Livingston サーバ を使用する RADIUS の設定

内容

概要

このドキュメントは、RADIUS を初めて使用するユーザが Livingston RADIUS サーバに対する RADIUS の設定をセットアップおよびデバッグする際に役立つことを目的としています。Cisco IOS® RADIUS の機能の包括的な説明ではありません。Livingston のドキュメントは Lucent Technologies の Web サイトから入手できます。

ルータの設定は、使用するサーバに関係なく同一です。シスコでは、Couscouses NA、Couscouses UNIX、Cisco Access Registrar で使用可能な RADIUS コードを販売しています。

このルータ設定は、Cisco IOS ソフトウェア リリース 11.3.3 を実行しているルータで開発されました。リリース 12.0.5.T 以降では、**radius ではなく、group radius** が使用されるため、**aaa authentication login default radius enable などのステートメントが aaa authentication login default group radius enable** として表示されます。

RADIUS ルータ コマンドの詳細については、Cisco IOS マニュアルの RADIUS 情報を参照してください。

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。

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。

[Authentication]

次のステップを実行します。

1. UNIX サーバ上で RADIUS コードがコンパイルされていることを確認します。サーバ設定は、Livingston RADIUS サーバ コードを使用することを前提としています。ルータ設定は、他のサーバ コードで動作する必要がありますが、サーバ設定は違います。コード radiusd は、root として実行する必要があります。
2. Livingston RADIUS コードには、個別のシステム用にカスタマイズされた次の 3 つのサンプル ファイルが付属しています。つまり、clients.example、users.example、および dictionary です。これらすべては通常、raddb ディレクトリにあります。このドキュメントの最後でこれらのファイルまたは users ファイルと clients ファイルを修正できます。3 つすべてのファイルを作業ディレクトリに配置する必要があります。この 3 つのファイルで RADIUS サーバが起動するかどうかをテストします。
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   スタートアップ中のエラーは、画面または directory_containing_3_files_logfile に出力する必要があります。別のサーバのウィンドウから、RADIUS が起動したかどうかを確認します。
   ```
   ps -aux | grep radiusd
   (or ps -ef | grep radiusd)
   ```
   2 つの radiusd プロセスが表示されます。
3. radius プロセスを終了します。
   ```
   kill -9 highest_radiusd_pid
   ```
4. ルータのコンソール ポートで、RADIUS の設定を開始します。イネーブル モードへ切り換え、コマンドを設定する前に **configure terminal** と入力します。この構文によって、RADIUS がサーバ上で実行していなければ、最初にルータからロックアウトされないように設定されます。

   ```
   !--- Turn on RADIUS aaa new-model enable password whatever !--- These are lists of
   authentication methods, !--- that is, "linmethod", "vtymethod", "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 the radiusd !--- not being
   started, the enable password will be !--- accepted because it is in each list. aaa
   authentication login default radius enable aaa authentication login linmethod radius enable
   aaa authentication login vtymethod radius enable aaa authentication login conmethod radius
   enable !--- Point the router to the server, that is, !--- #.#.#.# is the server IP address.
   radius-server host #.#.#.# !--- Enter a key for handshaking !--- with the RADIUS server:
   radius-server key cisco line con 0 password whatever !--- No time-out to prevent being !---
   locked out during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login
   authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400
   password whatever flowcontrol hardware line vty 0 4 password whatever !--- No time-out to
   prevent being !--- locked out during debugging. exec-timeout 0 0 login authentication
   vtymethod
   ```
5. 先に進む前に、コンソール ポート経由でルータにログインしたまま、Telnet 経由でもルータにアクセスできることを確認します。radiusd が実行していないため、任意の userid でイネーブル パスワードを受け入れる必要があります。**注意：コン**ソール・ポートのセッションをアクティブにしておき、イネーブルモードのままにします。このセッションがタイムアウトにならないようにしてください。設定の変更中に自分をロックアウトしないでください。ルータで次のコマンドを発行して、サーバとルータ間のやり取りを確認します。

```
terminal monitor
debug aaa authentication
```

6. サーバ上で、RADIUS を root として開始します。
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   スタートアップ中のエラーが画面または directory_containing_3_files_logfile に出力されます。別のサーバのウィンドウから、RADIUS が起動したかどうかを確認します。
   ```
   Ps -aux | grep radiusd
   (or Ps -ef | grep radiusd)
   ```
   2 つの radiusd プロセスを確認する必要があります。
7. 今後、Telnet (vty) ユーザは、RADIUS 経由で認証する必要があります。ルータとサーバ上のデバッグであるステップ 5 とステップ 6 を使用して、ネットワークの別の部分からルータに Telnet します。ルータが、ユーザ名とパスワードのプロンプトを生成するので、これに応答します。
   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```
   何がどこに送信されるか、要求、応答などの RADIUS インタラクションを確認する必要があるサーバとルータに注目します。問題がある場合は修正してから次へ進みます。
8. RADIUS 経由で認証するユーザもイネーブル モードにする場合は、コンソール ポート セッションがまだアクティブであることを確認して、次のコマンドをルータに追加します。

   ```
   !--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS
   not running. aaa authentication enable default radius enable
   ```
9. これで、ユーザは RADIUS 経由で**有効になる必要があります。**ルータとサーバ上のデバッグであるステップ 5 とステップ 6 を使用して、ネットワークの別の部分からルータに Telnet します。ルータが、ユーザ名とパスワードのプロンプトを生成するので、これに応答します。
   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```
   イネーブル モードに入ると、ルータは、ユーザ名 $enable15$ を送信してパスワードを要求するので、これに応答します。
   ```
   shared
   ```
   何がどこに送信されるか、要求、応答などの RADIUS インタラクションを確認する必要があるサーバとルータに注目します。問題がある場合は修正してから次へ進みます。
10. RADIUS 経由で認証する必要のあるルータへの Telnet セッションを確立することによって、RADIUS 経由のコンソール ポート ユーザの認証を検査します。ルータに Telnet した状態でイネーブル モードのまま、コンソール ポート経由でルータにログインできることを確認したら、コンソール ポート経由のルータへの元の接続からログアウトして、コンソール ポートに再接続します。コンソール ポート認証のとき、ステップ 9 においてユーザ ID とパスワードを使用してログインし、イネーブル モードに入りましたが、今後は RADIUS 経由で行うように変更する必要があります。
11. Telnet セッションまたはコンソール ポート経由で接続したまま、ルータとサーバ上のデバッグであるステップ 5 とステップ 6 を使用して、回線 1 へのモデム接続を確立します。これで、回線ユーザは RADIUS 経由でログインしてイネーブル モードに入る必要があります。ルータが、ユーザ名とパスワードのプロンプトを生成するので、これに応答します。
    ```
    ciscousr (username from users file)
    ciscopas (password from users file)
    ```
    イネーブル モードに入ると、ルータは、ユーザ名 $enable15$ を送信してパスワードを要求するので、これに応答します。
    ```
    shared
    ```
    何がどこに送信されるか、要求、応答などの RADIUS インタラクションを確認する必要があるサーバとルータに注目します。問題がある場合は修正してから次へ進みます。

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. アカウンティングは、ルータ内で設定されていなければ実行されません。次の例のように、ルータでアカウンティングを有効にします。
   ```
   aaa accounting exec default start-stop radius
   aaa accounting connection default start-stop radius
   aaa accounting network default start-stop radius
   aaa accounting system default start-stop radius
   ```
2. アカウンティング オプションを使用してサーバ上で RADIUS を開始します。
   ```
   Start RADIUS on the server with the accounting option:
   ```
3. ルータでサーバとルータ間のやり取りを確認するには：
   ```
   terminal monitor
   debug aaa accounting
   ```
4. ルータにアクセスして、デバッグによってサーバとルータ間のやり取りを観察し、アカウンティング ディレクトリにあるログ ファイルを確認します。

テストファイル

users テスト ファイルを以下に示します。

```
ciscousr        Password = "ciscopas"
                User-Service-Type = Login-User,
                Login-Host = 1.2.3.4,
                Login-Service = Telnet

$enable15$      Password = "shared"
                User-Service-Type = Shell-User
```

clients テスト ファイルを以下に示します。

```
# 1.2.3.4 is the ip address of the client router and cisco is the key
1.2.3.4         cisco
```

関連情報

- Remote Authentication Dial-In User Service (RADIUS)
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems