Lock-and-Key: Listas de Acesso Dinâmicas

Contents

Introduction

O acesso lock-and-key permite configurar listas de acesso dinâmicas que concedem acesso para cada usuário a um host específico de origem/destino por meio de um processo de autenticação de usuários. O acesso do usuário é permitido através de um Cisco IOS ® Firewall dinamicamente, sem qualquer comprometimento das restrições de segurança.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Nesse caso, o ambiente do laboratório consistia em um 2620 Router executando o Cisco IOS® Software Release 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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Considerações sobre falsificação

O acesso de tecla e bloqueio permite que um evento externo faça uma abertura no Cisco IOS Firewall. Quando essa abertura existir, o roteador ficará suscetível à falsificação do endereço de origem. Para evitar isso, forneça suporte de criptografia usando criptografia IP com autenticação ou criptografia.

Falsificação é um problema de todas as listas de acesso existentes. O acesso de chave e bloqueio não soluciona esse problema.

Como o acesso chave e bloqueio introduz um caminho potencial através do firewall de rede, é necessário considerar o acesso dinâmico. Outro host, falsificando seu endereço autenticado, obtém acesso por trás do firewall. Com o acesso dinâmico, há a possibilidade de que um host não autorizado, falsificando seu endereço autenticado, obtenha acesso por trás do firewall. O acesso de chave e bloqueio não causa o problema de falsificação de endereço. O problema é aqui identificado somente em consideração ao usuário.

Desempenho

O desempenho é afetado nessas duas situações.

- Cada lista de acesso dinâmico obriga uma reconstrução de lista de acesso no silicon switching engine (SSE). Isto faz o caminho de switching SSE ficar temporariamente lento.
- As listas de acesso dinâmicas exigem o recurso de timeout de ociosidade (mesmo que o timeout seja deixado como padrão). Portanto, as listas de acesso dinâmicas não podem ser comutadas por SSE. Essas entradas são tratadas no caminho de switching rápida do protocolo.

Observe as configurações do roteador de borda. Os usuários remotos criam entradas da lista de acesso no roteador de borda. A lista de acesso cresce e diminui dinamicamente. As entradas são dinamicamente removidas da lista depois do timeout ocioso ou do timeout máximo expirar. Listas de acesso grandes degradam o desempenho da switching de pacotes.

Quando usar o acesso chave e bloqueio

Dois exemplos de quando você usa o acesso de chave e bloqueio estão listados aqui:

- Quando você quiser que um host remoto possa acessar um host em sua internetwork pela Internet. O acesso de chave e bloqueio limita o acesso além do firewall em uma base individual de host ou rede.
- Quando quiser que um subconjunto de hosts em uma rede acesse um host em uma rede remota protegida por um firewall. Com o acesso lock-and-key, você pode habilitar apenas um conjunto desejado de hosts para obter acesso, fazendo com que eles se autentiquem por meio de um servidor TACACS+ ou RADIUS.

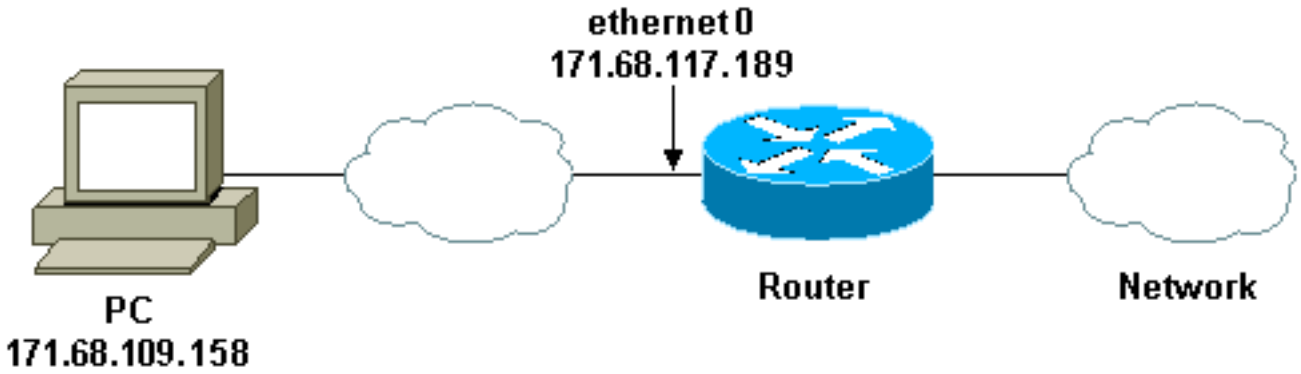
Operação de acesso de chave e bloqueio

Este processo descreve a operação de acesso de chave e bloqueio.

1. Um usuário abre uma sessão Telnet com um roteador de borda configurado para acesso lock-and-key.
2. O software Cisco IOS recebe o pacote Telnet. Ele executa um processo de autenticação de usuário. O usuário deve realizar a autenticação antes do acesso ser permitido. O processo de autenticação é feito pelo roteador ou por um servidor de acesso central, como um servidor TACACS+ ou RADIUS.

Exemplo de Configuração e Troubleshooting

Diagrama de Rede



A Cisco recomenda que você use um servidor TACACS+ para o processo de consulta de autenticação. O TACACS+ fornece serviços de autenticação, autorização e conta. Ele também oferece suporte a protocolo, especificação de protocolo e um banco de dados de segurança centralizado.

Você pode autenticar o usuário no roteador ou com um servidor TACACS+ ou RADIUS.

Observação: esses comandos são globais, a menos que indicado de outra forma.

No roteador, você precisa de um **nome de usuário** para o usuário para autenticação local.

```
username test password test
```

A presença de **login local** nas linhas vty faz com que esse nome de usuário seja usado.

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

Se você não confia no usuário para emitir o comando **access-enable**, você pode fazer uma das duas coisas:

- Associe o tempo limite ao usuário por usuário.

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

or

- Forçar todos os usuários que fazem Telnet a terem o mesmo tempo limite.

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

Observação: o **10** na sintaxe é o *timeout de ociosidade* da lista de acesso. Ele é substituído pelo tempo limite absoluto na lista de acesso dinâmico.

Defina uma lista de acesso estendida que é aplicada quando um usuário (qualquer usuário) faz login no roteador e o comando **access-enable** é emitido. O tempo absoluto máximo para este "orifício" no filtro é definido para 15 minutos. Depois de 15 minutos, o buraco fecha se alguém o usa ou não. A **lista de testes de** nome precisa existir, mas não é significativa. Limite as redes às quais o usuário tem acesso configurando o endereço de origem ou de destino (aqui, o usuário não está limitado).

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

Defina a lista de acesso necessária para bloquear tudo, exceto a capacidade de executar telnet no roteador (para abrir um buraco, o usuário precisa executar telnet para o roteador). O endereço IP aqui é o endereço IP Ethernet do roteador.

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

Há um **deny all** implícito no final (não inserido aqui).

Aplique essa lista de acesso à interface na qual os usuários entram.

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

Você terminou.

Éassim que o filtro está no roteador agora:

```
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)
```

Os usuários que obtêm acesso à sua rede interna não podem ver nada até que façam telnet para o roteador.

Observação: a **10** aqui é o tempo limite *ocioso* da lista de acesso. Ele é substituído pelo tempo

limite absoluto na lista de acesso dinâmico.

```
%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.
```

O filtro é assim.

```
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)
```

Há um buraco no filtro para este usuário com base no endereço IP de origem. Quando alguém faz isso, você vê *dois buracos*.

```
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)
```

Esses usuários podem ter acesso IP completo a qualquer endereço IP de destino de seu endereço IP *de origem*.

Utilizando TACACS+

Configurar TACACS+

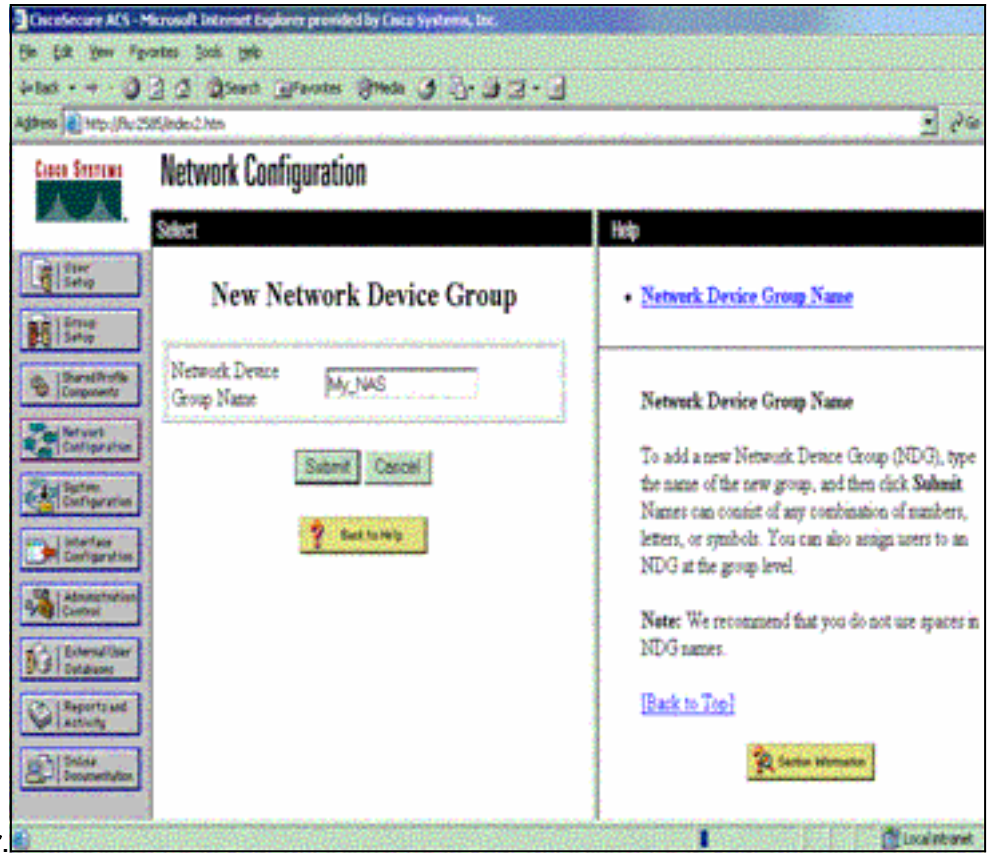
Configure um servidor TACACS+ para forçar a autenticação e a autorização a serem feitas no servidor TACACS+ para usar TACACS+, como mostra esta saída:

```
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
```

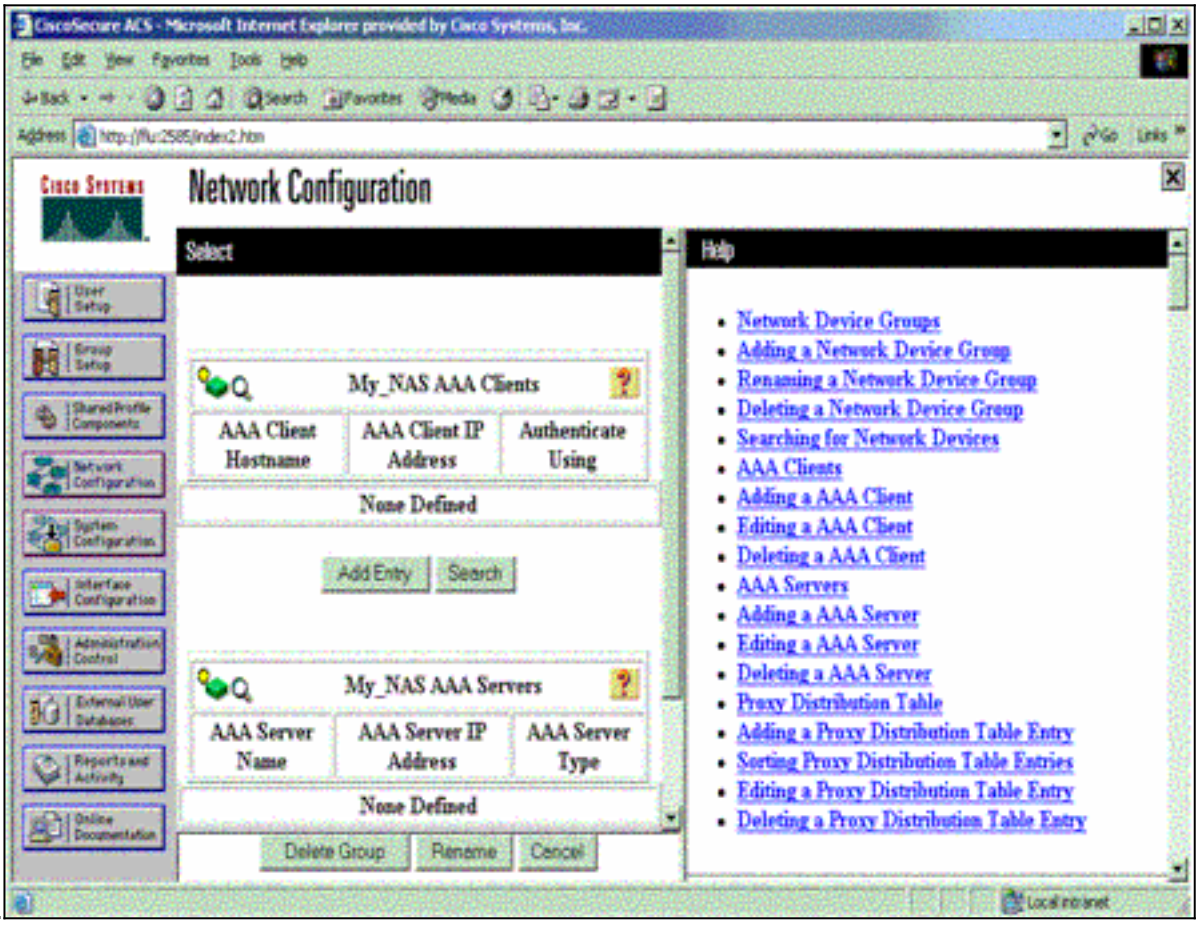
Conclua estes passos para configurar o TACACS+ no Cisco Secure ACS para Windows:

1. Abra um navegador da Web. Insira o endereço do servidor ACS, que está na forma de **http://*<endereço_IP ou nome_DNS>*:2002**. (Este exemplo usa uma porta padrão de 2002.) Faça login como administrador.
2. Clique em Network Configuration. Clique em **Add Entry** para criar um grupo de dispositivos de rede que contenha os servidores de acesso à rede (NAS). Digite um nome para o grupo e

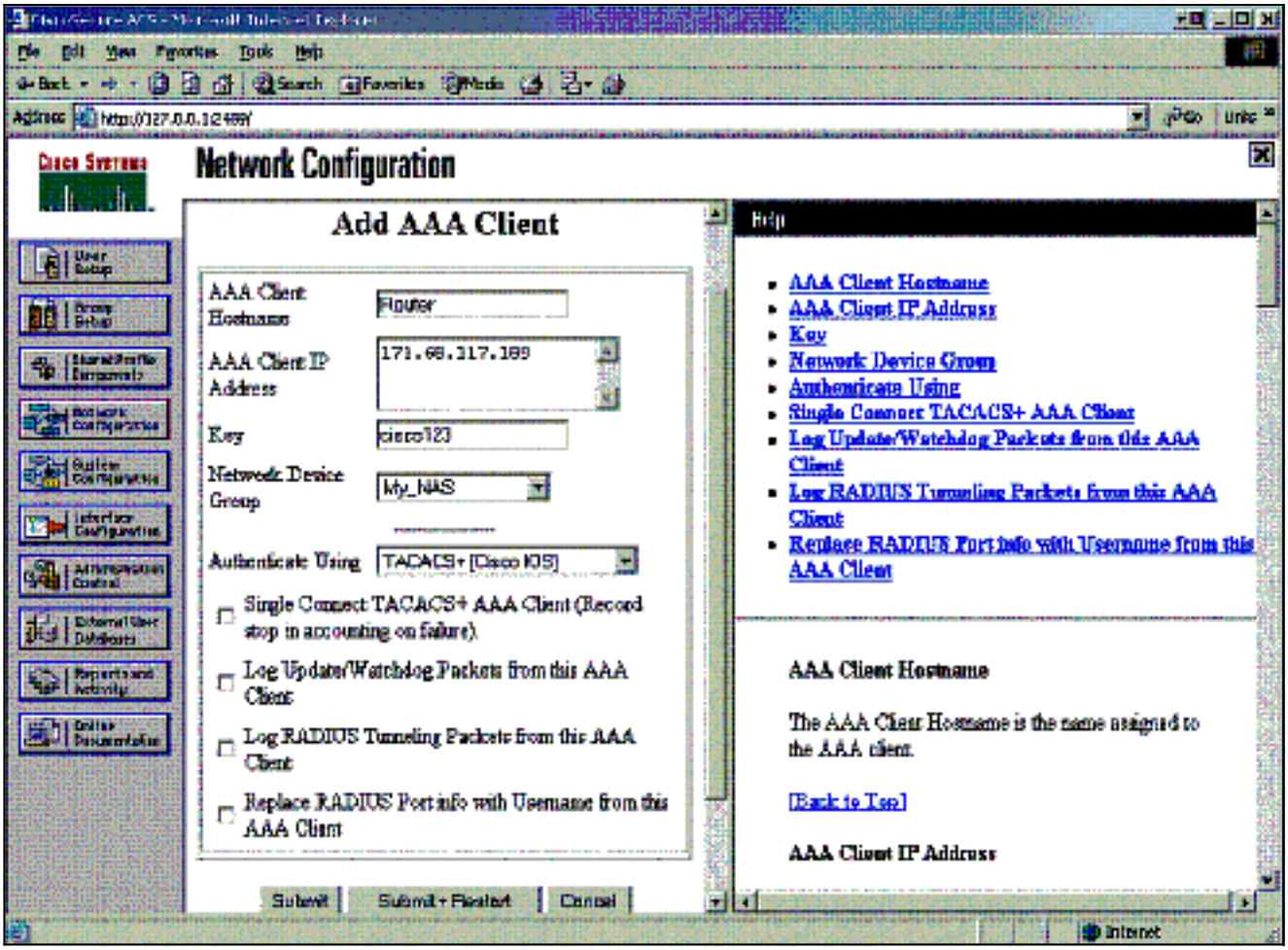
clique em **Enviar**.



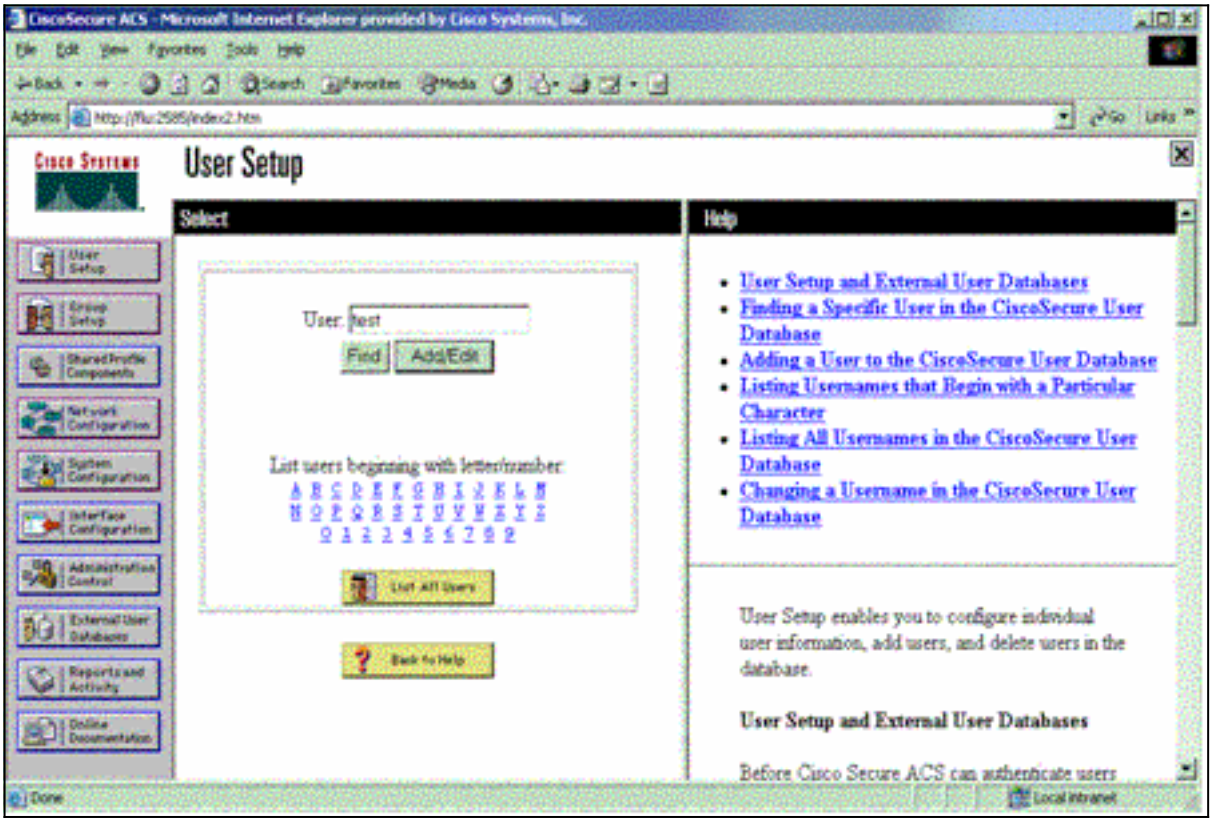
3. Clique em **Add Entry** para adicionar um cliente de autenticação, autorização e contabilização (AAA) (NAS).



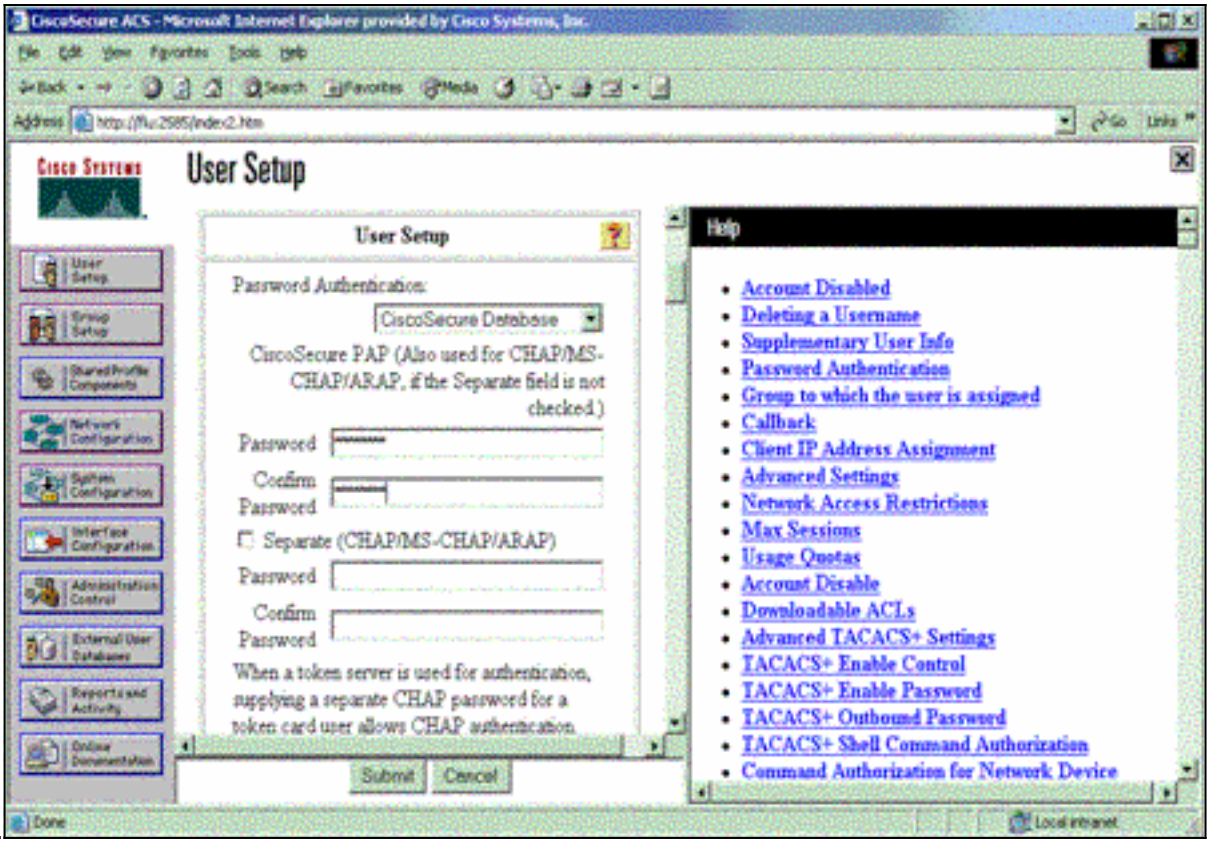
4. Insira o nome do host, o endereço IP e a chave usada para criptografar a comunicação entre o servidor AAA e o NAS. Selecione **TACACS+ (Cisco IOS)** como o método de autenticação. Quando terminar, clique em **Enviar +Reiniciar** para aplicar as alterações.



5. Clique em **User Setup**, digite uma ID de usuário e clique em **Add/Edit**.

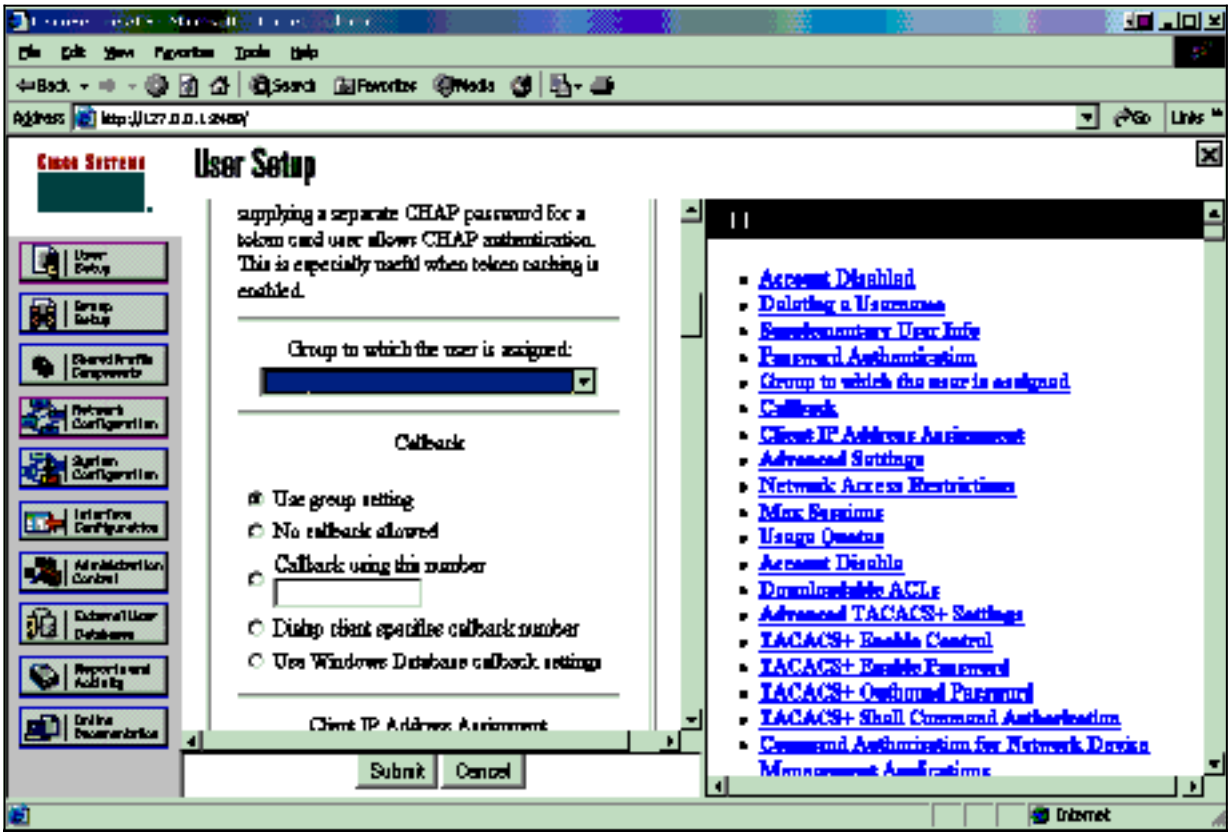


6. Escolha um banco de dados para autenticar o usuário. (Neste exemplo, o usuário é "test" e o banco de dados interno do ACS é usado para autenticação). Digite uma senha para o usuário e confirme a

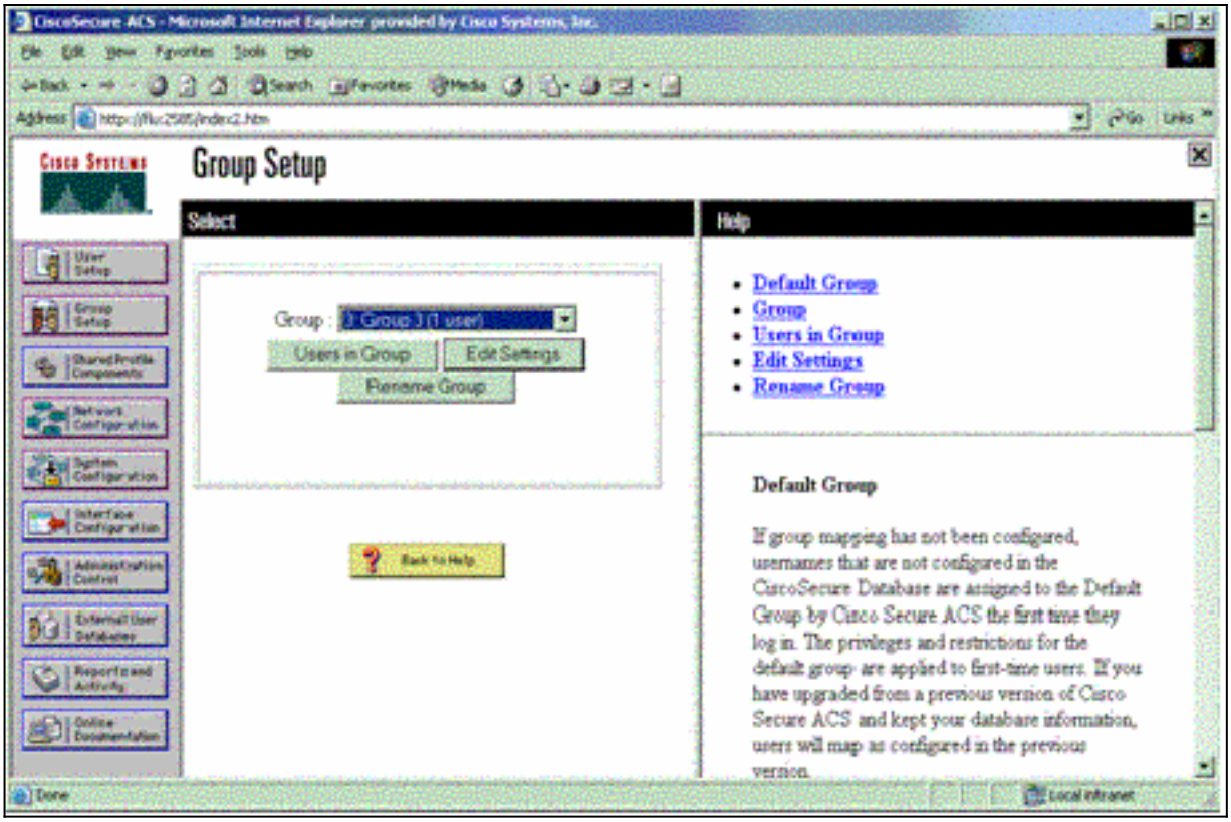


senha.

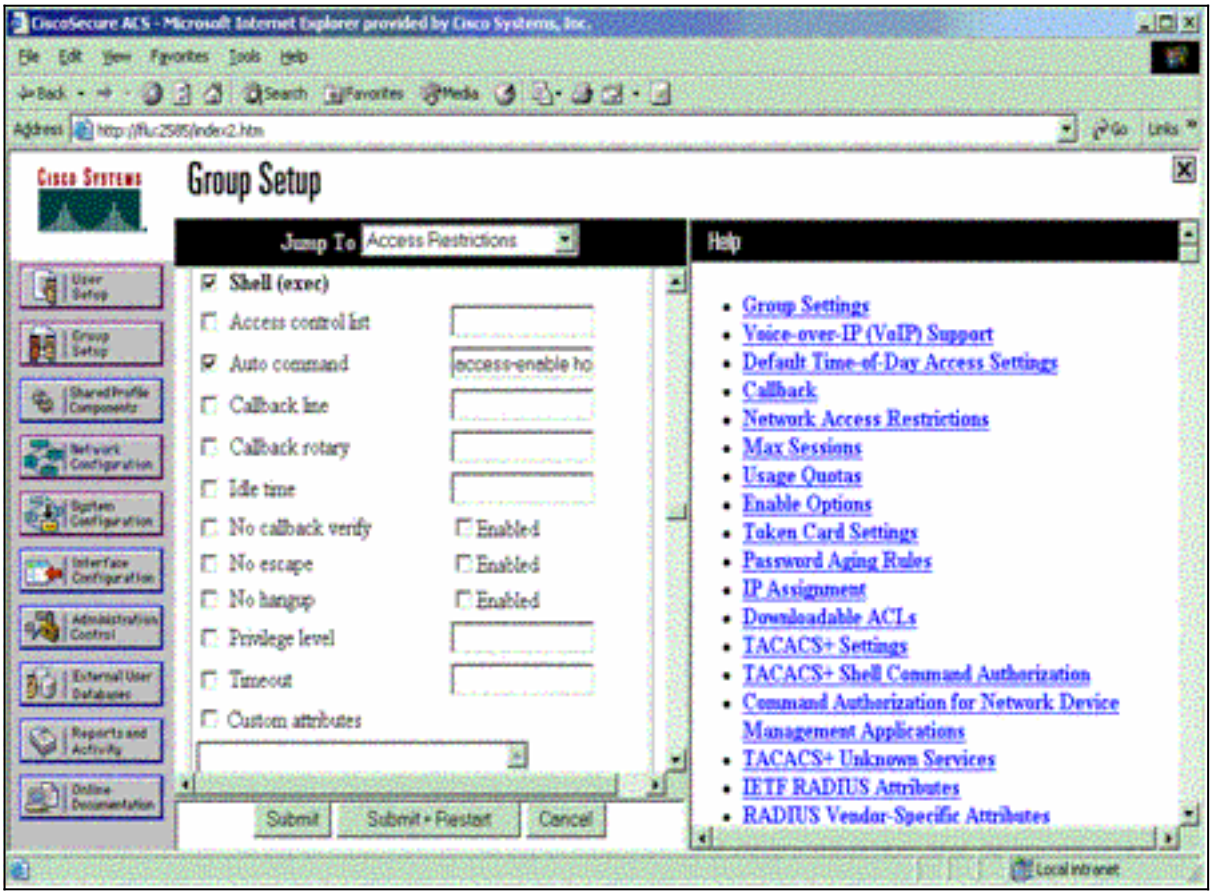
7. Escolha o grupo ao qual o usuário está atribuído e marque **Usar configuração de grupo**. Clique em Submit.



8. Clique em **Group Setup (Configuração do grupo)**. Selecione o grupo ao qual o usuário foi atribuído na etapa 7. Clique em **Editar configurações**.



9. Role para baixo até a seção TACACS+ Settings (Configurações do TACACS+). Marque a caixa para **Shell exec**. Marque a caixa do **comando Auto**. Insira o comando auto a ser executado após a autorização bem-sucedida do usuário. (Este exemplo usa o comando **access-enable host timeout 10**.) Clique em **Enviar+Reiniciar**.



[Solucionar problemas do TACACS+]

Use esses comandos **debug** no NAS para solucionar problemas do TACACS+.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- **debug tacacs authentication** — Exibe informações sobre o processo de autenticação TACACS+. Disponível apenas em algumas versões do software. Se não estiver disponível, use apenas **debug tacacs**.
- **debug tacacs authorization** — Exibe informações sobre o processo de autorização TACACS+. Disponível apenas em algumas versões do software. Se não estiver disponível, use apenas **debug tacacs**.
- **debug tacacs events** —Exibe informações do processo auxiliar TACACS+. Disponível apenas em algumas versões do software. Se não estiver disponível, use apenas **debug tacacs**.

Use estes comandos para solucionar problemas de AAA:

- **debug aaa authentication — Exibe informações sobre autenticação AAA/TACACS+.**
- **debug aaa authorization — Exibe informações sobre autorização AAA/TACACS+.**

A saída de **depuração** de exemplo aqui mostra uma autenticação e um processo de autorização bem-sucedidos no servidor 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
```

Usando RADIUS

Configurar RADIUS

Para usar o RADIUS, configure um servidor RADIUS para forçar a autenticação a ser feita no servidor RADIUS com parâmetros de autorização (o comando automático) a serem enviados no atributo 26 específico do fornecedor, como mostrado aqui:

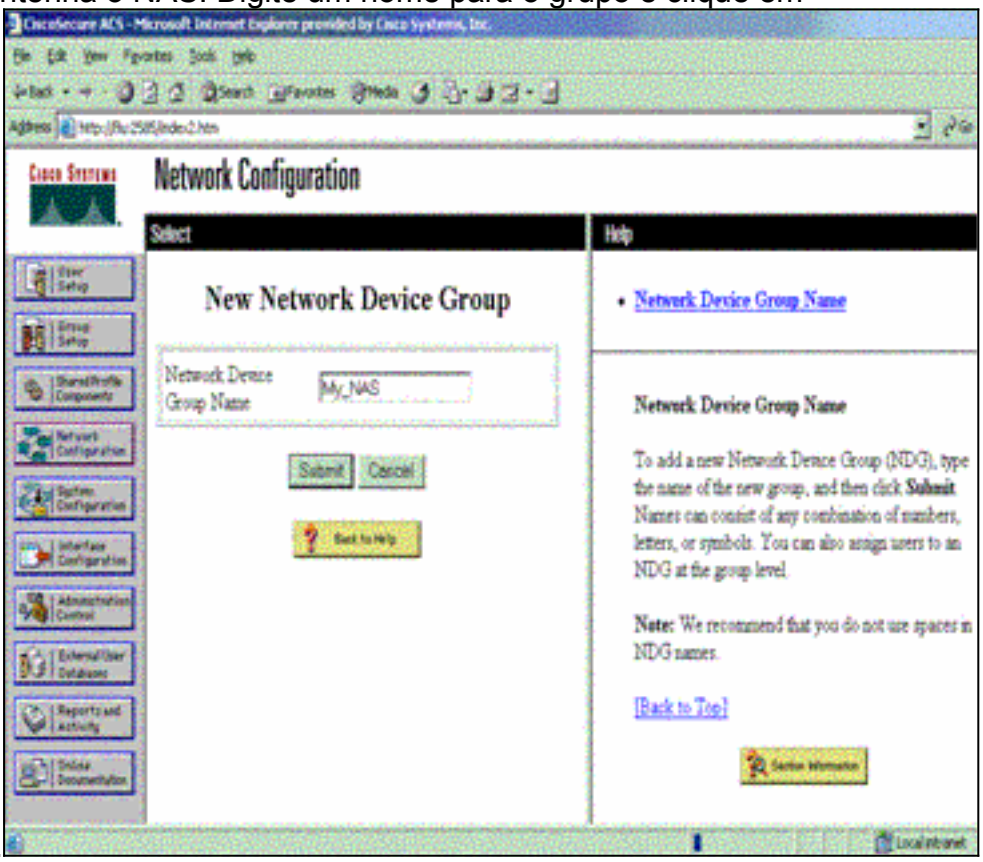
```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

Conclua estes passos para configurar o RADIUS no Cisco Secure ACS para Windows:

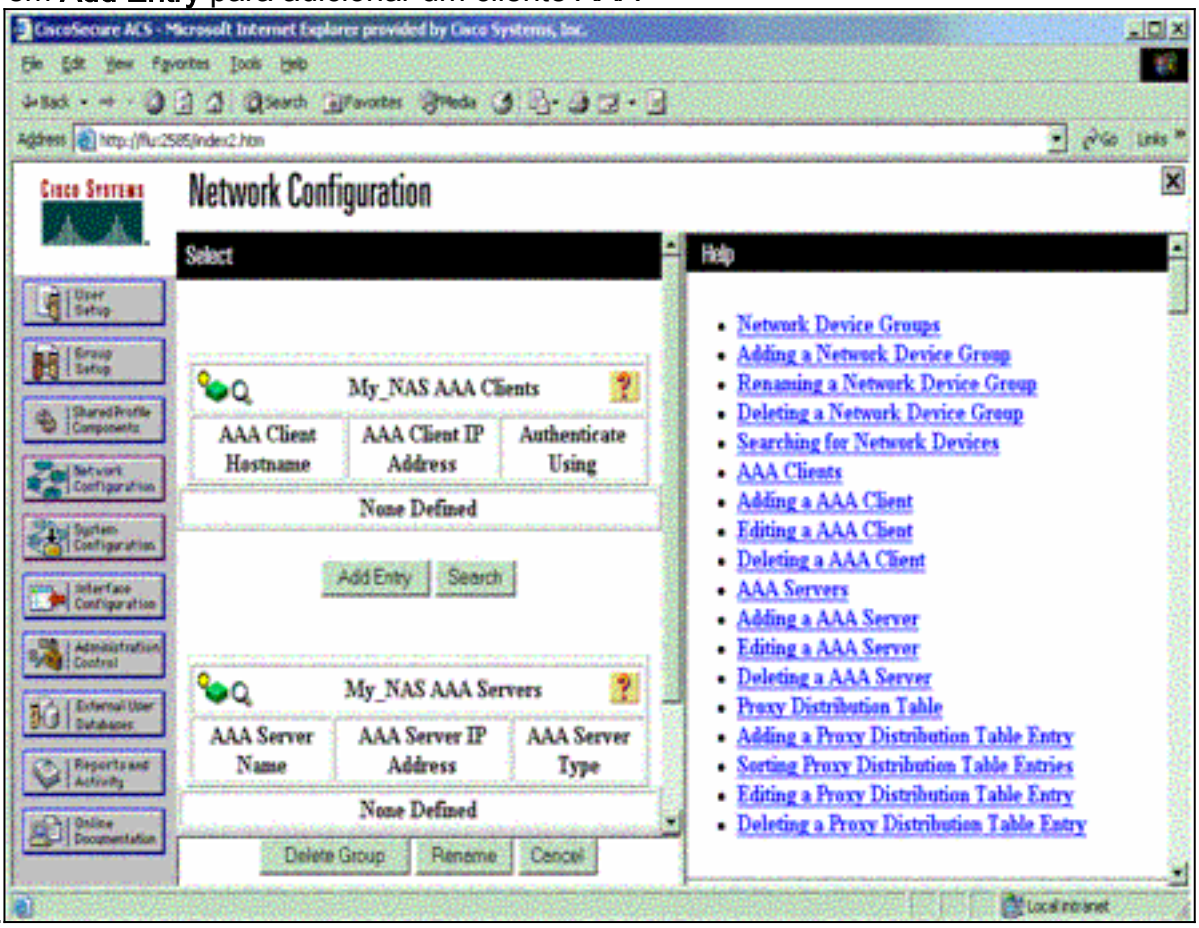
1. Abra um navegador da Web e digite o endereço do servidor ACS, que está na forma de

http:// *<endereço_IP ou nome_DNS>*:2002. (Este exemplo usa uma porta padrão de 2002.) Faça login como administrador.

2. Clique em Network Configuration. Clique em **Add Entry** para criar um Network Device Group que contenha o NAS. Digite um nome para o grupo e clique em **Enviar**.

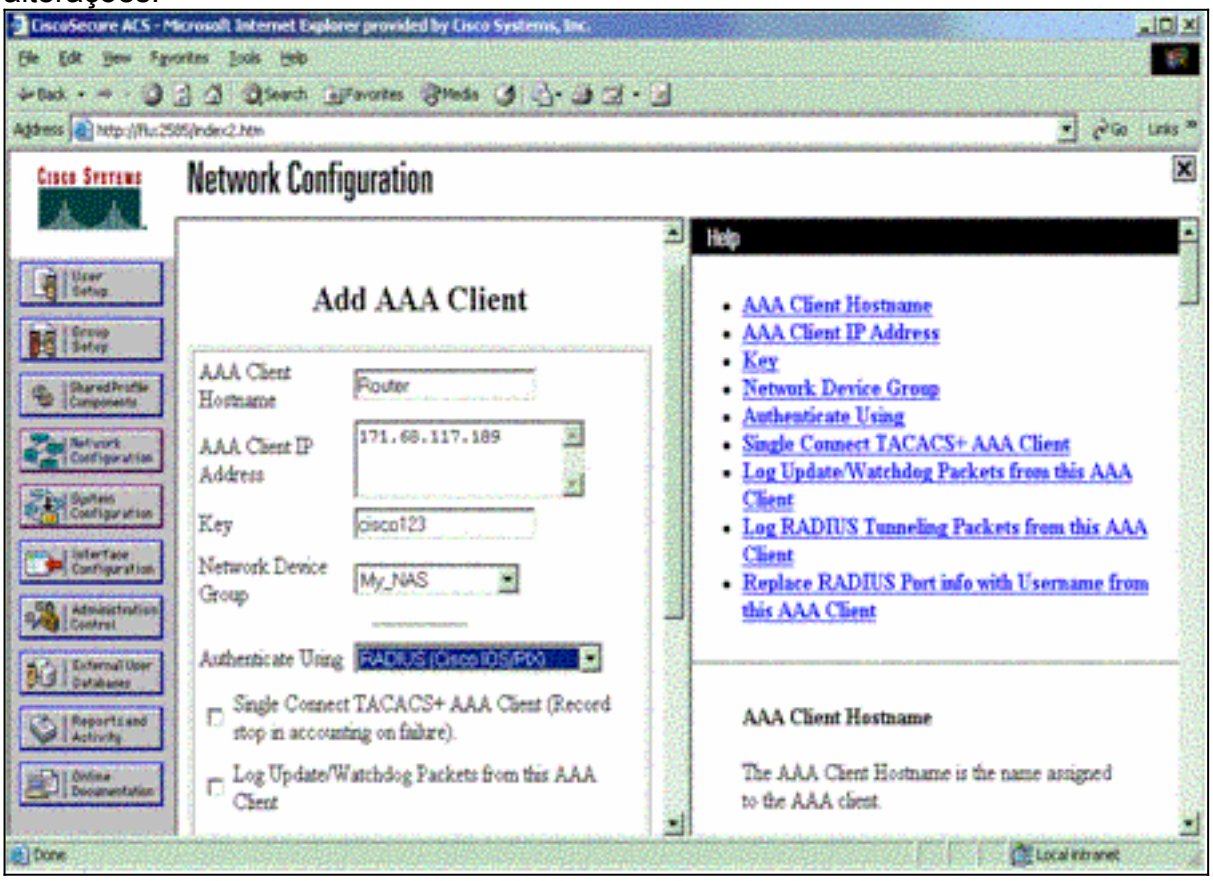


3. Clique em **Add Entry** para adicionar um cliente AAA (NAS).

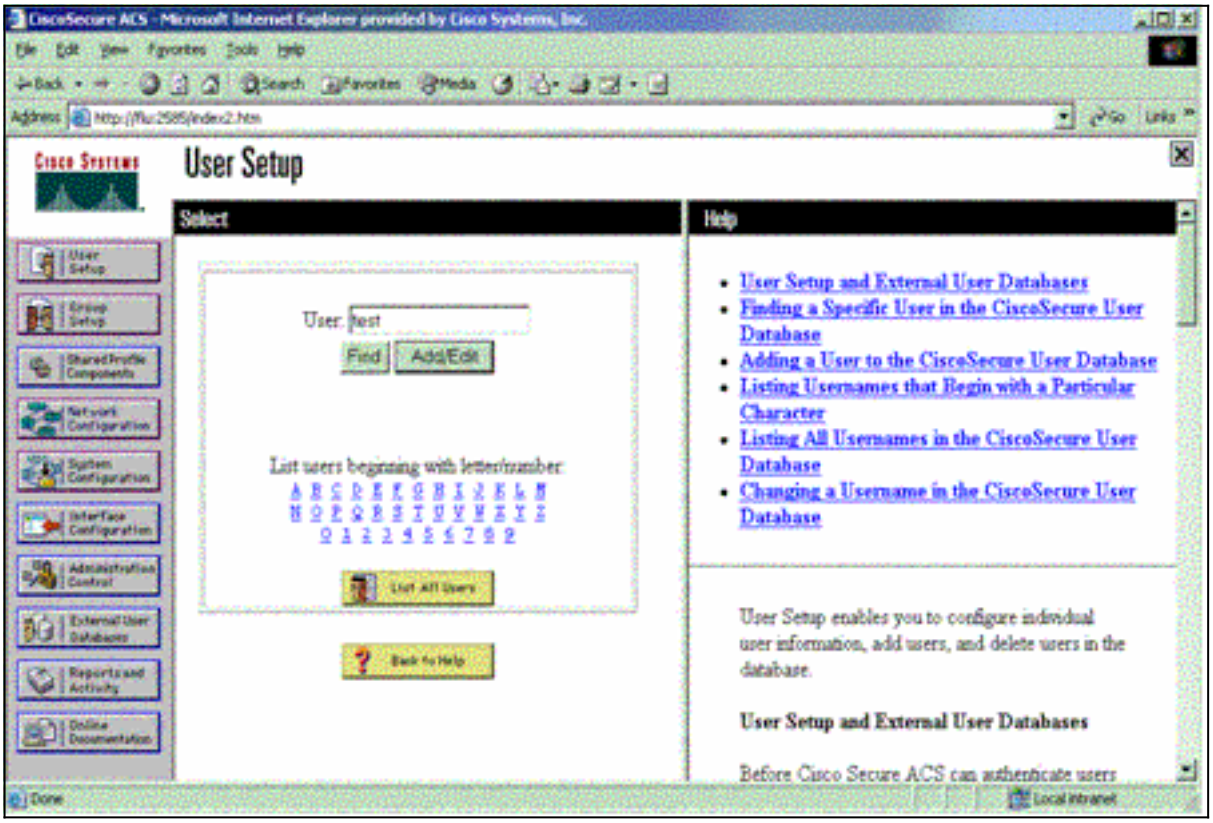


4. Insira o nome do host, o endereço IP e a chave usada para criptografar a comunicação entre

o servidor AAA e o NAS. Selecione **RADIUS (Cisco IOS/PIX)** como o método de autenticação. Quando terminar, clique em **Enviar +Reiniciar** para aplicar as alterações.

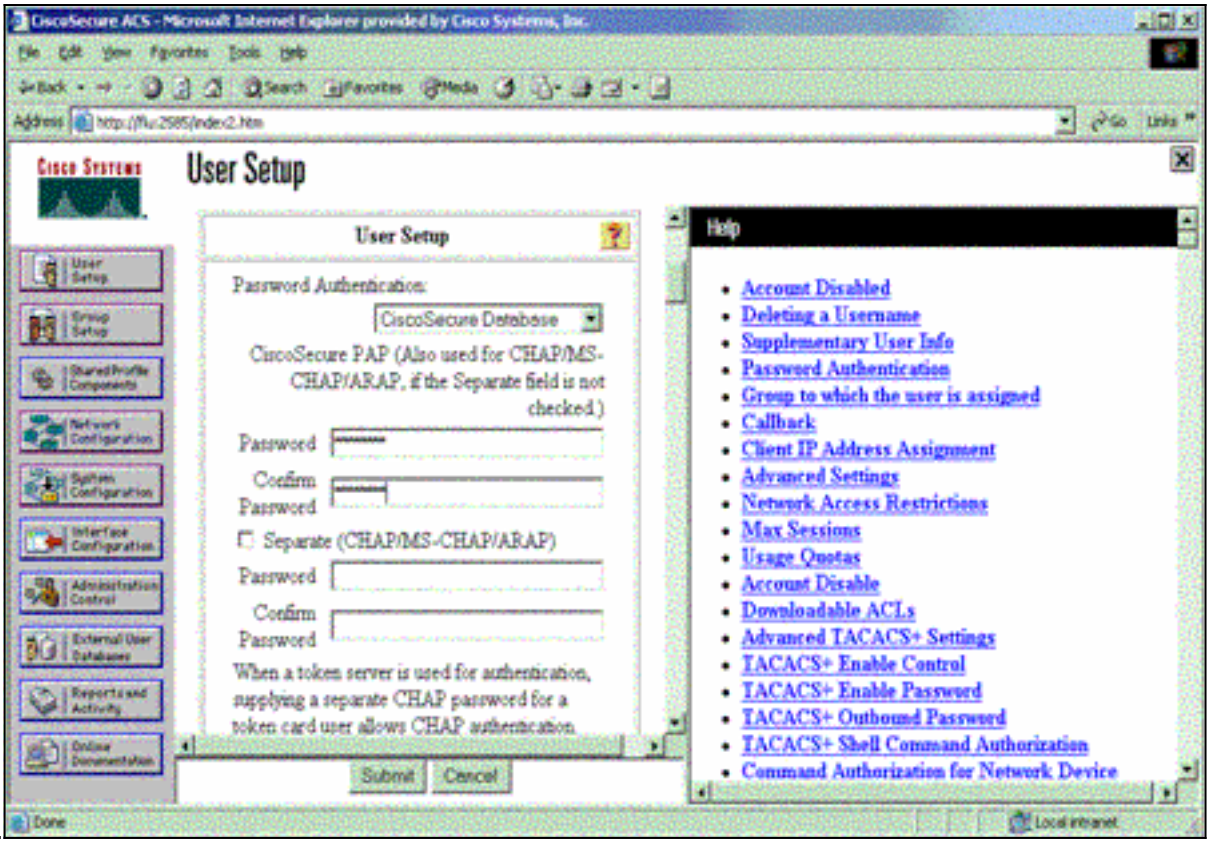


5. Clique em **User Setup**, digite uma ID de usuário e clique em **Add/Edit**.

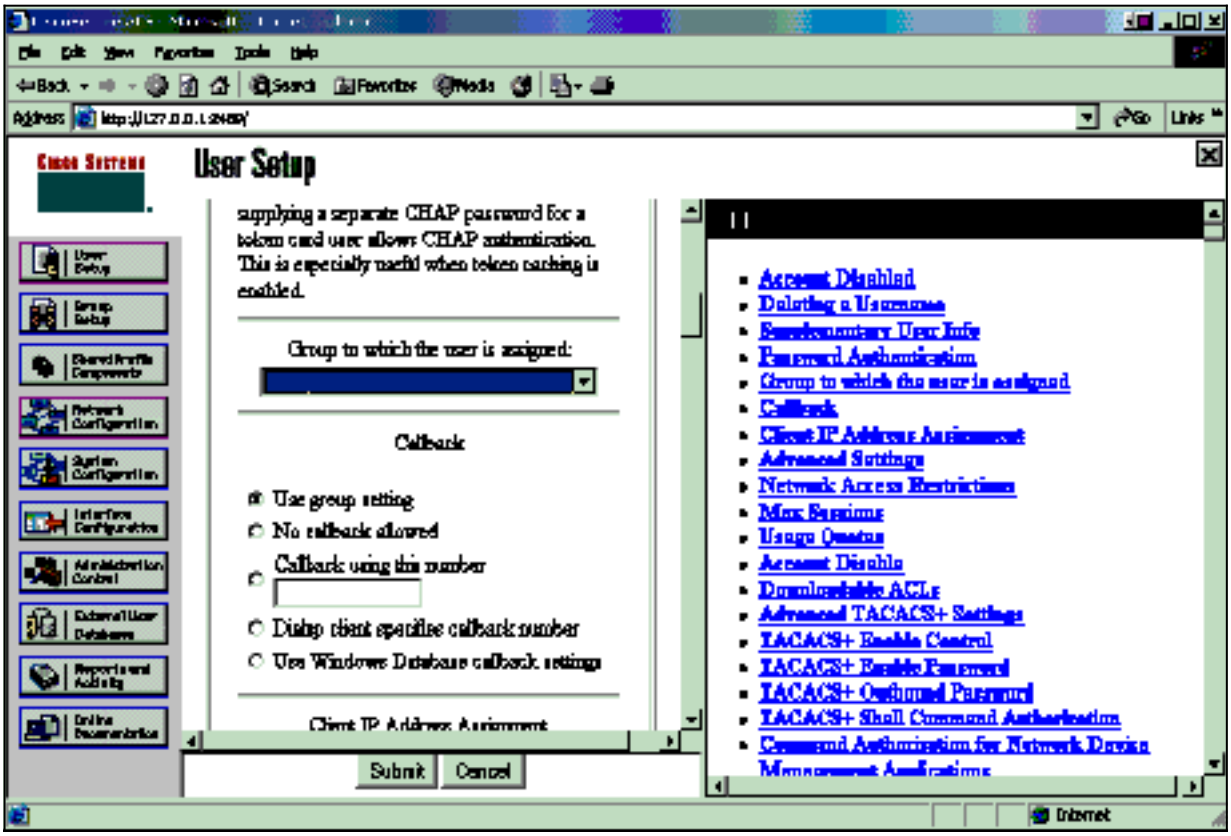


6. Escolha um banco de dados para autenticar o usuário. (Neste exemplo, o usuário é "test" e o banco de dados interno do ACS é usado para autenticação). Digite uma senha para o usuário e confirme a

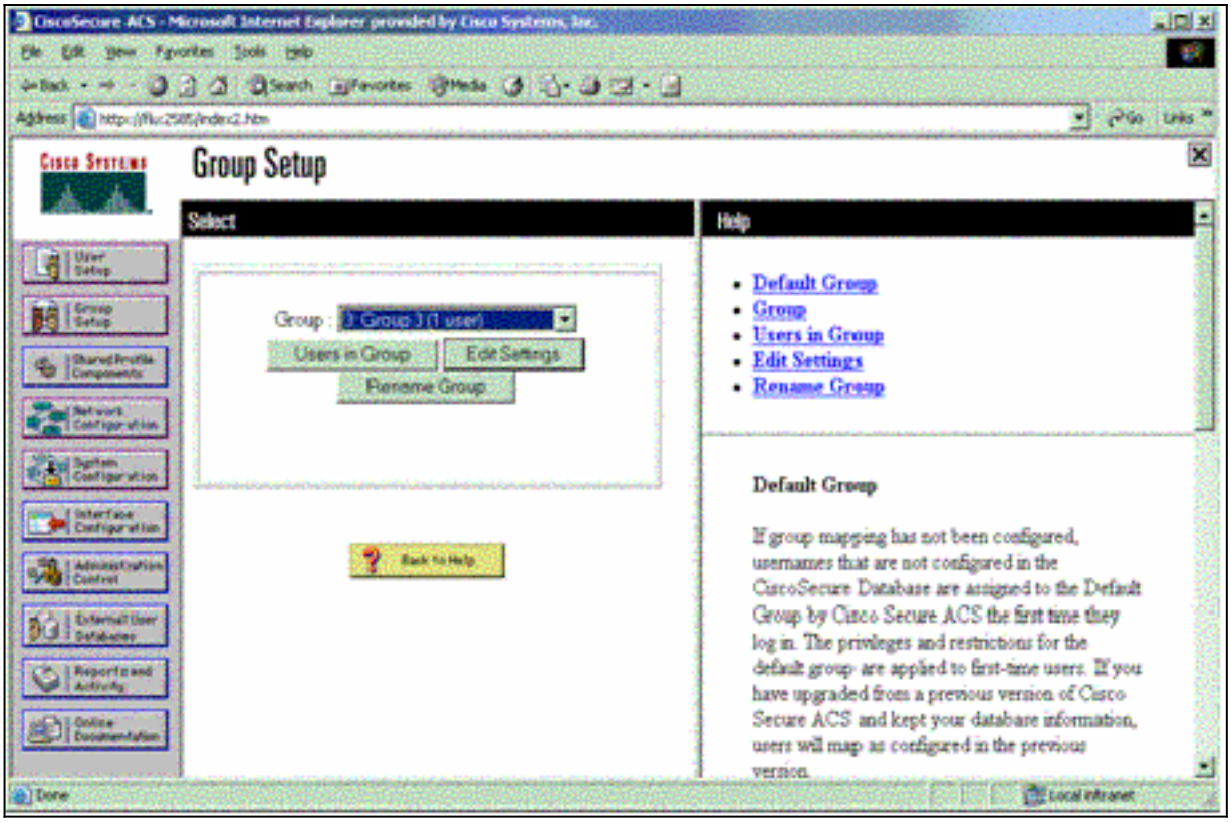
senha.



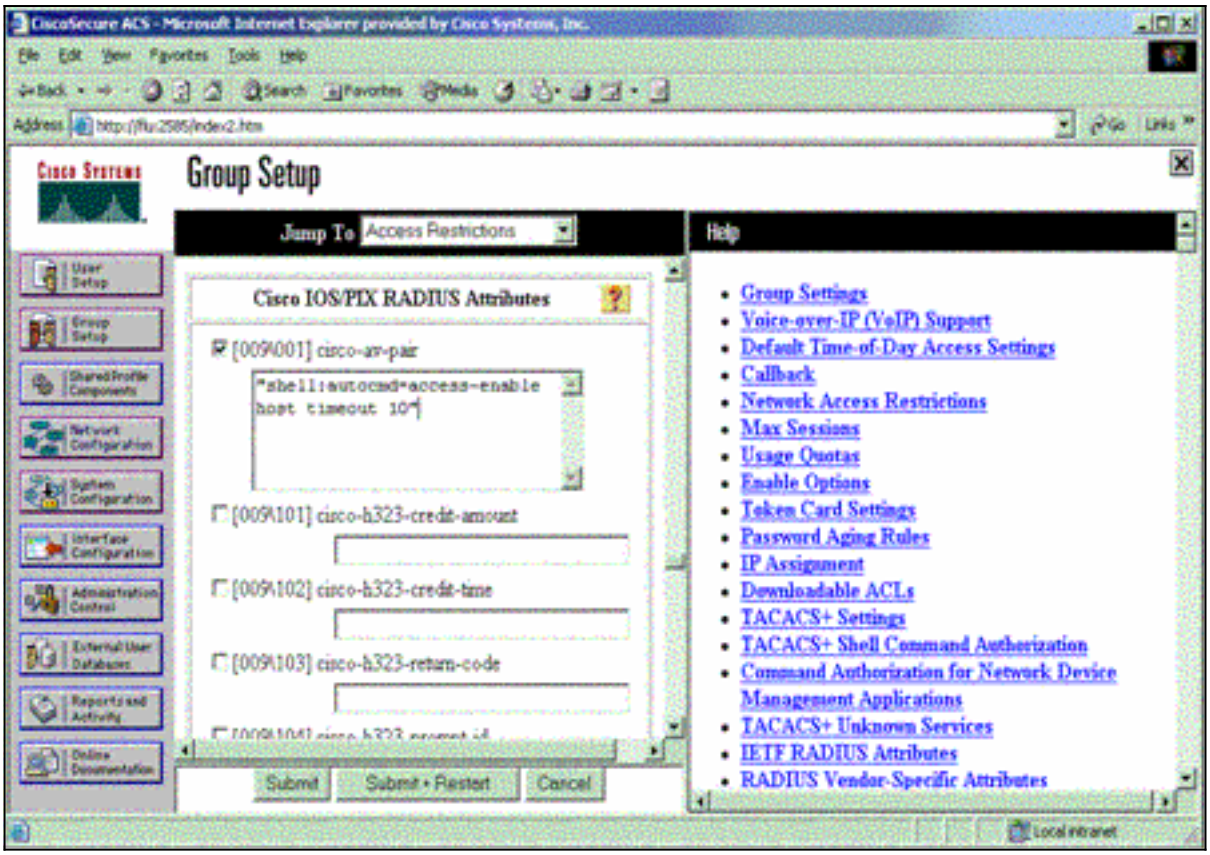
7. Escolha o grupo ao qual o usuário está atribuído e marque **Usar configuração de grupo**. Clique em Submit.



8. Clique em **Group Setup** e selecione o grupo ao qual o usuário foi atribuído na etapa anterior. Clique em **Editar configurações**.



9. Role para baixo até a seção Cisco IOS/PIX RADIUS Attributes. Marque a caixa para **cisco-av-pair**. Insira o comando **shell** a ser executado após uma autorização bem-sucedida do usuário. (Este exemplo usa **shell:autocmd=access-enable host timeout 10**.) Clique em **Enviar+Reiniciar**.



Solucionar problemas de RADIUS

Use esses comandos **debug** no NAS para solucionar problemas com o RADIUS.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- **debug radius** — Exibe informações associadas ao RADIUS.

Use estes comandos para solucionar problemas de AAA:

- **debug aaa authentication — Exibe informações sobre autenticação AAA/TACACS+.**
- **debug aaa authorization — Exibe informações sobre autorização AAA/TACACS+.**

A saída de **depuração de** exemplo aqui mostra uma autenticação e um processo de autorização bem-sucedidos no ACS configurado para 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
```

Informações Relacionadas

- Segurança de chave e bloqueio do Cisco IOS
- Página de Suporte do TACACS/TACACS+
- TACACS+ na Documentação do IOS
- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems