# AAA 用の TACACS+ サーバー

この章では、AAA で使われる TACACS+ サーバーの設定方法について説明します。



# AAA 用の TACACS+ サーバーについて

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 の各プロトコルで TACACS+ サーバー認証をサポートします。

## TACACS+ 属性

ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバーとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザーに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注） TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

次の表に、カットスループロキシ接続に対してサポートされる TACACS+ 許可応答属性の一覧を示します。

表 *1:* サポートされる *TACACS+* 許可応答属性

| 属性 | 説明 |
|---|---|
| acl | 接続に適用する、ローカルで設定済みの ACL を識別します。 |
| idletime | 認証済みユーザー セッションが終了する前に許可される非アクティブ時間（分）を示します。 |
| timeout | 認証済みユーザーセッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。 |

次の表に、サポートされる TACACS+ アカウンティング属性の一覧を示します。

。

表 *2:* サポートされる *TACACS+* アカウンティング属性

| 属性 | 説明 |
|---|---|
| bytes_in | この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。 |
| bytes_out | この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。 |
| cmd | 実行するコマンドを定義します（コマンド アカウンティングのみ）。 |
| disc-cause | 切断理由を特定する数字コードを示します（ストップ レコードのみ）。 |
| elapsed_time | 接続の経過時間（秒）を定義します（ストップ レコードのみ）。 |
| foreign_ip | トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。 |
| local_ip | トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。 |
| NAS port | 接続のセッション ID が含まれます。 |
| packs_in | この接続中に転送される入力パケット数を指定します。 |
| packs_out | この接続中に転送される出力パケット数を指定します。 |
| priv-level | コマンド アカウンティング要求の場合はユーザーの権限レベル、それ以外の場合は 1 に設定されます。 |
| rem_iddr | クライアントの IP アドレスを示します。 |

| 属性 | 説明 |
|---|---|
| service | 使用するサービスを指定します。コマンド アカウンティングの場合にのみ、常に「shell」に設定されます。 |
| task_id | アカウンティング トランザクションに固有のタスク ID を指定します。 |
| username | ユーザーの名前を示します。 |

# AAA 用の TACACS+ サーバーのガイドライン

ここでは、AAA 用の TACACS+ サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

### IPv6

AAA サーバーは、IPv4 または IPv6 アドレスを使用できます。

### その他のガイドライン

- シングルモードで最大200個のサーバーグループ、またはマルチモードでコンテキストごとに 4 つのサーバーグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。
- ASA アプライアンスモードで実行されている FPR1000、FPR2100、または FPR3100 シリーズの場合は、次のユーザー名規則に従う必要があります。
  - Linux に対して有効である必要があります。
  - 小文字のみを使用してください。
  - 英数字、ピリオド（.）、ハイフン（-）を含めることができます。
  - アット マーク（@）やスラッシュ（/）など、その他の特殊文字を含めることはできません。

# TACACS+ サーバーの設定

ここでは、TACACS+ サーバーを設定する方法について説明します。

手順

ステップ 1 TACACS+ サーバー グループの設定 （4 ページ）。
ステップ 2 グループへの TACACS+ サーバーの追加 （5 ページ）。
ステップ 3 （任意）認証プロンプトの追加 （6 ページ）。

# TACACS+ サーバー グループの設定

認証、許可、アカウンティングに TACACS+ サーバーを使用する場合は、まず TACACS+ サーバー グループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバーを追加する必要があります。TACACS+ サーバー グループは名前で識別されます。

TACACS+ サーバー グループを追加するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。
ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。
ステップ 4 [Protocol] ドロップダウン リストから、[TACACS+] サーバー タイプを選択します。
ステップ 5 [Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバーにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバーに送信されます。

ステップ 6 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバーは、グループ内のサーバーがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバーが非アクティブになった場合、そのサーバーは、グループの他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のすべてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。

Timed モードでは、障害が発生したサーバーは 30 秒の停止時間の後で再アクティブ化されます。

**ステップ 7** [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバーが再びイネーブルになるまでの時間間隔を分単位で指定します。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。

**ステップ 8** サーバーで許可される AAA トランザクションの失敗の最大数を追加します。

このオプションで設定するのは、応答のないサーバーを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

**ステップ 9** [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバー グループが [AAA Server Groups] テーブルに追加されます。

**ステップ 10** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

# グループへの TACACS+ サーバーの追加

TACACS+ サーバーをグループに追加するには、次の手順を実行します。

**手順**

**ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

**ステップ 2** サーバーを追加するサーバー グループをクリックします。

**ステップ 3** [Servers in the Selected Group] 領域で、[Add] をクリックします。

サーバー グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

**ステップ 4** 認証サーバーが存在するインターフェイス名を選択します。

**ステップ 5** グループに追加するサーバーのサーバー名または IP アドレスを追加します。

**ステップ 6** サーバーへの接続試行のタイムアウト値を指定します。

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the retry interval）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバーは非アクティブ化され、ASA は別の AAA サーバー（設定されている場合）への要求の送信を開始します。

**ステップ 7** サーバー ポートを指定します。サーバー ポートは、ポート番号 139、または ASA によって TACACS+ サーバーとの通信に使用される TCP ポートの番号です。

**ステップ 8** サーバー秘密キーを指定します。ASA でTACACS+サーバーを認証する際に使用される共有秘密キーを指定します。ここで設定したサーバー秘密キーは、TACACS+ サーバーで設定されたサーバー秘密キーと一致する必要があります。サーバー秘密キーが不明の場合は、TACACS+ サーバーの管理者に問い合わせてください。最大フィールド長は、64 文字です。

**ステップ 9** [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバーが AAA サーバー グループに追加されます。

**ステップ 10** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

# 認証プロンプトの追加

AAA 認証チャレンジ プロセスの実行中にユーザーに表示するテキストを指定できます。TACACS+ サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザーのログイン時に、ユーザー名プロンプトとパスワード プロンプトの上に表示されます。

認証プロンプトを指定しない場合、TACACS+ サーバーでの認証時にユーザーに対して表示される内容は次のようになります。

| Connection Type | デフォルトのプロンプト |
|---|---|
| FTP | FTP authentication |
| HTTP | HTTP 認証 |
| Telnet | なし |

認証プロンプトを追加するには、次の手順を実行します。

### 手順

**ステップ 1** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Authentication Prompt]** の順に選択します。

**ステップ 2** ログイン時にユーザーに表示されるユーザー名とパスワードのプロンプトの上に表示するテキストを追加します。

次の表に、認証プロンプトの文字数制限を示します。

| アプリケーション | 認証プロンプトの文字数制限 |
|---|---|
| Microsoft Internet Explorer | 37 |
| Telnet | 235 |

| アプリケーション | 認証プロンプトの文字数制限 |
|---|---|
| FTP | 235 |

**ステップ 3** [User accepted message] フィールドと [User rejected message] フィールドにメッセージを追加します。

Telnet からのユーザー認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が AAA サーバーにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージテキストをそれぞれ指定した場合、ASA では、AAA サーバーにより認証されたユーザーに対しては [User accepted message] テキストが表示され、認証されなかったユーザーに対しては ASA により [User rejected message] テキストが表示されます。HTTP セッションおよびFTPセッションの認証では、プロンプトにチャレンジテキストのみが表示されます。ユーザー承認メッセージテキストおよびユーザー拒否メッセージテキストは表示されません。

**ステップ 4** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

# TACACS+ サーバーの認証および許可のテスト

ASA が TACACS+ サーバーに接続してユーザーを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

**ステップ 1** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** の順に選択します。

**ステップ 2** サーバーが存在するサーバー グループをクリックします。

**ステップ 3** テストするサーバーをクリックします。

**ステップ 4** [Test] をクリックします。

選択したサーバーに対応する [Test AAA Server] ダイアログボックスが表示されます。

**ステップ 5** 実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

**ステップ 6** ユーザー名を入力します。

**ステップ 7** 認証をテストする場合は、ユーザー名のパスワードを入力します。

**ステップ 8** [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバーへ送信されます。テストが失敗した場合は、エラー メッセージが表示されます。

# AAA 用の TACACS+ サーバーのモニタリング

AAA 用の TACACS+ サーバーのモニタリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [AAA Servers]**

  このペインには、設定された TACACS+ サーバーの統計情報が表示されます。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

# AAA 用の TACACS+ サーバーの履歴

**表 *3 : AAA* 用の *TACACS+* サーバーの履歴**

| 機能名 | プラットフォーム リリース | 説明 |
|---|---|---|
| TACACS+ サーバ | 7.0(1) | AAA に TACACS+ サーバーを設定する方法について説明します。<br>次の画面が導入されました。<br>[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]<br>[Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]。 |
| AAA 向けの IPv6 アドレス TACACS+ サーバー | 9.7(1) | AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。 |
| グループごとの AAA サーバー グループとサーバーの制限が増えました。 | 9.13(1) | より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバー グループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。<br>さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。<br>これらの新しい制限を受け入れるために、AAA 画面が変更されました。 |

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。