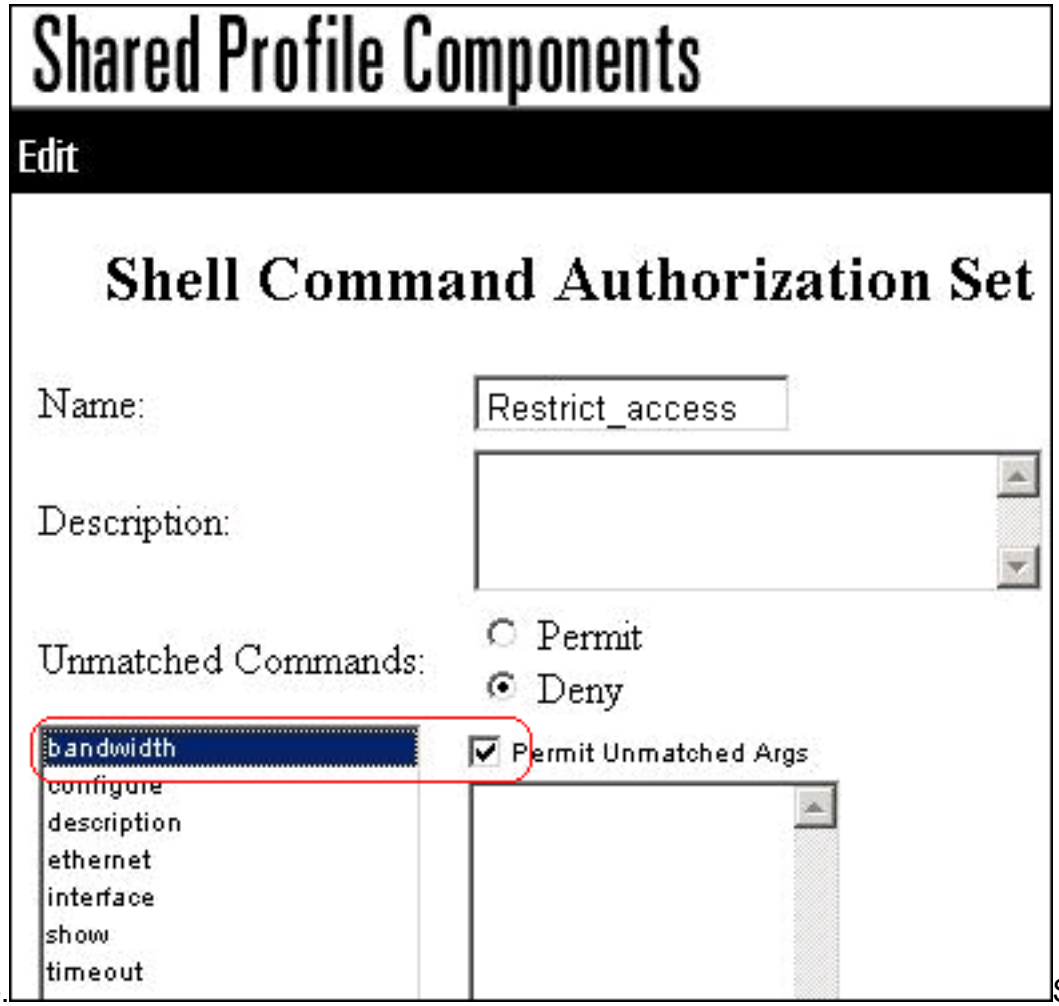
droite. Sélectionnez la **commande d'interface**, et cliquez sur Add la **commande**.Sélectionnez la **commande d'interface**, et écrivez les **Ethernets d'autorisation** dans le domaine vers la



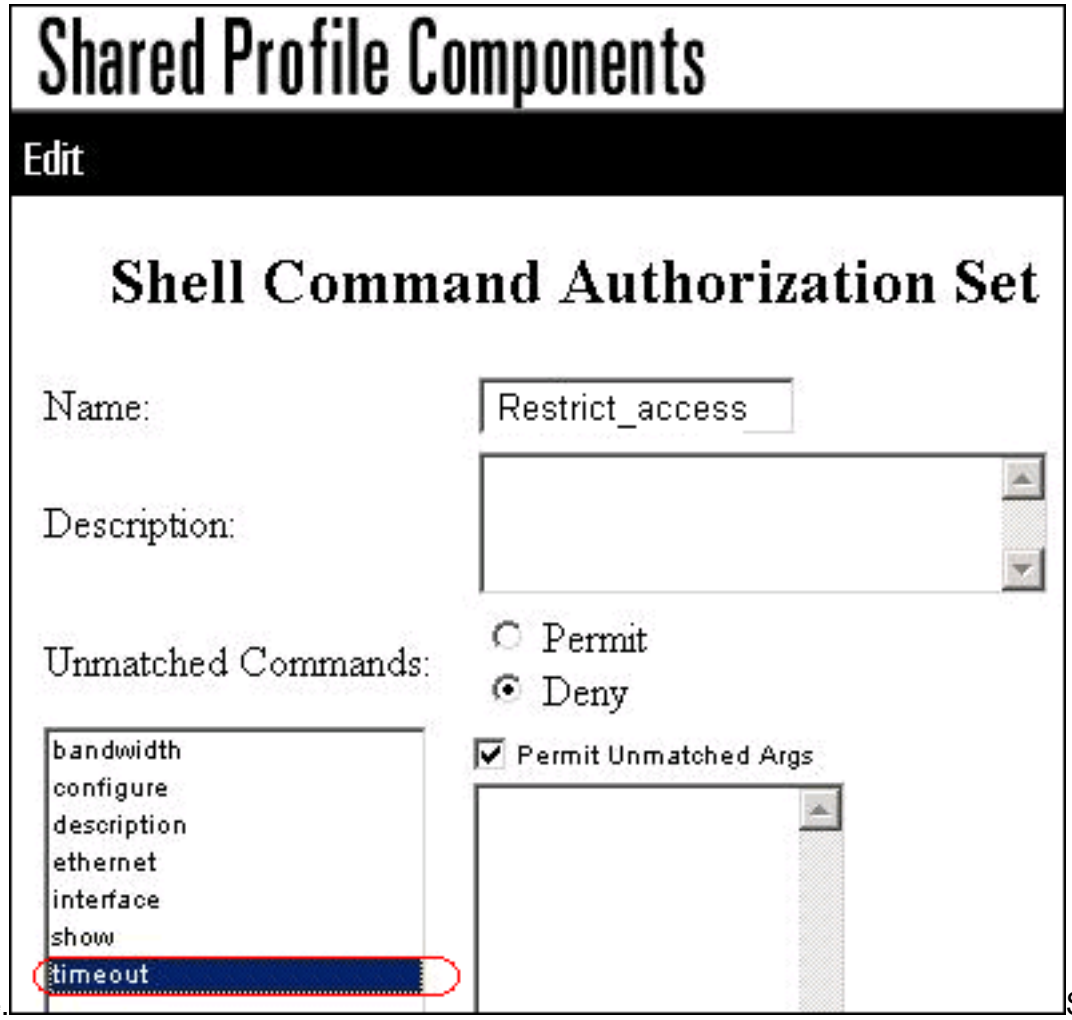
droite.Sélectionnez la commande d'**Ethernets**, et cliquez sur Add la **commande**.Sélectionnez la **commande d'interface**, et écrivez le **délai d'attente d'autorisation**, **permettez la bande passante**, et **permettez la description** dans le domaine vers la



droite.Sélectionnez la **commande bandwidth**, et cliquez sur Add la

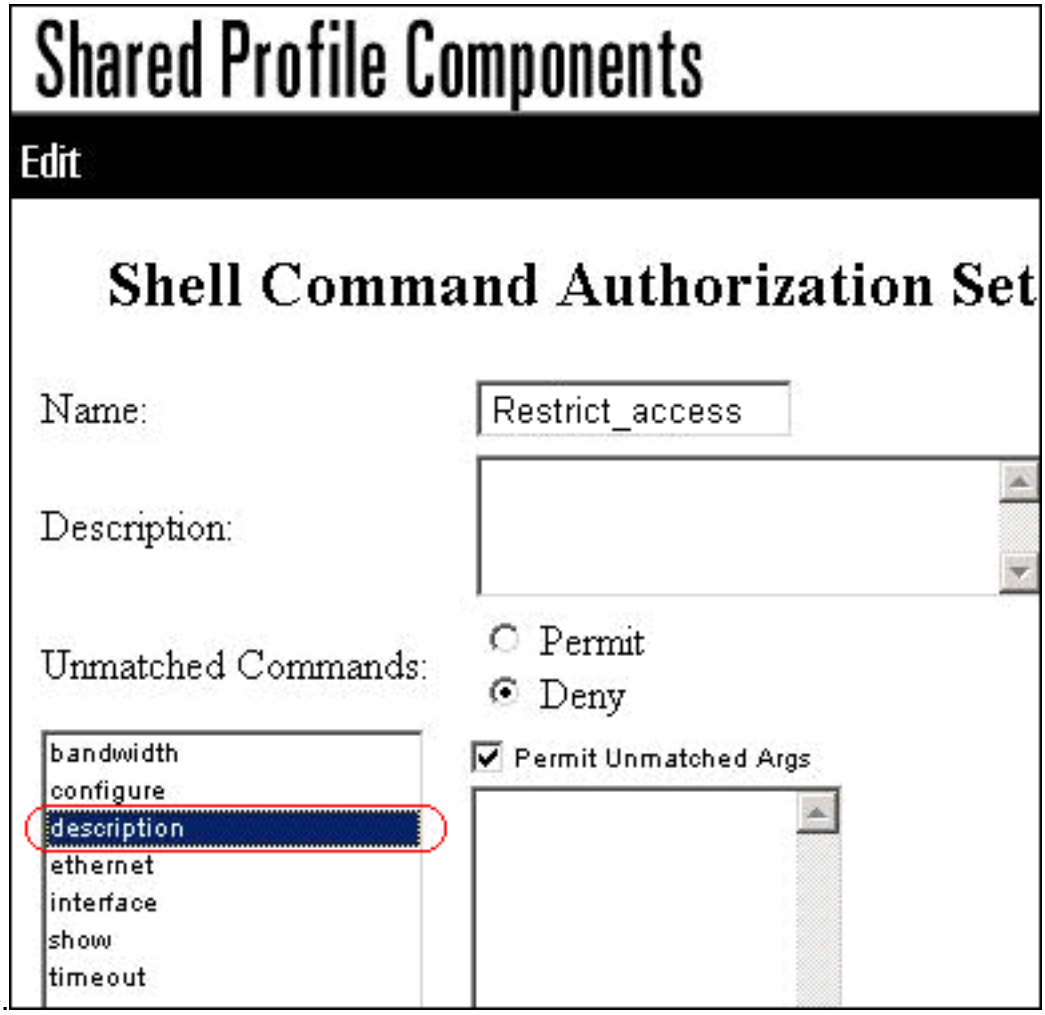


commande. Sélectionnez la commande de **délai d'attente**, et cliquez sur Add la



commande. Sélectionnez la **commande description**, et cliquez sur Add la

commande.



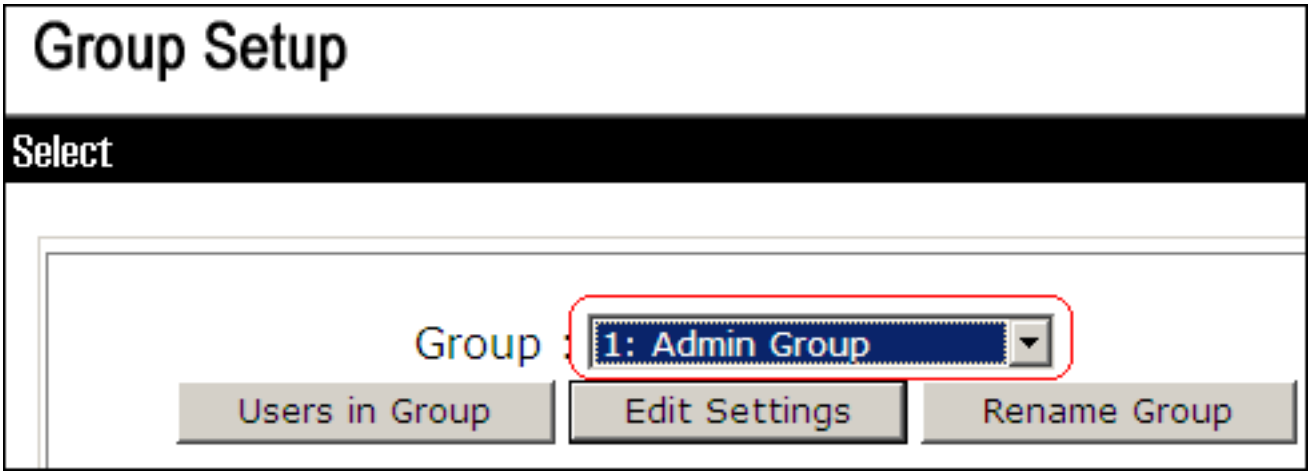
4. Cliquez sur **Submit**.

Associez l'autorisation de commande shell réglée au groupe d'utilisateurs

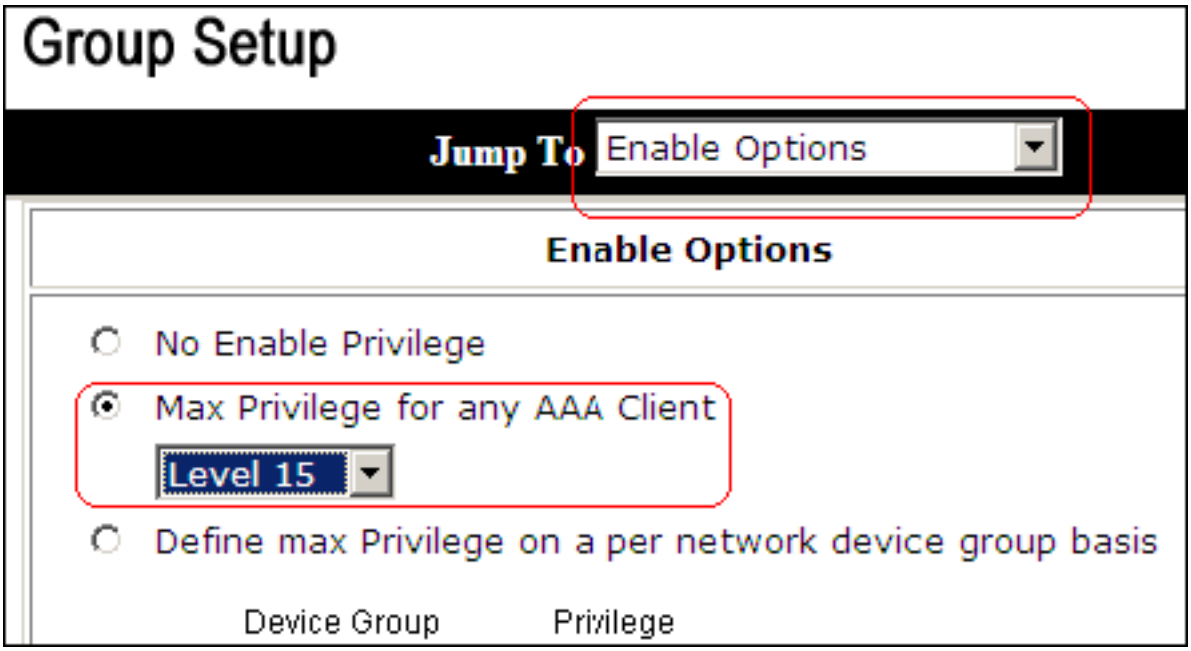
Référez-vous à configurer un positionnement d'autorisation de commande shell pour une section de groupe d'utilisateurs du guide utilisateur pour le Cisco Secure Access Control Server 4.1 pour plus d'informations sur la façon configurer la configuration réglée d'autorisation de commande shell pour des groupes d'utilisateurs.

Associez l'autorisation de commande shell réglée (Access lecture/écriture) au groupe d'utilisateurs (le groupe d'admin)

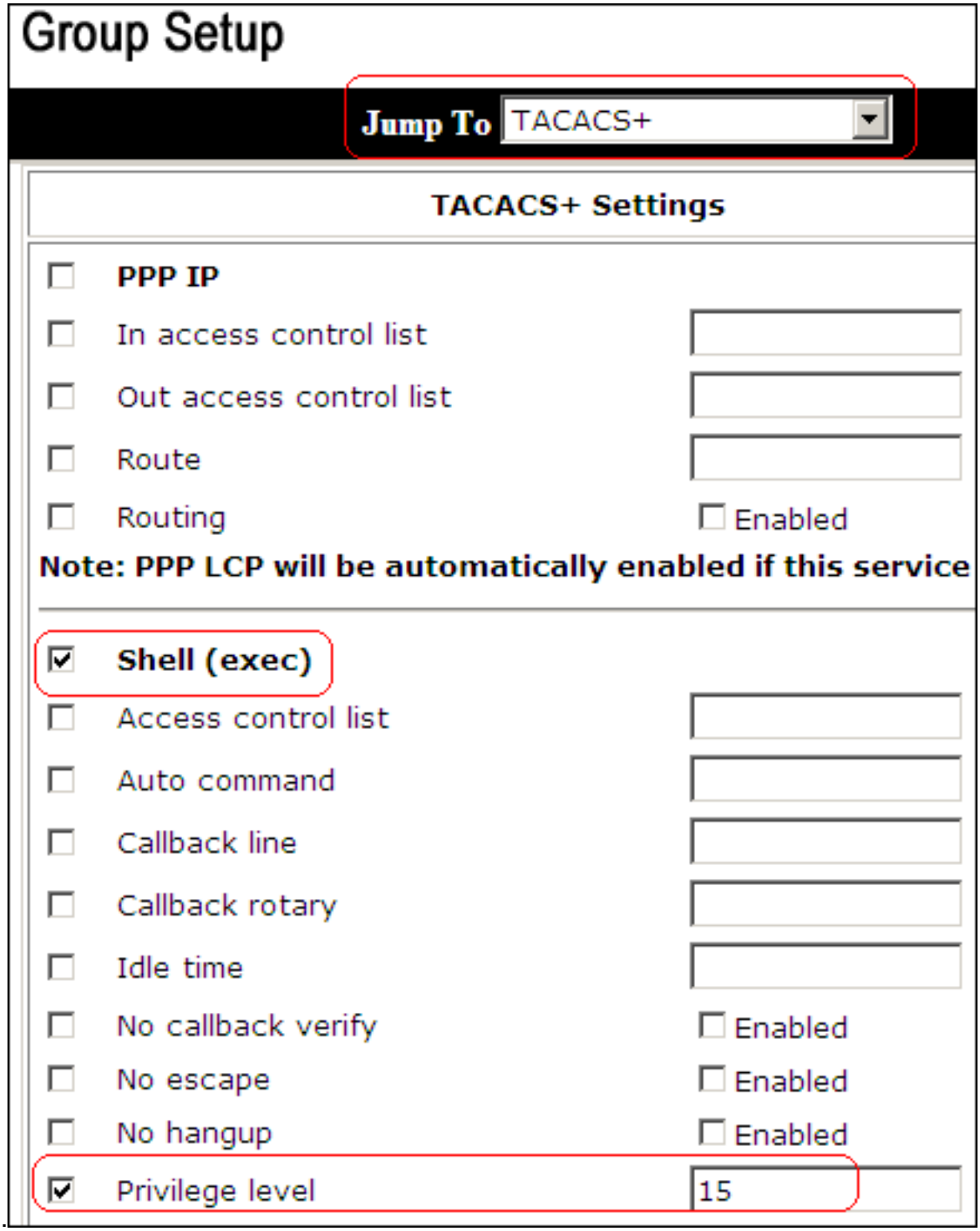
1. Dans la fenêtre ACS, cliquez sur le **Group Setup**, et choisissez le **groupe d'admin de la** liste déroulante de
groupe.



2. Cliquez sur Edit les **configurations**.
3. De l'accès à la liste déroulante, choisissez Enable les **options**.
4. Dans la région d'options d'enable, cliquez sur le **privilège maximum pour n'importe quel** bouton de **transmetteur client d'AAA**, et choisissez le **niveau 15 de la** liste déroulante.

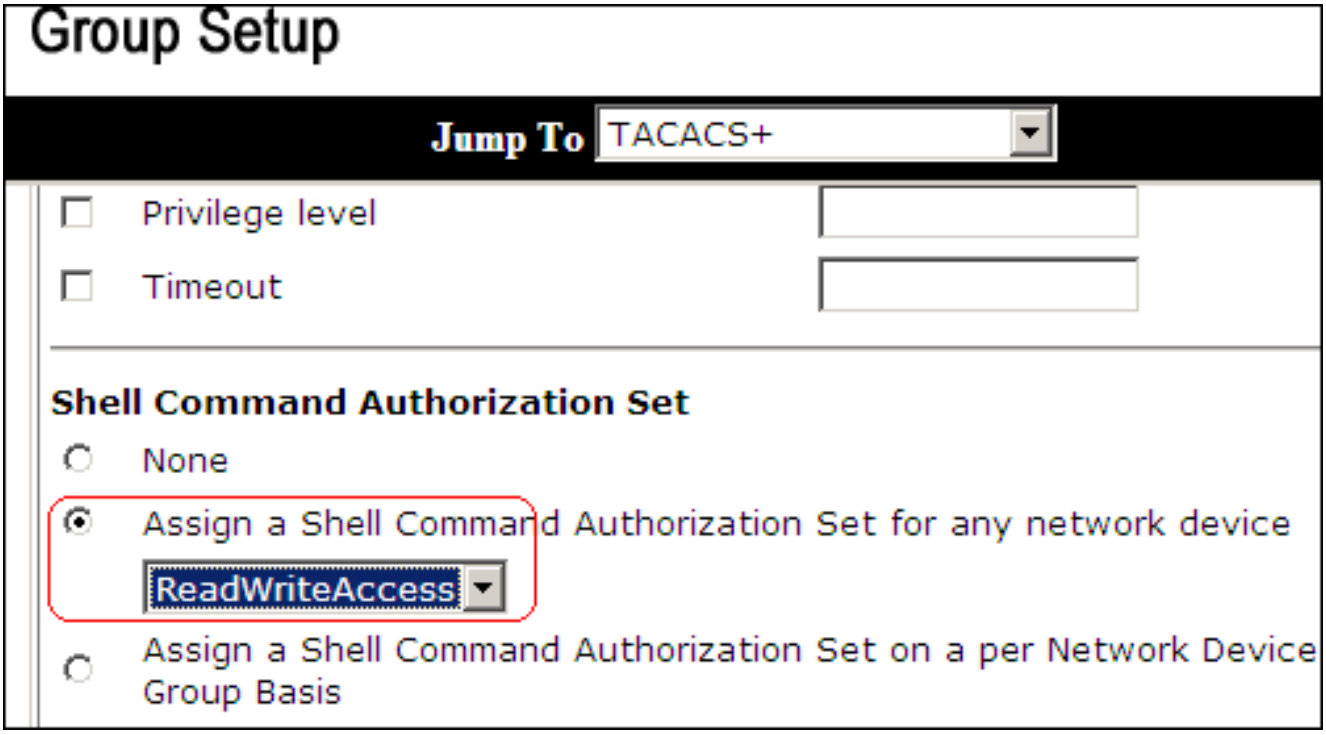


5. De l'accès à la liste déroulante, choisissez **TACACS+**.
6. Dans la région de configurations TACACS+, cochez la case de **shell (exécutif)**, cochez la case de **niveau de privilège**, et écrivez **15** dans le domaine de niveau de



privilège.

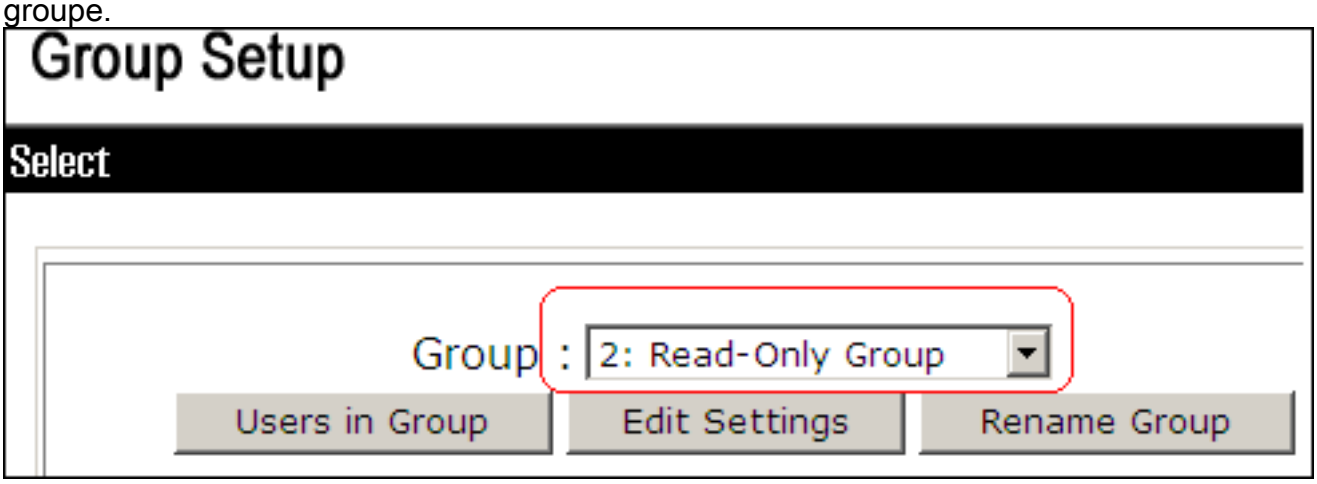
7. Dans la région réglée d'autorisation de commande shell, cliquez sur l'**assigner une autorisation de commande shell réglée pour n'importe quelle** case d'option de **périphérique de réseau**, et choisissez **ReadWriteAccess de la** liste déroulante.



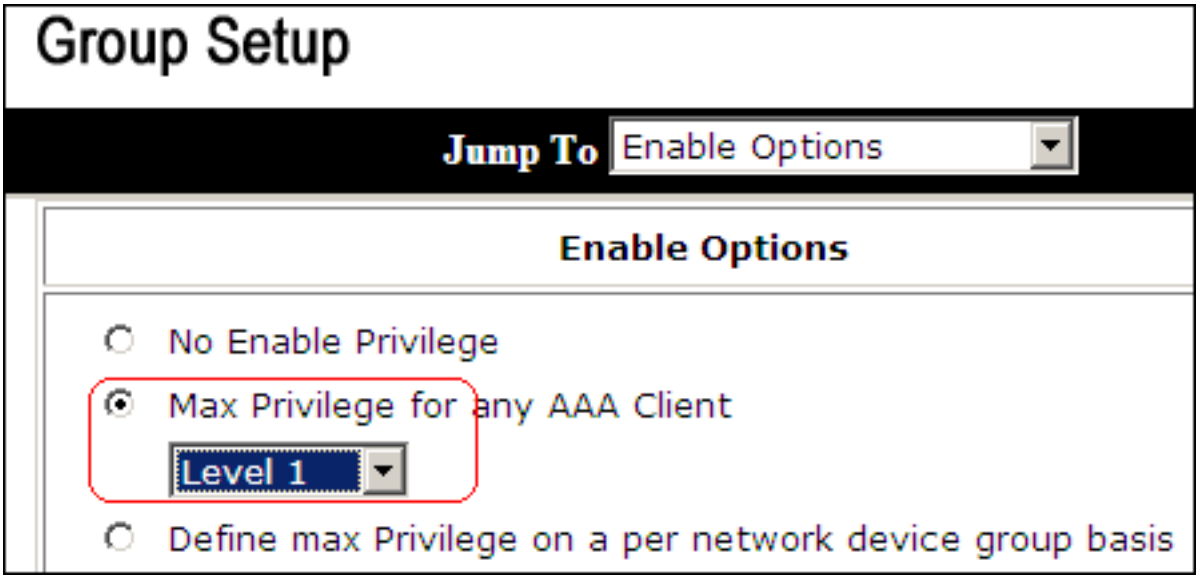
8. Cliquez sur Submit

Associez l'autorisation de commande shell réglée (Access inaltérable) au groupe d'utilisateurs (le groupe en lecture seule)

1. Dans la fenêtre ACS, cliquez sur le **Group Setup**, et choisissez le **groupe en lecture seule de la** liste déroulante de groupe.

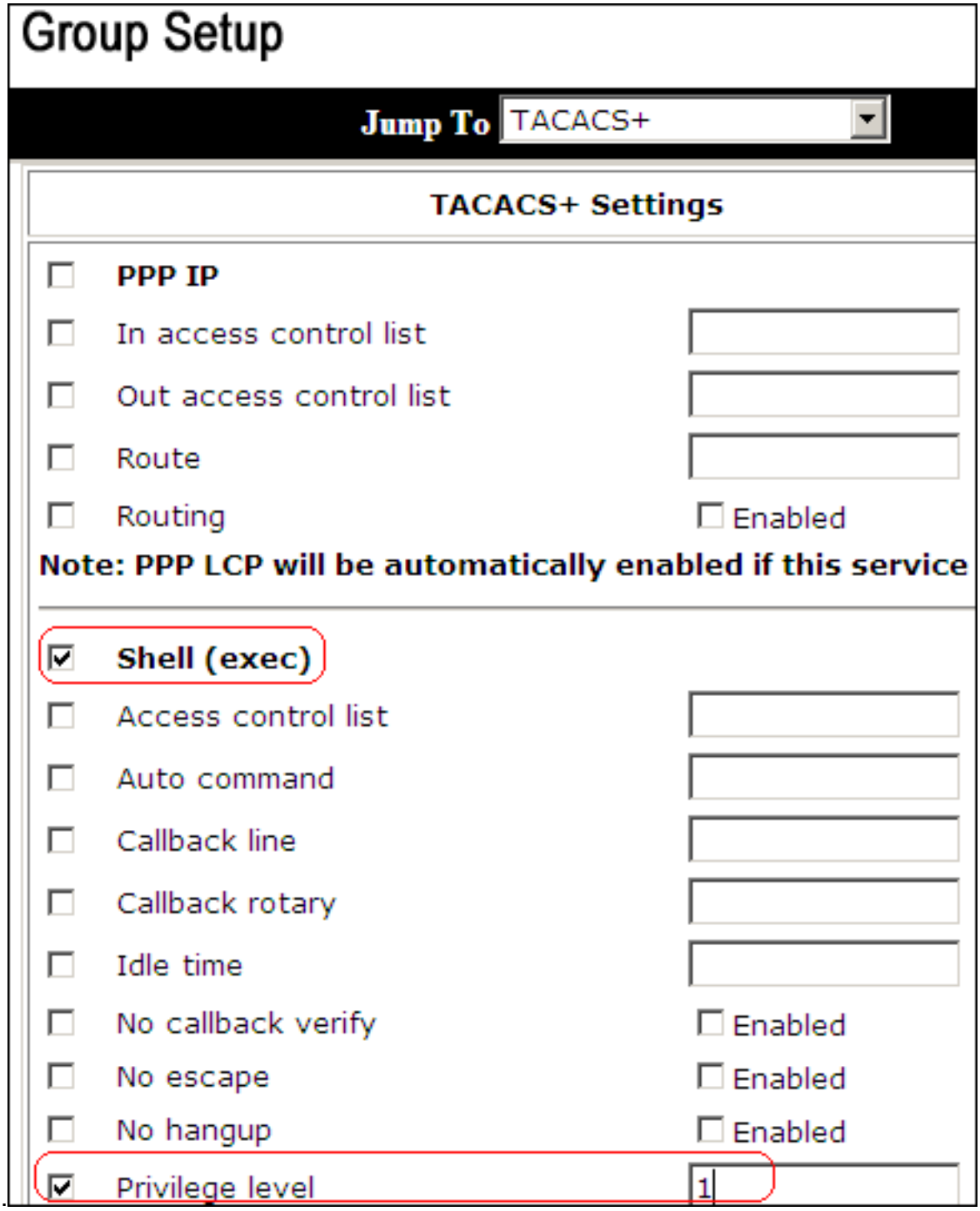


2. Cliquez sur Edit les **configurations**.
3. De l'accès à la liste déroulante, choisissez Enable les **options**.
4. Dans la région d'options d'enable, cliquez sur le **privilège maximum pour n'importe quel** bouton de **transmetteur client d'AAA**, et choisissez le **niveau 1 de la** liste déroulante.



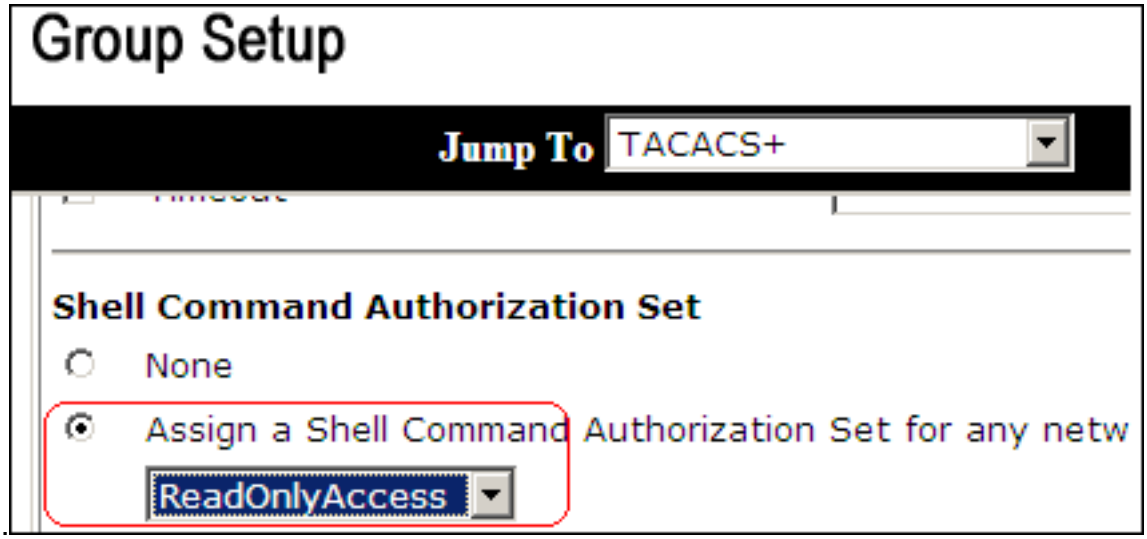
5. Dans la région de configurations TACACS+, cochez la case de **shell (exécutif)**, cochez la case de **niveau de privilège**, et écrivez **1** dans le domaine de niveau de

privilège.



6. Dans la région réglée d'autorisation de commande shell, cliquez sur l'**assigner une autorisation de commande shell réglée pour n'importe quelle** case d'option de **périphérique de réseau**, et choisissez **ReadOnlyAccess de la** liste

déroulante.



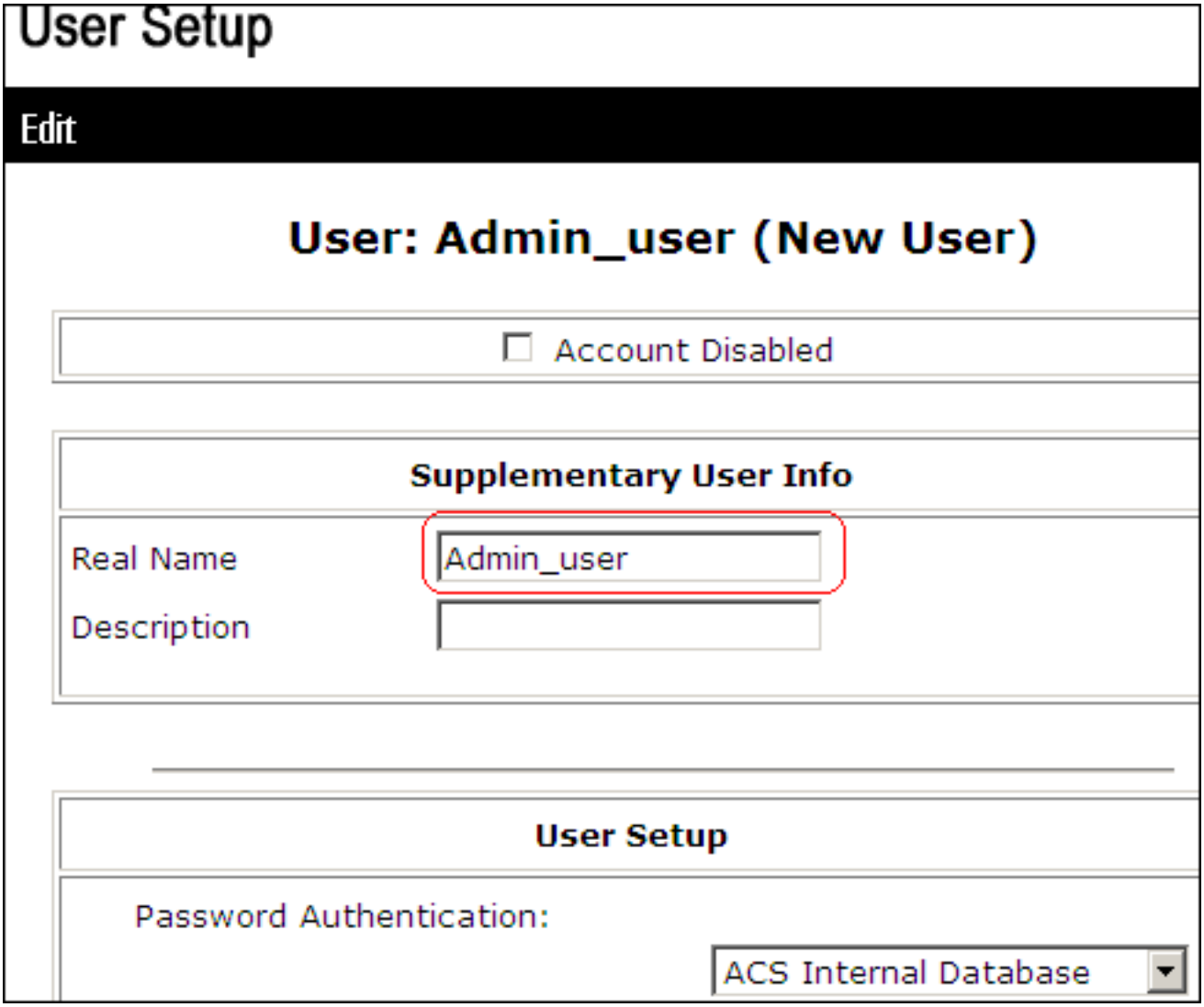
7. Cliquez sur Submit

Associez l'autorisation de commande shell réglée (Restrict_access) à l'utilisateur

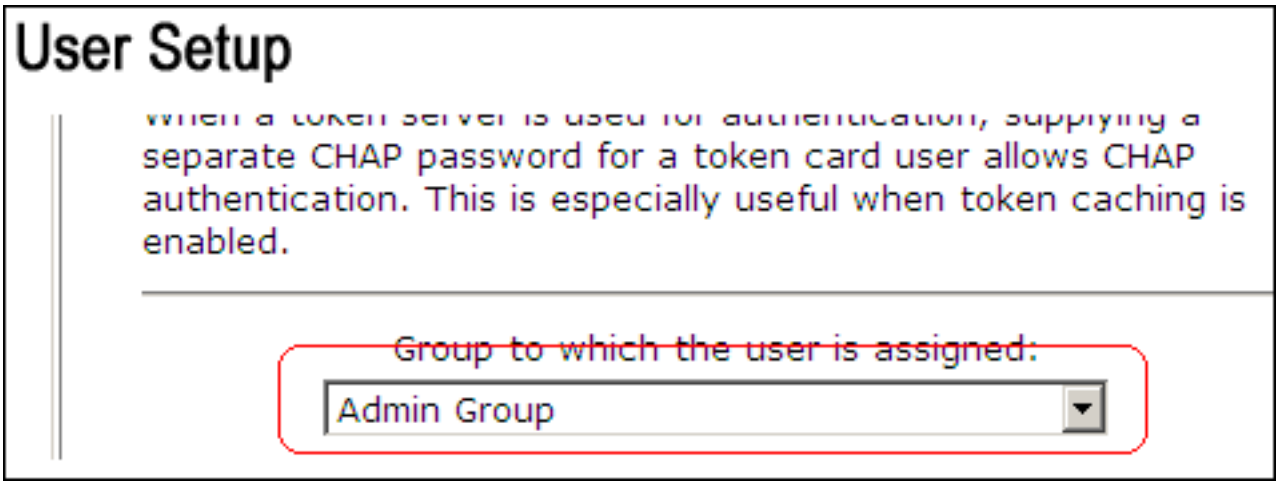
Référez-vous à configurer un positionnement d'autorisation de commande shell pour une section d'utilisateur du guide utilisateur pour le Cisco Secure Access Control Server 4.1 pour plus d'informations sur la façon configurer la configuration réglée d'autorisation de commande shell pour des utilisateurs.

Remarque: Les configurations de niveau utilisateur ignorent des configurations de niveau du groupe dans ACS, qui signifie si l'utilisateur fait placer l'autorisation de commande shell dans les configurations de niveau utilisateur, alors elle ignore les configurations de niveau du groupe.

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



2. Du groupe auquel l'utilisateur est assigné la liste déroulante, choisissez le **groupe d'admin**.



3. Dans la région réglée d'autorisation de commande shell, cliquez sur l'**assigner une autorisation de commande shell réglée pour n'importe quelle** case d'option de **périphérique de réseau**, et choisissez **Restrict_access de la** liste déroulante.**Remarque:** Dans ce scénario, cet utilisateur fait partie de groupe d'admin. Le positionnement d'autorisation de shell de *Restrict_access* s'applique ; le positionnement *lecture/écriture d'*autorisation de shell d'*Access* s'applique pas

applicable. **Remarque:** D ans la section TACACS+ (Cisco) du secteur de configuration d'interface, assurez-vous que l'option de **shell (exécutif)** est sélectionnée dans la colonne d'utilisateur.

Configuration de routeur IOS

En plus de votre configuration de présélection, ces commandes sont exigées sur un routeur ou le commutateur IOS afin d'implémenter l'autorisation de commande par 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

En plus de votre configuration de présélection, ces commandes sont exigées sur ASA/PIX/FWSM afin d'implémenter l'autorisation de commande par 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'employer le protocole RADIUS afin de limiter l'accès client à l'ASDM pour les buts en lecture seule. Puisque les paquets RADIUS contiennent l'authentification et l'autorisation en même temps, tous les utilisateurs qui sont authentifiés dans le serveur de

RAYON ont un niveau de privilège de 15. Vous pouvez réaliser ceci par TACACS avec l'implémentation des positionnements d'autorisation de commande.

Remarque: ASA/PIX/FWSM prennent un longtemps d'exécuter chaque commande tapée même si ACS est indisponible pour exécuter l'autorisation de commande. Si ACS est indisponible et l'ASA a l'autorisation de commande configurée, l'ASA demandera toujours l'autorisation de commande pour chaque commande.

Dépannez

Erreur : l'autorisation de commande a manqué

Problème

Après que vous ouvriez une session au Pare-feu par TACACS se connectant, les commandes ne fonctionnent pas. Quand vous sélectionnez une commande, cette erreur est reçue : `l'autorisation de commande a manqué`.

Solution

Procédez comme suit pour résoudre ce problème :

1. Assurez que le nom d'utilisateur correct est utilisé et que tous les privilèges exigés sont assignés à l'utilisateur.
2. Si le nom d'utilisateur et les privilèges sont corrects, vérifiez que l'ASA a la Connectivité avec l'ACS et que l'ACS est en activité.

Remarque: Cette erreur peut également se produire si l'administrateur configurait de manière erronée l'autorisation de commande pour des gens du pays, aussi bien que TACACS, des utilisateurs. Dans ce cas, exécutez une reprise 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 de support Cisco Secure de serveur de contrôle d'accès de contrôle
- Support et documentation techniques - Cisco Systems