CiscoSecure 2.x TACACS+のセットアップおよびデバッグ

目次

はじめに

この資料は Cisco Secure TACACS+ 設定のセットアップおよびデバッグの Cisco Secure 2.x ユーザを最初に支援するように意図されています。 それは Cisco Secure 機能の網羅的な記述ではないです。

サーバソフトウェアおよびユーザセットアップに関する完全情報詳細については Cisco Secure ドキュメントを参照して下さい。 router コマンドに関する詳細については適切なリリースのための Cisco IOSソフトウェア ドキュメンテーションを参照して下さい。

前提条件

要件

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure ACS 2.x およびそれ以降
- Cisco IOS ® ソフトウェアリリース 11.3.3 およびそれ以降

表記法

ドキュメント表記の詳細は、『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。

Cisco Secure のセットアップ

次の手順を実行します。

1. UNIXサーバで Cisco Secure コードをインストールするためにソフトウェアと来た手順を使用することを確かめて下さい。
2. 製品が停止し、開始することを確認するために、`/etc/rc0.d` およびルートとして `cd` 、実行します `./K80Cisco` 入力して下さい（デーモンを停止するため）。`/etc/rc2.d` およびルートとして `cd` 、実行します `./S80Cisco` 入力して下さい（デーモンを開始するため）。始動で、メッセージが表示されるはずです（以下を参照）:
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   個々のプロセスのそれぞれの少なくとも 1 つが、たとえば、SQLAnywhere か別のデータベース エンジン、Cisco Secure データベースサーバ プロセス、Netscape Webサーバ、Netscape Web Admin、Acme Webサーバ、Cisco Secure AAA プロセス、またはオート再始動 プロセス実行することをことを確かめるために順序で `$BASE/utils/psg` 実行して下さい。
3. 保証するためにシェル環境の適切なディレクトリ、セットアップ 環境変数およびパスにあって下さい。 c-shell はここでは使用されます。**$BASE は** Cisco Secure がインストールされているインストールの間に選択されるディレクトリです。 それは DOCS のようなディレクトリが、DBServer、CSU、等含まれています。この例では、/opt/CSCOacs のインストールは仮定されます、これはシステムで異なることができます:
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY はデフォルト Cisco Secure データベースがインストールされているインストールの間に選択されるディレクトリです。 製品が付いているデフォルト データベースが、SQLAnywhere、使用されたら、データベースのようなディレクトリが、ドキュメント、等含まれています。この例では、/opt/CSCOacs/SYBSsa50 のインストールは仮定されます、これはシステムで異なることができます。
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   シェル環境のパスをに追加して下さい:
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD への $BASE/config**CSU.cfg は** Cisco Secure サーバ コントロール ファイル**です**。 このファイルのバックアップコピーを撮って下さい。このファイルでは、 `config_license_key` ソフトウェアを購入した場合ライセンス プロセスによって受け取ったライセンスキーを示します; これが 4 ポート トライアル ライセンスである場合、この行を省くことができます。**NAS config_nas_config** セクションはデフォルトネットワーク アクセス サーバ（NAS）またはルータが含まれている場合がありますまたはインストールの間に入力した NAS。 デバッグするためにこの例で、NAS がキーなしで Cisco Secure サーバと通信するように許すできます。 たとえば、NAS の名前を取除けば`/* NAS` 含まれている行からのキーは `*/`」および */*NAS/Cisco セキュア秘密鍵 */*。 そのエリアの唯一のスタンザは読みます:
   ```
   NAS config_nas_config = {
     {
   ```

```
    "",          /* NAS name can go here */
    "",              /* NAS/Cisco Secure secret key */
    "",                          /* message_catalogue_filename */
    1,                           /* username retries */
    2,                           /* password retries */
    1                            /* trusted NAS for SENDPASS */
  }
};

AUTHEN config_external_authen_symbols = {
```

これをするとき、キーの交換無しですべての NAS と話すことができるように Cisco Secure に言います。

5. デバッグ情報を /var/log/csuslog に行ってもらいたい場合するべきかどの位デバッグをサーバに告げる CSU.cfg の上セクションの行がある必要があります。 0X7FFFFFFF はすべての可能性のある デバッグを追加します。 この行をそれに応じて追加するか、または修正して下さい:

```
NUMBER config_logging_configuration = 0x7FFFFFFF;
```

この追加行は local0 にデバッグ情報を送信 します:

```
NUMBER config_system_logging_level = 0x80;
```

また、/etc/syslog.conf ファイルを修正するためにこのエントリを追加して下さい:

```
local0.debug /var/log/csuslog
```

それから再読するために syslogd をリサイクルして下さい:

```
kill -HUP `cat /etc/syslog.pid`
```

Cisco Secure サーバをリサイクルして下さい:

```
/etc/rc0.d/K80Cisco Secure
/etc/rc2.d/S80Cisco Secure
```

それはまだ開始する必要があります。

6. ユーザ、グループ、等、または CSimport ユーティリティを追加するのにブラウザを使用したいと思う場合もあります。 この資料の終わりにフラットファイルのサンプル ユーザは CSimport を使用してデータベースに容易に移動することができます。 これらのユーザはテストの目的で機能し、あなた自身のユーザを得ればそれらを削除することができます。 インポートされる GUI によってインポートされたユーザに会う場合があれば。CSimport を使用することにすれば:

```
CD $BASE/utils
```

どこでもシステムのようなファイルにこの資料の終わりにユーザおよびグループ プロファイルを置いて下さい、そしてとして $BASE/utils ディレクトリから、およびユーザルート セキュア実行することは、デーモン テスト (- t) オプションと、たとえば、/etc/rc2.d/S80Cisco の CSimport を実行します:

```
./CSimport -t -p <path_to_file> -s <name_of_file>
```

これはユーザ向けに構文をテストします; メッセージを受け取る必要があります (以下を参照) :

```
Secure config home directory is: /opt/CSCOacs/config/CSConfig.ini
hostname = berry and port = 9900 and clientid = 100
/home/ddunlap/csecure/upgrade.log exists, do you want to write over 'yes' or 'no' ?
yes
Sorting profiles...
Done sorting 21 profiles!
Running the database import test...
```

メッセージを受け取らないで下さい (以下を参照) :

```
Error at line 2: password = "adminusr"
Couldn't repair and continue parse
```

エラーがあったかどうか、チェックされるプロファイルを確かめるために upgrade.log を検査して下さい。 エラーが $BASE/utils ディレクトリから、動作していてデーモンが (/etc/rc2.d/S80Cisco は保護します) 、およびユーザルートとして、訂正されたら、データ

ベースにユーザを移動する託 (- c) オプションと CSimport を実行して下さい:

```
./CSimport -c -p <path_to_file> -s <name_of_file>
```

再度、画面にまたは upgrade.log にエラーがないはずです。

7. サポート された ブラウザは Cisco Secure 互換性 テクニカル ティップにリストされています。 PC ブラウザから、Cisco Secure/Solarisボックス **http://#** へのポイント。**#.#.#.# が** Cisco Secure/Solaris サーバの IP であるところ **#.#.#/cs**。画面で、なぜならユーザは現われるパスワードのための**スーパーユーザを**入力し、**changeme を**入力して下さい。 パスワードをこの時点で変更しないで下さい。 前の手順で CSimport を使用するか、または参照ブロックを消し、GUI によって手動で ユーザおよびグループを追加できれば場合追加されるユーザ/グループに会うはずです。

認証のセットアップ

注: このルータコンフィギュレーションは Cisco IOS Software release 11.3.3 を実行するルータで作成されました。 Cisco IOS ソフトウェア リリース 12.0.5.T およびそれ以降は **tacacs** の代りに **グループ tacacs を**示します。

この時点で、ルータを設定して下さい。

1. ルータを設定する間、Cisco Secure を止めて下さい。

```
/etc/rc0.d/K80Cisco Secure to stop the daemons.
```

2. ルータで、TACACS+ を設定し始めて下さい。 モードを enable と入力し、設定 される コマンドの前に `conf t` 入力して下さい。 この構文は*最初に* Cisco Secure を提供するルータからロックアウトされない動作していないことを確認します。 `ps - ef` 入力して下さい | チェックするために Cisco Secure を次のとおりである場合動作しなくて、プロセス kill -9:

```
!--- Turn on TACACS+ aaa new-model enable password whatever !--- These are lists of
authentication methods, !--- that is, vtymethod and conmethod are !--- names of lists, and
the methods listed on the !--- same lines are the methods in the order to be !--- tried. As
used here, if authentication !--- fails due to Cisco Secure not being started, !--- the
enable password is accepted !--- because it is in each list. aaa authentication login
vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable !--- Point the
router to the server, that is, !--- #.#.#.# is the server IP address. tacacs-server host
#.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !---
during debugging. exec-timeout 0 0 login authentication conmethod line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0
0 login authentication vtymethod
```

3. 次に進む前に、Telnet およびコンソール ポート経由で引き続きルータへアクセスできること確認します。 Cisco Secure が動作していないので、イネーブルパスワードは受け入れる必要があります。**注意：** コンソールポートセッション アクティブを保存し、イネーブル モードに残して下さい; このセッションは時間を計るべきではありません。 ルータにアクセスをこの時点で制限し始め、あなた自身をロックしないでコンフィギュレーション変更を行なえます必要があります。ルータでサーバ ツー ルータの相互対話を確認するためにこれらのコマンドを発行して下さい:

```
terminal monitor
debug aaa authentication
```

4. ルートとして、サーバの Cisco Secure を開始して下さい:

```
/etc/rc2.d/S80Cisco Secure
```

そうこれはプロセスを開始しますが、セキュア S80Cisco で設定されるよりより多くのデバッグを有効にしたいと思います:

```
ps -ef | grep Cisco Secure
kill -9 <pid_of CS_process>
```

```
CD $BASE/CSU
./Cisco Secure -cx -f $BASE/config/CSU.cfg to start the Cisco Secure process with debugging
```

を使って- x オプションは、前景の Cisco Secure 実行従ってサーバ 相互対話へのルータ観察することができます。 エラーメッセージが表示されないで下さい。 CiscoSecureプロセスは- x オプションが原因でそこに開始し、ハングさせる必要があります。

5. 別のウィンドウから、開始する確実な Cisco Secure であるためにチェックして下さい。 `ps - ef` 入力し、CiscoSecureプロセスを探して下さい。
6. Telnet （ VTY ）ユーザは今 Cisco Secure を通って認証を受けなければならない必要があります。 ルータのデバッグを使って、ネットワークの他の一部からのルータへの Telnet。 ルータはユーザ名 および パスワード プロンプトを生成 する必要があります。 これらのユーザid/パスワード組み合わせを用いるルータにアクセスできるはずです:

   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```

   ところで送信 される何がサーバをおよび、応答および要求、等相互対話を、すなわち確認する、はずであるルータを監視して下さい。 問題がある場合は修正してから次へ進みます。
7. またユーザ向けにイネーブル モードに得るために Cisco Secure を通って認証し確かめるためにたいと思えばコンソールポートセッションは今でもアクティブアクティブこのコマンドをルータに追加するためにであり、:

   ```
   !--- For enable mode, list 'default' looks to Cisco Secure !--- then enable password if
   Cisco Secure is not running. aaa authentication enable default tacacs+ enable
   ```
8. 今 Cisco Secure を通って**有効に ならなければ**ならない必要があります。 ルータのデバッグを使って、ネットワークの他の一部からのルータへの Telnet。 ルータが username/password を頼むとき /と応答して下さい。ユーザー定義演算子がパスワード「モード（ 15 ）特権レベルを enable と入力することを試みるとき cisco」が必要となります。 他のユーザは特権レベル文できません（ または Cisco Secure デーモン ）なしでモードを enable と入力。ところで送信 されて いる何がサーバをおよびたとえば、応答および要求、等 Cisco Secure 相互対話を確認するはずであるルータを監視して下さい。 続く前に問題を訂正して下さい。
9. Cisco Secure がダウンしている場合ユーザはまだルータにアクセスできることを確かめるためにコンソールポートにまだ接続されて間サーバの CiscoSecureプロセスをダウンさせて下さい:

   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```

   前の手順で行った Telnet と enable を繰り返します。 ルータは CiscoSecureプロセスが応答しないし、ユーザがデフォルト イネーブルパスワードとログインし、有効に なることを可能にすることを認識する必要があります。
10. 始動は Cisco Secure を通って認証する必要がある USERID/パスワード **オペレータ/オペレーション**を用いるルータに Cisco Secure を通ってコンソールポート ユーザの認証があるように確認するために再度 Cisco Secure サーバ Telnetセッションを設定し。 remain ルータに Telnet で接続し、イネーブル モードでコンソールポートからルータにコンソールポートからルータに、たとえば、元の接続のログアウト ログインできることをことを確かめるまでそしてコンソールポートに再接続して下さい。 前の USERID/パスワード組み合わせの使用とログインするコンソールポート認証は Cisco Secure を通って今あるはずです。 たとえば、USERID/パスワード **オペレータ/オペレーション**それからパスワード **cisco は有効に なるために**使用されなければなりません。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

認可の追加

認可の追加はオプションです。

デフォルトでは、ルータには次の 3 つのコマンド レベルがあります。

- ディセーブル、イネーブル終了、ヘルプおよびログアウトが含まれている特権レベル 0
- 特権レベル 1 — Telnet およびプロンプトで水平な標準は `router>` 言います
- 特権レベル 15 —レベルを有効にすればプロンプトは `router#` 言います

利用可能 なコマンドが Cisco IOSフィーチャセットによって、Cisco IOS ソフトウェア リリース、ルータのモデル、等決まるので、すべてのコマンドの一覧はレベル 1 および 15 にありません。 たとえば、**show ipx route は** NAT がその時に導入されなかった、**show environment は**電源および温度 モニタリングなしでルータモデルにありませんので **IP NAT が** Cisco IOS ソフトウェア リリース 10.2.X コードに **TRANS** ないことを**示します** IP 機能セットだけで現在であることではないし。

特定のレベルで特定のルータで利用可能 なコマンドは入力しています a を見つけることができます**か。** ルータのプロンプト場合のその特権レベルで。

コンソールポート許可は機能として CSCdi82030 が設定されているまで追加されませんでした。コンソールポート許可はデフォルトでルータからロックアウトされる確率を偶然減すこと消えています。 ユーザがコンソールを通じて物理的にアクセスできる場合は、コンソール ポート認証はあまり効果的ではありません。 しかし、コンソールポート許可は CSCdi82030 が**許可 exec default** と設定された Cisco IOSイメージの **line con 0 コマンド**の下でつけることができます **|WORD** コマンド。

次の手順を実行します。

1. ルータは Cisco Secure まったく承認するためにかいくつかのレベルを通してコマンドを設定することができます。 次のルータ設定では、すべてのユーザに、サーバ上でのコマンド単位の認証の設定を許可しています。 Cisco Secure を通してすべてのコマンドを承認できますサーバがダウンしていれば、許可は必要、それ故にではないです。Cisco Secure サーバによって、これらのコマンドを入力して下さい:そのイネーブル 認証が Cisco Secure を通して実行される要件を取除くためにこのコマンドを入力して下さい:
   ```
   no aaa authentication enable default tacacs+ none
   ```
   コマンド許可が Cisco Secure を通して行われることを必要とするためにこれらのコマンドを入力して下さい:
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. Cisco Secure サーバが動作する間、USERID/パスワード **loneusr/lonepwd** でルータに Telnet で接続して下さい。 このユーザはコマンドを以外されませんべきであるはずです:
   ```
   show version
   ping <anything>
   logout
   ```
   以前のユーザは、**adminusr/adminusr**、まだ**オペレータ/オペレーション**、**desusr/暗号化**、 = によってすべてのコマンドをされますはずです。 プロセスに問題がある場合、ルータのモ

ードを enable と入力し、このコマンドで許可 デバッグをつけて下さい:

```
terminal monitor
debug aaa authorization
```

ところで送信 される何がサーバをおよびたとえば、応答および要求、等 Cisco Secure 相互対話を確認するはずであるルータを監視して下さい。 問題がある場合は修正してから次へ進みます。

3. ルータは Cisco Secure を通して EXECセッションを承認するために設定することができます。 **aaa authorization exec デフォルト TACACS+ はどれも** EXECセッションのための協会 TACACS+ 許可を命じません。これを適用する場合、ユーザ**時間/時間**、**telnet/telnet**、**todam/todam**、**todpm/todpm** および **somerouters/somerouters に**影響を与えます。 ルータにこのコマンドを追加した、ルータにユーザ**時間/時間**として Telnet で接続する後、EXECセッションは 1 分 (設定 された タイムアウト = 1) の間開いている残ります。 **telnet/telnet** ユーザはルータを入力しますが、他のアドレス (設定 された autocmd = 「telnet 171.68.118.102") にすぐに送信 されます。 ユーザ **todam/todam** および **todpm/todpm が**何時にテスト日のの間にあるか依存するルータにアクセスできたりまたはことは可能性のあるです。 ユーザ **somerouters は**ネットワーク 10.31.1.x からのルータ koala.rtp.cisco.com にだけ Telnet で接続できます。 Cisco Secure はルータの名前を変換することを試みます。 IP アドレス 10.31.1.5 を使用する場合、解像度が起こらなければ、そしてネーム コアラを使用すれば有効です、解像度がある場合有効なら。

アカウンティングの追加

アカウンティングの追加はオプションです。

1. 会計はルータが Cisco IOS ソフトウェア リリース 11.0 より Cisco IOS ソフトウェア リリース 以降を実行する場合ルータで設定されて起こりません。 ルータの会計をイネーブルにすることができます:

```
aaa accounting exec default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
aaa accounting network default start-stop tacacs+
aaa accounting system default start-stop tacacs+
```

注: コマンド アカウンティングは Cisco バグ ID CSCdi44140 で壊れていました、これが固定であるイメージを使用すれば、コマンド アカウンティングはまた有効に することができます。

2. ルータにアカウンティング レコード デバッグを追加して下さい:

```
terminal monitor
debug aaa accounting
```

3. コンソールのデバッグはユーザ ログインとしてサーバを入力するアカウンティング レコードを示す必要があります。
4. アカウンティング レコードを、ルートとして取得するため:

```
CD $BASE/utils/bin
./AcctExport <filename> no_truncate
```

`no_truncate` データがデータベースで保たれることを意味します。

ダイヤルアップユーザの追加

次の手順を実行します。

1. ダイヤル式ユーザを追加する前にことを Cisco Secure 作業の他の機能確かめて下さい。 Cisco Secure サーバおよびモデムがこのポイントの前にはたらかなかった場合、このポイン

トの後ではたらきません。

2. ルータコンフィギュレーションにこのコマンドを追加して下さい:

```
aaa authentication ppp default if-needed tacacs+
aaa authentication login default tacacs+ enable
aaa authorization network default tacacs+
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
```

インターフェイスコンフィギュレーションは異なります、認証が実行されるが、ダイヤルイン回線はこれらのコンフィギュレーションとこの例で、使用されますかによって決まる:

```
interface Ethernet 0
ip address 10.6.1.200 255.255.255.0
! !--- CHAP/PPP authentication user: interface Async1 ip unnumbered Ethernet0 encapsulation
ppp async mode dedicated peer default ip address pool async no cdp enable ppp
authentication chap ! !--- PAP/PPP authentication user: interface Async2 ip unnumbered
Ethernet0 encapsulation ppp async mode dedicated peer default ip address pool async no cdp
enable ppp authentication pap ! !--- login authentication user with autocommand PPP:
interface Async3 ip unnumbered Ethernet0 encapsulation ppp async mode interactive peer
default ip address pool async no cdp enable ip local pool async 10.6.100.101 10.6.100.103
line 1 session-timeout 20 exec-timeout 120 0 autoselect during-login script startup default
script reset default modem Dialin transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 2 session-timeout 20 exec-timeout 120 0 autoselect
during-login script startup default script reset default modem Dialin transport input all
stopbits 1 rxspeed 115200 txspeed 115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect ppp script startup default script
reset default modem Dialin autocommand ppp transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! access-list 101 deny icmp any any
```

3. Cisco Secure のユーザファイルから:chapuser - CHAP/PPP —ユーザは Line 1 でダイヤルインします; アドレスは**ピアデフォルトIPアドレスプール async およびルータの IPローカルプールasync 10.6.100.101 10.6.100.103** によって割り当てられますchapaddr - CHAP/PPP —ユーザは Line 1 でダイヤルインします; アドレス 10.29.1.99 はサーバによって割り当てられますchapacl - CHAP/PPP —ユーザは Line 1 でダイヤルインします; アドレス 10.29.1.100 はサーバによって割り当てられ、（ルータで定義する必要がある）インバウンドアクセスリスト 101 は適用しますpapuser - PAP/PPP —ユーザは Line 2 でダイヤルインします; アドレスは**ピアデフォルトIPアドレスプール async およびルータの IPローカルプールasync 10.6.100.101 10.6.100.103** によって割り当てられますpapaddr - PAP/PPP —ユーザは Line 2 でダイヤルインします; アドレス 10.29.1.98 はサーバによって割り当てられますpapacl - PAP/PPP —ユーザは Line 2 でダイヤルインします; アドレス 10.29.1.100 はサーバによって割り当てられ、ルータで定義する必要があるインバウンドアクセスリスト 101 は適用します、loginauto —ユーザは Line 3 でダイヤルインします; 行の autocommand でログイン認証は PPP 接続にユーザを強制し、プールからのアドレスを割り当てます

4. すべてのユーザ向けの Microsoft Windows Setup はユーザ loginauto を除外しますStart > Programs > Accessories > Dial-Up Networking の順に選択 して下さい。Connections > Make New Connection の順に選択 して下さい。 接続の名前を入力して下さい。モデム別の情報を入力して下さい。 **設定 > 一般**で、モデムの最高速度を選択して下さい、しかしこれの下でボックスをチェックしないで下さい。**設定 > 接続**では、8 データビット、no parity および 1 つのストップ・ビットを使用して下さい。 コール プリファレンスは**ダイヤルする前に 200 秒後に接続されなくてダイヤルトーンのための待機、コールを取り消します**。高度で、**ハードウェアフロー制御だけ**および**変調タイプ規格を**選択して下さい。**設定 > オプション**では、何も Status Control の下でを除いてチェックする必要がありません。 [OK] をクリックします。Next ウィンドウで、宛先の電話番号を入力し、そして『Next』 をクリック し、それから『Finish』 をクリック して下さい。新しい接続 アイコンが現われたら、それを右クリックし、『Properties』 を選択 し、それから『Server Type』 をクリック して下さい。『PPP』 を選択 して下さい: **WINDOWS 95 は、WINDOWS NT 3.5、インターネット**高度オプションをチェックしないし。許可されたネットワークプロトコルでは、少なくとも

TCP/IP をチェックして下さい。TCP/IP 設定の下で、サーバの割り当てたネームサーバアドレス リモートネットワークの『Server assigned IP address』 を選択 して下さいおよび**使用デフォルト ゲートウェイ。** [OK] をクリックします。始動にダイヤルするためにアイコンを Connect To ウィンドウ ダブルクリックするときユーザネームおよび Password フィールドを記入して下さい次に**接続応答を**クリックします。

5. ユーザ loginauto のために設定される Microsoft Windows 95ユーザ loginauto のための設定は、autocommand PPP で認証ユーザ、**設定の > Options ウィンドウ**を除く他のユーザのためと同じです。 **Bring up terminal window after dialing をチェックして下さい。始動にダイヤルするためにアイコンを Connect To ウィンドウ ダブルクリックするときユーザネームおよび Password フィールドを記入しません。 現われる黒い ウィンドウのユーザ名 および パスワードを『Connect』 をクリック し、ルータへの接続がなされた後、打ち込んで下さい。認証の後で、Continue(F7) をクリックして下さい。**

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

サーバ

```
./Cisco - cx - f $BASE/CSU $BASE/config/CSU.cfg
```

ルータ

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

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。 特定のコマンドに関する詳細については、Cisco IOS Debug コマンド レファレンスを参照して下さい。

- **terminal monitor** —現在のターミナルおよびセッションのための **debug コマンドの出力**およびシステム エラー メッセージを表示する。
- **debug ppp negotiation**：PPP の開始時に送信される PPP パケットを表示します。PPP の開始時には PPP オプションがネゴシエートされます。
- **debug ppp packet** —送信され、受信される PPP パケットを表示する。 このコマンドは低レベルのパケット ダンプを表示します。
- **debug ppp chap** — トラフィックの情報および Challenge Authentication Protocol（CHAP）を設定するインターネットワークの交換を表示する。
- どんな認証方式が使用され、ものこれらのメソッドの結果がであるか **debug aaa authentication** —参照して下さい。
- **debug aaa authorization** —許可のどんなメソッドが使用され、ものこれらのメソッドの結果がであるか参照して下さい。

Cisco Secure ユーザファイル

```
group = admin {
        password = clear "adminpwd"
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

group = oper {
        password = clear "oper"
        privilege = clear "cisco" 15
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

user = adminusr {
        password = clear "adminusr"
        default service = permit
        }

user = desusr {
        password = des "QjnXYd1kd7ePk"
        default service = permit
        }

user = operator {
        member = oper
        default service = permit
        }

user = time {
        default service = permit
        password = clear "time"
        service = shell  {
                set timeout = 1
                default cmd = permit
                default attribute = permit
        }
}

user = todam {
        password = clear "todam"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 0600 - 1200
        }
        }

user = todpm {
        password = clear "todpm"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 1200 - 2359
        }
        }
```

```
user = telnet {
        password = clear "telnet"
        service = shell  {
                set autocmd = "telnet 171.68.118.102"
                        }
        }

user = limit_lifetime {
        password = clear "cisco" from
        "2 may 2001" until
        "4 may 2001"
        }

user = loneusr {
        password = clear "lonepwd"
        service = shell  {
                cmd = show {
                permit "ver"
                }
                cmd = ping {
                permit "."
                }
                cmd = logout {
                permit "."
                }
        }
}

user = chapuser {
        default service = permit
        password = chap "chapuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = chapaddr {
        password = chap "chapaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.99
                }
        }
}

user = chapacl {
        default service = permit
        password = chap "chapacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = papuser {
```

```
        default service = permit
        password = pap "papuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = papaddr {
        default service = permit
        password = pap "papaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.98
                }
        }
}

user = papacl {
        default service = permit
        password = chap "papacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = loginauto {
        default service = permit
        password = clear "loginauto"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        }
        }
 }

user = somerouters {
   password = clear "somerouters"
   allow koala ".*" "10\.31\.1\.*"
   allow koala.rtp.cisco.com ".*" "10\.31\.1\.*"
   allow 10.31.1.5 ".*" "10\.31\.1\.*"
   refuse ".*" ".*" ".*"
   service=shell {
   default cmd=permit
   default attribute=permit
   }
   }
```

関連情報

- Cisco Secure ACS for UNIX 製品サポート
- セキュリティ製品に関する Field Notice (Cisco Secure UNIX を含む)