TACACS+ を使用したダイヤル認証のための Cisco ルータの設定

目次

概要
前提条件
要件
使用するコンポーネント
表記法
設定
Microsoft Windows Setup
ユーザ1 および2 向けのMicrosoft Windowsセットアップ
手順説明
ユーザ3 向けのMicrosoft Windowsセットアップ
確認
トラブルシューティング
ルータ
server
関連情報

概要

この資料に UNIX で動作する TACACS+ でダイヤル認証のための Ciscoルータを設定する方法を記述されています。 TACACS+ は商用化された Cisco Secure ACS for Windows か Cisco Secure ACS for UNIX 同様に多くの機能を提供しません。

これまでシスコから提供されていた TACACS+ は提供が終了しており、シスコのサポートの対象外になっています。

現在は、任意のインターネット検索エンジンで「TACACS+ フリーウェア」を検索すると、フリーウェア バージョンの TACACS+ が多数見つかります。 シスコでは、特定の TACACS+ フリーウェア の実装を推奨することは特にしていません。

Cisco Secure Access Control Server（ACS）は通常のシスコ営業担当者および世界各地の販売チャネルを通じて購入できます。 Cisco Secure ACS for Windows には、Microsoft Windows ワークステーションへの単体インストールに必要なすべてのコンポーネントが付属しています。 Cisco Secure ACS Solution Engine は Cisco Secure ACS のソフトウェア ライセンスがプリインストールされた状態で出荷されます。 製品番号のための Cisco Secure ACS 4.0 製品速報を参照して下さい。 シスコ発注ホームページ（登録ユーザ専用）からご注文ください。

注: Cisco Secure ACS for Windows （登録ユーザのみ）のための 90日間体験版を得る関連するサービス契約との CCO アカウントを必要とします。

このドキュメントで紹介するルータ設定は、Cisco IOS® ソフトウェア リリース 11.3.3 が稼働するルータ上で開発されたものです。 **TACACS+** の代りの Cisco IOS ソフトウェア リリース 12.0.5.T およびそれ以降の使用 **group tacacs+**。 **aaa authentication login default radius enable** のような文は **aaa authentication login default group tacacs+ enable** として現われます。

/pub/tacacs ディレクトリの ftp-eng.cisco.com に匿名FTP によって TACACS+ フリーウェアおよびユーザーズ ガイドをダウンロードできます。

前提条件

要件

このドキュメントに関しては個別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。

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。

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: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool を使用してください（登録ユーザ専用）。

このドキュメントでは、次の設定を使用します。

- ルータの設定
- フリーウェアサーバのTACACS+設定ファイル

ルータの設定

```
!
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication ppp default if-needed tacacs+
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-
authenticated
aaa authorization commands 15 default tacacs+ if-
authenticated
aaa authorization network default tacacs+
enable password ww
!
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
!
```

```
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!
 !--- Challenge Handshake Authentication Protocol !---
(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 ! !--- Password
Authentication Protocol (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 ! !---
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 tacacs-server host 171.68.118.101 tacacs-
server timeout 10 tacacs-server key cisco ! 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 ! end
```

フリーウェアサーバのTACACS+設定ファイル

```
!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }
```

Microsoft Windows Setup

ユーザ1 および2 向けのMicrosoft Windowsセットアップ

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。

手順説明

次の手順を実行します。

注: PC 設定は使用するオペレーティングシステムのバージョンにわずかに基づいて変わることが

できます。

1. Dial-up Networking ウィンドウを開くために Start > Programs > Accessories > Dial-Up Networking の順に選択 して下さい。
2. Connections メニューから『Make new connection』 を選択 し、接続の名前を入力して下さい。
3. モデム別の情報を入力し、『Configure』 をクリック して下さい。
4. General Properties ページでモデムの最高速度を選択して下さい、しかし**唯一を接続します この速度**...ボックス**で**チェックしないで下さい。
5. 設定/接続特性ページで、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。 **ダイヤルトーンのための待機 200 秒後に接続されなくて**使用し、**コールを取り消す**コール プリファレンスはです**ダイヤルする前に**。
6. Connection ページで、『Advanced』 をクリック して下さい。 高度接続 設定で、**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。Properties ページ設定/オプションで何も Status Control の下のボックスを除いてチェックする必要がありません。
7. 『OK』 をクリック し、次に『Next』 をクリック して下さい。
8. 宛先の電話番号を入力し、再度『Next』 をクリック し、それから『Finish』 をクリック して下さい。
9. 新しい接続アイコンが現われたら、それを右クリックし、**> サーバタイプ** 『Properties』 を選択 して下さい。
10. 『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。
11. 許可されたネットワークプロトコルの下で **TCP/IP を**チェックして下さい。
12. 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、および**使用**次に『OK』 をクリック します**デフォルト ゲートウエイ**。
13. Connect To ウィンドウ ディスプレイを作るようにユーザがダイヤルするためにアイコンをダブルクリックするときユーザはユーザネームおよび Password フィールドを記入する必要があり次に『Connect』 をクリック します。

ユーザ3 向けのMicrosoft Windowsセットアップ

ユーザ 3 向けの設定はこれらの例外を除くユーザ 1 および 2 のためと（autocommand PPP の認証ユーザ）同じです:

- Properties ページ設定/オプション（6）ステップは、**Bring up terminal window after dialing を**チェックします。
- Connect To ウィンドウを開くようにユーザがダイヤルするためにアイコンをダブルクリックするとき（13）ステップ、ユーザはユーザネームおよび Password フィールドを記入しません。 ユーザは『Connect』 をクリック します。 ルータへの接続がなされた後、現われる黒い ウィンドウのユーザ名 および パスワードのユーザー定義型。 認証の後で、ユーザは『Continue（F7）』 を押します。

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

ルータ

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。

- terminal monitor - 現在の端末およびセッションの debug コマンドの出力とシステム エラー メッセージを表示します。
- **debug ppp negotiation** — PPP オプションがネゴシエートされる PPP 始動の間に送信される PPP パケットを表示します。
- **debug ppp packet** —送信され、受信される PPP パケットを表示します。（このコマンドは、下位レベルのパケット ダンプを表示します。）
- クライアントが認証を取得するかについて **debug ppp chap** —情報を表示します（より 11.2）先の Cisco IOS ソフトウェア リリースのために。
- **debug aaa authentication** — 認証、許可、アカウンティング（AAA）/TACACS+ 認証の情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。

server

注: これは Cisco TACACS+ フリーウェア サーバ コードを使用します。

```
tac_plus_executable -C config.file -d 16
  tail -f /var/tmp/tac_plus.log
```

関連情報

- TACACS+ Support Page
- IOS での TACACS+ に関するドキュメント
- Cisco Secure Access Control Server
- CiscoSecure 2.x TACACS+のセットアップおよびデバッグ
- テクニカル サポートとドキュメント – Cisco Systems