アクセスサーバでの基本的なAAAの設定

内容

概要

このドキュメントでは、RadiusまたはTACACS+プロトコルを使用するCiscoルータで認証、認可

、アカウンティング(AAA)を設定する方法について説明します。

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。

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。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS®ソフトウェアリリース12のメインラインに基づくものです。

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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

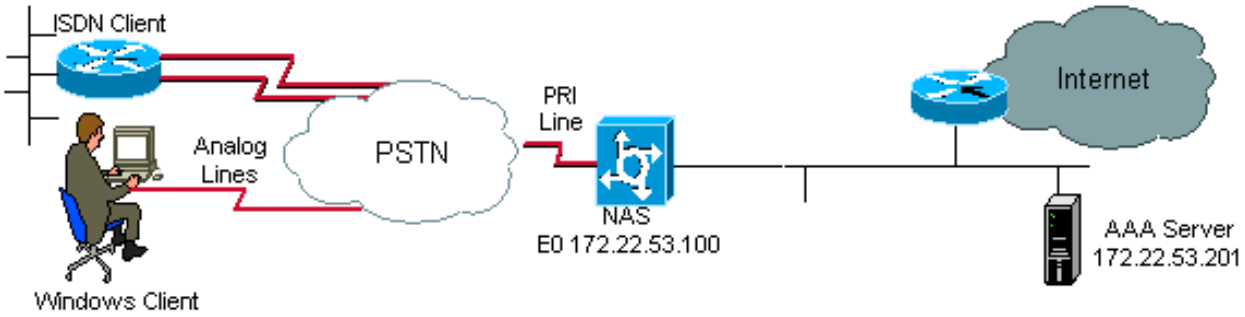
背景説明

このドキュメントでは、RadiusまたはTACACS+プロトコルを使用するCiscoルータで認証、認可、アカウンティング(AAA)を設定する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の設定に進む前に、「一般的なAAA設定」の項を読んでください。これを行わないと、設定ミスと後続のロックアウトが発生する可能性があります。

詳細については、『Authentication, Authorization and Accounting Configuration Guide』を参照してください。

ネットワーク図



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 コマンドにより、ローカル認証がすべての回線およびインターフェイス (コンソール回線 line con 0 を除く) にただちに適用されます。** このコマンドをイネーブルにした後で、telnetセッションがルータに対して開かれた場合 (または接続がタイムアウトし、再接続が必要な場合) 、ユーザはルータのローカルデータベースで認証される必要があります。AAA設定を開始する前に、アクセスサーバでユーザ名とパスワードを定義しておくことを推奨します。これにより、ルータからロックアウトされることはありません。次のコード例を参照してください。

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

> **ヒント**：AAAコマンドを設定する前に、 save 設定を確認します。次のことが可能です save 設定は、AAAの設定が完了した後 (正しく動作することに満足した後) にのみ再度行われます。 これにより、ルータのリロードで変更をロールバックできるため、予期しないロックアウトから回復できます。

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+を使用する場合は、**tacacs-server host <AAAサーバのIPアドレス> <key>** コマンドを使用します。

Radiusを使用する場合は、**radius-server host <AAAサーバのIPアドレス> <key>**コマンドを使用します。

AAA サーバ設定

AAAサーバで、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、デフォルトでは、アクセスサーバはAAAパケットを送信するときに、イーサネットインターフェイスで定義された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。

- アクセス サーバに設定されているのとまったく同じキー<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）

前述のパラメータの設定に使用した正確な手順については、AAAサーバのマニュアル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、接続が失敗する可能性があります。

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、デフォルトのメソッドリスト(**default**という名前)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。

これらの認証例では、メソッドや名前付きリストなどの概念を説明するために、Radius、ログイン、およびPoint-to-Point Protocol(PPP)認証を使用します。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を拒否する場合（FAILで示されます）、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とローカルを使用したEXECアクセス

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

前のコマンドでは、次のコマンドを使用します。

- 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サーバで認証されます（最初の方法）。 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が使用されます（2番目の方法）。 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コマンドのlist defaultが使用されるため、ログイン認証はすべてのログイン接続（tty、vty、コンソール、auxなど）に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+）はアクセスサーバによって送信された aaa authentication要求に応答できません。

> **注**：前の例をlocalキーワードなしで使用すると、結果は次のようになります。

```
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（ルータには試行する代替方式がないため）。

> **注**：groupキーワードは、現在のサーバホストをグループ化する方法を提供します。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。

例 2：回線パスワードで使用されるコンソールアクセス

例1の設定を展開して、コンソールログインがline con 0に設定されたパスワードによってのみ認証されるようにします。

リスト CONSOLE を定義し、line con 0 に適用します。

設定：

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

前のコマンドでは、次のコマンドを使用します。

- 名前付きリストは CONSOLE です。
- 認証方式（回線）は1つだけです。

名前付きリスト（この例ではCONSOLE）を作成する場合、実行する前に回線またはインターフェイスに適用する必要があります。この操作は、 login authentication コマンドにより、WLC CLI で明確に示されます。

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

CONSOLEリストは、line con 0のデフォルトの方式リストdefaultを上書きします。line con 0でこの設定を行った後、コンソールアクセスを取得するにはパスワードciscoを入力する必要があります。tty、vty、およびauxでは、デフォルトのリストが引き続き使用されます。

> **注**：コンソールアクセスをローカルのユーザ名とパスワードで認証するには、次のコード例を使用します。

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

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**：認証を行わないようにするには、次のコード例を使用します。

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

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サーバで使用される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）。

設定：

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

要求できるのはパスワードだけです。ユーザ名は$enab15$です。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は、ルータでローカルに設定されたイネーブル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。通常は、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またはアナログリモートユーザを認証するために使用されます。

例 1：すべてのユーザに対する、単一の PPP 認証方式

アクセスサーバには、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インターフェイスがあります。ここではdialer rotary-group 0を使用していますが、設定はメイン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行うことができます。

設定：

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

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

例 2：特定のリストで使用される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)#interface dialer 0
Router(config-if)#ppp 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。

モデムユーザが最初にキャラクタモードexecセッション（たとえば、ダイヤル後にターミナルウィンドウを使用するなど）でルータにアクセスすると、ユーザはtty回線で認証されます。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2回目の認証を回避するには、if-neededキーワードを使用します。

```
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ないため、PPP認証が直接実行されます。

認可の設定

認可は、ユーザが実行できる処理を制御できるプロセスです。

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。このドキュメントでは、Execおよびネットワーク認証タイプを中心に説明します。

その他の認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』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。この機能は、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、アクセスリストと特権、およびその他のユーザごとの要因などのユーザプロファイル情報を返すことができます。

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、半径を使用します。

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される場合：

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

アクセスサーバにログインするすべてのユーザは、Radius（1番目の方法）またはローカルデータベース（2番目の方法）で認証される必要があります。

設定：

```
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、認可は不可能であり、接続が失敗する可能性があります。

注：次の例2および3では、ルータにコマンドを追加する必要はありません。必要な設定は、アクセスサーバのプロファイルだけです。

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、ユーザがアクセスサーバにログインして直接イネーブルモードに入ることができるように、AAAサーバで次のCisco AVペアを設定します。

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

これで、ユーザはイネーブルモードに直接移行できます。

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入ることはできませんが、enableコマンドを入力して**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を設定するには（アイドルタイムアウト後にトラフィックがない場合にセッションが切断されるように）、IETF Radiusアトリビュート28を使用します。ユーザプロファイルの下のアイドルタイムアウト。

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要求に対して認可を実行します。このセクションでは、最も一般的に使用されるPPPに焦点を当てています。

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に対して、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、およびCisco IOSソフトウェアがダウンロードしてこのクライアントに適用できるその他のユーザごとの属性を含めることができます。

次の例は、Radiusによる認可を示しています。

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

アクセスサーバは、PPPダイヤルイン接続を受け入れるために使用されます。

ユーザは次のコマンドで認証されます（以前に設定したとおりです）。

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

次のコマンドを使用して、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**(framed)および**Framed-Protocol=PPP**。

例 2：ユーザ固有の属性の適用

AAAサーバを使用して、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のユーザごとの属性を割り当てることができます。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

認証と同様に、デフォルトのリスト名ではなく、リスト名を設定します（次の例を参照）。

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

アカウンティング設定

AAAアカウンティング機能を使用すると、ユーザがアクセスするサービスと、ユーザが消費するネットワークリソースの量を追跡できます。

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。

- 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。

次の例では、情報をAAAサーバに送信する方法を中心に説明します。

アカウンティングの設定例

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、クライアントが認証されてからキーワードstart-stopを使用して接続解除された後に、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：ストップアカウンティングレコードのみを生成する

クライアントの接続解除後にのみアカウンティング情報を送信する必要がある場合は、キーワードstopを使用して次の行を設定します。

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

例3：認証およびネゴシエーションの失敗に対する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：完全なリソースアカウンティングの有効化

（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。これらの2つのアカウンティングレコードのセットは、コールの一意のセッションIDと相互にリンクされます。

関連情報

- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。