アクセス サーバの基本 AAA の設定

目次

概要

この文書では、Radius または TACACS+ プロトコルを使用している Cisco ルータでの Authentication、Authorization、Accounting（AAA; 認証、許可、アカウンティング）の設定方法について説明します。 この文書の目的は、AAA 機能全体を説明することではなく、主なコマンドについて説明し、その例とガイドラインを提供することです。

注: Cisco IOS® 設定を続行する前に汎用AAA設定でセクションを読んで下さい。 そうしないと、誤設定が行われ、その後ロックアウトが発生することがあります。

はじめに

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。

前提条件

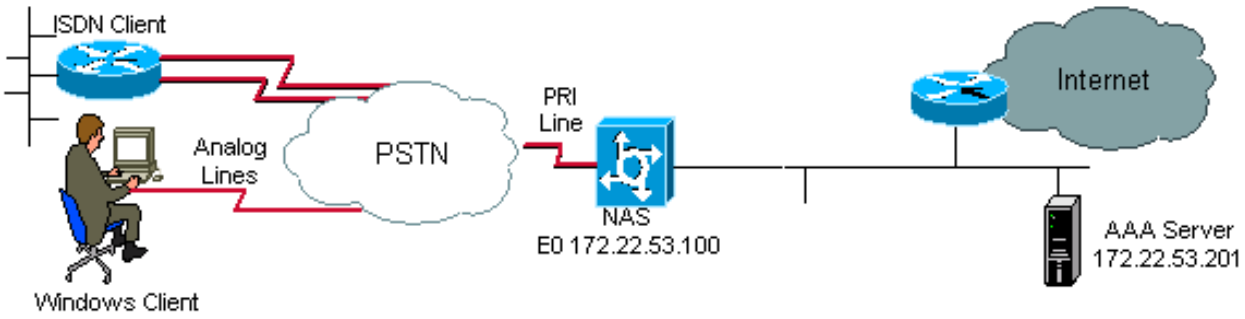
AAA の、および Aaa コマンドおよびオプションについての完全な詳細については外観を得るために、IOS 12.2 セキュリティ構成ガイドを参照して下さい: 認証、許可、会計。

使用するコンポーネント

この文書の情報は、Cisco IOS ソフトウェア リリース 12.1 メイン ラインに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、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。

ネットワーク図



一般的なAAA設定

AAA の有効化

AAA をイネーブルにするには、グローバル コンフィギュレーションで aaa new-model コマンドを設定する必要があります。

注: このコマンドをイネーブルにするまで、他のすべての AAA コマンドは隠しコマンドとされています。

警告： aaa new-model コマンドはすべてのラインおよびインターフェイスにすぐにローカル認証を適用します（コンソール ライン **line con 0** を除いて）。 このコマンドをイネーブルにすると、telnet セッションがルータに対して開かれていた場合（あるいは接続がタイムアウトになり、再接続する必要がある場合）、ルータのローカル データベースを使ってユーザの認証を行う必要があります。 ルータのロックアウトを回避するため、アクセス サーバ上でユーザ名とパスワードを設定してから、AAA 設定を開始することをお勧めします。 そのためには、次の手順を実行します。

```
Router(config)# username xxx password yyy
```

ヒント： Aaa コマンドを設定する前に設定を保存して下さい。 その次に設定の保存を行うのは、すべての AAA の設定が完了し、これが正常に動作していることを確認してからにする必要があります。 そうすることにより、予期しないロックアウトが（設定を保存する前に）発生した場合でも、ルータをリロードすれば回復できます。

外部AAAサーバの指定

グローバル コンフィギュレーションでは、AAA を使ってセキュリティ プロトコル（Radius、TACACS+）を定義します。 この 2 つのプロトコルをどちらも使わない場合は、ルータ上のローカル データベースを使用できます。

TACACS+ を使用している場合、**tacacs-server host** < *AAA server*> <*key*> コマンドの *IP アドレス*を使用して下さい。

Radius を使用している場合、**radius サーバ ホスト** < *AAA server*> <*key*> コマンドの *IP アドレス* を使用して下さい。

AAA サーバ設定

AAA サーバ上で、次のパラメータを設定します。

- アクセス サーバ名
- AAA サーバとの通信にアクセス サーバが使用する IP アドレス**注:** 両方のデバイスが同じイーサネット ネットワーク上にある場合、アクセス サーバはデフォルトでは、AAA パケットの送信時に、イーサネット インターフェイス上で定義されている IP アドレスを使用します。 ルータが複数のインターフェイスを備えている（したがって複数のアドレスが割り当てられている）場合、この問題は重要です。
- 正確のアクセス サーバで設定される同じキー *<key>*。**注:** このキーは大文字と小文字を区別します。
- アクセス サーバが使用するプロトコル（TACACS+ または Radius）

上記パラメータの設定に使用する手順そのものについては、使用中の AAA サーバの文書を参照してください。 AAA サーバが正しく設定されていない場合、NAS からの AAA 要求は AAA サーバによって無視されるため、接続が失敗することがあります。

AAA サーバは、アクセス サーバから IP 上到達可能である必要があります（接続を確認するには、ping テストを実行します）。

認証の設定

認証によりユーザを確認してから、ユーザによるネットワークとネットワーク サービス（これらは認証を使って確認されます）への接続を許可します。

AAA 認証を設定するには、次の手順を実行します。

1. まず認証方式の名前付きリストを（グローバル コンフィギュレーション モードで）定義します。
2. このリストを 1 つまたは複数のインターフェイスに（インターフェイス コンフィギュレーション モードで）適用します。

唯一の例外は、（「default」という名前の）デフォルトの方式リストです。 デフォルトの方式リストは、明示的に定義された名前付き方式リストが存在するインターフェイス以外のすべてのインターフェイスに、自動的に適用されます。 定義された方式リストは、デフォルトの方式リストを無効にします。

次の認証例では、方式や名前付きリストなどのコンセプトを説明するため、Radius、ログイン、および（最も一般的に使われている）Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）認証が使われています。 すべての例中で、Radius またはローカル認証を TACACS+ で置き換えることが可能です。

Cisco IOS ソフトウェアは、ユーザを認証するため、リストに掲載されている最初の方式が使用されます。 その方式で応答に失敗した場合（ERROR によって示されます）、Cisco IOS ソフトウェアは、方式リストに掲載されている次の認証方式を選択します。 リストに掲載されている認証方式での通信に成功するか、方式リストで定義されているすべての方式がなくなるまで、このプロセスが続きます。

注意する必要がある重要な点は、Cisco IOS ソフトウェアは、前の方式では応答がなかった場合にだけ、次に掲載されている認証方式を使って認証を実行するということです。 このサイクルのいずれかの時点で認証が失敗した場合、つまり、AAA サーバまたはローカル ユーザ名データベースの応答がユーザ アクセスの拒否であった場合（FAIL によって示されます）、認証プロセスは停止し、他の認証方式は試行されません。

ユーザ認証を許可するには、AAA サーバ上でユーザ名とパスワードを設定する必要があります。

ログイン認証

aaa authentication login コマンドを使って、アクセス サーバへ EXEC アクセスする（tty、vty、コンソール、および aux）ユーザを認証できます。

例 1： Radius の後にローカルを使った EXEC アクセス

```
Router(config)# aaa authentication login default group radius local
```

上のコマンドでは、次の設定を使用します。

- 名前付きリストはデフォルトのリスト（default）です。
- 2 つの認証方式（グループ radius とローカル）があります。

すべてのユーザは、Radius サーバ（最初の方式）を使って認証されます。 Radius サーバが応答しない場合、ルータのローカル データベース（2 番目の方式）が使われます。 ローカル認証の場合、ユーザ名とパスワードを定義します。

```
Router(config)# username xxx password yyy
```

aaa authentication login コマンドで default リストを使用しているため、すべてのログイン接続（tty、vty、コンソールおよび aux）に対し、ログイン認証が自動的に適用されます。

注: IP 接続がない場合、AAA サーバ上でアクセス サーバが正しく定義されていない場合、またはアクセス サーバ上で AAA サーバが正しく定義されていない場合、サーバ（Radius または TACACS+）はアクセス サーバが送信した aaa authentication 要求に応答しません。

注: 上記の例を使う場合に、キーワード local を含めないと、次のメッセージが表示されます。

```
Router(config)# aaa authentication login default group radius
```

注: AAA サーバが認証要求に応答しない場合、認証は失敗します（試行する代替方式がルータにないため）。

注: group キーワードを使うと、既存のサーバ ホストをグループ化する方法が提供されます。 この機能により、ユーザは設定されたサーバ ホストのサブセットを選択し、特定のサービスに対してそのサブセットを使用できます。 この拡張機能の詳細については、文書『AAA Server-Group』を参照してください。

例 2： 回線パスワードを使ったコンソール アクセス

line con 0 で設定されたパスワードでしかコンソール ログインが認証されないように、例 1 の設定を拡張してみましょう。

リスト CONSOLE を定義し、line con 0 に適用します。

次のように設定できます。

```
Router(config)# aaa authentication login CONSOLE line
```

上のコマンドでは、次の設定を使用します。

- 名前付きリストは CONSOLE です。
- 認証方式は 1 つしかありません（回線）。

名前付きリスト（この例では CONSOLE）を作成した後、そのリストを有効にするには、回線またはインターフェイスにそのリストを適用する必要があります。 login authentication list_name コマンドを使うことによって、これが実現されます。

```
Router(config)# line con 0
Router(config-line)# exec-timeout 0 0
Router(config-line)# password cisco
Router(config-line)# login authentication CONSOLE
```

コンソール リストは line con 0 のデフォルトの方式リスト デフォルトを無効にします。 コンソールアクセスを得るためにパスワード「cisco」を（line con 0 で設定される）入力する必要があります。 tty、vty および aux ではこれまでと同じように、デフォルト リストが使用されます。

注: ローカルなユーザ名とパスワードを使ってコンソール アクセスが認証されるようにするには、次のコマンドを使います。

```
Router(config)# aaa authentication login CONSOLE local
```

注: このケースでは、ルータのローカル データベースでユーザ名とパスワードを設定する必要があります。 このリストは回線またはインターフェイスにも適用する必要があります。

注: 認証を使用しない場合は、次のコマンドを使用します。

```
Router(config)# aaa authentication login CONSOLE none
```

注: このケースでは、コンソール アクセスを有効にするための認証はありません。 このリストは回線またはインターフェイスにも適用する必要があります。

例 3： 外部 AAA サーバを使ったイネーブル モード アクセス

authentication を発行して、イネーブル モードにできます（特権レベル 15）。

次のように設定できます。

```
Router(config)# aaa authentication enable default group radius enable
```

パスワードだけが要求され、ユーザ名は $enab15$ となります。 したがって、ユーザ名 $enab15$ を AAA サーバで定義する必要があります。

Radius サーバが応答しない場合、ルータ上でローカルに設定された enable パスワードを入力する必要があります。

PPP認証

PPP 接続を認証するには、aaa authentication ppp コマンドを使用します。 このコマンドは通常、アクセス サーバを介してインターネットまたはセントラル オフィスにアクセスする ISDN ユーザまたはアナログ リモート ユーザの認証に使用します。

例 1： すべてのユーザに対する、単一の PPP 認証方式

アクセス サーバは、PPP ダイヤルイン クライアントを受け入れるように設定された ISDN インターフェイスを備えています。 ここでは dialer rotary-group 0 を使いますが、主要インターフェイスまたはダイヤラ プロファイル インターフェイスで設定を実行できます。

次のように設定します。

```
Router(config)# aaa authentication ppp default group radius local
```

このコマンドは、Radius を使ってすべての PPP ユーザを認証します。 Radius サーバが応答しない場合、ローカル データベースが使用されます。

例 2： 固有のリストを使った PPP 認証

デフォルト リストではなく名前付きリストを使用するには、次のコマンドを設定します。

```
Router(config)# aaa authentication ppp ISDN_USER group radius Router(config)# int dialer 0
Router(config-if)# pp authentication chap ISDN_USER
```

この例では、リストは ISDN_USER で、方式は Radius です。

例 3： キャラクタ モード セッション内から起動した PPP

アクセス サーバは、内部モデム カード（Mica、Microcom または Next Port）を備えています。 aaa authentication login コマンドと aaa authentication ppp コマンドの両方が設定されていると仮定します。.

モデム ユーザがキャラクタ モード EXEC セッション（ダイヤル後のターミナル ウィンドウなど）を使って、最初にルータにアクセスすると、そのユーザは tty 回線上で認証されます。 パケット モード セッションを起動するには、ppp default または ppp をタイプする必要があります。 PPP 認証は（aaa authentication ppp を使って）明示的に設定されているため、ユーザは PPP レベルで再度認証されます。

この二度目の認証を回避するには、if-needed キーワードを使用できます。

```
Router(config)# aaa authentication login default group radius local Router(config)# aaa
authentication ppp default group radius local if-needed
```

注: クライアントが PPP セッションを直接開始すると、アクセス サーバへのログイン アクセスが存在しないため、PPP 認証が直接実行されます。

AAA 認証の詳細については、文書『IOS 12.2 セキュリティ設定ガイド： 認証の設定』と『シスコの\ AAA\ 実装ケース\ スタディ』を参照してください。

許可の設定

許可とは、ユーザが実行できる操作と実行できない操作を制御できる処理です。

AAA 許可には認証と同じルールがあります。

1. まず、許可方式の名前付きリストを定義します。
2. 次にそのリストを 1 つまたは複数のインターフェイスに適用します (デフォルトの方式リストを除きます) 。
3. リストに掲載されている最初の方式が使用されます。 最初の方式で応答に失敗すると、2 番目の方式が使用され、以降同様の処理が実行されます。

方式リストは要求された許可タイプに固有です。 この文書では、EXEC およびネットワークの各許可タイプを中心に説明します。

その他の許可タイプの詳細については、『Cisco IOS セキュリティ設定ガイド、リリース 12.2』を参照してください。

エグゼクティブ認証

aaa authorization exec コマンドは、ユーザが EXEC シェルの実行を許可されているかどうかを決定します。 この機能により、自動コマンド情報、アイドル タイムアウト、セッション タイムアウト、アクセス リスト、特権、その他のユーザごとの要素などのユーザ プロファイル情報が返されることがあります。

EXEC 許可は、vty または tty 回線を介してしか実行されません。

次の例では、Radius を使います。

例 1： すべてのユーザに対する、同一の EXEC 認証方式

次のコマンドで認証します。

```
Router(config)# aaa authentication login default group radius local
```

その後、Radius (最初の方式) またはローカル データベース (2 番目の方式) を使って、アクセス サーバへログインするすべてのユーザを認証する必要があります。

次のように設定できます。

```
Router(config)# aaa authorization exec default group radius local
```

注: AAA サーバ上で、Service-Type=1 (ログイン) を選択する必要があります。

注: この例では、local キーワードが含まれておらず、AAA サーバが応答しない場合、許可は有効にならず、接続は失敗します。

注: 次の例 2 と 3 では、ルータ上でコマンドを追加する必要はありませんが、アクセス サーバ上でしかプロファイルを設定できません。

例 2： AAA サーバからの EXEC 特権レベルの割り当て

例 1 に基づいて、アクセス サーバにログインするユーザが直接イネーブル モードへの移行を許可されている場合、AAA サーバで次の Cisco AV ペアを設定します。

```
shell:priv-lvl=15
```

これは、ユーザがイネーブル モードに直接移行することを意味します。

注: 最初の方式で応答に失敗すると、ローカル データベースが使われます。 ただし、ユーザは直接イネーブル モードに移行するのではなく、enable コマンドを入力し、enable パスワードを入力する必要があります。

例 3： AAA サーバからのアイドル タイムアウトの割り当て

（アイドル タイムアウトになった後、トラフィックがない場合にセッションが接続解除されるように）アイドル タイムアウトを設定するには、IETF Radius 属性 28： ユーザのプロファイルの下のアイドル タイムアウトを使用します。

ネットワーク許可

aaa authorization network コマンドは、PPP、SLIP、ARAP など、ネットワーク関連のすべてのサービス リクエストに対し、許可を実行します。 このセクションでは、最も一般的に使われている PPP を中心に説明します。

AAA サーバは、PPP セッションがクライアントに許可されているかどうかをチェックします。さらに、クライアントは コールバック、圧縮、IP アドレスなどの PPP オプションを要求できます。 こうしたオプションは、AAA サーバ上のユーザ プロファイルで設定する必要があります。さらに特定のクライアントでは、AAA プロファイルにアイドル タイムアウト、アクセス リスト、Cisco IOS ソフトウェアがダウンロードし、このクライアントに適用されるその他のユーザ固有の属性を含めることができます。

次の例は、Radius を使った許可を示します。

例 1： すべてのユーザに対して同一のネットワーク許可方式

PPP ダイヤルイン接続を承認するために、アクセス サーバを使用します。

最初に次のコマンドを使って（以前設定したように）ユーザを認証します。

```
Router(config)# aaa authentication ppp default group radius local
```

次に、次のコマンドを使ってユーザを許可します。

```
Router(config)# aaa authorization network default group radius local
```

注: AAA サーバで次のように設定します。

- Service-Type=7（フレーム付き）
- Framed-Protocol = PPP

例 2： ユーザ固有の属性の適用

AAA サーバを使って、IP アドレス、コールバック番号、ダイヤラ アイドル タイムアウト値、ア

クセス リストなど、ユーザ固有の属性を割り当てられます。 このような実装では、NAS は適切な属性を AAA サーバのユーザ プロファイルからダウンロードします。

例 3： 固有のリストを使った PPP 許可

認証と同様、デフォルトのリスト名の代わりに、次のようにリスト名を設定できます。

```
Router(config)# aaa authorization network ISDN_USER group radius local
```

次にこのリストをインターフェイスに適用します。

```
Router(config)# int dialer 0
Router(config-if)# ppp authorization ISDN_USER
```

AAA 認証の詳細については、文書『IOS 12.2 セキュリティ設定ガイド： 認証の設定』と『シスコの\ AAA\ 実装ケース\ スタディ』を参照してください。

アカウンティングの設定

AAA アカウンティング機能を有効にすると、ユーザがアクセスしているサービスやネットワーク リソースの使用量を追跡できます。

AAA アカウンティングには認証や許可と同じルールがあります。

1. 最初にアカウンティング方式の名前付きリストを定義する必要があります。
2. 次にそのリストを 1 つまたは複数のインターフェイスに適用します（デフォルトの方式リストを除きます）。
3. リストに掲載されている最初の方式を使用した場合に応答に失敗すると、次の方式が使用され、以降同様の処理が実行されます。

リストに掲載されている最初の方式を使用した場合に応答に失敗すると、次の方式が使用され、以降同様の処理が実行されます。

- ネットワーク アカウンティングにより、PPP、Slip、および AppleTalk Remote Access Protocol（ARAP）のすべてのセッションに、 パケット数、オクテット数、セッション時間、開始時間、および終了時間に関する情報を提供します。
- EXEC アカウンティングにより、ネットワーク アクセス サーバのユーザ EXEC 端末セッション（telnet セッションなど）に関する情報（セッション時間、開始時間、終了時間）が提供されます。

その他の許可タイプの詳細については、『Cisco IOS セキュリティ設定ガイド、リリース 12.2』を参照してください。

次の例では、AAA サーバへの情報の送信方法に焦点を当てています。

アカウンティング設定の例

例 1： 開始および終了アカウンティング レコードの生成

すべてのダイヤルイン PPP セッションでは、クライアントが認証された後、キーワード start-stop を使って接続解除を行うと、アカウンティング情報が AAA サーバに送信されます。

```
Router(config)# aaa accounting network default start-stop group radius local
```

例 2： 終了アカウンティング レコードだけの生成

クライアントを接続解除した後だけアカウンティング情報を送信する必要がある場合、キーワード stop を使って、次の行を設定します。

```
Router(config)# aaa accounting network default stop group radius local
```

例 3： 認証とネゴシエーションの失敗のリソース レコードの生成

この時点まで、AAA アカウンティングは、ユーザ認証をパスしたコールに対して開始と終了レコードのサポートを提供します。

認証または PPP ネゴシエーションが失敗した場合、認証のレコードは生成されません。

この問題の解決策が、AAA リソース失敗の終了アカウンティングを使用することです。

```
Router(config)# aaa accounting send stop-record authentication failure
```

終了レコードは AAA サーバに送信されます。

例 4： フル リソース アカウンティングのイネーブル

（コール セットアップ時の開始レコードと、コール終了時の終了レコードの両方を生成する）フル リソース アカウンティングをイネーブルにするには、次のように設定します。

```
Router(config)# aaa accounting resource start-stop
```

このコマンドは、Cisco IOS ソフトウェア リリース 12.1(3)T でサポートされました。

このコマンドを使うと、コール セットアップとコール接続解除の開始 - 終了アカウンティング レコードにより、デバイスに対するリソース接続の経過が追跡できます。 個別のユーザ認証の開始 - 終了アカウンティング レコードにより、ユーザ管理の経過が追跡できます。 この 2 つのアカウンティング レコード セットは、コールの一意のセッション ID により相互リンクされます。

AAA 認証の詳細については、文書『IOS 12.2 セキュリティ設定ガイド： 認証の設定』と『シスコの\ AAA\ 実装ケース\ スタディ』を参照してください。

関連情報

- テクニカルサポート - Cisco Systems