ロック アンド キー：ダイナミック アクセス リスト

内容

概要

Lock-and-key アクセスを使用すると、ユーザ認証プロセスを使用して特定の発信元/送信先ホストへのアクセスをユーザ単位で許可する、ダイナミック アクセス リストを設定できます。Cisco IOS®ファイアウォールを介したユーザアクセスは、セキュリティ上の制約を受けずに動的に許可されます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。この場合、ラボ環境は、Cisco IOS®ソフトウェアリリース12.3(1)が稼働する2620ルータで構成されています。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについ

ても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

スプーフィングについて

ロックアンドキーアクセスを使用すると、外部イベントがCisco IOSファイアウォールに開口部を配置できます。この穴が開いてしまうと、ルータは発信元アドレスのスプーフィングを受ける可能性があります。これを防ぐために、認証または暗号化を使用したIP暗号化を使用した暗号化サポートを提供します。

スプーフィングの問題はすべての既存のアクセス リストに存在します。ロック アンド キー アクセスではこの問題に対処できません。

ロック アンド キー アクセスでは、ネットワーク ファイアウォールに潜在的な通路が作成されるため、ダイナミック アクセスを検討する必要があります。別のホストは、認証されたアドレスをスプーフィングし、ファイアウォールの背後でアクセスを取得します。ダイナミックアクセスでは、不正なホストが認証されたアドレスをスプーフィングし、ファイアウォールの背後でアクセスする可能性があります。ロック アンド キー アクセスでは、アドレス スプーフィングの問題は発生しません。この文書では、この問題はユーザが懸念すべき問題として認識されるにとどまります。

パフォーマンス

この2つの状況では、パフォーマンスが影響を受けます。

- それぞれのダイナミック アクセス リストによって、Silicon Switching Engine (SSE; シリコン スイッチング エンジン) では強制的にアクセス リストが再作成されます。 これが原因で、SSE スイッチング パスの速度が一瞬低下します。
- ダイナミックアクセスリストには、アイドルタイムアウト機能が必要です (タイムアウトがデフォルトのままでも) 。 したがって、ダイナミックアクセスリストはSSEスイッチングできません。これらのエントリは、プロトコルファーストスイッチングパスで処理されます。

境界ルータの設定を確認します。リモート ユーザは、境界ルータにアクセス リストのエントリを作成します。アクセスリストは動的に拡大および縮小します。idle-timeout または max-timeout の期間が経過すると、エントリがリストから動的に削除されます。アクセス リストが大きくなると、パケット交換のパフォーマンスが低下します。

ロック アンド キー アクセスを使用する状況

ロックアンドキーアクセスを使用する場合の2つの例を次に示します。

- リモートホストがインターネット経由でインターネットワーク内のホストにアクセスできるようにする場合。ロックアンドキーアクセスは、ファイアウォールを越えたアクセスを個々のホストまたはネットベースで制限します。
- ネットワーク上の一部のホストが、ファイアウォールで保護されたリモート ネットワーク上

のホストにアクセスできるようにする場合。ロック アンド キー アクセスを使用すると、TACACS+ または RADIUS サーバによる認証を行うことで、希望するホスト群のみにアクセスを許可できます。

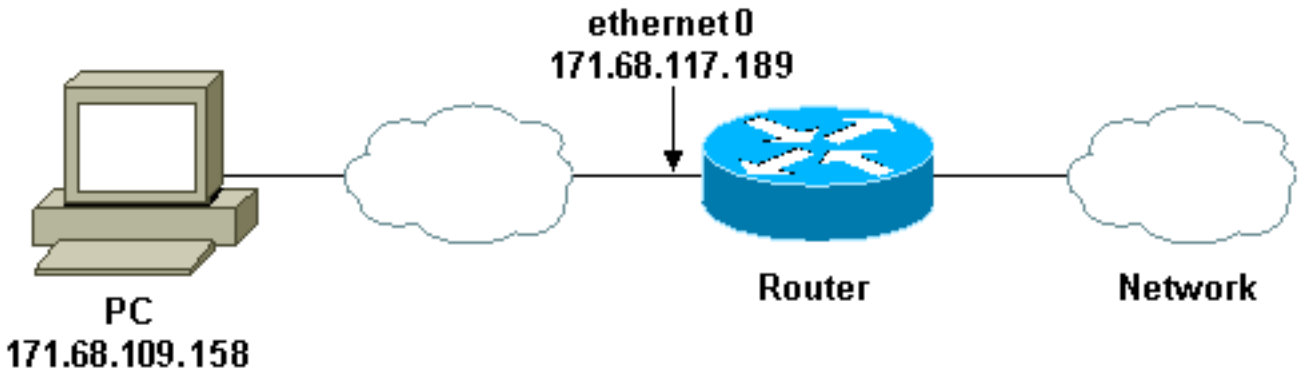
ロック アンド キー アクセスの動作

このプロセスでは、ロックアンドキーアクセス操作について説明します。

1. ユーザが、ロック アンド キー アクセス用に設定された境界ルータへの Telnet セッションを開きます。
2. Cisco IOSソフトウェアはTelnetパケットを受信します。ユーザ認証プロセスを実行します。ユーザは認証をパスしない限り、アクセスを許可されません。認証プロセスは、ルータまたはTACACS+サーバやRADIUSサーバなどの中央アクセスサーバによって実行されます。

設定例とトラブルシューティング

ネットワーク図



認証クエリプロセスにはTACACS+サーバを使用することを推奨します。TACACS+ では、認証、許可、および会計サービスが提供されます。また、プロトコル サポート、プロトコル仕様、および中央集中型セキュリティ データベースも提供されます。

ユーザの認証は、ルータで行うことも、TACACS+ または RADIUS サーバを使用することもできます。

注： これらのコマンドは、特に指示がない限り、グローバルです。

ルータでは、ローカル認証のためにユーザーのユーザ名が必要です。

```
username test password test
```

vty回線にlogin localが存在すると、このユーザ名が使用されます。

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

ユーザがaccess-enableコマンドを発行することを信頼できない場合は、次の2つのいずれかを実行できます。

- ユーザごとにタイムアウトをユーザに関連付けます。

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

または

- Telnet接続するすべてのユーザに同じタイムアウトを強制します。

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

注：構文の10は、アクセス・リストの*アイドル・*タイムアウトです。ダイナミックアクセスリストの絶対タイムアウトによって上書きされます。

ユーザ（任意のユーザ）がルータにログインし、access-enableコマンドを発行したときに適用される拡張**アクセスリスト**を定義します。フィルタのこの「穴」の最大絶対時間は15分に設定されます。15分後、穴は誰かが使用するかどうかによって閉じます。testlist という名前は存在している必要がありますが、重要ではありません。送信元アドレスまたは宛先アドレスを設定して、ユーザがアクセスできるネットワークを制限します（ここでは、ユーザは制限されません）。

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

ルータにTelnetする機能を除くすべての機能をブロックするために必要なアクセスリストを定義します（穴を開けるには、ユーザがルータにTelnetする必要があります）。 このIPアドレスは、ルータのイーサネットIPアドレスです。

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

最後に暗黙的なdeny allが存在します（ここでは入力しません）。

このアクセスリストを、ユーザが入ってくるインターフェイスに適用します。

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

これで完了です。

現在、ルータ上のフィルタは次のようになります。

```
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)
```

内部ネットワークにアクセスするユーザは、ルータにTelnet接続するまで何も表示されません。

注：この10はアクセスリストのアイドルタイムアです。ダイナミックアクセスリストの絶対タイムアウトによって上書きされます。

```
%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.
```

フィルタは次のようになります。

```
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)
```

送信元IPアドレスに基づいて、この1人のユーザのフィルタに穴があります。他の人がこうすると、2つの穴が*見えます*。

```
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)
```

これらのユーザは、送信元IPアドレスから任意の宛先IPアドレスへの完全なIPアクセスが可能です。

TACACS+ の使用

TACACS+の設定

次の出力に示すように、TACACS+を使用するために、TACACS+サーバで認証と認可を強制的に実行するようにTACACS+サーバを設定します。

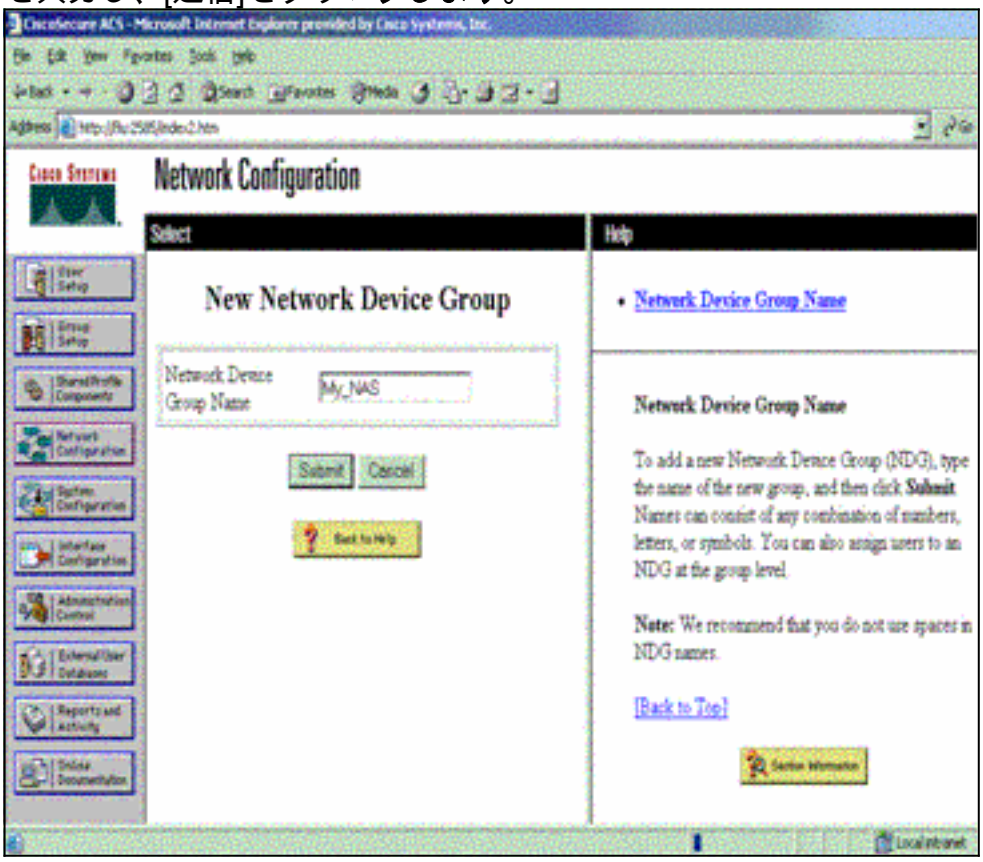
```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

Cisco Secure ACS for WindowsでTACACS+を設定するには、次の手順を実行します。

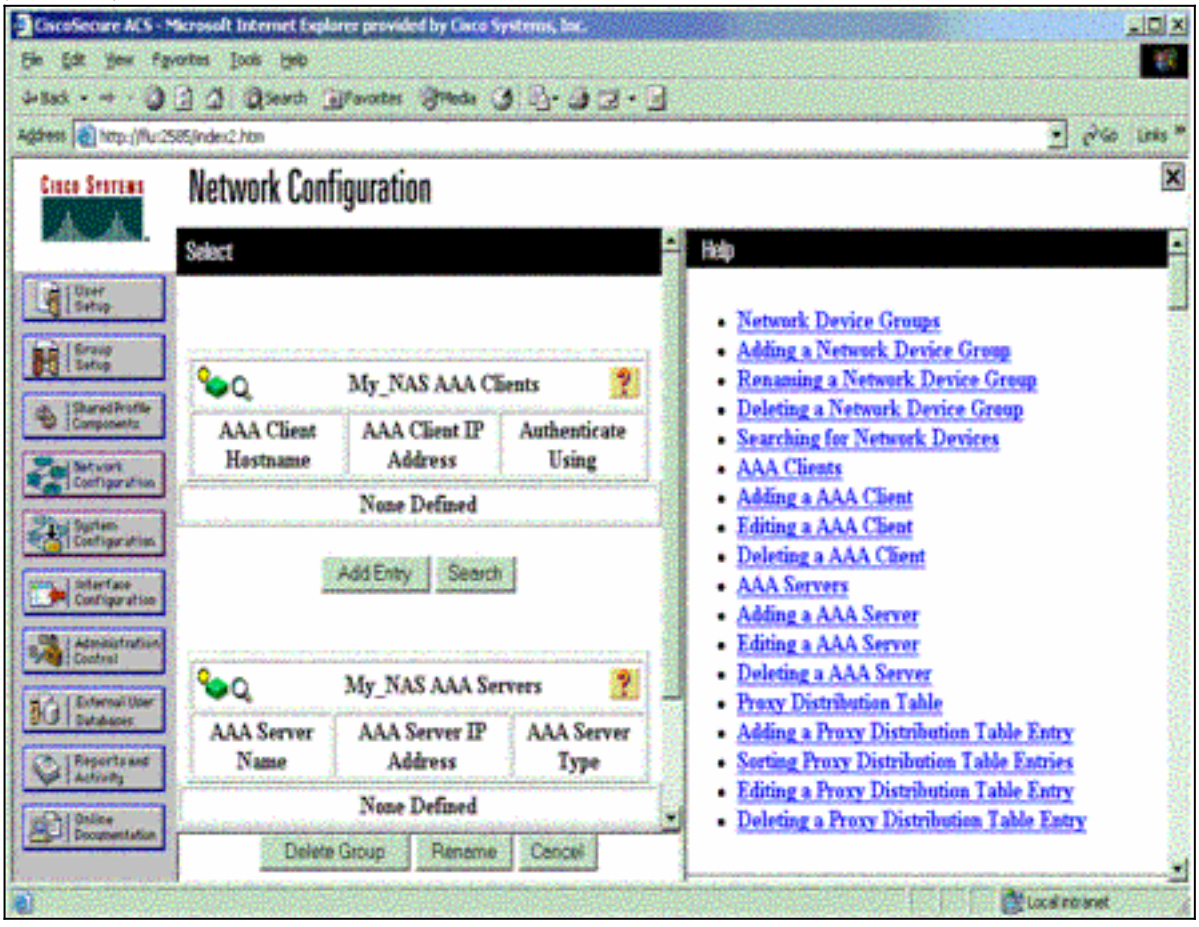
1. Web ブラウザを開きます。ACSサーバのアドレスを**http://*<IP_address or DNS_name>*:2002**の形式で入力します（この例では、デフォルトポート2002を使用します

）。 adminとしてログインします。

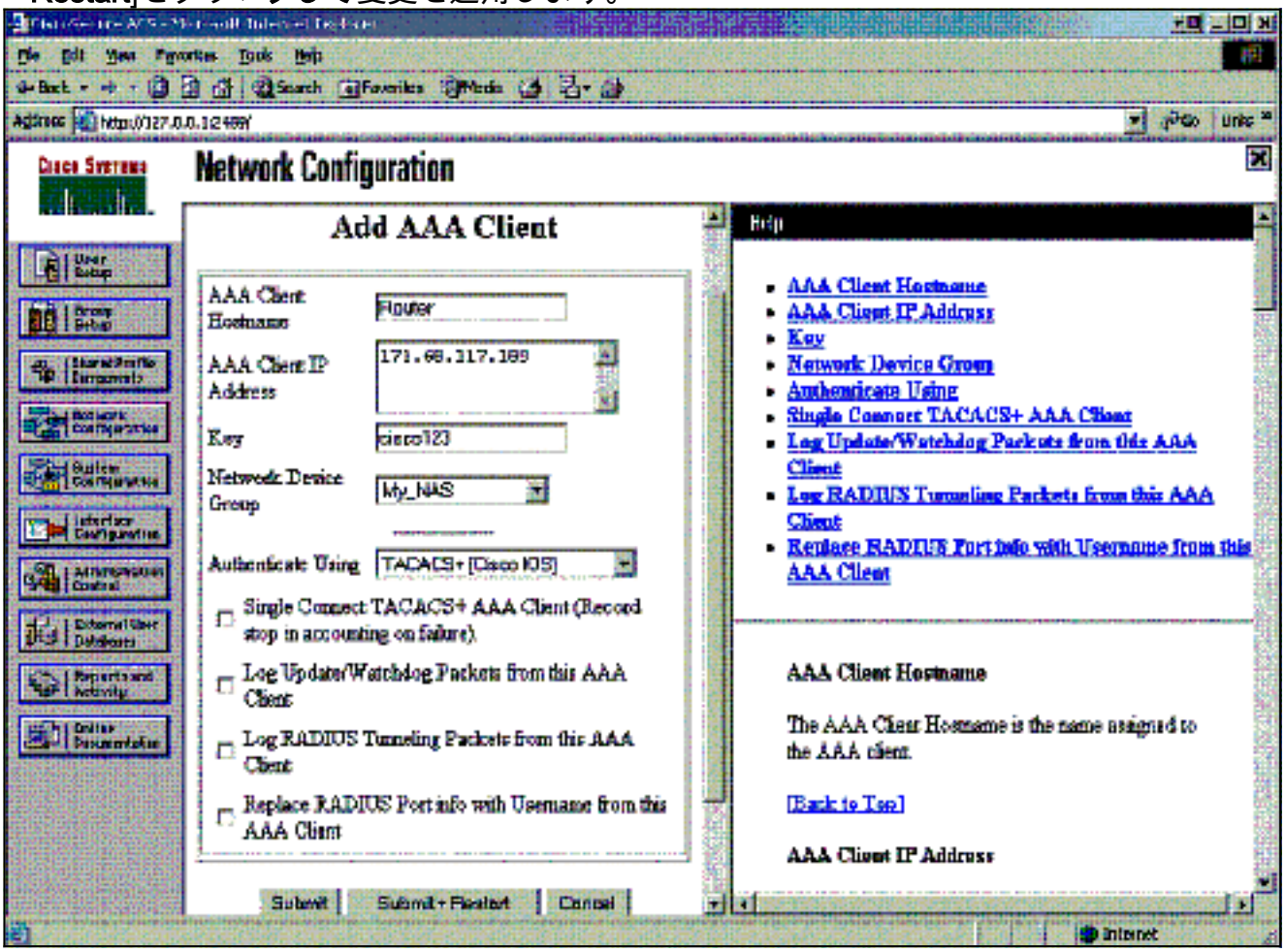
2. Network Configuration をクリックします。[エントリの追加]をクリックして、ネットワークアクセスサーバ(NAS)を含むネットワークデバイスグループを作成します。 グループの名前を入力し、[送信]をクリックします。



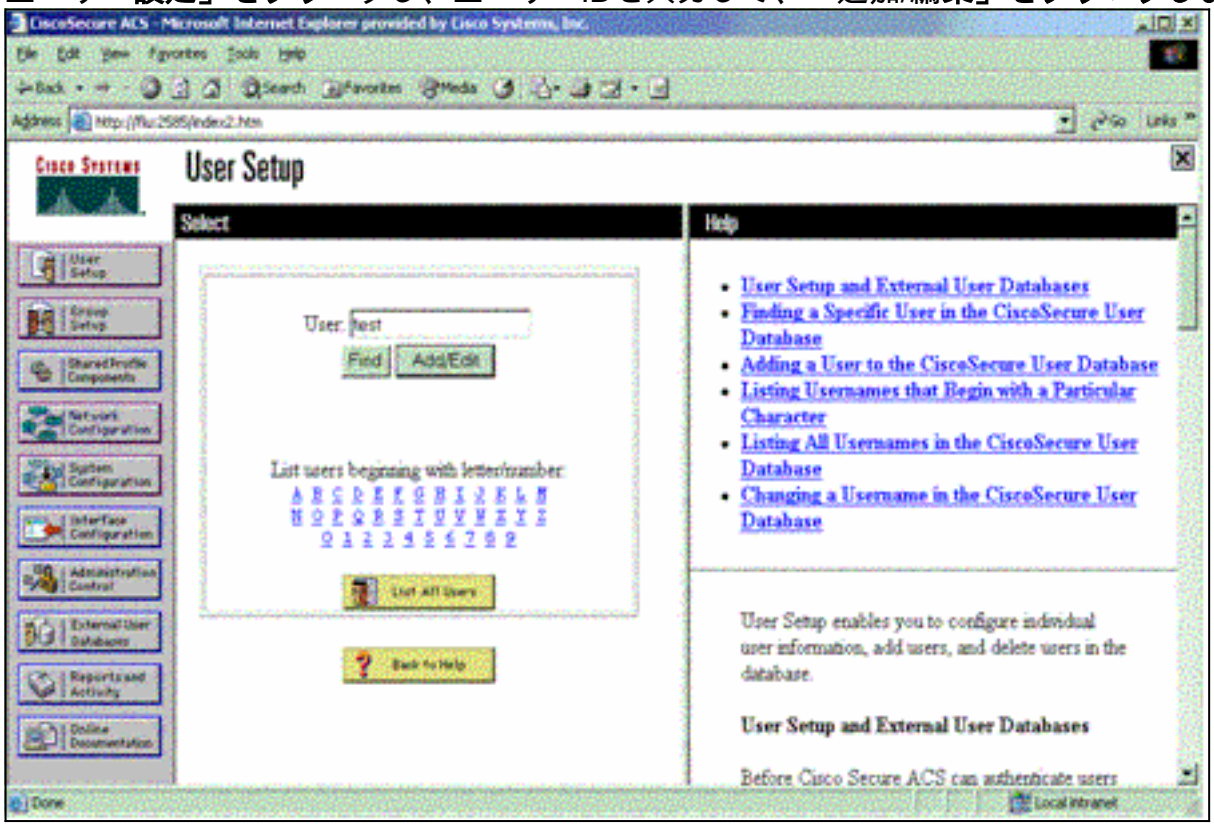
3. [Add Entry] をクリックして、認証、許可、アカウンティング(AAA)クライアント(NAS)を追加します。



4. AAAサーバとNAS間の通信を暗号化するために使用するホスト名、IPアドレス、およびキーを入力します。認証方法として[TACACS+ (Cisco IOS)]を選択します。完了したら、[Submit + Restart]をクリックして変更を適用します。

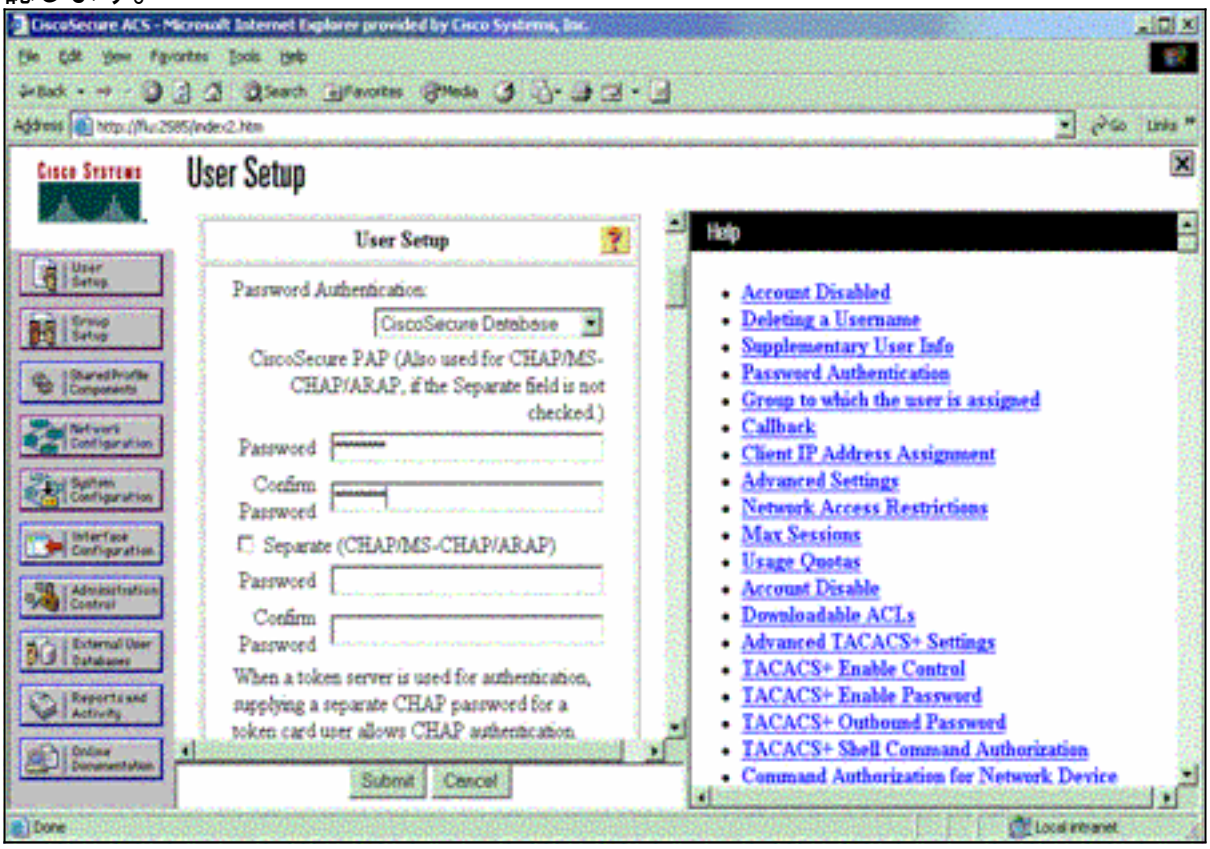


5. 「ユーザー設定」をクリックし、ユーザーIDを入力して、「追加/編集」をクリックします。

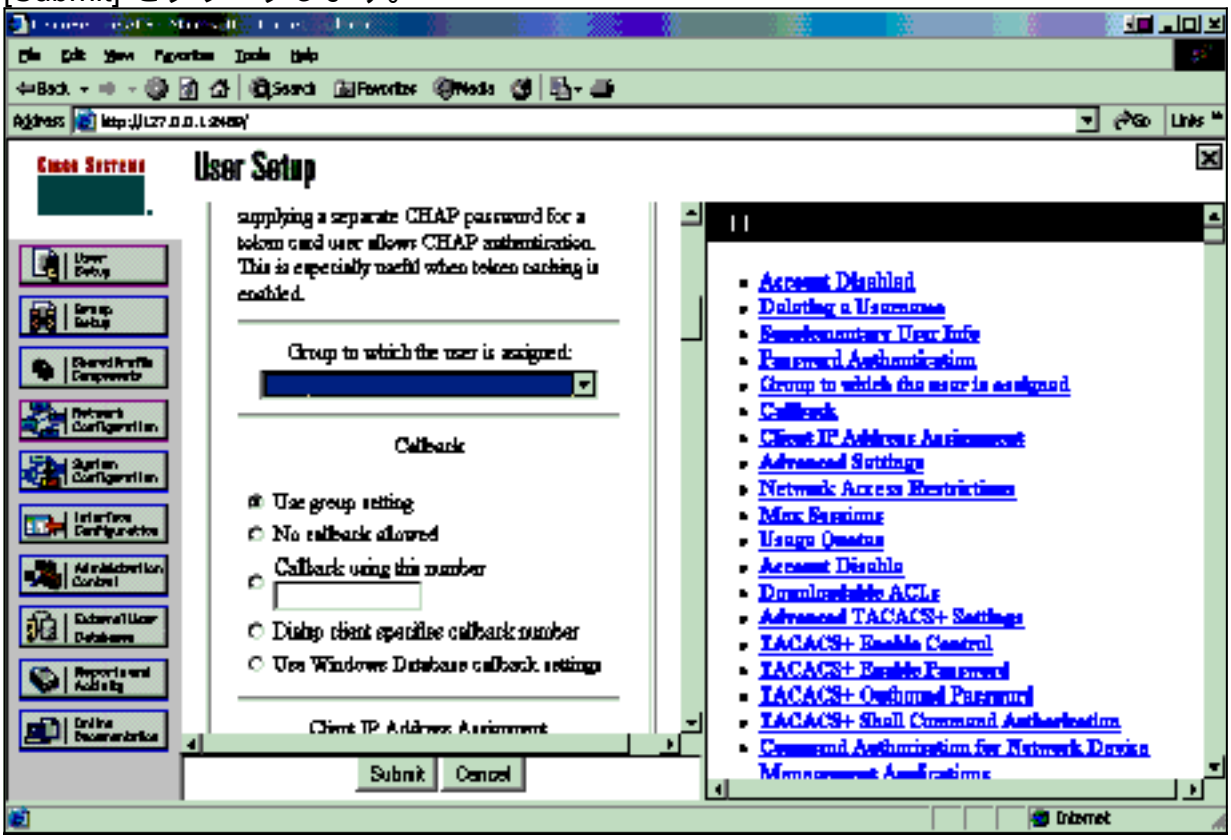


6. ユーザを認証するデータベースを選択します。（この例では、ユーザは「test」、ACSの内部データベースは認証に使用されます）。 ユーザのパスワードを入力し、パスワードを確

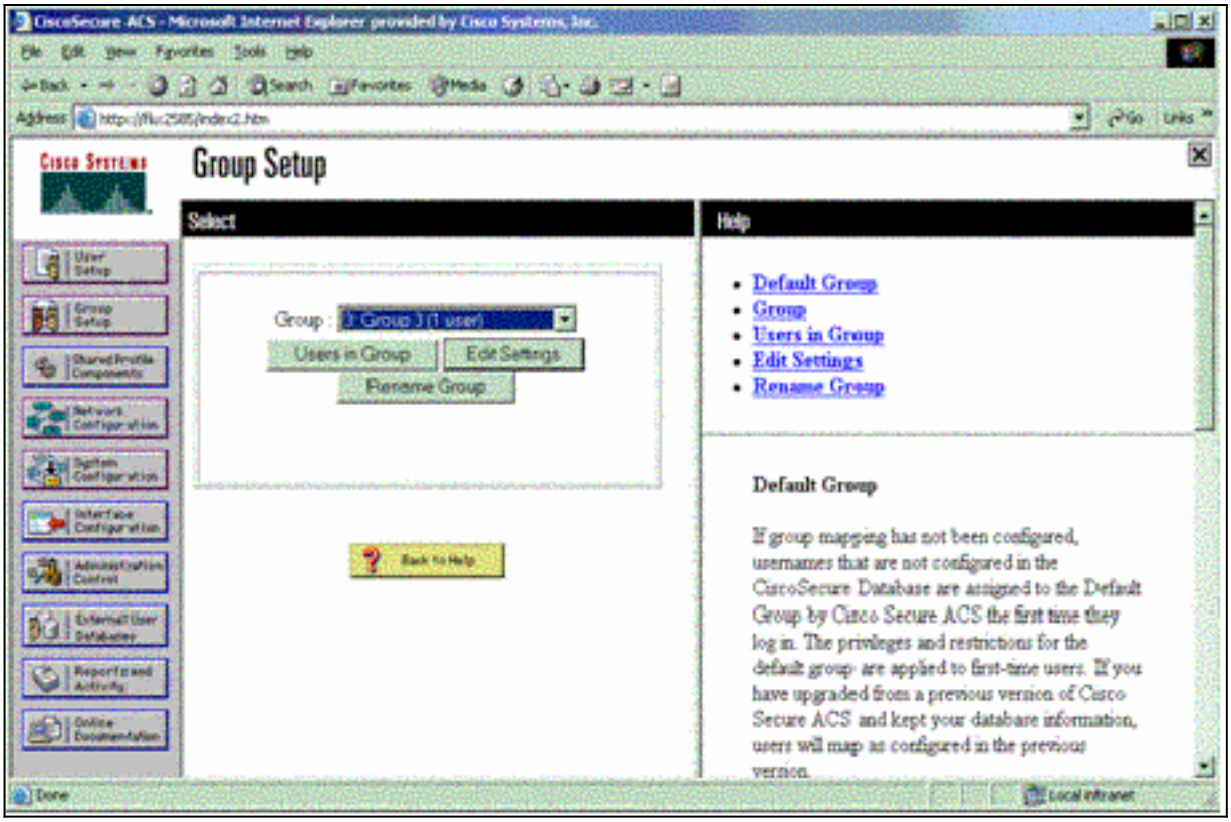
認します。



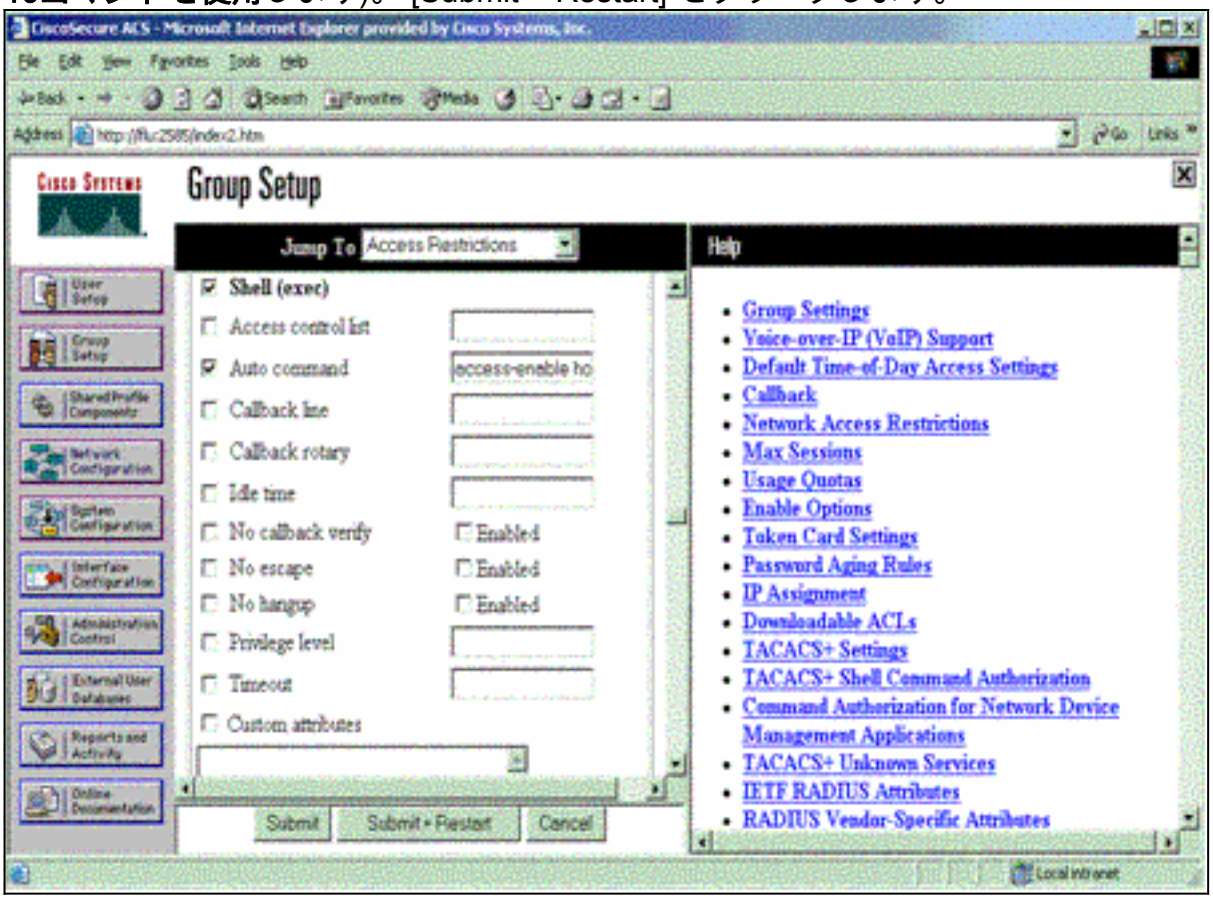
7. ユーザが割り当てられているグループを選択し、[グループ設定を使用]**をオンにします。** [Submit] をクリックします。



8. [グループ設定]**をクリックします。**手順7でユーザーが割り当てられたグループを選択します。[設定の編集]をクリック**します。**



9. [TACACS+ Settings]セクションまでスクロールします。[Shell exec]のチェックボックスを**オンにします**。[自動]コマンドのチェックボックス**をオンにします**。ユーザの認証が成功した場合に実行するauto-commandを入力します。(この例では、**access-enable host timeout 10コマンドを使用**します)。 [Submit + Restart] をクリックします。



TACACS+のトラブルシューティング

NASで次の**debug**コマンドを使用して、TACACS+の問題をトラブルシューティングします。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug tacacs authentication**:TACACS+認証プロセスに関する情報を表示します。一部のバージョンのソフトウェアでのみ使用可能です。使用できない場合は、**debug tacacsのみ使用**します。
- **debug tacacs authorization**:TACACS+認可プロセスに関する情報を表示します。一部のバージョンのソフトウェアでのみ使用可能です。使用できない場合は、**debug tacacsのみ使用**します。
- **debug tacacs events**:TACACS+ヘルパープロセスからの情報を表示します。一部のバージョンのソフトウェアでのみ使用可能です。使用できない場合は、**debug tacacsのみ使用**します。

AAAの問題をトラブルシューティングするには、次のコマンドを使用します。

- **debug aaa authentication**：AAA/TACACS+ 認証に関する情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。

次の**debug**の出力例は、ACS TACACS+サーバでの認証および認可プロセスの成功を示しています。

```
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
```

RADIUS の使用

RADIUSの設定

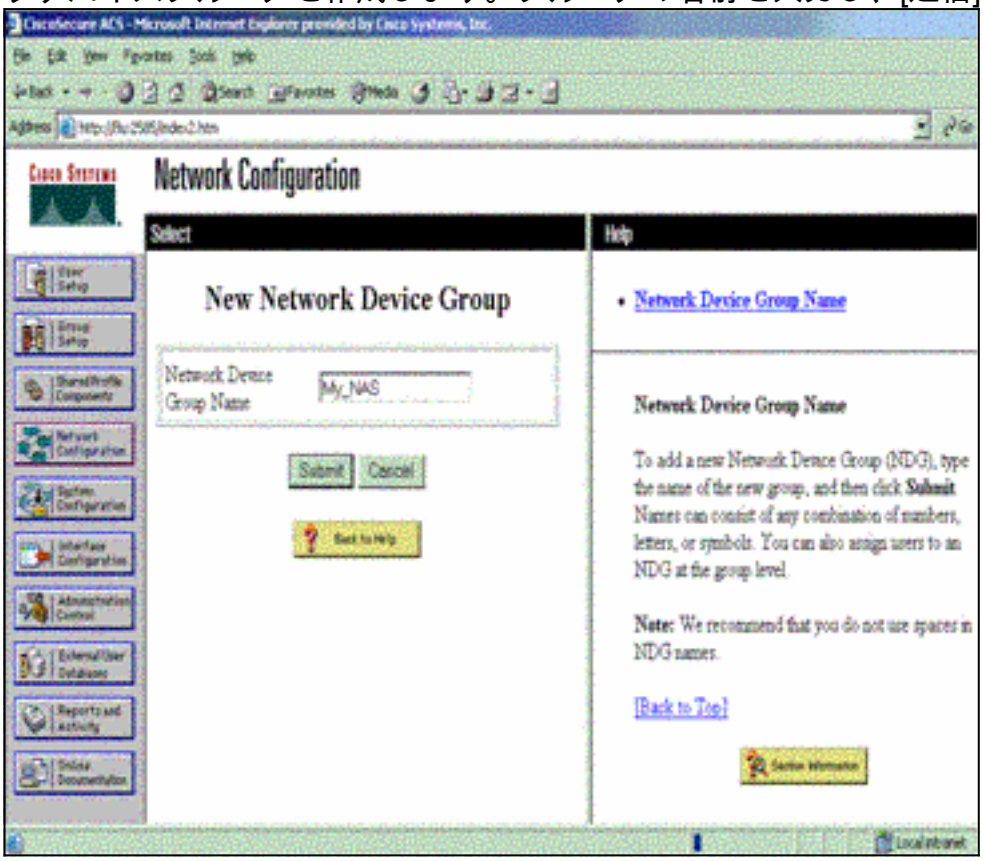
RADIUSを使用するには、次に示すように、RADIUSサーバを設定して、認証パラメータ(autocommand)を使用してRADIUSサーバで認証を強制的に実行し、ベンダー固有の属性26に送信します。

```
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
```

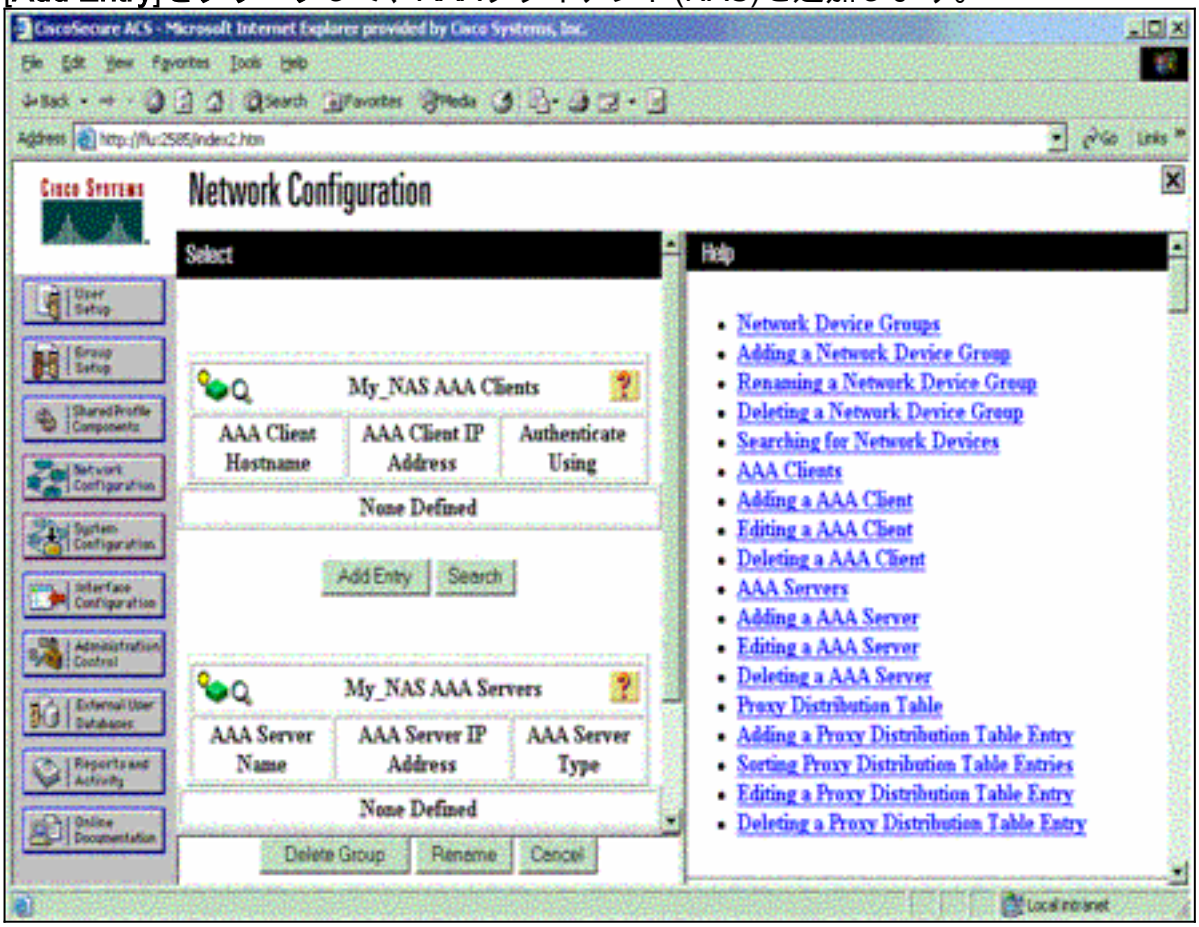
Cisco Secure ACS for WindowsでRADIUSを設定するには、次の手順を実行します。

1. Webブラウザを開き、ACSサーバのアドレスをhttp:// *<IP_address or DNS_name>*:2002の形式で入力します（この例では、デフォルトポート2002を使用します）。 adminとしてログインします。

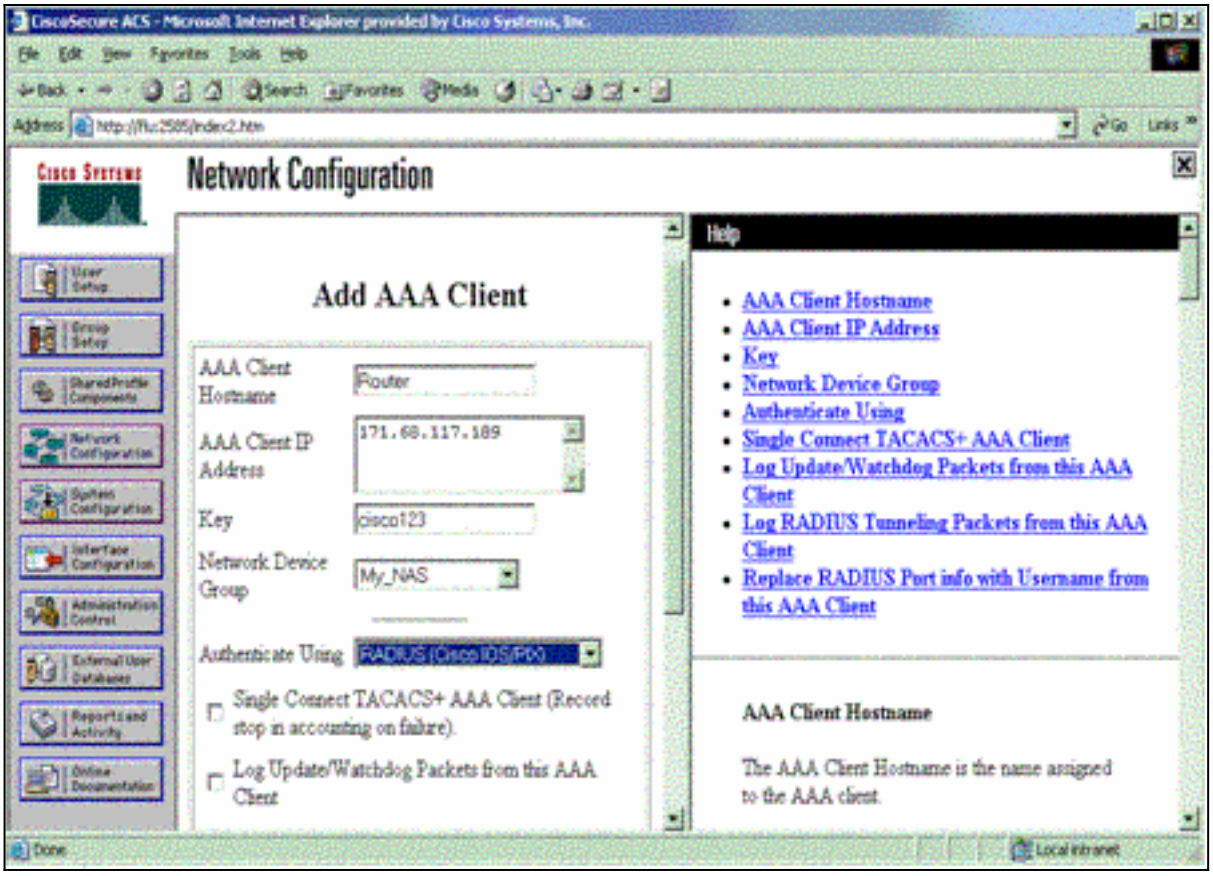
2. Network Configuration をクリックします。[Add Entry]をクリックし、NASを含むネットワークデバイスグループを作成します。グループの名前を入力し、[送信]をクリックします。



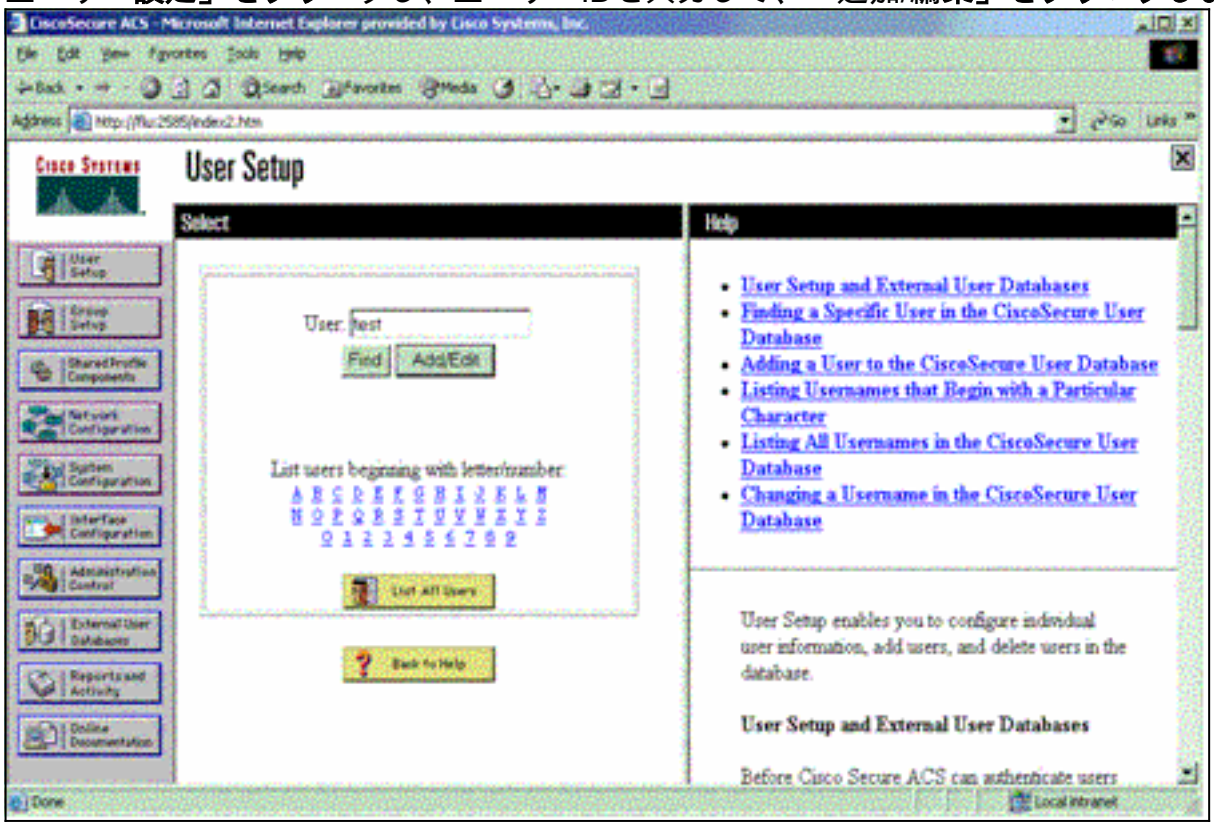
3. [Add Entry]をクリックして、AAAクライアント(NAS)を追加します。



4. AAAサーバとNAS間の通信を暗号化するために使用するホスト名、IPアドレス、およびキーを入力します。認証方法としてRADIUS(Cisco IOS/PIX)を選択します。完了したら、[Submit + Restart]をクリックして変更を適用します。

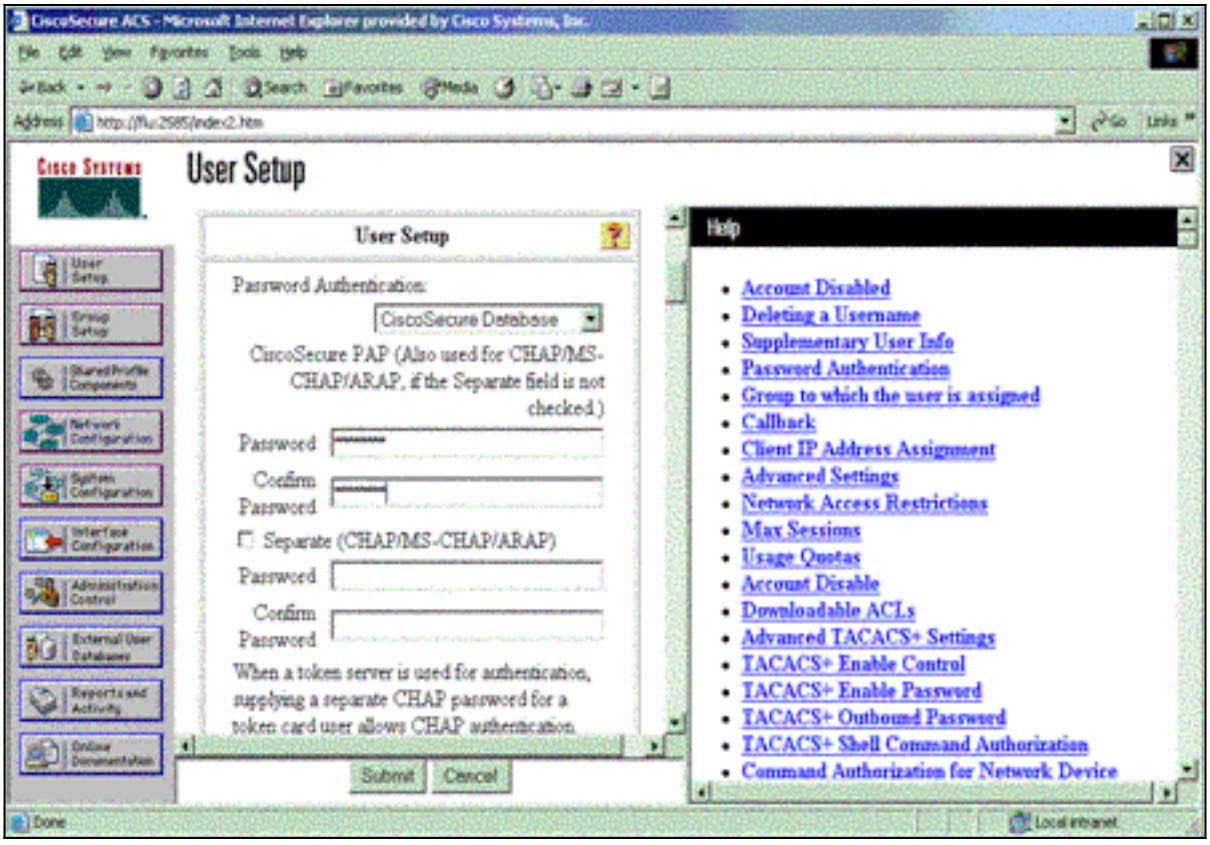


5. 「ユーザー**設定」をクリ**ックし、ユーザーIDを入力して、「追加/**編集」をクリックします**

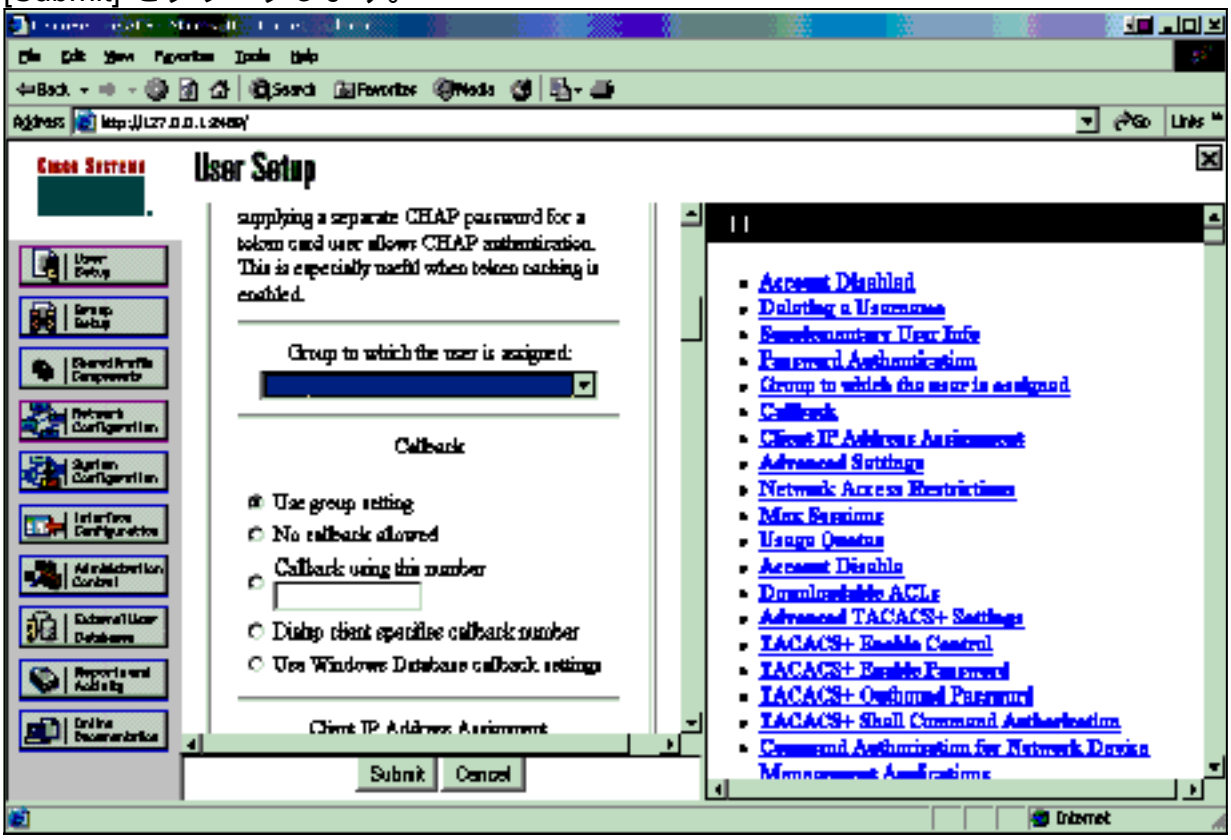


。

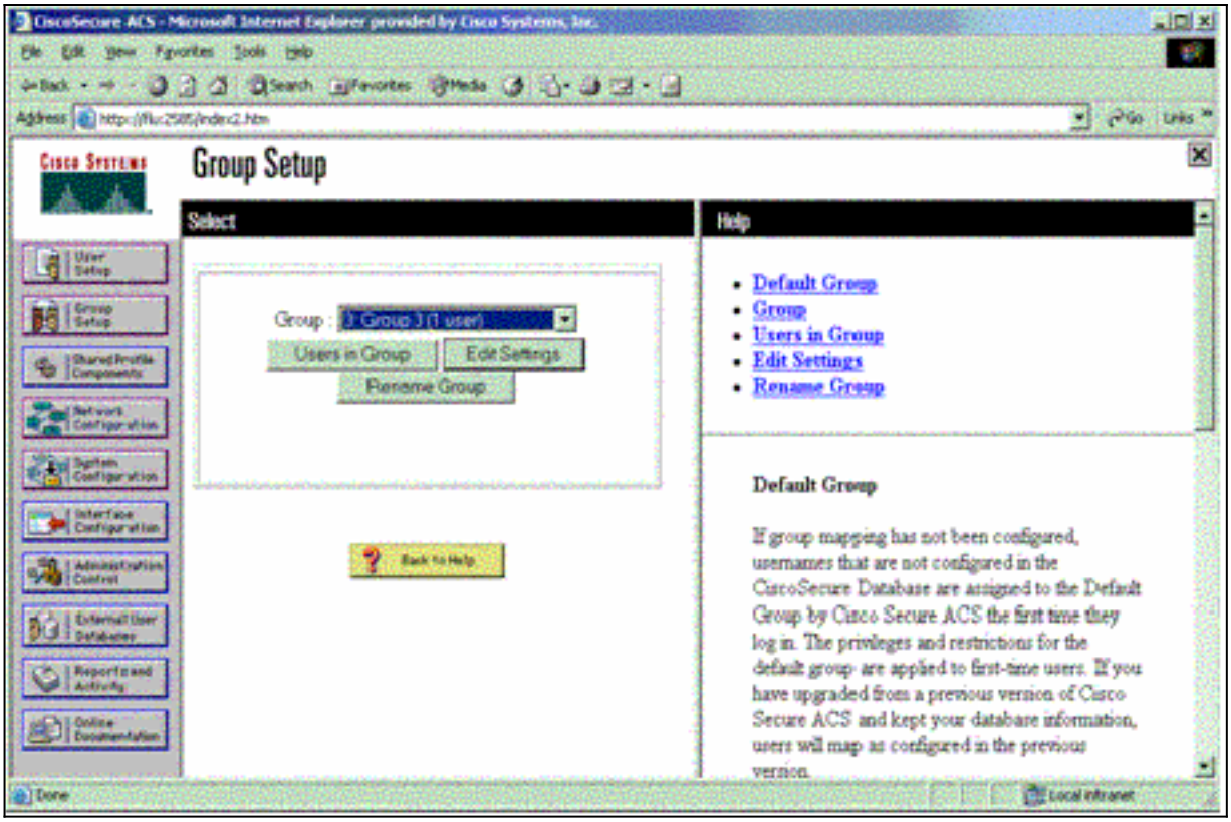
6. ユーザを認証するデータベースを選択します。（この例では、ユーザは「test」、ACSの内部データベースは認証に使用されます）。 ユーザのパスワードを入力し、パスワードを確認します。



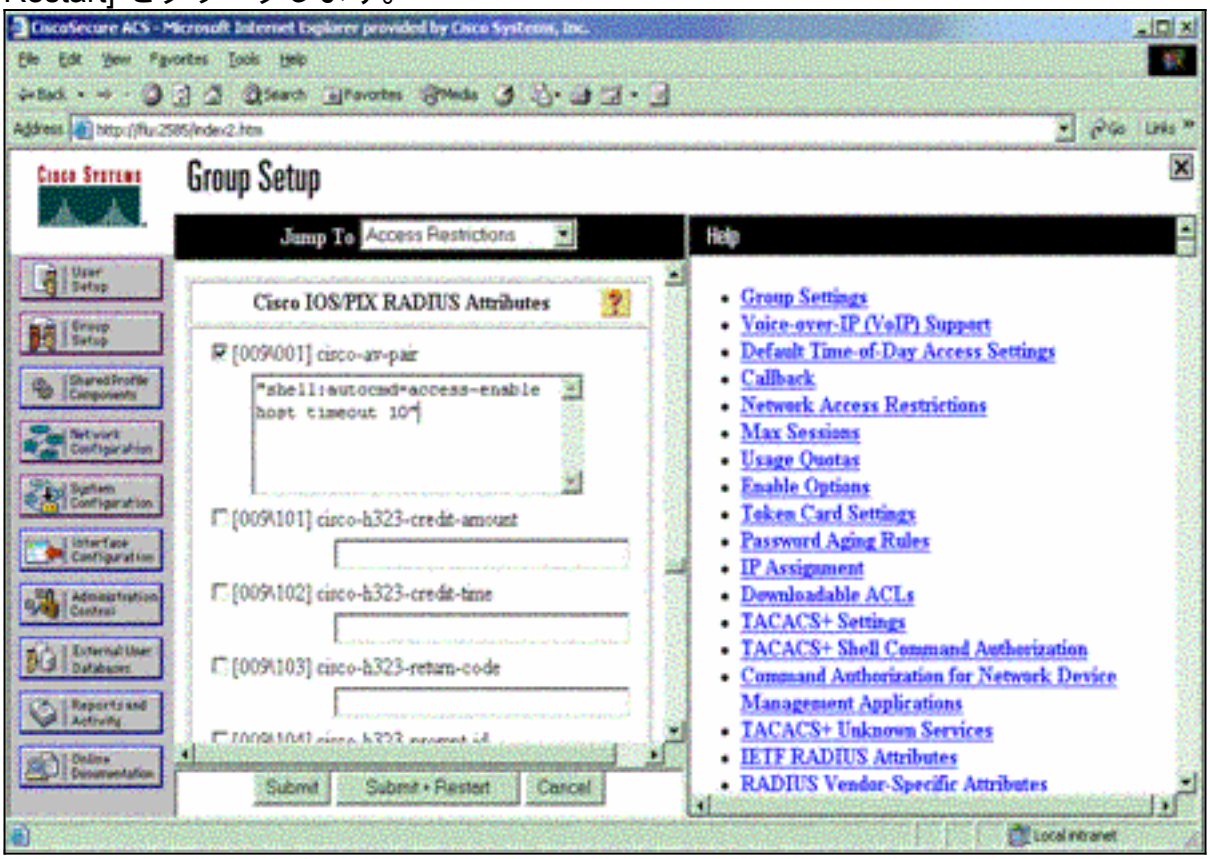
7. ユーザが割り当てられているグループを選択し、[グループ設定を使用]**をオンにします。**[Submit] をクリックします。



8. [グループ**設定]をク**リックし、前の手順でユーザが割り当てられたグループを選択します。[Edit Settings] をクリックします。



9. [Cisco IOS/PIX RADIUS Attributes]セクションまでスクロールダウンします。**cisco**-av-pairのボックス**をオンにします**。ユーザーの**承認**が成功した場合に実行するshellコマンドを入力します。(この例では**shell:autocmd=access-enable host timeout 10を使用します**)。 [Submit + Restart] をクリックします。



RADIUSのトラブルシューティング

NASで次の**debugコマンド**を使用して、RADIUSの問題をトラブルシューティングします。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug radius**:RADIUSに関連する情報を表示します。

AAAの問題をトラブルシューティングするには、次のコマンドを使用します。

- **debug aaa authentication**：AAA/TACACS+ 認証に関する情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。

次の**debug**出力例は、RADIUS用に設定されたACSでの認証および認可プロセスの成功を示しています。

```
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
```

関連情報

- Cisco IOSロックアンドキーセキュリティ
- TACACS/TACACS+ サポート ページ
- IOS での TACACS+ に関するドキュメント
- RADIUS に関するサポート ページ
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems