Verrou et clé : Listes d'accès dynamique

Contenu

Introduction

L'accès de verrou vous permet d'installer les listes d'accès dynamique qui accordent l'accès par utilisateur à une source/hôte de destination spécifique par un processus d'authentification de l'utilisateur. L'accès utilisateur est autorisé par le biais d'un pare-feu Cisco IOS® dynamiquement, sans aucun compromis dans les restrictions de sécurité.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Dans ce cas, l'environnement des travaux pratiques était constitué d'un routeur 2620 exécutant le logiciel Cisco IOS® Version 12.3(1). 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.

Considérations relatives à l'usurpation

L'accès par clé et verrouillage permet à un événement externe de placer une ouverture dans le pare-feu Cisco IOS Firewall. Après cette ouverture, le routeur est susceptible d'usurpation d'adresse source. Afin d'empêcher cela, fournir la prise en charge du chiffrement à l'aide du chiffrement IP avec authentification ou chiffrement.

L'usurpation d'adresse est un problème avec toutes les listes d'accès existantes. L'accès par verrouillage de clé ne résout pas ce problème.

Comme l'accès par clé et verrouillage introduit un chemin potentiel via votre pare-feu réseau, vous devez considérer l'accès dynamique. Un autre hôte, usurpant votre adresse authentifiée, obtient l'accès derrière le pare-feu. Avec l'accès dynamique, il est possible qu'un hôte non autorisé, usurpant votre adresse authentifiée, obtienne l'accès derrière le pare-feu. L'accès par verrouillage de clé ne cause pas de problème d'usurpation d'adresse. Le problème n'est identifié ici qu'en tant que préoccupation pour l'utilisateur.

Performances

Les performances sont affectées dans ces deux situations.

- Chaque liste d'accès dynamique force la reconstruction d'une liste d'accès sur le moteur de commutation de silicium (SSE). Cela entraîne un ralentissement momentané du chemin de commutation SSE.
- Les listes d'accès dynamiques nécessitent la fonction de délai d'inactivité (même si le délai d'attente est laissé à la valeur par défaut). Par conséquent, les listes d'accès dynamiques ne peuvent pas être commutées SSE. Ces entrées sont traitées dans le chemin de commutation rapide du protocole.

Observez les configurations des routeurs périphériques. Les utilisateurs distants créent des entrées de liste d'accès sur le routeur périphérique. La liste de contrôle d'accès se développe et se réduit dynamiquement. Les entrées sont supprimées dynamiquement de la liste après l'expiration du délai d'inactivité ou du délai maximal. Les grandes listes d'accès dégradent les performances de commutation de paquets.

Quand utiliser l'accès par clé et verrouillage

Voici deux exemples d'utilisation de l'accès par verrouillage et clé :

- Lorsque vous souhaitez qu'un hôte distant puisse accéder à un hôte de votre interréseau via Internet. L'accès par clé et verrouillage limite l'accès au-delà de votre pare-feu sur un hôte ou un réseau individuel.
- Lorsque vous souhaitez qu'un sous-ensemble d'hôtes d'un réseau accède à un hôte d'un réseau distant protégé par un pare-feu. Avec l'accès par clé et verrou, vous pouvez

uniquement activer un ensemble d'hôtes désiré pour obtenir l'accès en les faisant authentifier via un serveur TACACS+ ou RADIUS.

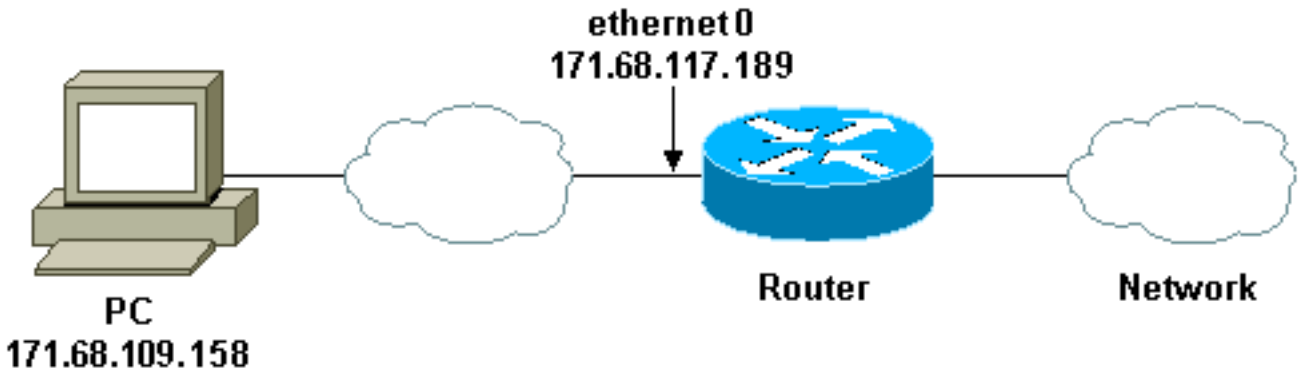
Fonctionnement de l'accès par clé et verrouillage

Ce processus décrit l'opération d'accès par clé et verrou.

1. Un utilisateur ouvre une session Telnet à un routeur périphérique configuré pour l'accès par verrouillage et clé.
2. Le logiciel Cisco IOS reçoit le paquet Telnet. Il effectue un processus d'authentification des utilisateurs. L'utilisateur doit passer l'authentification avant d'autoriser l'accès. Le processus d'authentification est effectué par le routeur ou un serveur d'accès central tel qu'un serveur TACACS+ ou RADIUS.

Exemple de configuration et de dépannage

Diagramme du réseau



Cisco vous recommande d'utiliser un serveur TACACS+ pour votre processus de requête d'authentification. TACACS+ fournit des services d'authentification, d'autorisation et de comptabilité. Il fournit également la prise en charge des protocoles, la spécification des protocoles et une base de données de sécurité centralisée.

Vous pouvez authentifier l'utilisateur sur le routeur ou avec un serveur TACACS+ ou RADIUS.

Remarque : ces commandes sont globales sauf indication contraire.

Sur le routeur, vous avez besoin d'un **nom d'utilisateur** pour l'authentification locale de l'utilisateur.

```
username test password test
```

La présence de **login local** sur les lignes vty entraîne l'utilisation de ce nom d'utilisateur.

```
line vty 0 4
login local
```

Si vous ne faites pas confiance à l'utilisateur pour émettre la commande **access-enable**, vous pouvez effectuer l'une des deux opérations suivantes :

- Associez le délai d'attente à l'utilisateur par utilisateur.

```
username test autocommand access-enable host
timeout 10
```

ou

- Forcer tous les utilisateurs de Telnet à avoir le même délai d'attente.

```
line vty 0 4
login local
autocommand access-enable host timeout 10
```

Remarque : Le **10** de la syntaxe correspond au délai d'*inactivité* de la liste d'accès. Il est remplacé par le délai d'attente absolu dans la liste d'accès dynamique.

Définissez une liste d'accès étendue qui est appliquée lorsqu'un utilisateur (n'importe quel utilisateur) se connecte au routeur et que la commande **access-enable** est exécutée. La durée maximale absolue de ce trou dans le filtre est de 15 minutes. Au bout de 15 minutes, le trou se ferme, que quelqu'un l'utilise ou non. La **liste de tests** de noms doit exister mais n'est pas significative. Limitez les réseaux auxquels l'utilisateur a accès en configurant l'adresse source ou de destination (ici, l'utilisateur n'est pas limité).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

Définissez la liste de contrôle d'accès nécessaire pour bloquer tout le réseau, à l'exception de la possibilité d'établir une connexion Telnet avec le routeur (pour ouvrir un trou, l'utilisateur doit établir une connexion Telnet avec le routeur). L'adresse IP ici correspond à l'adresse IP Ethernet du routeur.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

Il y a un **refus** implicite à la fin (non entré ici).

Appliquez cette liste d'accès à l'interface sur laquelle les utilisateurs entrent.

```
interface ethernet1
       ip access-group 120 in
```

Tu as fini.

Voici à quoi ressemble le filtre sur le routeur en ce moment :

```
Router#show access-lists
Extended IP access list 120
```

```
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Les utilisateurs qui accèdent à votre réseau interne ne peuvent rien voir tant qu'ils n'ont pas établi une connexion Telnet avec le routeur.

Remarque : Le **10** ici correspond au délai d'*inactivité* de la liste d'accès. Il est remplacé par le délai d'attente absolu dans la liste d'accès dynamique.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

Le filtre ressemble à ceci.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Il y a un trou dans le filtre pour cet utilisateur en fonction de l'adresse IP source. Quand quelqu'un d'autre fait ça, vous voyez *deux trous*.

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Ces utilisateurs peuvent avoir un accès IP complet à toute adresse IP de destination à partir de leur adresse IP *source*.

Utilisation de TACACS+

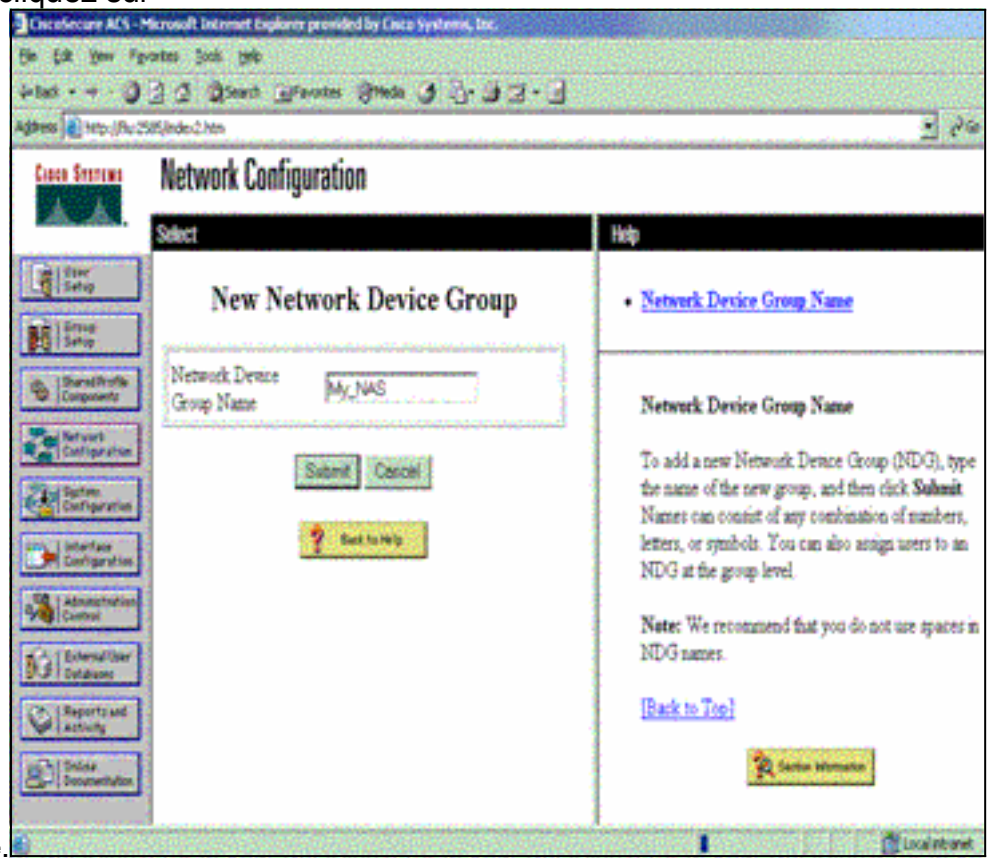
Configurer TACACS+

Configurez un serveur TACACS+ pour forcer l'authentification et l'autorisation sur le serveur TACACS+ afin d'utiliser TACACS+, comme le montre ce résultat :

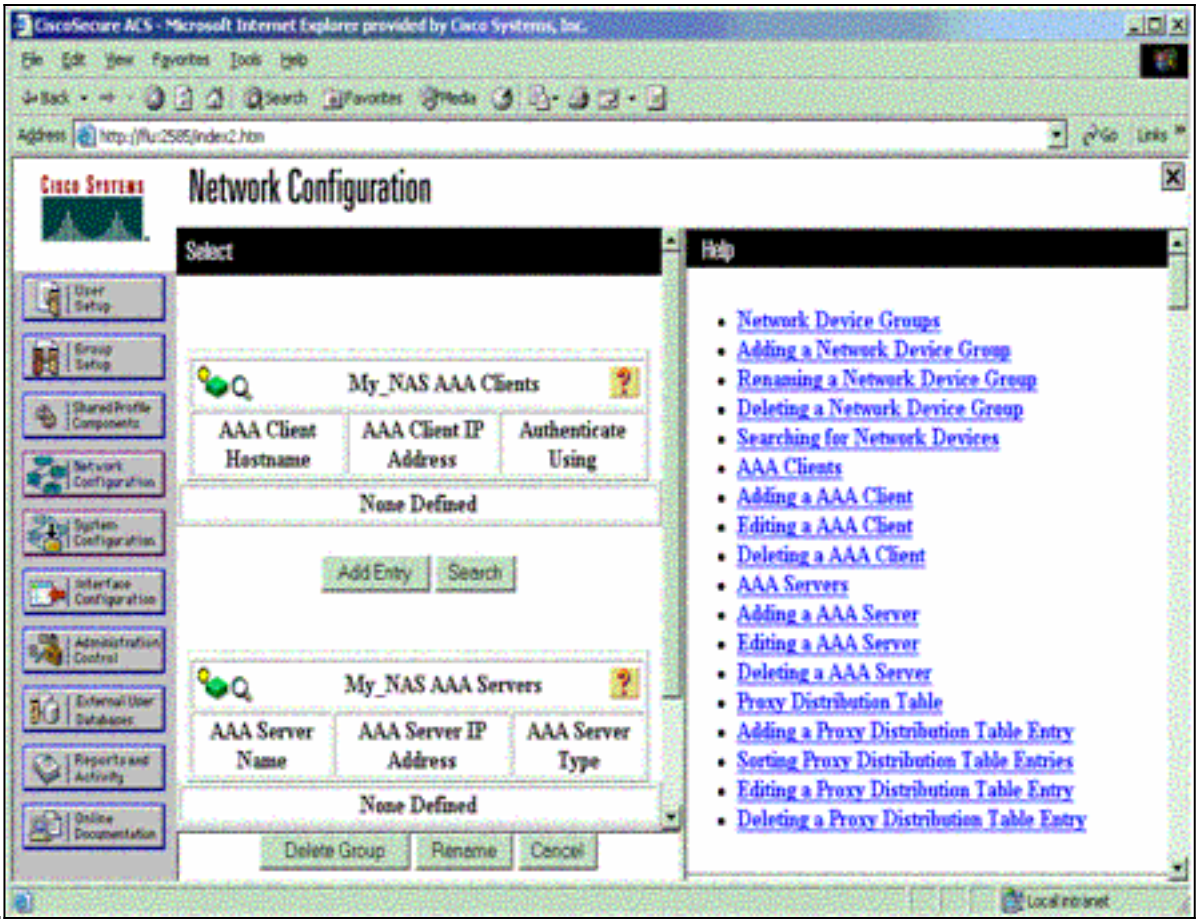
```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

Complétez ces étapes pour configurer TACACS+ sur Cisco Secure ACS pour Windows :

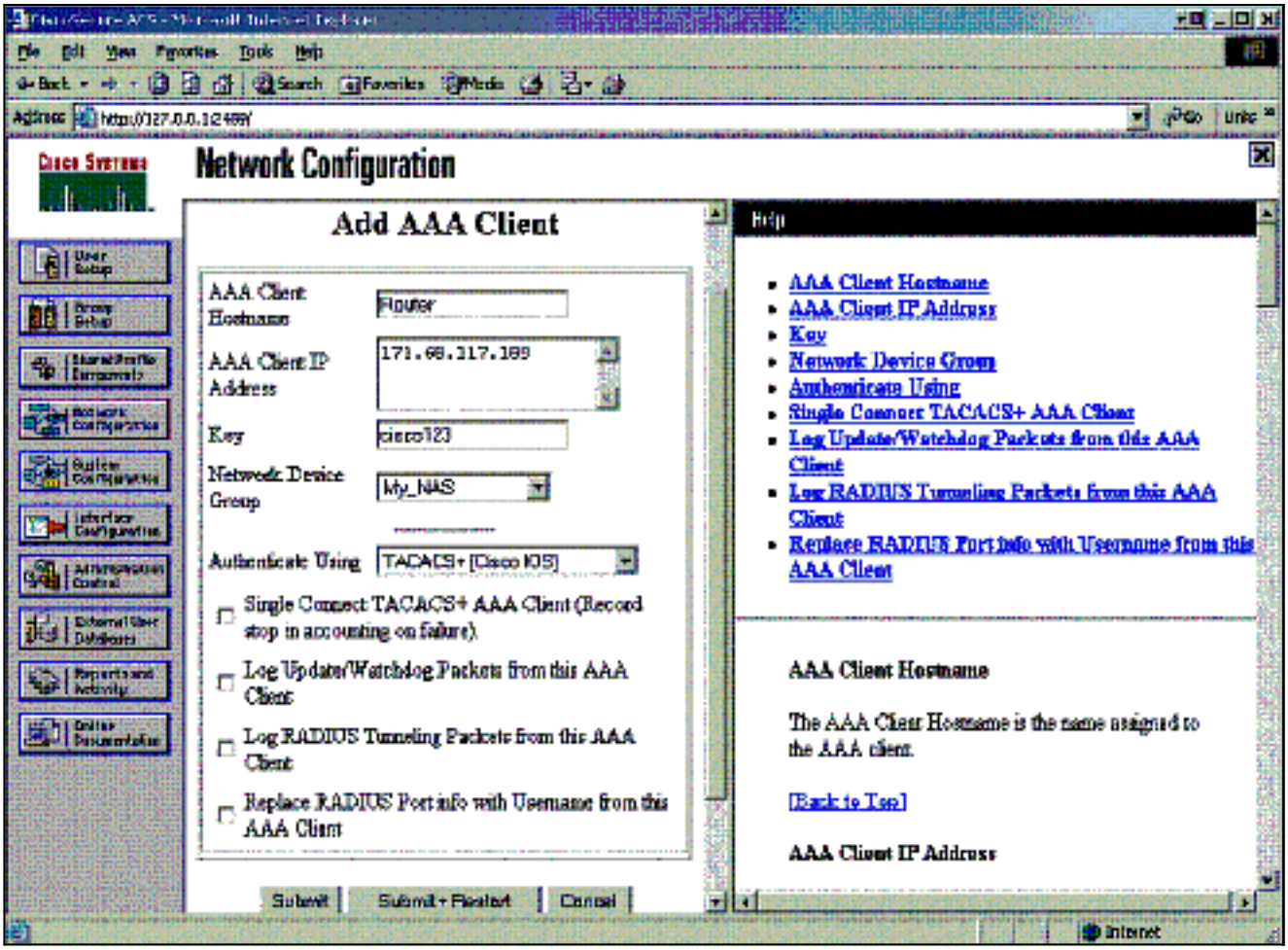
1. Ouvrez un navigateur Web. Entrez l'adresse de votre serveur ACS, sous la forme de **http://*<adresse_IP ou nom_DNS>*:2002**. (Cet exemple utilise un port par défaut de 2002.) Connectez-vous en tant qu'administrateur.
2. Cliquez sur **Configuration du réseau**. Cliquez sur **Ajouter une entrée** pour créer un groupe de périphériques réseau contenant les serveurs d'accès réseau (NAS). Entrez un nom pour le groupe et cliquez sur **Soumettre**.



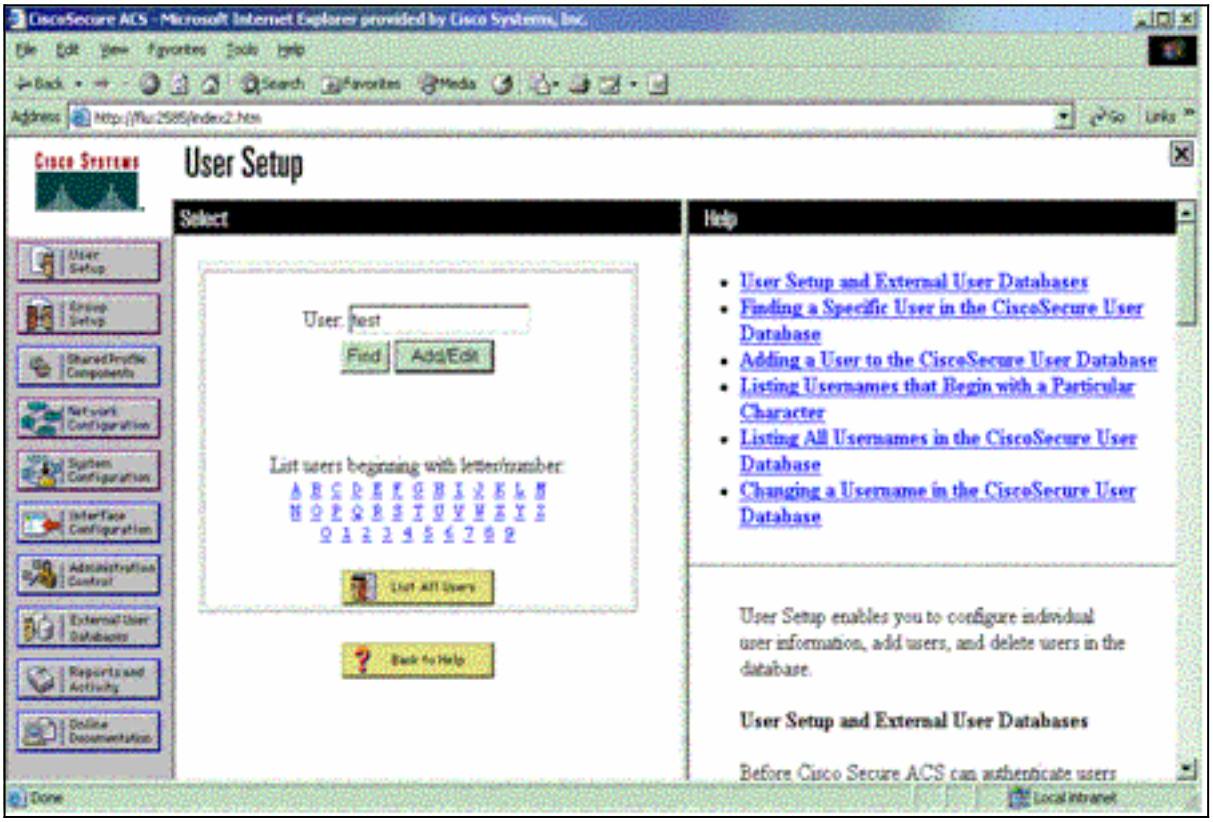
3. Cliquez sur **Ajouter une entrée** pour ajouter un client AAA (Authentication, Authorization and Accounting)

(NAS). 

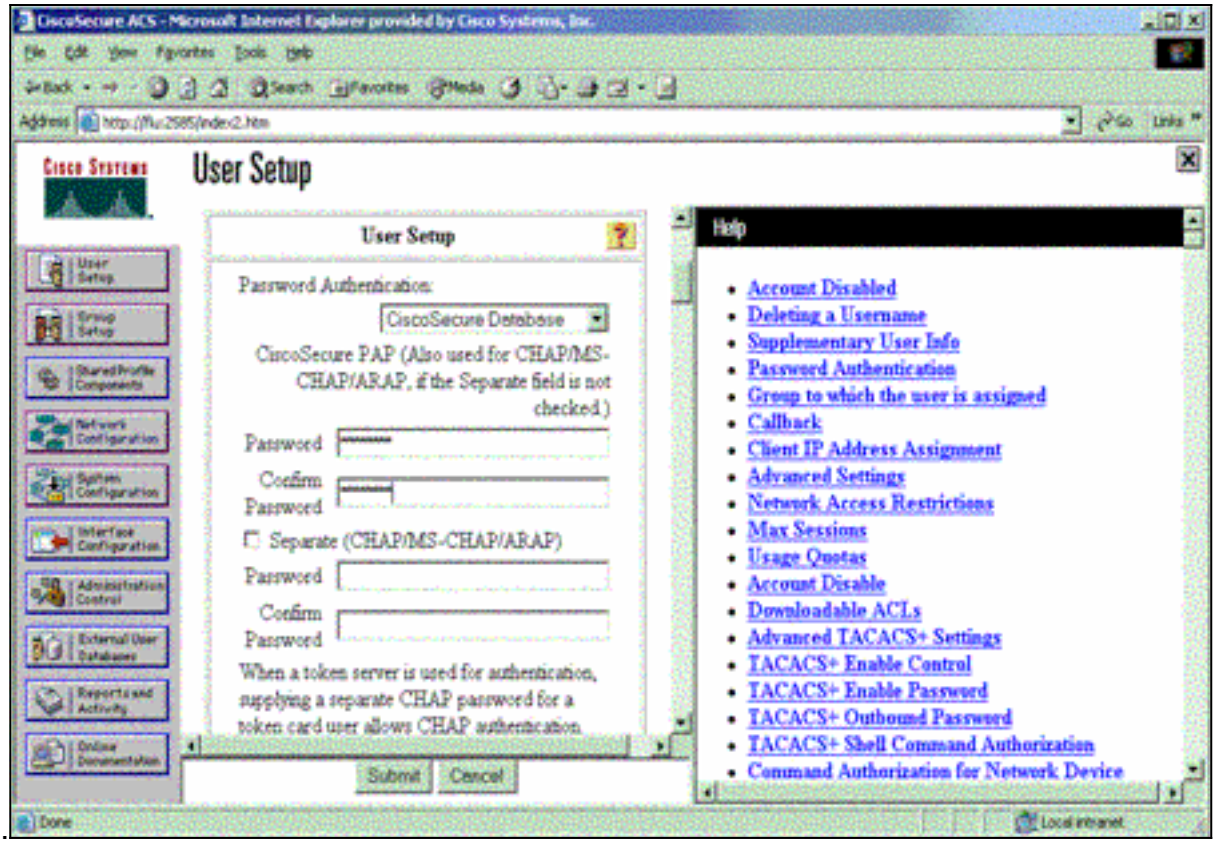
4. Saisissez le nom d'hôte, l'adresse IP et la clé utilisée pour chiffrer la communication entre le serveur AAA et le serveur NAS. Sélectionnez **TACACS+ (Cisco IOS)** comme méthode d'authentification. Lorsque vous avez terminé, cliquez sur **Soumettre +Redémarrer** pour appliquer les
modifications.



5. Cliquez sur **User Setup**, saisissez un ID utilisateur, puis cliquez sur **Add/Edit**.

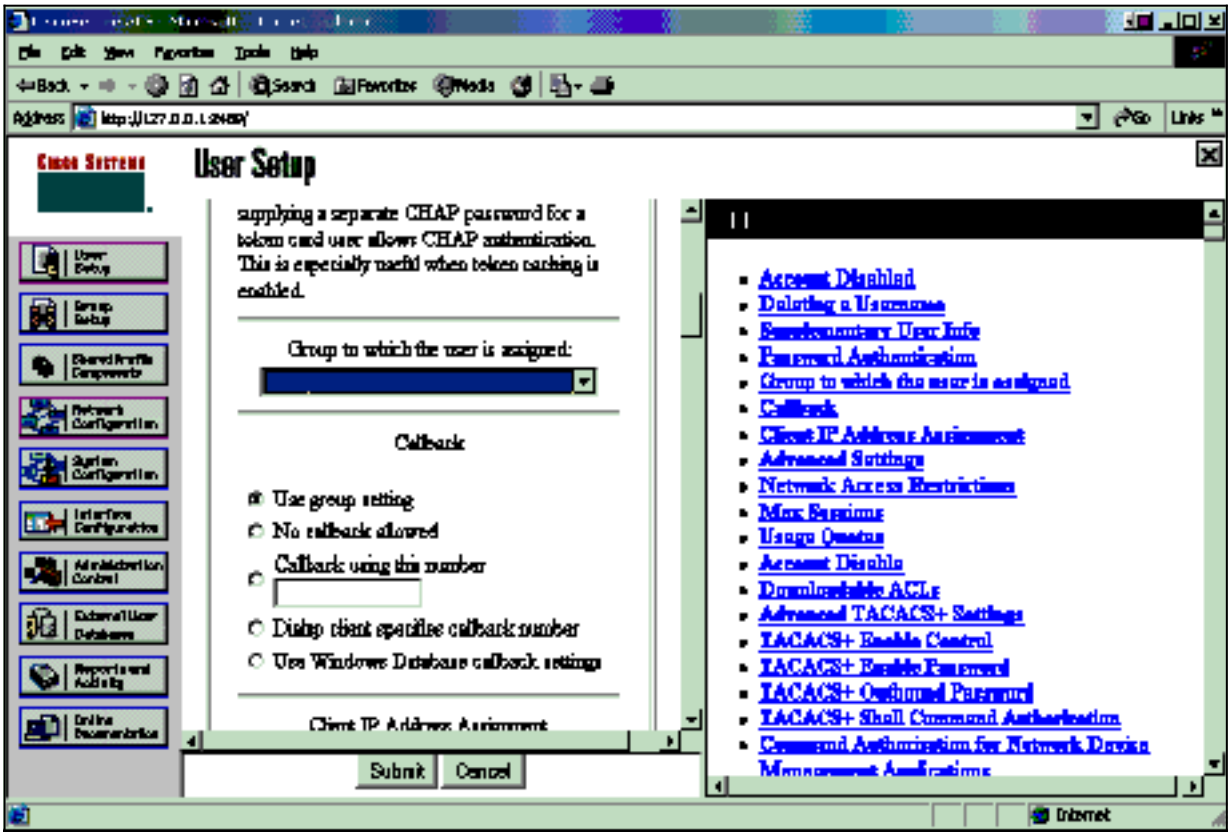


6. Sélectionnez une base de données pour authentifier l'utilisateur. (Dans cet exemple, l'utilisateur est « test » et la base de données interne de l'ACS est utilisée pour l'authentification). Entrez un mot de passe pour l'utilisateur et confirmez-

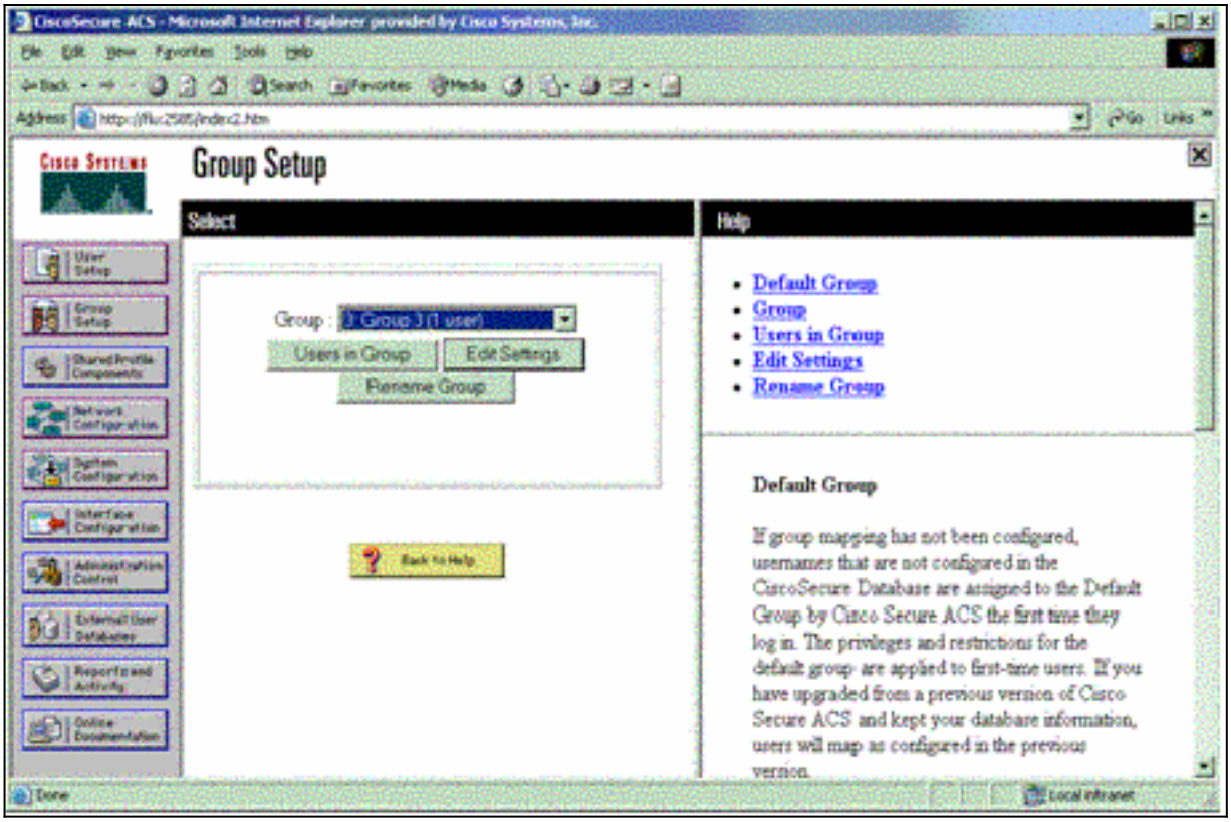


le.

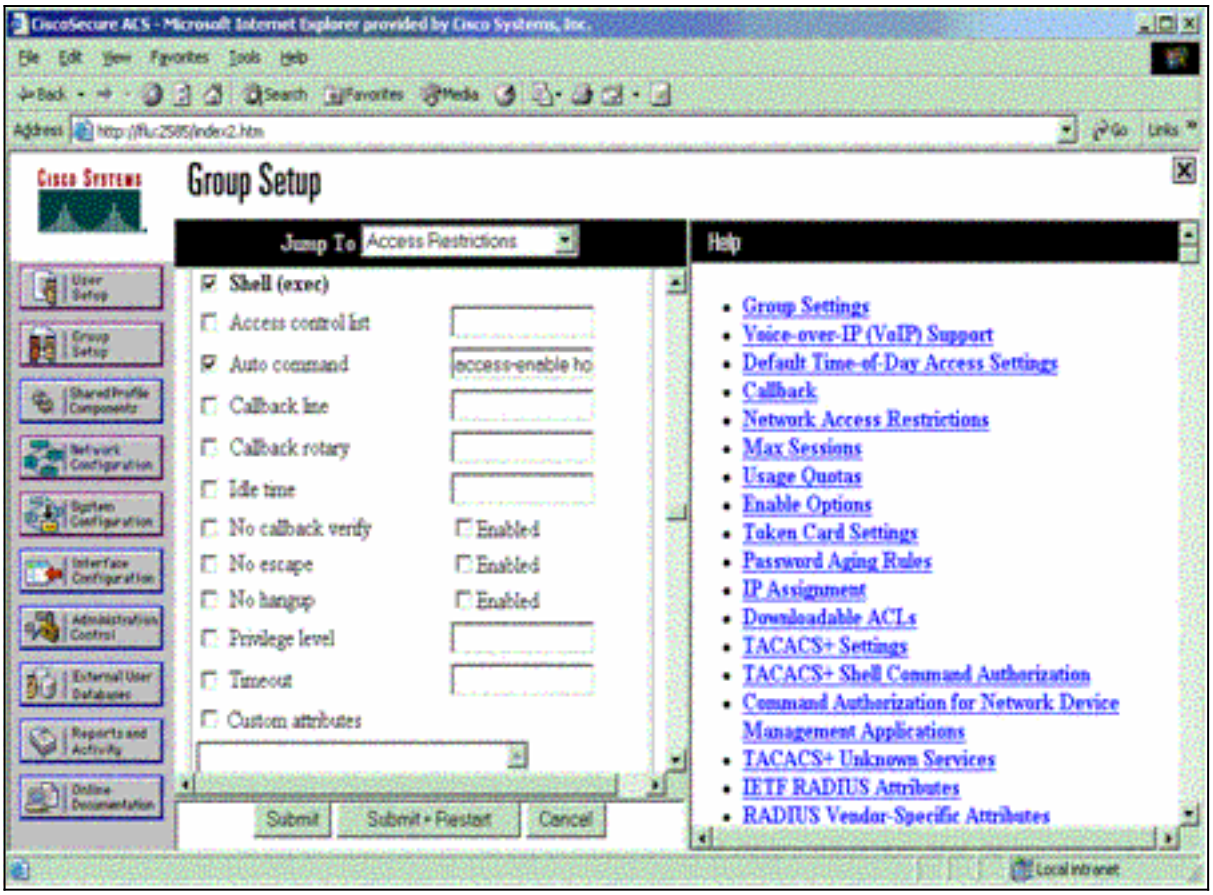
7. Choisissez le groupe auquel l'utilisateur est affecté et cochez la case **Utiliser le groupe**. Cliquez sur
Submit.



8. Cliquez sur **Configuration du groupe**. Sélectionnez le groupe auquel l'utilisateur a été affecté à l'étape 7. Cliquez sur **Modifier les paramètres**.



9. Faites défiler jusqu'à la section TACACS+ Settings. Cochez la case pour **Shell exec**. Cochez la case de la **commande Auto**. Entrez la commande auto à exécuter après autorisation de l'utilisateur. (Cet exemple utilise la commande **access-enable host timeout 10**.) Cliquez sur **Soumettre+Redémarrer**.



Dépannage de TACACS+

Utilisez ces commandes **debug** sur le NAS pour résoudre les problèmes TACACS+.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug tacacs authentication** - Affiche des informations sur le processus d'authentification TACACS+. Uniquement disponible dans certaines versions de logiciel. Si non disponible, utilisez **debug tacacs** uniquement.
- **debug tacacs autorisation** - Affiche des informations sur le processus d'autorisation TACACS+. Uniquement disponible dans certaines versions de logiciel. Si non disponible, utilisez **debug tacacs** uniquement.
- **debug tacacs events** : affiche les informations du processus d'assistance TACACS+. Uniquement disponible dans certaines versions de logiciel. Si non disponible, utilisez **debug tacacs** uniquement.

Utilisez ces commandes pour résoudre les problèmes AAA :

- **debug aaa authentication** - Affiche des informations sur l'authentification AAA/TACACS+.
- **debug aaa Authorization** : affiche des informations sur l'autorisation AAA/TACACS+.

L'exemple de sortie **de débogage** ici montre un processus d'authentification et d'autorisation réussi sur le serveur ACS TACACS+.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/8347F3FC: Processing the reply packet
```

```
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Utilisation de RADIUS

Configurer RADIUS

Afin d'utiliser RADIUS, configurez un serveur RADIUS pour forcer l'authentification à être effectuée sur le serveur RADIUS avec les paramètres d'autorisation (la commande automatique) à être envoyée dans l'attribut 26 spécifique au fournisseur, comme indiqué ici :

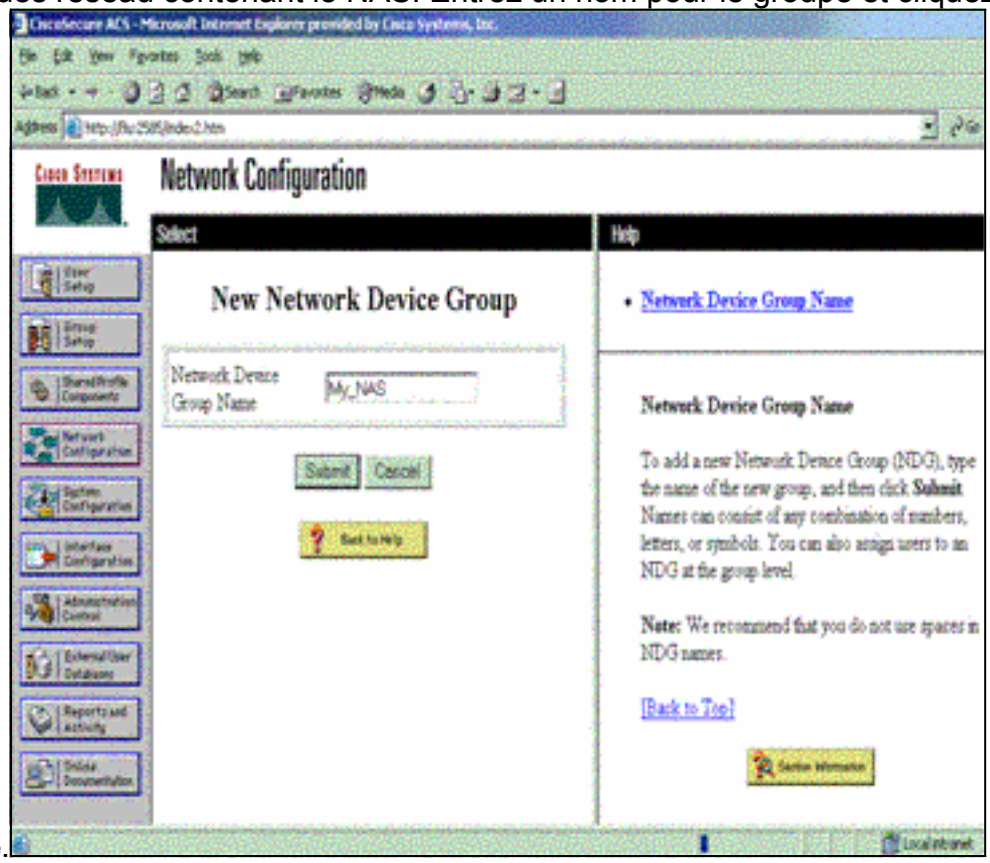
```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

Complétez ces étapes pour configurer RADIUS sur Cisco Secure ACS pour Windows :

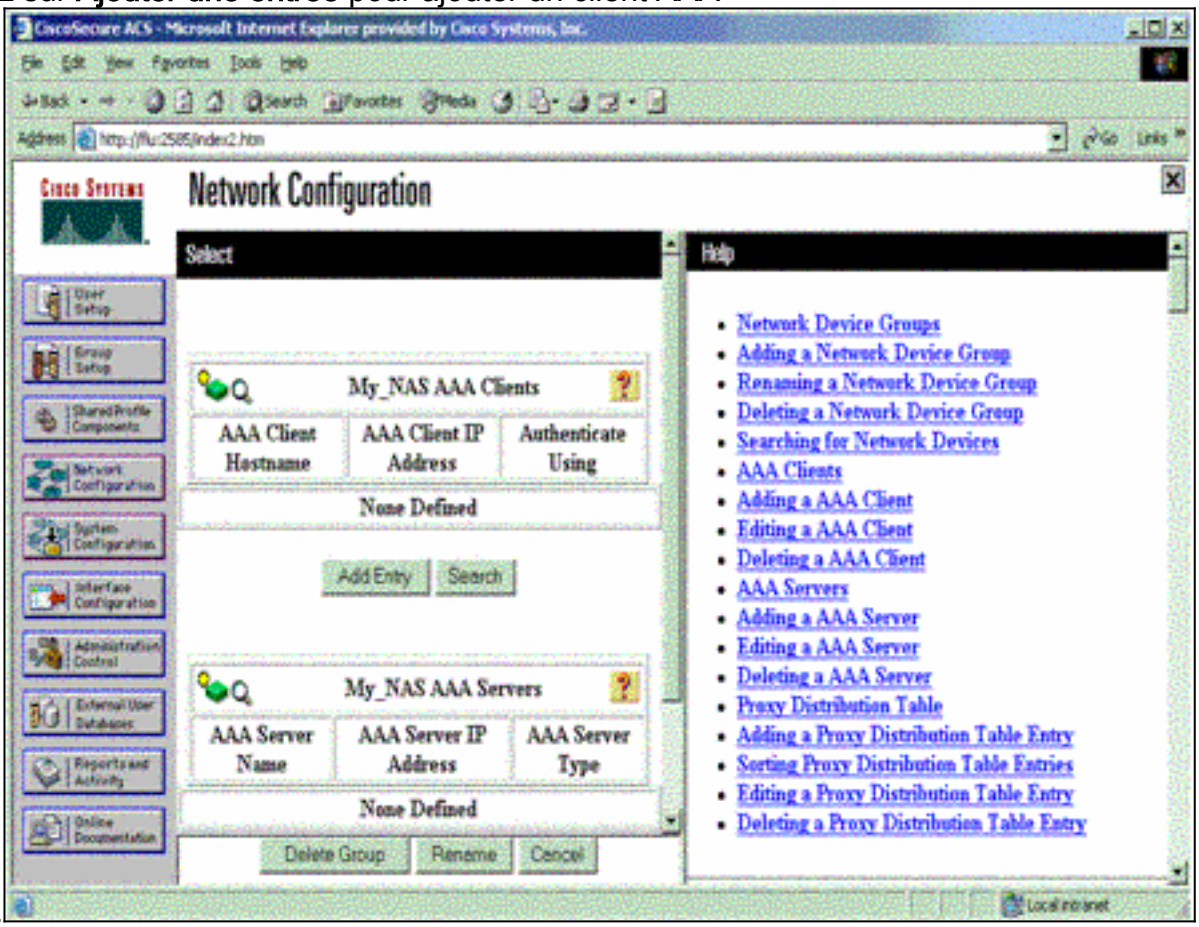
1. Ouvrez un navigateur Web et entrez l'adresse de votre serveur ACS, sous la forme de **http://*<adresse_IP ou nom_DNS>*:2002**. (Cet exemple utilise un port par défaut de 2002.)

Connectez-vous en tant qu'administrateur.

2. Cliquez sur **Configuration du réseau**. Cliquez sur **Ajouter une entrée** pour créer un groupe de périphériques réseau contenant le NAS. Entrez un nom pour le groupe et cliquez sur **Soumettre**.

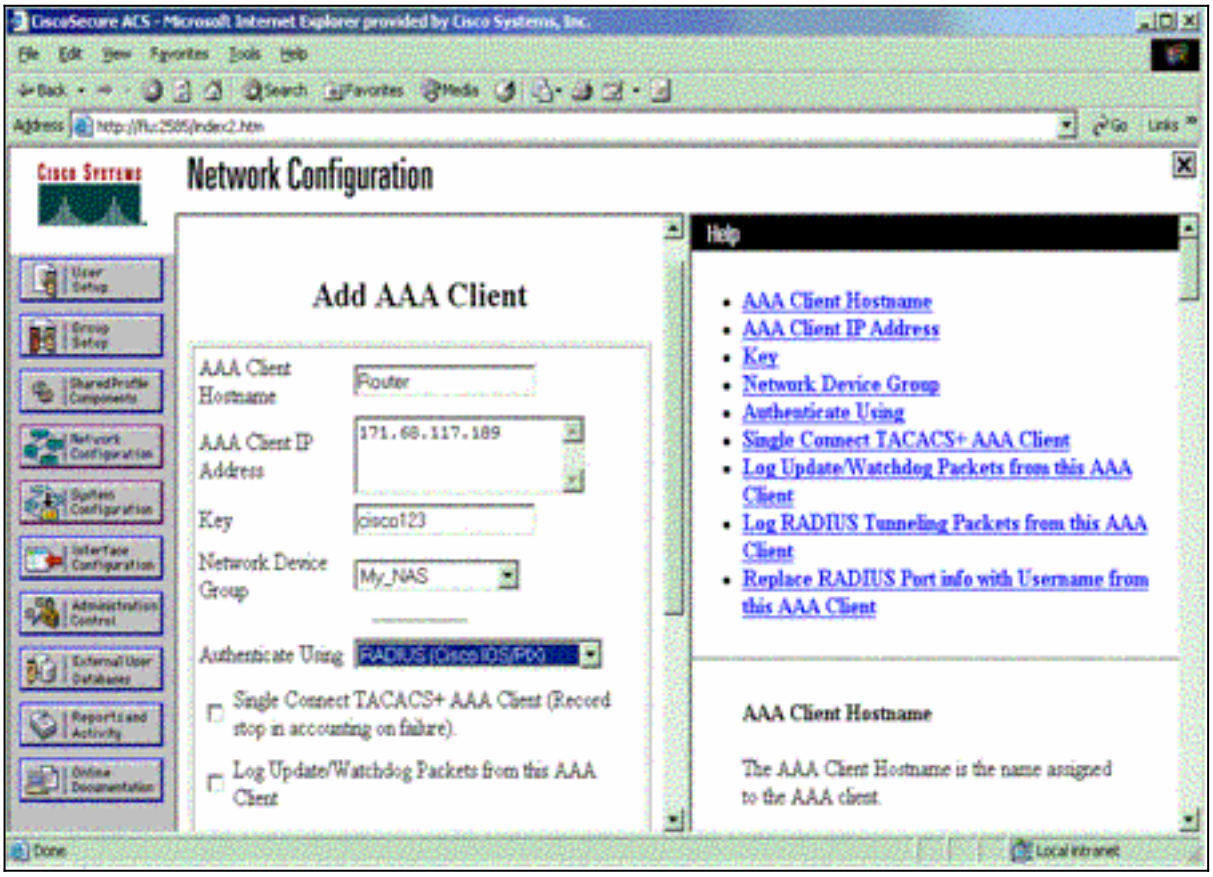


3. Cliquez sur **Ajouter une entrée** pour ajouter un client AAA (NAS).

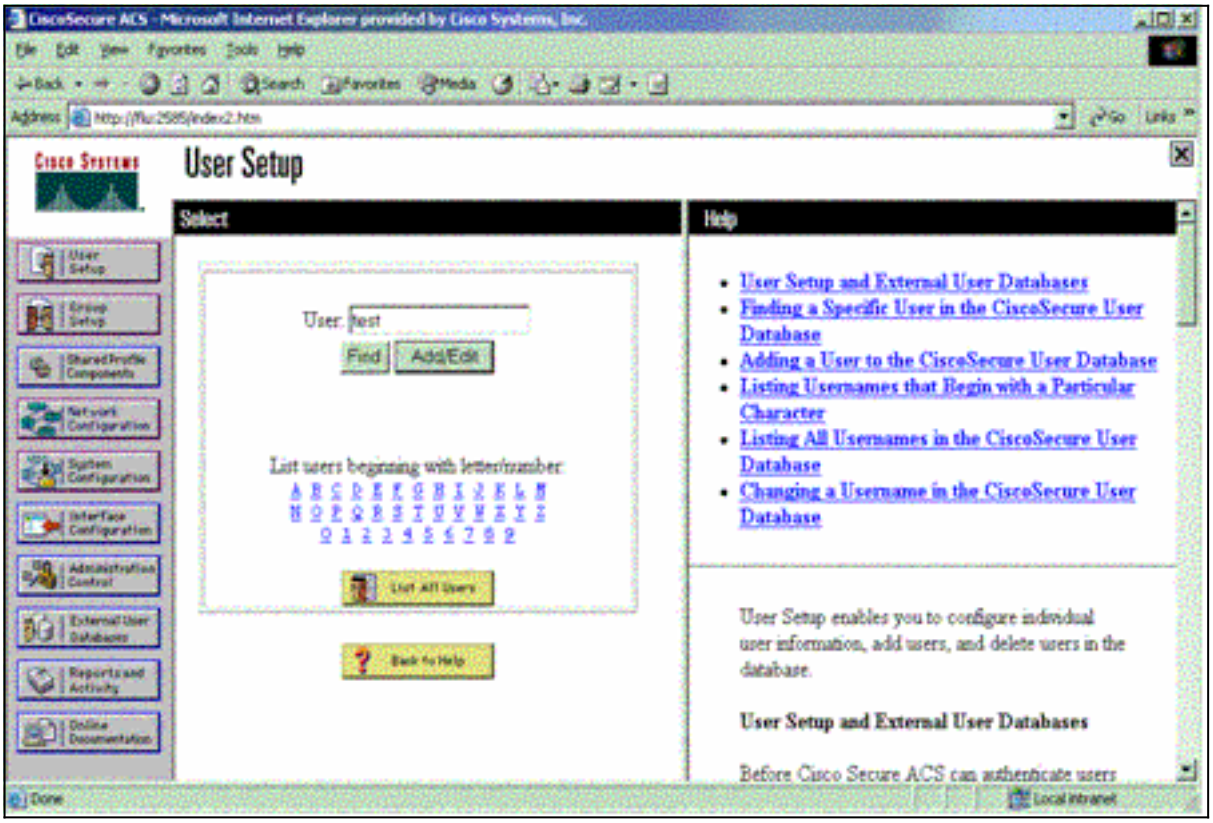


4. Saisissez le nom d'hôte, l'adresse IP et la clé utilisée pour chiffrer la communication entre le serveur AAA et le serveur NAS. Sélectionnez **RADIUS (Cisco IOS/PIX)** comme méthode

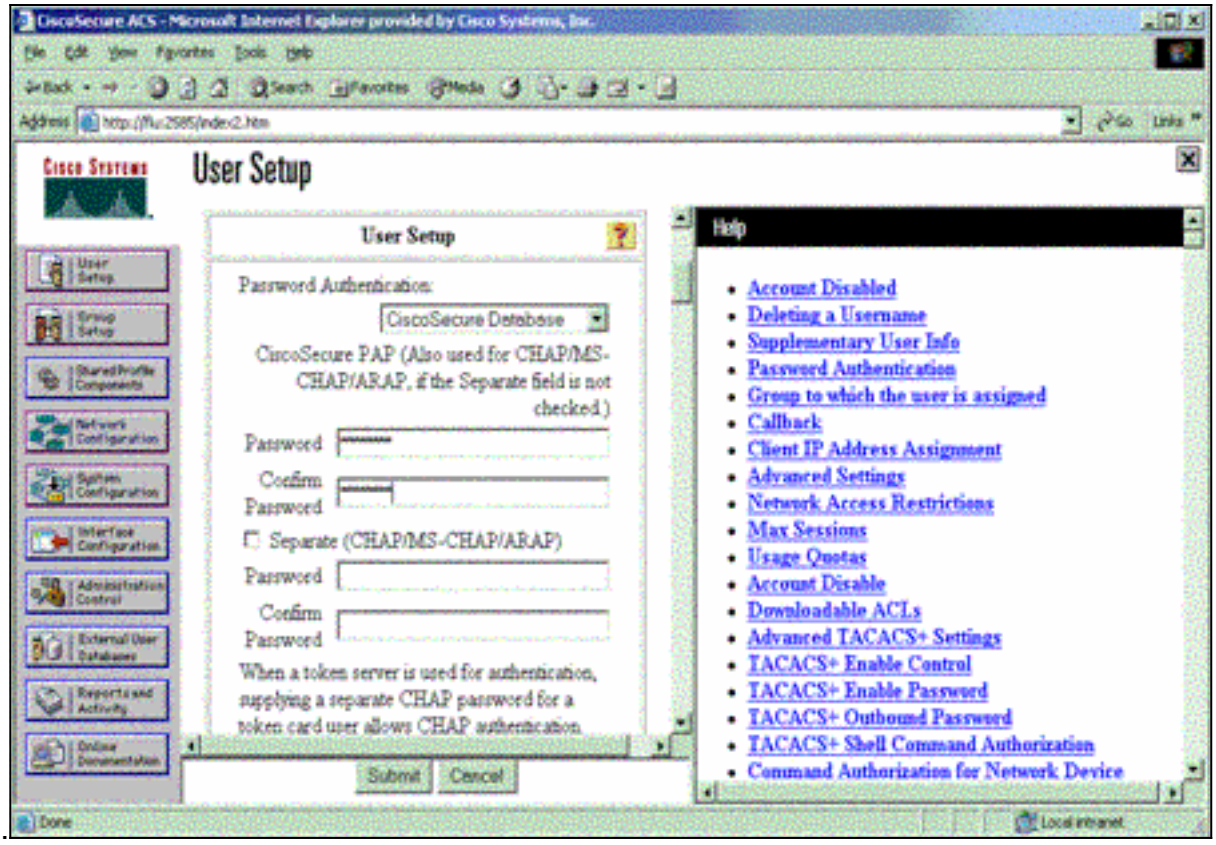
d'authentification. Lorsque vous avez terminé, cliquez sur **Soumettre +Redémarrer** pour appliquer les
modifications.



5. Cliquez sur **User Setup**, saisissez un ID utilisateur, puis cliquez sur **Add/Edit**.

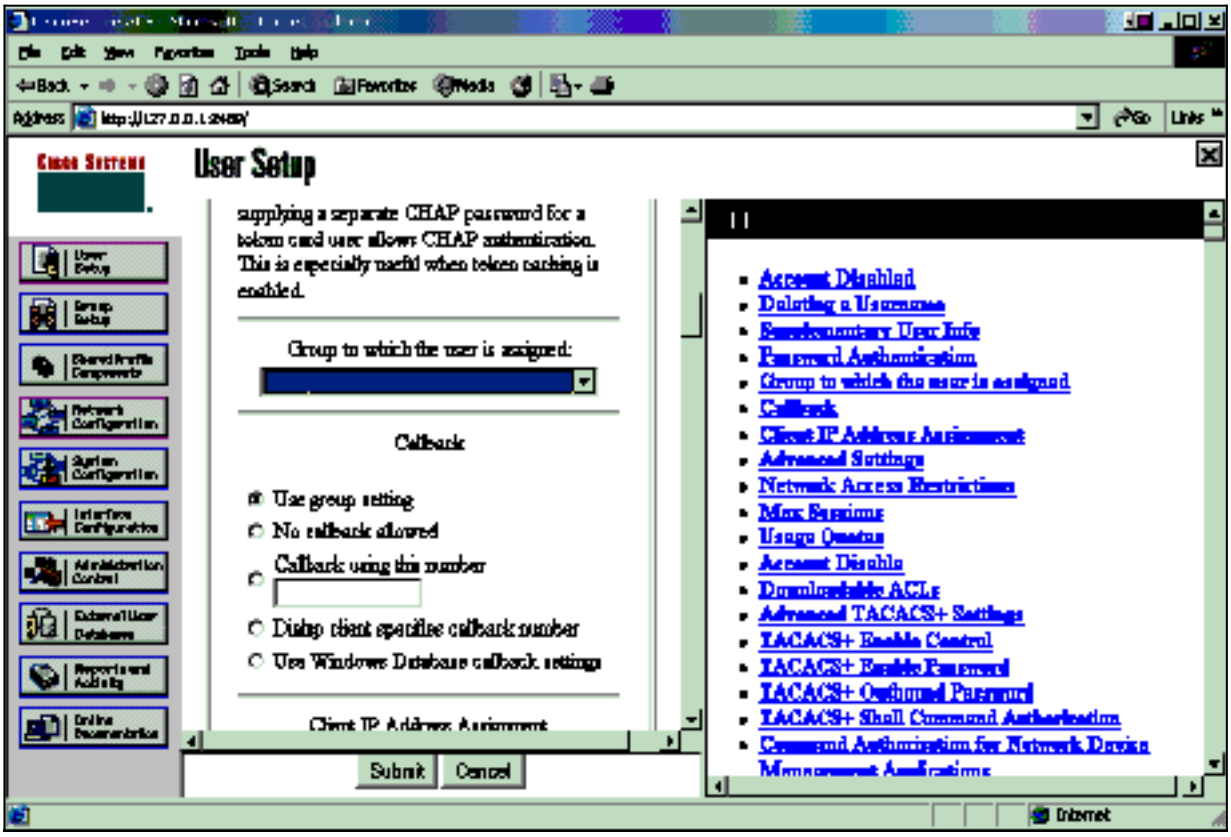


6. Sélectionnez une base de données pour authentifier l'utilisateur. (Dans cet exemple, l'utilisateur est « test » et la base de données interne de l'ACS est utilisée pour l'authentification). Entrez un mot de passe pour l'utilisateur et confirmez-

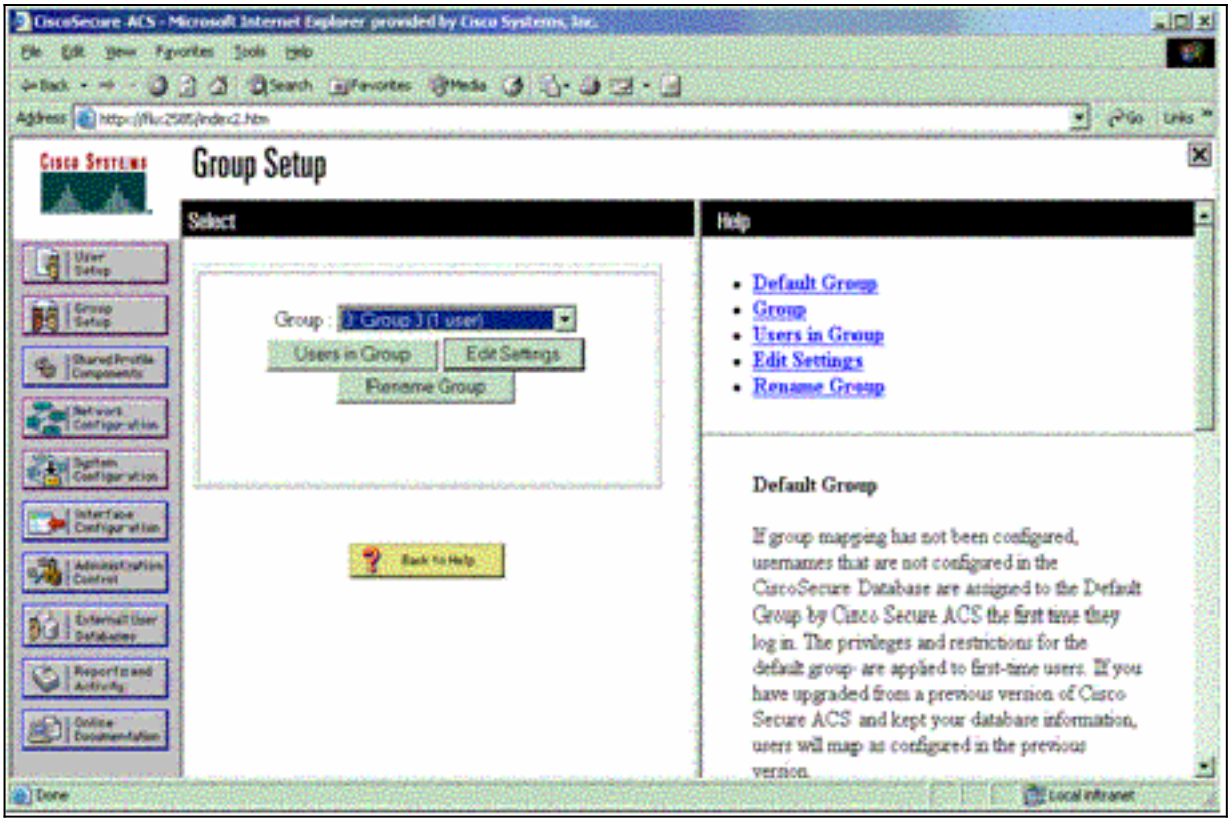


le.

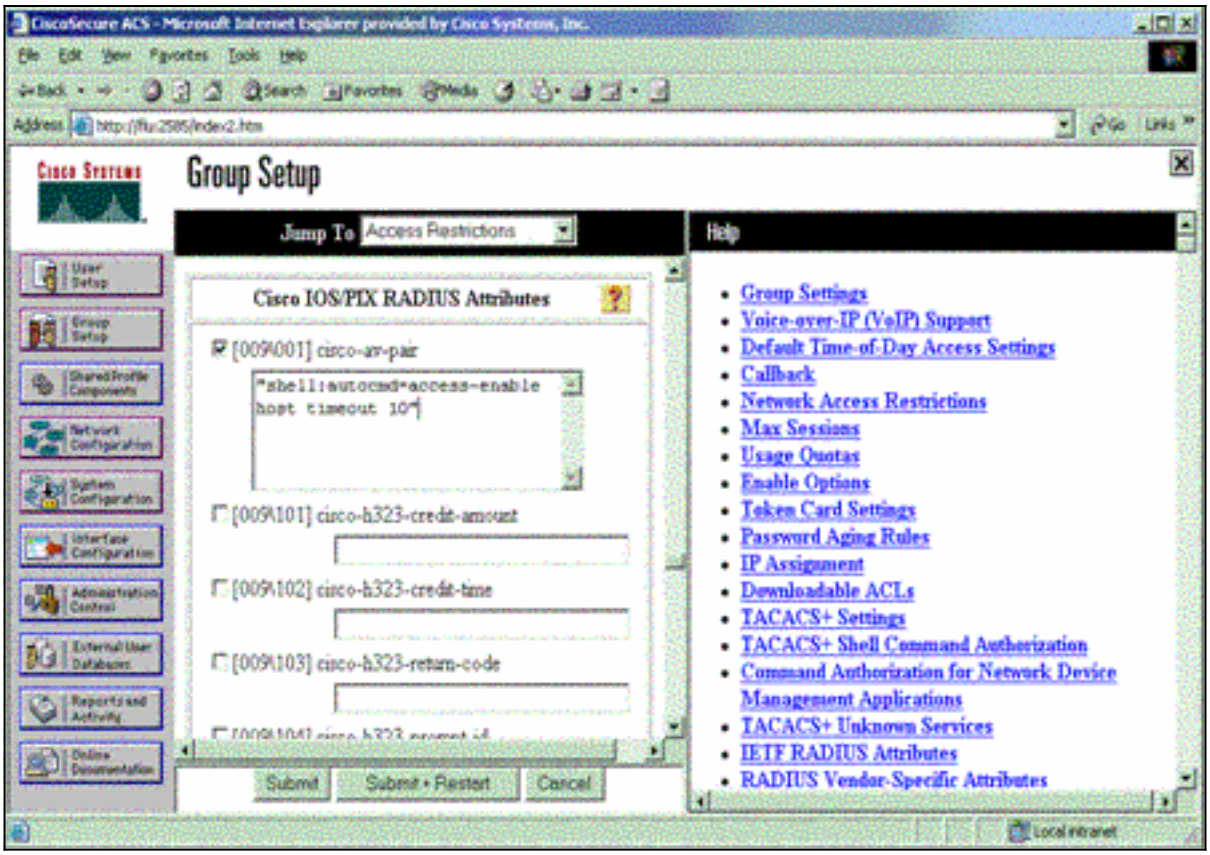
7. Choisissez le groupe auquel l'utilisateur est affecté et cochez la case **Utiliser le groupe**. Cliquez sur
Submit.



8. Cliquez sur **Configuration du groupe** et sélectionnez le groupe auquel l'utilisateur a été affecté à l'étape précédente. Cliquez sur **Modifier les paramètres**.



9. Faites défiler jusqu'à la section Cisco IOS/PIX RADIUS Attributes. Cochez la case correspondant à **cisco-av-pair**. Entrez la commande **shell** à exécuter après autorisation de l'utilisateur. (Cet exemple utilise **shell : autocmd=access-enable host timeout 10**.) Cliquez sur **Soumettre+Redémarrer**.



Dépannage de RADIUS

Utilisez ces commandes **debug** sur le NAS pour résoudre les problèmes RADIUS.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug radius** : affiche les informations associées à RADIUS.

Utilisez ces commandes pour résoudre les problèmes AAA :

- **debug aaa authentication** - Affiche des informations sur l'authentification AAA/TACACS+.
- **debug aaa Authorization** : affiche des informations sur l'autorisation AAA/TACACS+.

L'exemple de sortie **de débogage** ici montre un processus d'authentification et d'autorisation réussi sur l'ACS configuré pour RADIUS.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=====================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
 RADIUS:  AAA Unsupported     [152] 5
 RADIUS:   74 74 79                        [tty]
 RADIUS(00000003): Storing nasport 66 in rad_db
 RADIUS/ENCODE(00000003): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off
 RADIUS(00000003): Config NAS IP: 0.0.0.0
 RADIUS/ENCODE(00000003): acct_session_id: 1
 RADIUS(00000003): sending
 RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
   for Radius-Server 10.48.66.53
 RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
   id 21645/1, len 77
 RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
   BE B5 07 BD E9 05 5B 5D
 RADIUS:  User-Name           [1]   7   "test"
 RADIUS:  User-Password       [2]   18  *
 RADIUS:  NAS-Port            [5]   6   66
 RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
 RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
 RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
 RADIUS: Received from id 21645/1 10.48.66.53:1645,
   Access-Accept, len 93
 RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
   68 4B C3 FC 25 21 47 CD
 RADIUS:  Vendor, Cisco       [26]  51
 RADIUS:   Cisco AVpair       [1]   45
   "shell:autocmd=access-enable host timeout 10"
 RADIUS:  Class               [25]  22
 RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
   [CISCOACS:ac127c0]
 RADIUS:   31 2F 36 36                [1/66]
 RADIUS(00000003): Received from id 21645/1
 AAA/AUTHOR/EXEC(00000003): processing AV
```

```
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

Informations connexes

- Sécurité par clé et verrouillage Cisco IOS
- Page de support TACACS/TACACS+
- TACACS+ dans la documentation d'IOS
- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems